Paul Pollack

Unreal Analysis

Visions of the p-adic Realm

October 8, 2024

In memory of Kurt Hensel, Reinhold Strassmann, and the countless others persecuted or murdered by the National Socialists.

Preface

A few months ago, on his last visit to New Jersey, I was telling [Paul] Erdős something about p-adic analysis. Erdős was not interested. "You know," he said about the p-adic numbers, "they don't really exist."

Melvyn Nathanson

In the long history of mathematics, 'number' has always meant real number, and it is only relatively recently that we have become aware of the world of p-adic numbers. The situation is akin to someone who has only experienced daylight gazing in astonishment at the night sky.

Kazuya Kato
Nobushige Kurokawa
Takeshi Saito

p-adic numbers were birthed into the world by Kurt Hensel in 1897, at a lecture for the annual meeting of the German Mathematical Society. Initially, these new objects were viewed with some skepticism. Helmut Hasse recollects that in 1920, no less a figure than Richard Courant advised him against studying with Hensel, dismissing Hensel's 1913 book on p-adic numbers as an unproductive detour ("unfruchtbarer Seitenweg"). Yet today p-adic numbers have thoroughly permeated number theory. Local-global principles, which relate solubility in number fields to solubility in p-adic fields, are central to modern arithmetic geometry. Tate's thesis and the adelic viewpoint on class field theory are bread and butter to algebraic number theorists. And those on the analytic side of the fence can point to 'local densities' as p-adically motivated objects that arise in nearly every study of arithmetic counting problems. We live in an age when activists and arithmeticians universally agree on the need to think (and act) both globally and locally.

These problem sets, written for a topics course at the 2024 Ross Indiana summer mathematics camp, do not describe any of these significant modern applications of p-adic numbers. Rather, they offer a hands-on — better, *minds-on*! — approach to the foundational theory of $\mathbf{Q}_p$, working towards elementary but attractive number-theoretic applications. Whenever there was a choice to be made, I have elected to treat special cases rather than develop general theory. This has allowed prerequisites to be kept to a minimum. Readers

are expected to have seen number theory and rigorous calculus, as well as both abstract and matrix algebra, but most of what is needed belongs to the standard undergraduate curriculum.

Notwithstanding the chosen title, these problem sets aim to offer a general introduction to p-adic numbers, privileging neither analysis nor algebra. Analysts will be disappointed by the absence of material on continuity, differentiability, and p-adic interpolation. Algebraists will be disheartened that the discussion never ventures beyond $\mathbf{Q}_p$ to any of its finite or infinite extensions. Despite the many omissions, I am optimistic that as individuals engage with these problem sets, they will catch a glimpse of an alluring territory begging to be charted. The suggested readings listed below have been selected as particularly approachable, and we commend their consideration to those with an adventurous spirit.

How to use this book

This manuscript is intended as a resource for undergraduates and beginning graduate students looking to dip their toes into non-Archimedean waters.

For the teacher using the text as a resource for a class on p-adic numbers: First of all, congratulations! As you are probably aware, courses on this topic at the specified level are rare.

If the book is used as the primary course text, problems should be distributed to students independently of solutions. Class time can be spent discussing ideas and approaches, with conversations led by students but facilitated by the instructor. Experts will often see more in the problems than beginning students and they are encouraged to use these discussions to share insights.

Solutions to Problem Set (p-Set) X can be passed out once the class, as a whole (or at least, *on* the whole), is ready to move on to Set $X + 1$. For those on the semester system, a reasonable aim is to cover roughly one set per week, with the expectation that later material will take a bit more time. The book can also be used in a supplementary fashion, with an instructor handpicking interesting-seeming problems to spice up their own exercise sheets.

For students: Congratulations to you as well! p-adic numbers are a(n) (un)real treat to think about. If you are using the book for a course, follow the directions of your instructor. If you are using the book for self-study, I strongly recommend working through the problems systematically, tackling one set completely before moving on to the next. Please give yourself enough time for the mental fermentation process to occur before giving up on a question! Of course, you should not feel bad if after a long struggle certain problems continue to elude you; solutions are included for precisely these moments.

I should emphasize that this is not meant to be your only book on p-adic numbers. The author, for instance, learned about p-adic numbers from entirely different sources! After mastering the material on each problem set, it is recommended that you look at how the corresponding content is treated in the suggested references. One only truly understands a topic after examining it from all angles, and different texts bring out different perspectives.

Saying what we mean and meaning what we say

Exercises are typically introduced as assertions, without the use of "show that" or "prove." (The Extra Explorations, embedded in the solutions, are exceptions.) Problem solvers should recognize they are on the hook to validate every claim.

We take no position on the hotly contested issue of whether 0 is a natural number. Integers greater than or equal to 0 are — naturally enough — referred to as nonnegative integers. As is customary in English, positive means *strictly* larger than zero. We write $\mathbf{Z}^+$, $\mathbf{Q}^+$, and $\mathbf{R}^+$ for the sets of positive integers, rational numbers, and real numbers, respectively.

Our terminology around quotient rings is slightly unconventional. To start with, the term ring always refers to a commutative ring with unity. If I is an ideal of the ring R, and $a \in R$, the class of a with respect to congruence modulo I is typically denoted "a mod I." We break this rule when (and only when) $R = \mathbf{Z}$ and $I = m\mathbf{Z}$, instead writing "a mod m." Additionally, we use "$\mathbf{Z}/m$" in place of "$\mathbf{Z}/m\mathbf{Z}$"; this is a mild concession to the notation $\mathbf{Z}_m$ appearing on the first-year Ross Program problem sets.

Acknowledgements

Assembling these problem sets involved much scouring and borrowing. Deserving of particular mention: Exercise 4.53 was sourced from an article by Catherine Crompton in the Rose Hulman Undergrad. Mathematics Journal. Exercises 7.90 and 9.117 were inspired by discussions in Murty's text [6]. Exercise 11.132 was taken from Koblitz's book [5]. The proof of Ramanujan's conjecture on integer solutions to $x^2 + 7 = 2^m$ follows closely the exposition in Cassels's monograph [1]. The proof "from-the-Book" of Skolem's theorem on integer linear recurrences, outlined on Set #11, is due to Tao (loosely based on an argument of Georges Hansel):

`https://terrytao.wordpress.com/2007/05/25/open-question-effective-skolem-mahler-lech-theorem/`

In this connection it was also helpful to consult a post of Seewoo Lee:

`https://seewoo5.github.io/jekyll/update/2023/02/21/p-adic-numbers-application.html`

Exercises 9.112 and 10.129 are based on a paper of Mahler:

> *On some irrational decimal fractions*. J. Number Theory **13** (1981), 268–269.

The proofs on Set #13 of the Adams and Kummer theorems on Bernoulli numbers are adapted from a delightful article of Wells Johnson:

> *p-adic proofs of congruences for the Bernoulli numbers*. J. Number Theory **7** (1975), 251–265.

Various tech tools were employed to produce the book in front of you. The cover, which features 19th-century illustrations from the Hirayama Fireworks company*, was designed in Canva. Typesetting was done with LaTeX, using Springer's SVMono document class. Several calculations were farmed out to the fantastically capable PARI/GP. ChatGPT assisted by offering English translations, hunting down typos, and suggesting alternative phrasings.

This manuscript would not exist without the backing and encouragement of the Ross Mathematics Foundation. Site directors Timothy All and Jim Fowler have my profound appreciation for their inspiring efforts, year after year, to ensure that the Ross Program provides a supportive, welcoming, and stimulating environment for all camp participants (students, counselors, and even us lecturers!). Special thanks to Phoebe Watkins for her service as course assistant, Paco Adajar for suggesting the term "p-set" as an alternative to the more mundane "problem set," and Jacob Bucciarelli for sharing his expertise in orbital mechanics.

Work on this project was facilitated by a grant from the US National Science Foundation, award DMS-2001581.

Suggestions for further reading

1. J. W. S. Cassels, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986.
2. K. Conrad, *Expository papers*, `https://kconrad.math.uconn.edu/blurbs/`.
3. F. Q. Gouvêa, *p-adic numbers: An introduction*, third ed., Universitext, Springer, Cham, 2020.
4. S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37, American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007.
5. N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984.
6. M. R. Murty, *Introduction to p-adic analytic number theory*, AMS/IP Studies in Advanced Mathematics, vol. 27, Amrican Mathematical Society, Providence, RI; International Press, Somerville, MA, 2002.

* see `https://www.city.yokohama.lg.jp/kurashi/kyodo-manabi/library/shuroku/hirayama.html`

7. W. H. Schikhof, *Ultrametric calculus: An introduction to p-adic analysis*, Cambridge Studies in Advanced Mathematics, vol. 4, Cambridge University Press, Cambridge, 2006.
8. J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, New York-Heidelberg, 1973.
9. J. Steuding, *Die p-adischen Zahlen*. Online survey article. URL: `https://www.uni-marburg.de/de/fb12/fachbereich/profil/geschichte-des-fachbereichs/biographisches/hensel_p_adischen_zahlen.pdf`

University of Georgia *Paul Pollack*

Part I

Problems

Problem Set #1

Valuation Theory (the Theory of Absolute Values)

> . . . true faith is belief in the reality of absolute values. It is in this kingdom of absolute values that we must look for and find our immortality.
>
> William R. Inge

Let K be a field. An absolute value on K is a function $|\cdot|\colon K \to \mathbf{R}$ satisfying

(i) $|x| \geq 0$, with $|x| = 0$ if and only if $x = 0$,
(ii) $|x + y| \leq |x| + |y|$ (the triangle inequality),
(iii) $|xy| = |x||y|$.

for all $x, y \in K$. We refer to the pair $(K, |\cdot|)$ as a valued field.

1.1. Let $(K, |\cdot|)$ be a valued field. Then:

(a) $|\pm 1| = 1$,
(b) $|x - y| \geq |x| - |y|$ for all $x, y \in K$,
(c) $|xy^{-1}| = |x||y|^{-1}$ for all $x, y \in K$ with $y \neq 0$.

1.2. Let K be a field. Define $|x|$ by letting $|x| = 0$ if $x = 0$ and $|x| = 1$ for all $x \neq 0$. Show that $|\cdot|$ is an absolute value on K (the trivial absolute value).

Let p be a prime number. For each $x \in \mathbf{Q}^\times$, there is a unique integer v with the property that $x = p^v \frac{a}{b}$ for some integers a, b not divisible by p. We set $v_p(x) = v$. In order to have v_p defined on all of $\mathbf{Q}$, we take $v_p(0) = \infty$. The function $v_p\colon \mathbf{Q} \to \mathbf{Z} \cup \{\infty\}$ is called the p-adic valuation.

1.3. Let p be a prime. For each $x \in \mathbf{Q}$, define $|x|_p = p^{-v_p(x)}$, where $p^{-\infty}$ is taken to be 0. Then $|\cdot|_p$ is an absolute value on $\mathbf{Q}$ (p-adic absolute value).

The absolute value $|\cdot|_p$ will play a starring role throughout the course. You are strongly advised to compute several examples to develop a feel for this notion of absolute value. Here are a few to get you started:

$$\left|\frac{5\cdot 2^{10}}{2^{10}+1}\right|_2 = 2^{-10}, \quad |3^{-5}|_2 = 1, \quad \left|\frac{2}{21}\right|_3 = 3, \quad |100!|_7 = 7^{-16}.$$

If $|\cdot|$ is an absolute value on the field K, we call $|\cdot|$ non-Archimedean if it satisfies the following strong triangle inequality:

$$|x+y| \le \max\{|x|,|y|\} \quad \text{for all } x,y \in K.$$

Sensibly enough, an absolute value that is not non-Archimedean is Archimedean. For example, the trivial absolute value is non-Archimedean, while the usual absolute value on $\mathbf{Q}$ is Archimedean.

1.4. For each prime p, the absolute value $|\cdot|_p$ on $\mathbf{Q}$ defined in Exercise 1.3 is non-Archimedean.

The following Darwinian property of non-Archimedean absolute values ("survival of the greatest") is central to the theory.

1.5. If $|\cdot|$ is a non-Archimedean absolute value on a field K, then

$$|x+y| = \max\{|x|,|y|\} \quad \text{whenever } x,y \in K \text{ with } |x| \neq |y|.$$

1.6. Let K be a field equipped with an absolute value $|\cdot|$ for which $|2| \le 1$. Then $|2^{e_1}+2^{e_2}+\cdots+2^{e_n}| \le n$ for all nonnegative integers $e_1,\dots,e_n$. It follows that $|\binom{n}{k}| \le n$ whenever n is a positive integer and $0 \le k \le n$.

1.7 (Product Formula). Let $|\cdot|_\infty$ denote the standard Archimedean absolute value on $\mathbf{Q}$. For every $x \in \mathbf{Q}^\times$,

$$|x|_\infty \prod_{p \text{ prime}} |x|_p = 1.$$

Factorials and Factorization

1.8. For each prime p and positive integer n: $\quad |n!|_p > p^{-n/(p-1)}$.

1.9. $|n!|_\infty$ grows faster than C^n for any fixed C. Hence, the product formula implies that there are infinitely many primes.

'p's and Harmony

1.10. Let $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$, the nth harmonic number. From calculus, $|H_n|_\infty$ tends to infinity. The same holds for $|H_n|_2$.

1.11 (Wolstenholme). When p is odd, $H_{p-1} = p \sum_{0<i<p/2} \frac{1}{i(p-i)}$. Hence, $|H_{p-1}|_p \leq p^{-2}$ for $p > 3$.

p-Set #2

Distance Learning

> Today we are far from the standpoint of viewing the measure or size of a number or geometric figure as something given by nature and necessity. We view the size of a figure or number rather as a function of its essential components, whose determination is entirely at our discretion, and in whose choice we let ourselves be guided by reasons of expediency.
>
> Kurt Hensel

In $\mathbf{R}$ it is often useful to view $|x-y|$ as the distance between x and y. One can adopt the same interpretation for any absolute value on any field K, but only if one is prepared to welcome a few surprises!

2.12. If $|\cdot|$ is non-Archimedean, every triangle with vertices in K is isosceles.

Let $(K, |\cdot|)$ be a valued field. For $x_0 \in K$ and real $r > 0$, the open and closed discs of radius r centered at x_0 are defined, respectively, by

$$\mathbf{D}_{<r}(x_0) = \{x \in K : |x - x_0| < r\} \text{ and } \mathbf{D}_{\leq r}(x_0) = \{x \in K : |x - x_0| \leq r\}.$$

2.13. Suppose $|\cdot|$ is non-Archimedean. Let $D = \mathbf{D}_{<r}(x_0)$ be an open disc in K. Show that if $x \in D$, then $D = \mathbf{D}_{<r}(x)$. That is: Every point of an open disc is a center.

2.14. Suppose $|\cdot|$ is non-Archimedean. Then any two open discs are either disjoint or one contains the other.

2.15. Let $K = \mathbf{Q}$ and $|\cdot| = |\cdot|_p$ with p prime. Every open disc is a closed disc, and vice versa.

Valuation Theory

2.16. How many absolute values can you find on $\mathbf{F}_{2027}$? (Here and below, $\mathbf{F}_p$ denotes the field with p elements, or equivalently the residue ring $\mathbf{Z}/p$.)

2.17. Let $(K, |\cdot|)$ be a valued field. For all $x, y \in K$ and all $n \in \mathbf{Z}^+$,

$$|x+y| \leq (n+1)^{1/n} \left(\max_{0 \leq k \leq n} \left| \binom{n}{k} \right|^{1/n} \right) \max\{|x|, |y|\}.$$

Let $\mathbf{F}_p(T)$ denote the fraction field of the polynomial ring $\mathbf{F}_p[T]$, so that

$$\mathbf{F}_p(T) = \left\{ \frac{F(T)}{G(T)} : F(T), G(T) \in \mathbf{F}_p[T], G(T) \neq 0 \right\}.$$

2.18. Every absolute value on $\mathbf{F}_p(T)$ is non-Archimedean.

2.19. If $\pi(T), \tilde{\pi}(T)$ are distinct monic irreducibles in $\mathbf{F}_p[T]$, then there is an absolute value $|\cdot|$ on $\mathbf{F}_p(T)$ with $|\pi(T)| < 1$ and $|\tilde{\pi}(T)| = 1$. Is there an absolute value on $\mathbf{F}_p(T)$ with $|T| > 1$?

2.20. If K is a field equipped with a non-Archimedean absolute value $|\cdot|$, then $\mathbf{D}_{\leq 1}(0) = \{x \in K : |x| \leq 1\}$ is a ring. When $K = \mathbf{Q}$ and $|\cdot| = |\cdot|_p$, this ring is denoted $\mathbf{Z}_{(p)}$ and called the ring of p-integral rational numbers. Explain in pedestrian terms what it means for a rational number to be p-integral.

2.21. Determine $\bigcap_{p \text{ prime}} \mathbf{Z}_{(p)}$.

'p's and Harmony

2.22. For every prime p and each integer $0 < k < p$: $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1} \equiv p \cdot \frac{(-1)^{k-1}}{k} \pmod{p^2}$. (Part of the problem is to make sense of the congruence, since $p \cdot \frac{(-1)^{k-1}}{k} \notin \mathbf{Z}$ if $1 < k < p$.)

2.23 (Eisenstein). If p is an odd prime, then $|1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{p-1}|_p < 1 \iff 2^p \equiv 2 \pmod{p^2}$.

When $2^p \equiv 2 \pmod{p^2}$, we call p a Wieferich prime, alluding to the appearance of such primes in Wieferich's early 20th century investigations into Fermat's last theorem. 1093 and 3511 are the only known Wieferich primes. Other examples (if they exist) exceed 10^{19}.

Variations on a Theme of Euclid

2.24 (Schur). Let $F(T) \in \mathbf{Z}[T]$ be nonconstant. There are infinitely many primes that divide $F(n)$ for some $n \in \mathbf{Z}$. In other words: F has a root in $\mathbf{Z}/p$ for infinitely many primes p.

2.25. If $p \mid n^4 + 1$ for some $n \in \mathbf{Z}$, either $p = 2$ or $p \equiv 1 \pmod 8$. Hence, there are infinitely many primes $p \equiv 1 \pmod 8$.

2.26. Let $n \in \mathbf{Z}^+$. If $p \mid (2n+1)^2 - 2$, then $p \equiv \pm 1 \pmod 8$. Not every prime dividing $(2n+1)^2 - 2$ can be congruent to $1 \pmod 8$. Hence, $(2n+1)^2 - 2$ is always divisible by some prime congruent to $-1 \pmod 8$. By varying n, we can find infinitely many primes $p \equiv -1 \pmod 8$.

2.27. Every coprime residue class mod 8 contains infinitely many primes.

In this last statement, "mod 8" can be replaced with "mod m," for any $m \in \mathbf{Z}^+$. This is a celebrated (and difficult!) theorem of Dirichlet that you will meet in courses on analytic number theory.

p-Set #3

Knowing Your Limits

> One cannot blame a respectable mathematician for looking twice at the equation
>
> $$-1 = 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots.$$
>
> ... It is obvious that [this] is absurd if ordinary convergence is intended. The whole point to Hensel's theory is that this is not ordinary convergence, but a new type of convergence which, from the point of view of abstract algebra, is equally worthy of the name.
>
> Cyrus Colton MacDuffee

Let $(K, |\cdot|)$ be a valued field, and let $\{x_n\}$ be a sequence of elements of K. Suppose $x \in K$. We say $\{x_n\}$ converges to x, and write $x_n \to x$ or $\lim_{n\to\infty} x_n = x$ or simply $\lim x_n = x$, if the following holds.

> For every real number $\epsilon > 0$, there is an $N \in \mathbf{Z}^+$ with the property that
>
> $$|x_n - x| < \epsilon \quad \text{whenever} \quad n \geq N.$$

(The inequality "$|x_n - x| < \epsilon$" could have been written as "$x_n \in \mathbf{D}_{<\epsilon}(x)$.") We say $\{x_n\}$ converges if it converges to some x in K. Those who already grok convergence in the context of calculus will notice that $x_n \to x$ in $(K, |\cdot|)$ precisely when $|x_n - x| \to 0$ in the familiar sense.

3.28. Every sequence in a valued field has at most one limit.

3.29 (calculus classics).

(i) If $x_n = x$ for all n, then $x_n \to x$.
(ii) If $x_n \to x$ and $y_n \to y$, then $x_n + y_n \to x + y$.
(iii) If $x_n \to x$ and $y_n \to y$, then $x_n y_n \to xy$.

3.30. $x_n = 1 + 3 + 3^2 + \cdots + 3^n$ converges to $-\frac{1}{2}$ in $(\mathbf{Q}, |\cdot|_3)$. So defining the value of a series as the limit of its partial sums, $\sum_{k=0}^{\infty} 3^k = -\frac{1}{2}$. Does $\{x_n\}$ converge in $(\mathbf{Q}, |\cdot|_p)$ for any other values of p?

3.31. Evaluate $\sum_{n=0}^{\infty} n \cdot n!$ and $\sum_{n=0}^{\infty} n^2 \cdot 2^n$ in $(\mathbf{Q}, |\cdot|_2)$.

3.32. Explain how the calculations

$$\begin{aligned} \frac{11}{7} &= 2 + 3 \cdot \frac{-1}{7} & \qquad \frac{-6}{7} &= 0 + 3 \cdot \frac{-2}{7} \\ \frac{-1}{7} &= 2 + 3 \cdot \frac{-5}{7} & \qquad \frac{-2}{7} &= 1 + 3 \cdot \frac{-3}{7} \\ \frac{-5}{7} &= 1 + 3 \cdot \frac{-4}{7} & \qquad \frac{-3}{7} &= 0 + 3 \cdot \frac{-1}{7} \\ \frac{-4}{7} &= 2 + 3 \cdot \frac{-6}{7} \end{aligned}$$

imply that in $(\mathbf{Q}, |\cdot|_3)$,

$$\frac{11}{7} = 2 + 2 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + 0 \cdot 3^4 + 1 \cdot 3^5 + 0 \cdot 3^6 + 2 \cdot 3^7 + 1 \cdot 3^8 + \ldots,$$

where the "digits" in the right-hand expansion follow the eventually periodic pattern $2, \overline{2, 1, 2, 0, 1, 0}$.

3.33. Find $c_0, c_1, c_2, \ldots \in \{0, 1, 2, 3, 4\}$ with $\sum_{k=0}^{\infty} c_k 5^k = \frac{2}{7}$ in $(\mathbf{Q}, |\cdot|_5)$.

Valuation Theory

3.34. Let $(K, |\cdot|)$ be a valued field. Then $|\cdot|$ is non-Archimedean $\iff |2| \leq 1$. (Here 2 means $1 + 1$.) Is this equivalence true with 3 in place of 2?

3.35. If $|\cdot|$ is a nontrivial non-Archimedean absolute value on $\mathbf{Q}$, then $|p| < 1$ for some prime p.

3.36. Let $|\cdot|$ be a non-Archimedean absolute value on $\mathbf{Q}$. If m and n are relatively prime integers, either $|m| = 1$ or $|n| = 1$. (Use Bézout!)

3.37. Let $|\cdot|$ be a non-Archimedean absolute value on K and $\mathcal{O} = \mathbf{D}_{\leq 1}(0)$. We have seen in Problem 2.20 that $\mathcal{O}$ is a subring of K.

Show that $x \in \mathcal{O}$ is a unit in $\mathcal{O} \iff |x| = 1$. Furthermore, if M is the collection of all nonunits of $\mathcal{O}$ — that is, $M = \mathbf{D}_{<1}(0)$ — then M is a proper ideal of $\mathcal{O}$ containing every proper ideal of $\mathcal{O}$. Hence, M is the unique maximal ideal of $\mathcal{O}$.

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
u_m	0	1	1	-1	-3	-1	5	7	-3	-17	-11	23	45	-1	-91	-89	93

Sequence $\{u_m\}_{m\geq 0}$ appearing in Exercise 3.40.

3.38. Every nonzero element of $\mathbf{Z}_{(p)}$ is uniquely expressible in the form $p^v u$ where v is a nonnegative integer and u is a unit of $\mathbf{Z}_{(p)}$.

3.39. $\mathbf{Z}_{(p)}$ is a principal ideal domain (PID) with $p\mathbf{Z}_{(p)}$ its only maximal ideal.

A Question of Ramanujan

When is a power of 2 equal to 7 more than a square? This happens for $2^3, 2^4, 2^5, 2^7$, and 2^{15} (in this last case, $2^{15} = 32\,768 = 7 + 181^2$). In a 1913 issue of the *Journal of the Indian Mathematical Society*, Ramanujan listed all of these examples and posed the problem of finding others.

Let $R = \mathbf{Z}[\frac{1+\sqrt{-7}}{2}]$ (viewed as a subring of $\mathbf{C}$). Since $(\frac{1+\sqrt{-7}}{2})^2 = \frac{1+\sqrt{-7}}{2} - 2$,

$$R = \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{-7}}{2} = \left\{\frac{1}{2}(a + b\sqrt{-7}) : a, b \in \mathbf{Z} \text{ and } a \equiv b \pmod 2\right\}.$$

3.40 (Nagell). Assume as known that R is a unique factorization domain whose only units are ± 1. Show that if x, m are integers with $x^2 + 7 = 2^m$, then $u_{m-2} = \pm 1$, where u_m is the sequence defined by the Binet-type formula

$$u_m = \frac{\alpha^m - \beta^m}{\alpha - \beta} \quad \text{for} \quad \alpha = \frac{1+\sqrt{-7}}{2},\ \beta = \frac{1-\sqrt{-7}}{2}, \qquad m = 0, 1, 2, 3, \ldots.$$

Does the converse hold?

On our final problem set (Set #13) you will determine all solutions to $u_{m-2} = \pm 1$ by p-adic methods.

p-Set #4

Berning Questions

> ... It took me less than half a quarter of an hour to find that the tenth powers of the first 1000 numbers, starting from 1, being added together make
>
> 91 409 924 241 424 243 424 241 924 242 500.
>
> This renders apparent the futility of the work Ismaël Boulliau spent on the compilation of his voluminous *Arithmetica Infinitorum*, in which he did nothing more than laboriously compute the sums of the first six powers...
>
> Jacob Bernoulli

The Bernoulli numbers B_k $(k = 0, 1, 2, 3, \dots)$ are defined as the coefficients in the formal power series* expansion

$$\frac{T}{\mathrm{e}^T - 1} = \sum_{k=0}^{\infty} B_k \frac{T^k}{k!}.$$

Equivalently, $B_0, B_1, B_2, \dots$ are determined by the identity

$$T = \left(T + \frac{T^2}{2!} + \frac{T^3}{3!} + \frac{T^4}{4!} + \dots\right)\left(B_0 + B_1 T + B_2 \frac{T^2}{2!} + B_3 \frac{T^3}{3!} + \dots\right).$$

Since $\frac{\mathrm{e}^T - 1}{T} = 1 + \frac{T}{2!} + \frac{T^2}{3!} + \dots$ is a power series with rational coefficients and nonzero constant term, its reciprocal $\frac{T}{e^T - 1}$ is also a power series with rational coefficients. Therefore, every $B_k \in \mathbf{Q}$.

For positive integers n and k, define $S_k(n) = 1^k + 2^k + \dots + (n-1)^k$.

* We assume acquaintance with basic facts about formal power series, as found for instance in §1.1 of Stanley's *Enumerative Combinatorics*.

k	0	1	2	3	4	5	6	7	8	9	10	11	12
B_k	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$

First several Bernoulli numbers.

4.41. $1 + \mathrm{e}^T + \mathrm{e}^{2T} + \cdots + \mathrm{e}^{(n-1)T} = \sum_{k=0}^{\infty} S_k(n) \frac{T^k}{k!}$ (as formal power series).

4.42 (Faulhaber's Formula). $S_k(n) = \displaystyle\sum_{j=0}^{k} \binom{k}{j} B_{k-j} \frac{n^{j+1}}{j+1}$.

In view of the widespread applications of Faulhaber's formula, the Bernoulli numbers are natural objects of study. The following two exercises ask you to pluck some low-hanging fruit.

4.43. If $\coth T := \frac{e^{2T}+1}{e^{2T}-1}$, then $T \coth T = T + \frac{2T}{e^{2T}-1} = T + \sum_{k=0}^{\infty} B_k \frac{(2T)^k}{k!}$ (as formal series). $T \coth(T)$ is invariant under the substitution $T \mapsto -T$. Hence, $B_k = 0$ for every odd $k > 1$.

4.44. $\coth T = \frac{1}{T} + \sum_{k \geq 1} B_{2k} \frac{2^{2k}}{(2k)!} T^{2k-1}$ and $\frac{\mathrm{d}}{\mathrm{d}T} \coth T = 1 - \coth^2 T$.
As a consequence: $(-1)^{k+1} B_{2k} > 0$ for each $k \in \mathbf{Z}^+$.

Other properties of Bernoulli numbers lie a bit further below the surface. For instance, based on the above table one might conjecture that Bernoulli numbers always have squarefree denominators. We will prove this — and much more — in due time!

Take It to the Limit, One More Time

4.45. Compute the first several partial sums of $\sum_{k=1}^{\infty} 2^k/k$, noting their 2-adic absolute values. Any conjectures?

4.46. For every $r \in \mathbf{Z}_{(p)}$, there is a unique sequence $d_0, d_1, d_2, d_3, \ldots \in \{0, 1, 2, \ldots, p-1\}$ with $\sum_{k=0}^{\infty} d_k p^k = r$ in $(\mathbf{Q}, |\cdot|_p)$. The sequence $\{d_k\}$ is eventually periodic.

4.47. If $x_n \to x$ in $(K, |\cdot|)$, then $|x_n| \to |x|$ in the real numbers. In fact, if $|\cdot|$ is non-Archimedean and $x_n \to x$, where $x \neq 0$, then $|x_n| = |x|$ for all large n.

Valuation Theory

4.48. Every nontrivial non-Archimedean absolute value on $\mathbf{Q}$ has the form $|\cdot|_p^c$ for some prime p and some $c > 0$.

4.49. If $|\cdot|$ is an Archimedean absolute value on $\mathbf{Q}$, we know from Exercise 3.34 that $|2| = 2^c$ and $|3| = 3^d$ for some real numbers $c, d > 0$.

Write 2^n in base 3, say $2^n = \epsilon_m 3^m + \epsilon_{m-1}3^{m-1} + \cdots + \epsilon_0$, where each $\epsilon_i = 0, 1,$ or 2 and $\epsilon_m > 0$. There is a positive constant B with

$$2^{cn} = |2^n| \leq B \cdot |3|^m = B \cdot 3^{dm};$$

e.g., $B = \frac{|2|\cdot|3|}{|3|-1}$ works. Since $3^m \leq 2^n$ and n can be taken arbitrarily large, it must be that $c \leq d$. Reversing the roles of 2 and 3 shows $d \leq c$, and so $c = d$.

4.50. If $|\cdot|$ is an Archimedean absolute value on $\mathbf{Q}$, then $|\cdot| = |\cdot|_\infty^c$, where $|2| = 2^c$.

Let $|\cdot|$ and $|\cdot|'$ be absolute values on K. We say $|\cdot|$ and $|\cdot|'$ are equivalent absolute values if they induce the same notion of convergence, meaning that $x_n \to x$ in $(K, |\cdot|)$ if and only if $x_n \to x$ in $(K, |\cdot|')$.

4.51. If $|\cdot|$ and $|\cdot|'$ are equivalent, then $|\cdot|$ and $|\cdot|'$ are both Archimedean or both non-Archimedean.

Suggestion. Look at convergent *geometric* sequences.

4.52 (Ostrowski's Theorem). Every nontrivial absolute value on $\mathbf{Q}$ is equivalent to exactly one of $|\cdot|_p$ (p prime) or $|\cdot|_\infty$.

4.53. It is easy to find p distinct rational numbers equidistant with respect to $|\cdot|_p$; simply consider $0, 1, 2, \ldots, p-1$. Can you find $p+1$ such numbers?

'p's and Harmony

4.54 (Eswarathasan–Levine, Boyd). Recall our notation H_n for the nth harmonic number, $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$. If $|H_m|_p \geq 1$, then $|H_n|_p = p|H_m|$ whenever $pm \leq n < p(m+1)$.

4.55. (electronic assistance recommended!) $|H_n|_3$ and $|H_n|_5$ tend to infinity.

Open problem: $|H_n|_p$ tends to infinity for every fixed prime p.

p-Set #5

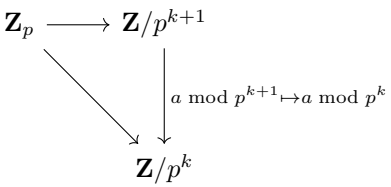
And Introducing...

Let p be a prime number. A p-adic integer is an infinite tuple $(a_1 \bmod p, a_2 \bmod p^2, a_3 \bmod p^3, \dots) \in \prod_{k=1}^{\infty} \mathbf{Z}/p^k$ that satisfies the compatibility condition

$$a_{k+1} \equiv a_k \pmod{p^k} \quad \text{for all positive integers } k. \tag{*}$$

We write $\mathbf{Z}_p$ for the collection of all p-adic integers.

A p-adic integer is no more and no less than an object which can be sensibly "reduced" modulo an arbitrary power of p. Initially one might think that all elements of $\prod_{k=1}^{\infty} \mathbf{Z}/p^k$ meet this description: any of these can be "reduced" mod p^k by projecting from the kth component. But for a general element of $\prod_{k=1}^{\infty} \mathbf{Z}/p^k$, these reductions need not be compatible. "Compatible" means commutativity of the diagram



This is precisely what (*) buys us.

Here are some examples of elements of $\mathbf{Z}_5$:

$$(101 \bmod 5, 101 \bmod 5^2, 101 \bmod 5^3, \dots) = (1 \bmod 5, 1 \bmod 5^2, 101 \bmod 5^3, \dots),$$
$$(-1 \bmod 5, -1 \bmod 5^2, -1 \bmod 5^3, \dots) = (4 \bmod 5, 24 \bmod 5^2, 124 \bmod 5^3, \dots),$$
$$(4 \bmod 5, 34 \bmod 5^2, 334 \bmod 5^3, \dots) = (4 \bmod 5, 9 \bmod 5^2, 84 \bmod 5^3, \dots).$$

Take a moment to convince yourself that this last example satisfies our compatibility condition!

5.56. $\mathbf{Z}_p$ is a subring of $\prod_{k=1}^{\infty} \mathbf{Z}/p^k$.

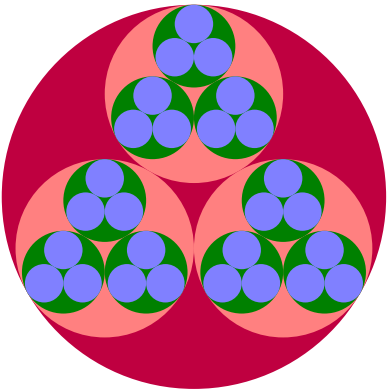


Figure for Exercise 5.64.

5.57. $\mathbf{Z}_p$ is an integral domain.

5.58. $\mathbf{Z}_p$ has characteristic 0. (Thus, $\mathbf{Z}$ sits canonically inside $\mathbf{Z}_p$.)
Which elements of $\mathbf{Q}$ can be said to belong to $\mathbf{Z}_p$? Is our third example of a 5-adic integer an element of $\mathbf{Q}$? (Assume the nth component is $3\ldots34 \bmod 5^n$, where 3 is repeated $n-1$ times.)

5.59. $u = (a_1 \bmod p, a_2 \bmod p^2, \ldots) \in \mathbf{Z}_p$ is a unit $\iff p \nmid a_1$ (in $\mathbf{Z}$) $\iff p \nmid u$ (in $\mathbf{Z}_p$).

5.60. Every nonzero element of $\mathbf{Z}_p$ admits a unique expression in the form $p^v u$, where v is a nonnegative integer and u is a unit in $\mathbf{Z}_p$.

5.61. $\mathbf{Z}_p$ is a principal ideal domain with $p\mathbf{Z}_p$ its only nonzero prime ideal.

5.62. The canonical inclusion $\mathbf{Z} \hookrightarrow \mathbf{Z}_p$ induces an isomorphism $\mathbf{Z}/p^n \cong \mathbf{Z}_p/p^n\mathbf{Z}_p$, for every positive integer n.

5.63. The definition of $\mathbf{Z}_p$ makes sense without requiring p to be prime. However, considering $\mathbf{Z}_g$ for composite g does not give anything essentially new. In fact: $\mathbf{Z}_g \cong \prod_{p|g} \mathbf{Z}_p$ for each integer $g > 1$. (For instance, $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$.)

5.64. What does the picture on this page — created by TEX StackExchange user `Qrrbrbirlbel`* — have to do with $\mathbf{Z}_3$?

5.65 (Steuding). Repeat the last exercise for Salvador Dali's painting *La Cara de la Guerra*.

5.66 ($\mathbf{Z}_p$ is uncountable). There is no map from $\mathbf{Z}^+$ onto $\mathbf{Z}_p$.

* `https://tex.stackexchange.com/a/695157`

Well, Color Me Impressed!

5.67 (Thomas, Monsky). Consider the following 3-coloring of the rational plane $\mathbf{Q}^2$: (x, y) is red if $|x|_2 < 1, |y|_2 < 1$, blue if $|x|_2 \geq 1$, $|x|_2 \geq |y|_2$, and green if $|y|_2 \geq 1$, $|y|_2 > |x|_2$. Show that any trio of differently colored points forms a triangle Δ with $|\text{Area}(\Delta)|_2 > 1$.

This observation plays a key role in the proof of Monsky's Theorem: *It is impossible to dissect a square into an odd number of triangles all of which have the same area.*

p-Set #6

Enter Cauchy

Let K be a field equipped with an absolute value $|\cdot|$. If $\{x_n\}$ converges to x in $(K, |\cdot|)$, then for any real number $\epsilon > 0$, all terms far enough out in the sequence $\{x_n\}$ are within $\frac{1}{2}\epsilon$ of x. By the triangle inequality, all such terms are within ϵ of each other. That is:

> For each $\epsilon > 0$, there is a positive integer N with
>
> $$|x_n - x_m| < \epsilon \quad \text{whenever } n, m \geq N. \tag{C}$$

Any sequence $\{x_n\}$ with property (C) is called a Cauchy sequence.

6.68. If $|\cdot|$ is non-Archimedean, then $\{x_n\}$ is Cauchy $\iff |x_{n+1} - x_n| \to 0$.

This need not hold if $|\cdot|$ is Archimedean; a counterexample is provided by the partial sums of the harmonic series in $(\mathbf{Q}, |\cdot|_\infty)$.

6.69. The sequence $\{2^{5^n}\}$ is Cauchy in $(\mathbf{Q}, |\cdot|_5)$.

6.70 (a common calculus Cauchy claim). Let $(K, |\cdot|)$ be a valued field. If $\{x_n\}$ is a Cauchy sequence in K, then $\{|x_n|\}$ is a bounded sequence of real numbers.

6.71 (and another). Let $(K, |\cdot|)$ be a valued field. If a sequence $\{x_n\}$ of elements of K is Cauchy, and some subsequence of $\{x_n\}$ converges to $x \in K$, then $\{x_n\}$ converges to x.

If $\mathbf{R}$ is equipped with the usual absolute value, then every Cauchy sequence in $\mathbf{R}$ converges to an element of $\mathbf{R}$. This need not be the case for a general valued field. For example, the sequence of rational numbers

$$x_1 = 1, \quad x_2 = 1.4, \quad x_3 = 1.41, \quad x_4 = 1.414, \quad \ldots,$$

obtained by successively truncating the decimal expansion of $\sqrt{2}$, is Cauchy in $(\mathbf{Q}, |\cdot|_\infty)$ but does not converge to any element of $\mathbf{Q}$, since $\sqrt{2} \notin \mathbf{Q}$. Coping with this unsettling scenario was one of the motivations behind the invention (discovery?) of the real numbers in the first place!

Disconcerting examples of this same kind can also be found when $K = \mathbf{Q}$ and $|\cdot| = |\cdot|_p$. Take any sequence $\{c_k\}_{k\geq 0}$ from $\{0, 1, \ldots, p-1\}$ that is not eventually periodic. Then $x_n = \sum_{k=0}^{n} c_k p^k$ defines a Cauchy sequence in $(\mathbf{Q}, |\cdot|_p)$. To check the Cauchy condition (C), we may assume that $m < n$ (why?). Then

$$|x_n - x_m|_p = |c_{m+1}p^{m+1} + c_{m+2}p^{m+2} + \cdots + c_n p^n|_p < p^{-m},$$

which is smaller than ϵ once $m > \frac{\log(1/\epsilon)}{\log p}$. So (C) is satisfied for any $N > \frac{\log(1/\epsilon)}{\log p}$. But $\{x_n\}$ cannot converge to an element of $\mathbf{Q}$, on account of Exercise 4.46.

To get out of this mess, we need to fill in the following blank: $\mathbf{R}$ is to $(\mathbf{Q}, |\cdot|_\infty)$ as _____ is to $(\mathbf{Q}, |\cdot|_p)$. The answer here turns out to be $\mathbf{Q}_p$! But ... what is $\mathbf{Q}_p$?

The p-adic Numbers, At Last!

We define the field of p-adic numbers, denoted $\mathbf{Q}_p$, as the fraction field of $\mathbf{Z}_p$. Since $\mathbf{Z}_p$ has characteristic 0, so does $\mathbf{Q}_p$, and thus $\mathbf{Q} \subseteq \mathbf{Q}_p$.

6.72. $\mathbf{Q}_p = \bigcup_{n\geq 0} p^{-n}\mathbf{Z}_p = \mathbf{Z}_p[1/p]$.

6.73. Every nonzero $x \in \mathbf{Q}_p$ admits a unique expression in the form $p^v u$, where v is an integer and u is a unit in $\mathbf{Z}_p$.

For $x \in \mathbf{Q}_p^\times$, we set $v_p(x) = v$, where v is the integer from Problem 6.73. In order to have v_p defined on all of $\mathbf{Q}_p$, we let $v_p(0) = \infty$. (Compare with the definition of v_p on Set #1.)

6.74. When $x \in \mathbf{Q}$, we have defined $v_p(x)$ twice: once on Set #1 and again just now, since x is also an element of $\mathbf{Q}_p$.

Check that when $x \in \mathbf{Q}$ our two definitions of $v_p(x)$ agree (so our sin is venial, rather than mortal). Furthermore, if we set $|x|_p = p^{-v_p(x)}$ for $x \in \mathbf{Q}_p$, then $|\cdot|_p$ defines a non-Archimedean absolute value on $\mathbf{Q}_p$. (We continue to call v_p the p-adic valuation and $|\cdot|_p$ the p-adic absolute value.)

6.75. $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x|_p \leq 1\}$. (That is, $\mathbf{Z}_p = \mathbf{D}_{\leq 1}(0)$ in $\mathbf{Q}_p$.)
Also, $\mathbf{Z}_p^\times = \{x \in \mathbf{Q}_p : |x|_p = 1\}$.

6.76 ($\mathbf{Z}_p$ is compact). Let $x_1, x_2, x_3, \ldots$ be a sequence of elements of $\mathbf{Z}_p$. Infinitely many x_n share the same mod p component, say $a_1 \bmod p$. Among these, infinitely many share the same mod p^2 component, $a_2 \bmod p^2$. Etc. Thus: $x_1, x_2, x_3, \ldots$ contains a subsequence converging to $(a_1 \bmod p, a_2 \bmod p^2, a_3 \bmod p^3, \ldots) \in \mathbf{Z}_p$.

Curious Congruences

6.77 (Stern). Recall that $\log \frac{1}{1-t} = t + \frac{1}{2}t^2 + \frac{1}{3}t^3 + \ldots$ whenever t is a complex number with $|t| < 1$ (usual absolute value). Exponentiating, $\mathrm{e}^T \mathrm{e}^{T^2/2} \mathrm{e}^{T^3/3} \cdots = \frac{1}{1-T}$, as formal power series. Expanding and comparing coefficients of T^p shows that $|1 - \frac{1}{p!} - \frac{1}{p}|_p \leq 1$. Hence, $(p-1)! \equiv -1 \pmod p$ (Wilson's theorem).

6.78. For each prime p and each $a \in \mathbf{Z}$ coprime to p, put $q_p(a) = \frac{a^{p-1}-1}{p}$. By Fermat's little theorem, $q_p(a) \in \mathbf{Z}$.

Prove: If a and b are both coprime to p, then $q_p(ab) \equiv q_p(a) + q_p(b) \pmod p$.

p-Set #7

You Complete Me

> Why does $\mathbf{Q}$ want to grow to $\mathbf{R}$ or $\mathbf{Q}_2$ or $\mathbf{Q}_3$? Its heart has holes, for example at $\sqrt{2}$ and $\sqrt{3}$. This is similar to mankind; we can grow to be big boys or big girls, but there is still some sadness in our hearts, and we grow to love another person.
>
> Kazuya Kato

Let $(K, |\cdot|)$ be a valued field. We call K complete if every Cauchy sequence of elements of K converges to an element of K. Intuitively, completeness means that "everything in the world happens for a reason"*: the far-out terms of a sequence only clump together when they have a compelling justification for doing so, namely heading towards a single value.

7.79. Every Cauchy sequence in $\mathbf{Z}_p$ has a limit belonging to $\mathbf{Z}_p$.

7.80. Every Cauchy sequence in $\mathbf{Q}_p$ has a limit belonging to $\mathbf{Q}_p$. That is, $\mathbf{Q}_p$ is complete.

7.81. In $\mathbf{Q}_5$, $\lim 2^{5^n}$ is a 4th root of 1. Is $\lim 2^{5^n} \in \mathbf{Q}$?

7.82. $\mathbf{Z}$ is dense in $\mathbf{Z}_p$. In other words, every element of $\mathbf{Z}_p$ is the limit of a sequence of terms from $\mathbf{Z}$.

7.83. $\mathbf{Q}$ is dense in $\mathbf{Q}_p$.

Suppose K and L are fields equipped with absolute values and that the absolute value $|\cdot|$ on L extends the absolute value on K. If $(L, |\cdot|)$ is complete and K

* Disclaimer: "Everything in the world" means every occurrence of a sequence being Cauchy.

is a dense subset of L, we call L the completion of K with respect to $|\cdot|$. For example, $\mathbf{R}$ is the completion of $\mathbf{Q}$ with respect to $|\cdot|_\infty$. By Exercises 7.80 and 7.83, $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ with respect to $|\cdot|_p$.

Why do we say the completion and not a completion? Completions are unique, up to isometric (absolute-value preserving) isomorphism.

7.84. If $(L, |\cdot|)$ and $(L', |\cdot|')$ are two completions of the same valued field $(K, |\cdot|_0)$, then there is an isomorphism $\phi\colon L \to L'$ that fixes K and satisfies $|\phi(x)|' = |x|$ for all $x \in L$.

Hands On, Digits Out

7.85. If $c_0, c_1, c_2, \ldots$ is any sequence of integers, then $\sum_{k\geq 0} c_k p^k$ converges to an element of $\mathbf{Z}_p$.

Restricting the "digits" c_k in Problem 7.85 to $\{0, 1, 2, \ldots, p-1\}$, we find that every infinite base p expansion determines an element of $\mathbf{Z}_p$. What about the other way around? Does every element of $\mathbf{Z}_p$ admit an infinite base p expansion?

Let's suppose that $x \in \mathbf{Z}_p$ can be expanded in base p and see where this leads us. Write $x = c_0 + c_1 p + c_2 p^2 + \ldots$, with all $c_i \in \{0, 1, \ldots, p-1\}$. Then the digit in the p^k-place is given by

$$c_k = \frac{(c_0 + c_1 p + \cdots + c_k p^k) - (c_0 + c_1 p + \cdots + c_{k-1} p^{k-1})}{p^k}.$$

The parenthesized terms in the numerator are the (least nonnegative integer) reductions of x modulo $p^{k+1}\mathbf{Z}_p$ and modulo $p^k \mathbf{Z}_p$. (Make sure you see why!) So we've determined the digits c_k in any possible expansion of x. Now that we know to try these digits, we are home free, as you are asked to check in the next exercise.

7.86. Let $x \in \mathbf{Z}_p$, and let x_k $(k = 0, 1, 2, 3, \ldots)$ be the unique integer in the range $0 \leq x_k < p^k$ with $x \equiv x_k \pmod{p^k \mathbf{Z}_p}$. Define

$$c_k = \frac{x_{k+1} - x_k}{p^k} \quad \text{for } k = 0, 1, 2, \ldots,$$

Then each $c_k \in \{0, 1, 2, \ldots, p-1\}$, each $x_k = c_0 + c_1 p + \cdots + c_{k-1} p^{k-1}$, and

$$x = c_0 + c_1 p + c_2 p^2 + c_3 p^3 + \ldots.$$

Thus, the (finite) base p expansions of the x_k coalesce to an infinite base p expansion of x. The representation produced in this way is not merely *an* infinite base p expansion of x, but — as the lead-in to the problem establishes — its *unique* base p expansion.

7.87 (canonical expansions for elements of $\mathbf{Q}_p$). For each $x \in \mathbf{Q}_p$, there is a unique two-sided sequence of integers $\{c_k\}_{k=-\infty}^{\infty}$ satisfying

(i) each $c_k \in \{0, 1, 2, \ldots, p-1\}$,
(ii) c_k is nonzero for only finitely many $k < 0$,
(iii) $x = \sum_k c_k p^k$.

7.88. The canonical expansion of $x \in \mathbf{Q}_p$ terminates (meaning that $c_k = 0$ for all large enough k) $\iff$ $x = 0$ or $x \in \mathbf{Q}^+$ with denominator a power of p.

7.89. The canonical expansion of $x \in \mathbf{Q}_p$ is eventually periodic $\iff$ $x \in \mathbf{Q}$.

Curious Congruences

7.90. For every odd prime p: $\displaystyle\sum_{a=1}^{p-1} \frac{a^{p-1}-1}{p} \equiv \frac{(p-1)!+1}{p} \pmod{p}$.

Method of Successive Approximation

7.91 (computing a value of $\sqrt{2}$ in $\mathbf{Z}_7$). We can compute a square root of 2 in $\mathbf{Z}_7$ by determining a root in $\mathbf{Z}/7$, then $\mathbf{Z}/7^2$, then $\mathbf{Z}/7^3$, ..., being mindful to maintain compatibility throughout the process.

To start things off, the residue class $x_1 = 3 \bmod 7$ satisfies $x^2 = 2$ in $\mathbf{Z}/7$. This solution can be lifted, uniquely, to a solution of $x^2 = 2$ in $\mathbf{Z}/7^2$. To see why, note that a generic integer congruent to 3 (mod 7) has the form $3 + 7k$, and $(3+7k)^2 = 9 + 42k + 7^2k^2 \equiv 9 + 42k \pmod{7^2}$. The congruence $9 + 42k \equiv 2 \pmod{7^2}$ is satisfied precisely when $k \equiv 1 \pmod 7$. For integers $k \equiv 1 \pmod 7$, we have $3 + 7k \equiv 10 \pmod{7^2}$. Therefore, $x_2 := 10 \bmod 7^2 \in \mathbf{Z}/7^2$ is the lift we are after.

Expanding $(10 + 7^2k)^2 \bmod 7^3$, and reasoning analogously, will show that $x_2 = 10 \bmod 7^2$ lifts uniquely to $x_3 := 10 + 7^2 \cdot 2 = 108 \bmod 7^3$.

This process can be continued indefinitely, uniquely determining $x_1, x_2, x_3, \ldots$. Then $x := (x_1, x_2, x_3, \ldots) \in \prod_{k=1}^{\infty} \mathbf{Z}/7^k$ is a solution in $\mathbf{Z}_7$ to $x^2 = 2$. The canonical base 7 expansion of x begins

$$3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \ldots.$$

After that wall of text, you might be wondering what exactly you are being asked to do. Your job: Check that the process can be continued indefinitely, uniquely determining all the x_k, that setting $x = (x_1, x_2, x_3, \dots)$ really does define a $\mathbf{Z}_7$-solution to $x^2 = 2$, and finally, that the 7-adic expansion of x starts the way we claimed.

p-Set #8

The World (of p-adic) Series

8.92. Let K be a field complete with respect to a non-Archimedean absolute value $|\cdot|$ (for instance, $\mathbf{Q}_p$!).

(a) A series $\sum_{k=1}^{\infty} a_k$ converges in $K \iff a_k \to 0$ in K.
(b) If $\sum_{k=1}^{\infty} a_k$ converges, then $|\sum_{k=1}^{\infty} a_k| \leq \max_{k=1,2,3,\ldots} |a_k|$.

For the next exercise, recall that a rearrangement of a series $\sum_{k=1}^{\infty} a_k$ is a series of the form $\sum_{k=1}^{\infty} a_{\sigma(k)}$, where σ is a permutation of $\mathbf{Z}^+$ (a bijection of $\mathbf{Z}^+$ with itself).

8.93. Let K be a field complete with respect to a non-Archimedean absolute value. If $\sum_{k=1}^{\infty} a_k$ is a series in K that converges to $s \in K$, then every rearrangement of $\sum_{k=1}^{\infty} a_k$ also converges to s.

8.94. Suppose that $\sum_{n=0}^{\infty} a_n$ and $\sum_{n=0}^{\infty} b_n$ are convergent series in the field K, which is assumed complete with respect to a non-Archimedean absolute value. Define $c_n = \sum_{k=0}^{n} a_k b_{n-k}$, for $n = 0, 1, 2, \ldots$. Then $\sum_{n=0}^{\infty} c_n$ converges and in fact $\sum_{n=0}^{\infty} c_n = (\sum_{n=0}^{\infty} a_n)(\sum_{n=0}^{\infty} b_n)$.

Important consequence: If $F(T) = \sum_{k=0}^{\infty} a_k T^k$, $G(T) = \sum_{k=0}^{\infty} b_k T^k \in K[[T]]$ both converge at the point $z \in K$, so does $F(T)G(T)$, and $F(T)G(T)|_{T=z} = F(z)G(z)$.

8.95 (a doubleheader?). Let K be a field complete with respect to a non-Archimedean absolute value $|\cdot|$. Let $\{a_{i,j}\}_{i,j \geq 0}$ be a doubly-indexed sequence of elements of K. Suppose there is a sequence of real numbers $\{\epsilon_N\}_{N \geq 0}$ tending to 0 with the property that

$$|a_{i,j}|_p \leq \epsilon_N \quad \text{whenever } i \geq N \text{ or } j \geq N.^*$$

Show: The double series $\sum_i \sum_j a_{i,j}$ and $\sum_j \sum_i a_{i,j}$ both converge.

* This may seem a strange condition to impose on $\{a_{i,j}\}$. In fact, it's very natural; it's equivalent to asking that for each $\epsilon > 0$, the inequality $|a_{i,j}| < \epsilon$ fails at most finitely often. We could have phrased the requirement this way to start with, but our more elaborate formulation will turn out to be easier to work with in proofs.

8.96 (a double switch). Continue with the notation and assumptions of Exercise 8.95. For every nonnegative integer N,

$$\left|\sum_i\sum_j a_{i,j} - \sum_{i=0}^{N}\sum_j a_{i,j}\right| \le \epsilon_{N+1}, \quad \left|\sum_j\sum_i a_{i,j} - \sum_j\sum_{i=0}^{N} a_{i,j}\right| \le \epsilon_{N+1},$$

$$\left|\sum_{i=0}^{N}\sum_j a_{i,j} - \sum_{i=0}^{N}\sum_{j=0}^{N} a_{i,j}\right| \le \epsilon_{N+1}, \quad \left|\sum_j\sum_{i=0}^{N} a_{i,j} - \sum_{j=0}^{N}\sum_{i=0}^{N} a_{i,j}\right| \le \epsilon_{N+1}.$$

Therefore, $\sum_i \sum_j a_{i,j} = \sum_j \sum_i a_{i,j}$.

Are You Feeling the Bern?

Recall from Set #4 that when $k, n \in \mathbf{Z}^+$, we are writing $S_k(n) = 1^k + 2^k + \cdots + (n-1)^k$.

8.97. For p prime, $k \in \mathbf{Z}^+$: $\quad p \mid (S_k(p) + \mathbf{1}_{p-1|k})$.

$\mathbf{1}_C$ denotes the indicator function of the condition C. Thus, $\mathbf{1}_{p-1|k}$ is 1 if $p-1$ divides k and 0 otherwise.

8.98. For p prime, $k \in \mathbf{Z}^+$: $\quad B_k + \frac{\mathbf{1}_{p-1|k}}{p} + \sum_{0<j<k} \binom{k}{j} B_{k-j} \frac{p^j}{j+1} \in \mathbf{Z}_{(p)}$.

8.99. For p an odd prime, $k \in \mathbf{Z}^+$: $\quad B_k + \frac{\mathbf{1}_{p-1|k}}{p} \in \mathbf{Z}_{(p)}$.

8.100. For $k \in 2\mathbf{Z}^+$: $\quad B_k + \frac{1}{2} \in \mathbf{Z}_{(2)}$.

8.101 (Clausen, von Staudt). For $k \in 2\mathbf{Z}^+$: $\quad B_k + \sum_{\substack{p \text{ prime} \\ p-1|k}} \frac{1}{p} \in \mathbf{Z}$.

It follows from Exercise 8.101 that the denominator of B_k is the (squarefree!) product of the primes p for which $p-1 \mid k$.

Finding Your Roots

8.102 (Teichmüller representatives). For each $u \in \mathbf{Z}_p^\times$, the field $\mathbf{Q}_p$ contains a unique $(p-1)$th root of unity congruent to u mod $p\mathbf{Z}_p$, namely $\omega(u) := \lim_{n\to\infty} u^{p^n}$.

8.103. Find $\omega(2)$ (exactly) when $p = 3$. Then take $p = 7$ and determine the digits c_0, c_1, c_2 in the canonical expansion $\omega(2) = c_0 + c_1 \cdot 7 + c_2 \cdot 7^2 + \ldots$.

8.104. If $u \in \mathbf{Z}$ has order 3 modulo p, then $1 + u$ has order 6 mod p, and $\omega(1+u) = 1 + \omega(u)$.

p-Set #9

> Is $\mathbf{R}$ special? Well, physical reality, as we and Archimedes believe it, has no infinitesimals. . . . Hence we say that the field $\mathbf{R}$ and its absolute value $|\cdot|_\infty$ are *archimedean*. . . . *pace* Archimedes, in recent years the theoretical physicists have learned about the p-adic fields and have begun to wonder whether they may not help in modeling just what happens in the nuclei of atoms, for instance. So much for reality.
>
> Alf van der Poorten

Gazing at the Newfound Stars

9.105. Let p be odd. Let $a \in \mathbf{Z}_p^\times$, and let $a_1 \bmod p$ be the mod p component of a. Then a is a square in $\mathbf{Q}_p \iff a_1 \bmod p$ is a square in $\mathbf{Z}/p$.

Suggestion. Adapt the method of successive approximation described in Exercise 7.91.

9.106. Let p be odd, and let $n \in \mathbf{Z}$ be a nonsquare mod p. Then $1, n$ are coset representatives for $\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^2$, while $1, n, p, np$ are coset representatives for $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$.

9.107. If $a \in \mathbf{Z}_2^\times$, then a is a square in $\mathbf{Q}_2 \iff a \equiv 1 \pmod{8\mathbf{Z}_2}$.

9.108. Find coset representatives for $\mathbf{Z}_2^\times/(\mathbf{Z}_2^\times)^2$ and $\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2$.

9.109. For $a \in \mathbf{Q}_p^\times$:

$$a \in \mathbf{Z}_p^\times \iff (\text{some value of}) \ \sqrt[n]{a} \in \mathbf{Q}_p \text{ for infinitely many } n \in \mathbf{Z}^+.$$

9.110 (a Liouville approximation theorem in $\mathbf{Z}_p$). Suppose $\alpha \in \mathbf{Z}_p$ is a root of a polynomial $F(T) \in \mathbf{Z}[T]$ of degree d having no integer roots. For every nonzero $n \in \mathbf{Z}$,

$$|n - \alpha|_p \geq |F(n) - F(\alpha)|_p = |F(n)|_p \geq |F(n)|_\infty^{-1} \geq c|n|_\infty^{-d},$$

where c is a positive constant depending only on F.

9.111 (a transcendental element of $\mathbf{Q}_p$). $\sum_{k\geq 1} p^{k!} \in \mathbf{Q}_p$ is not a root of any nonconstant polynomial in $\mathbf{Q}[x]$.

9.112. $2^{4\cdot 5^n} \to 1$ in $\mathbf{Z}_5$ while $2^{4\cdot 5^n} \to 0$ in $\mathbf{Z}_2$. Since 0 and 1 are distinct rational numbers, the $\mathbf{Z}_{10}$-limit of $2^{4\cdot 5^n}$ has a nonperiodic 10-adic expansion.

Since 10 is not prime, your solution should start with a sensible definition of convergence in $\mathbf{Z}_{10}$.

Strassmann Series

Let $F(T) = \sum_{n\geq 0} a_n T^n$ be a formal power series with $\mathbf{Q}_p$-coefficients.

9.113. For $x \in \mathbf{Q}_p$: $F(x)$ converges $\iff |a_n x^n|_p \to 0$.
Hence, $F(x)$ converges for all $x \in \mathbf{Z}_p \iff a_n \to 0$ in $\mathbf{Q}_p$.

When $F(x)$ converges for all $x \in \mathbf{Z}_p$, we call $F(T)$ a Strassmann (power) series.*

In courses on complex function theory, one learns that an analytic function has only finitely many zeros in a closed disc, unless it vanishes identically on that disc. The next three exercises guide you through a proof of an analogous result for zeros of Strassmann series within $\mathbf{Z}_p$.

9.114. Let $F(T)$ be a Strassmann series with a nonzero coefficient. Any nonzero $x \in \mathbf{Z}_p$ with $F(x) = 0$ satisfies $|x|_p \geq \delta$, where $\delta > 0$ is a constant depending only on F. If $F(T)$ has $\mathbf{Z}_p$-coefficients, we can take $\delta = |a_m|_p$, where a_m is the first nonvanishing coefficient of $F(T)$.

In particular: If $F(T)$ is a Strassmann series and $F(x) = 0$ for all $x \in \mathbf{Z}_p$, then $F(T) = 0$ in $\mathbf{Q}_p[[T]]$.

9.115 (recentering Strassmann series). Let $F(T) = \sum_{k\geq 0} a_k T^k$ be a Strassmann power series, and let $x_0 \in \mathbf{Z}_p$. For every $x \in \mathbf{Z}_p$,

* Here we depart from convention; the usual terms are restricted power series or strictly convergent power series.

$$F(x+x_0)=\sum_{j\geq 0} b_j x^j, \quad \text{where} \quad b_j := \sum_{k\geq j} a_k \binom{k}{j} x_0^{k-j}.$$

The recentered series $\sum_{j\geq 0} b_j T^j$ is also Strassmann.

9.116. A Strassmann series with a nonvanishing coefficient has finitely many zeros in $\mathbf{Z}_p$.

Curious Congruences

9.117 (Glaisher). For all primes p: $\quad p^2 \mid (p-1)!+1 \iff B_{p-1}+\frac{1}{p}-1 \in p\mathbf{Z}_{(p)}$.

Primes p for which $p^2 \mid (p-1)!+1$ are known as Wilson primes. The only known examples, and the only examples smaller than $2\cdot 10^{13}$, are 5, 13, and 563.

9.118 (Johnson). Recall that when $u \in \mathbf{Z}_p^\times$, we are writing $\omega(u)$ for the unique $(p-1)$th root of unity congruent to u modulo $p\mathbf{Z}_p$ (see Exercise 8.102). Show that if $u \in \mathbf{Z}$ has order 3 modulo p, and $v \in \mathbf{Z}$ satisfies $v \equiv \omega(u) \pmod{p^k\mathbf{Z}_p}$, where $k \in \mathbf{Z}^+$, then

$$(1+v)^p \equiv 1+v^p \pmod{p^{2k+1}}.$$

Use this to explain the congruence $325^7 \equiv 1+324^7 \pmod{7^7}$.

u	$\omega(u)$
2	$2+4\cdot 7+6\cdot 7^2+3\cdot 7^3+2\cdot 7^5+\ldots$
3	$3+4\cdot 7+6\cdot 7^2+3\cdot 7^3+2\cdot 7^5+\ldots$
4	$4+2\cdot 7+3\cdot 7^3+6\cdot 7^4+4\cdot 7^5+\ldots$
5	$5+2\cdot 7+3\cdot 7^3+6\cdot 7^4+4\cdot 7^5+\ldots$

Sixth roots of unity in $\mathbf{Q}_7$, omitting $\omega(\pm 1)=\pm 1$. Notice that $\omega(3)=1+\omega(2)$ and $\omega(5)=1+\omega(4)$, as guaranteed by Problem 8.104.

p-Set #10

If you claim a series sums to S
Your metric you must not suppress
The danger, you can now see
Is that another may disagree
And you may both be right: what a mess!

Edward B. Burger
Thomas Struppeck

I . . . Have . . . the . . . Power. . . (Series)

One can often leverage identities from the real universe to establish corresponding results in the p-adic realm. As a proof of concept, consider the following formula you may have encountered in your study of Taylor series: For all real numbers x with $|x| < 1$,

$$\begin{aligned}\sqrt{1+x} &= 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4 + \dots \\ &= \sum_{k\geq 0} \binom{\frac{1}{2}}{k} x^k, \qquad \text{where} \quad \binom{\frac{1}{2}}{k} := \frac{\frac{1}{2}(\frac{1}{2}-1)\cdots(\frac{1}{2}-(k-1))}{k!}.\end{aligned}$$

We will argue that the same sum on k defines a square root of $1+x$ in $\mathbf{Q}_p$ whenever it converges.

Getting from $\mathbf{R}$ to $\mathbf{Q}_p$ requires a stopover in the land of formal power series. Let $B_{\frac{1}{2}}(T) = \sum_{k\geq 0} \binom{\frac{1}{2}}{k} T^k \in \mathbf{Q}[[T]]$, and let $C(T) = B_{\frac{1}{2}}(T)^2$, the formal square of $B_{\frac{1}{2}}(T)$. We claim that $C(T) = 1 + T$.

To fashion a proof, suppose x is a real number with $|x| < 1$. Then $B_{\frac{1}{2}}(x)$ converges absolutely (e.g., by the ratio test). So if we multiply $B_{\frac{1}{2}}(x)$ by $B_{\frac{1}{2}}(x)$, we can reshuffle the terms as we please. One such regrouping gives us $C(x)$. On the other hand, our "real world" identity says that $B_{\frac{1}{2}}(x)^2 = 1 + x$ whenever $|x| < 1$. It follows that $C(x) - (1+x) = 0$ when $|x| < 1$. But a power series that vanishes on an open interval around 0 has all its coefficients equal to 0. This forces $C(T) = 1 + T$, as formal series.

Armed with this formal identity, we can head back to $\mathbf{Q}_p$. Suppose we have in hand an $x \in \mathbf{Q}_p$ for which $B_{\frac{1}{2}}(x)$ converges. If we multiply $B_{\frac{1}{2}}(x)$ by $B_{\frac{1}{2}}(x)$, we can rearrange the result into $C(x)$ — this time justifying ourselves not on the basis of absolute convergence but by an appeal to Problem 8.94. Since $C(x) = 1 + x$, this shows that $B_{\frac{1}{2}}(x)$ represents a square root of $1 + x$ in $\mathbf{Q}_p$ whenever $B_{\frac{1}{2}}(x)$ converges.

10.119. If p is odd, then $B_{\frac{1}{2}}(x)$ converges when $|x|_p \leq 1/p$. If $p = 2$, then $B_{\frac{1}{2}}(x)$ converges when $|x|_2 \leq 1/2^3$. Are these conditions necessary for convergence?

10.120. $B_{\frac{1}{2}}(\frac{9}{16}) = \sum_{k\geq 0} \binom{\frac{1}{2}}{k} (\frac{9}{16})^k$ converges to $\frac{5}{4}$ in $\mathbf{R}$ but to $-\frac{5}{4}$ in $\mathbf{Q}_3$.

Lifting and Embedding

10.121 (Taylor's Formula). If $F(T) \in \mathbf{Q}_p[T]$, and $a \in \mathbf{Q}_p$, then

$$F(a + T) = \sum_{j\geq 0} \frac{F^{(j)}(a)}{j!} T^j.$$

Furthermore: If $F(T) \in \mathbf{Z}_p[T]$, so is $\frac{1}{j!}F^{(j)}(T)$, for all nonnegative integers j.

10.122 (p-adic Newton's method). Let $F(T) \in \mathbf{Z}_p[T]$. If $x \in \mathbf{Z}_p$ and $|F'(x)|_p = 1$, then $\tilde{x} := x - \frac{F(x)}{F'(x)}$ satisfies $|F(\tilde{x})|_p \leq |F(x)|_p^2$.

10.123 (Hensel's Lemma). Let $F(T) \in \mathbf{Z}_p[T]$. Suppose $x_1 \in \mathbf{Z}_p$ satisfies $F(x_1) \equiv 0 \pmod{p\mathbf{Z}_p}$ and $F'(x_1) \not\equiv 0 \pmod{p\mathbf{Z}_p}$. Then F has a zero $x \in \mathbf{Z}_p$ satisfying $x \equiv x_1 \pmod{p\mathbf{Z}_p}$.

10.124. Suppose $F(T) \in \mathbf{Z}[T]$ is nonconstant with all complex roots distinct. Then $F(T)\mathbf{Q}[T] + F'(T)\mathbf{Q}[T] = \mathbf{Q}[T]$. Hence, $F(T)\mathbf{Z}[T] + F'(T)\mathbf{Z}[T]$ contains a nonzero integer R. Deduce: $F(T)$ and $F'(T)$ are coprime over $\mathbf{Z}/p$ for all but finitely many p.

10.125. Every nonconstant $F(T) \in \mathbf{Z}[T]$ has a root in $\mathbf{Z}_p$ for infinitely many primes p.

10.126. Let K be a number field (a finite extension of $\mathbf{Q}$). By the primitive element theorem, $K = \mathbf{Q}(\theta)$ for some $\theta \in K$. Choose $F(T) \in \mathbf{Z}[T]$ irreducible over $\mathbf{Q}$ and vanishing at θ. Then K embeds into $\mathbf{Q}_p$ whenever $F(T)$ has a root in $\mathbf{Q}_p$. Deduce: There is an embedding $K \hookrightarrow \mathbf{Q}_p$ for infinitely many p.

Don't Ever Change

10.127. The only ring homomorphism from $\mathbf{Q}_p$ to $\mathbf{Q}_p$ is the identity.

10.128. There is no ring homomorphism from $\mathbf{Q}_p$ to $\mathbf{Q}_q$ (q prime, $q \neq p$) or to $\mathbf{R}$.

There *is* a field embedding of $\mathbf{Q}_p$ into $\mathbf{C}$ (assuming the Axiom of Choice). In fact, there are many such embeddings, but none are canonical, and none carry convergent sequences in $\mathbf{Q}_p$ to convergent sequences in $\mathbf{C}$. Thus (channeling Hermann Weyl*), choosing such an embedding must always be regarded as something of a brute act.

Is Sticking Together Irrational?

10.129 (Mahler). The real number $0.248163264128\ldots$ obtained by concatenating the decimal digits of powers of 2 is irrational.

* Weyl famously wrote "The introduction of numbers as coordinates ... is an act of violence."

p-Set #11

> In 1926, when he was nearly 40 years old, Skolem obtained his doctorate... The somewhat advanced age has the following explanation. In their younger years, Viggo Brun and Skolem agreed that neither of them would bother to obtain the degree of Doctor, probably feeling that, in Norway, it served no useful function in the education of a young scientist. But in the middle twenties a younger generation of Norwegian mathematician emerged. It seems that Skolem then felt he too ought to fulfil the formal requirement of having a doctorate, and he "obtained permission" from Brun to submit a thesis.
>
> Jens Erik Fenstad

I ... Have ... the ... Power... (Series)

11.130 (p-adic lumber theory). Recall from calculus that

$$\log x = \log(1 + (x-1)) = \sum_{k\geq 1} \frac{(-1)^{k-1}}{k}(x-1)^k \quad \text{whenever} \quad |x-1| < 1.$$

This motivates us to define, for each prime p,

$$\log_p(T) = \sum_{k\geq 1} \frac{(-1)^{k-1}}{k}(T-1)^k \in \mathbf{Q}_p[[T-1]].$$

Show: $\log_p x$ converges for all $x \in \mathbf{Q}_p$ with $|x-1|_p < 1$.

Passing the familiar identity $\log xy = \log x + \log y$ (valid for $x, y \in \mathbf{R}^+$) from $\mathbf{R}$ to $\mathbf{Q}_p[[X-1, Y-1]]$, and then on to $\mathbf{Q}_p$, one can show that

$$\log_p x + \log_p y = \log_p(xy) \quad \text{whenever } x, y \in 1 + p\mathbf{Z}_p. \tag{$\dagger$}$$

Filling in the details here is a bit finicky. If you enjoy this kind of work (you know who you are...), give it a try!

11.131. Go ahead and assume (†).

Show: $\displaystyle\sum_{k=1}^{\infty}\left(1+\frac{1}{2^k}+\frac{1}{3^k}+\cdots+\frac{1}{(p-1)^k}\right)\frac{p^k}{k}=0$ in $\mathbf{Q}_p$.

In particular ($p=2$): $\displaystyle\sum_{k=1}^{\infty}\frac{2^k}{k}=0$ in $\mathbf{Q}_2$.*

11.132 (derive responsibly!). Critique the following proof that π is irrational: Suppose that $\pi=\frac{a}{b}$, where a and b are positive integers. Let p be an odd prime not dividing a. Then

$$0=\sin(pb\pi)=\sin(ap)=\sum_{k\geq 0}(-1)^k\frac{(ap)^{2k+1}}{(2k+1)!},$$

where this last series converges in $\mathbf{Q}_p$. Therefore,

$$p^{-1}=|-ap|_p=\left|\sum_{k\geq 0}(-1)^k\frac{(ap)^{2k+1}}{(2k+1)!}-ap\right|_p=\left|\sum_{k\geq 1}(-1)^k\frac{(ap)^{2k+1}}{(2k+1)!}\right|_p\leq p^{-2}.$$

Contradiction!

Strassmann Series

11.133. Let $F(T)=1+T+(pT)^2+(pT)^4+(pT)^8+(pT)^{16}+\dots$. There is exactly one $x\in\mathbf{Z}_p$ with $F(x)=0$.

It will be convenient for the next exercise, and certain others afterward, to name the coefficients of the falling factorial $T(T-1)\cdots(T-(N-1))$. For nonnegative integers N and K, we let $s(N,K)$ be the integer defined by the formal equality

$$T(T-1)\cdots(T-(N-1))=\sum_{K=0}^{\infty}s(N,K)T^K.$$

* "Ordinary analysis has amassed a great stock of identities between power series. Many of these are valid in p-adic analysis too. But here an identity between power series yields congruences between partial sums." — Max Zorn

For example, when $N = 5$, we have $T(T-1)(T-2)(T-3)(T-4) = 24T - 50T^2 + 35T^3 - 10T^4 + T^5$, so that

$$s(5,0) = 0, \quad s(5,1) = 24, \quad s(5,2) = -50, \quad s(5,3) = 35,$$
$$s(5,4) = -10, \quad s(5,5) = 1, \quad \text{and} \quad s(5,K) = 0 \text{ for } K > 5.$$

When $N = 0$, the product $T(T-1)\cdots(T-(N-1))$ is empty and assigned the value 1; hence, $s(0,0) = 1$ and $s(0,K) = 0$ for $K > 0$. The $s(N,K)$ are known as Stirling numbers of the first kind. Don't let the fancy name fool you; while the Stirling numbers are important in combinatorics, for us they play only a notational role.

11.134 (p-adically interpolating $(1+a)^x$). Let p be an odd prime, and let $a \in p\mathbf{Z}_p$. If n is a nonnegative integer, then

$$\begin{aligned}(1+a)^n &= \sum_{k=0}^{\infty} n(n-1)(n-2)\cdots(n-(k-1))\frac{a^k}{k!} \\ &= \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} s(k,j)n^j\right)\frac{a^k}{k!} = \sum_{j=0}^{\infty} C_{a,j}n^j,\end{aligned}$$

where

$$C_{a,j} := \sum_{k\geq j} s(k,j)\frac{a^k}{k!}.$$

Moreover, $|C_{a,j}|_p \to 0$ as $j \to \infty$.

Your job: Fill in the missing details. In particular, justify the swapping of the sums on k and j.

NOTATION. For future use, we let

$$\mathrm{Binom}(1+a;T) := \sum_{j=0}^{\infty} C_{a,j}T^j \in \mathbf{Q}_p[[T]].$$

As you have just shown, $\mathrm{Binom}(1+a;T)$ is a Strassmann series satisfying $\mathrm{Binom}(1+a;n) = (1+a)^n$ for all nonnegative integers n.

Zeros of Linear Recurrence Sequences

Let $\{x_n\}_{n\geq 0}$ be a sequence of integers satisfying a linear recurrence

$$x_n = a_1x_{n-1} + a_2x_{n-2} + \cdots + a_dx_{n-d} \quad \text{for } n = d, d+1, d+2, \ldots,$$

where $a_1, \ldots, a_d \in \mathbf{Z}$, and $a_d \neq 0$. Put

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ a_d & a_{d-1} & a_{d-2} & \dots & a_1 \end{bmatrix} \qquad \text{and} \qquad \mathbf{v} = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{d-1} \end{bmatrix}, \quad \mathbf{e} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

11.135. $x_n = \langle A^n \mathbf{v}, \mathbf{e} \rangle$.

11.136. If $p \nmid a_d$, then A is invertible over $\mathbf{F}_p$.

11.137. Let p be as in Problem 11.136, and let k be the order of A in $\mathrm{GL}(d, \mathbf{F}_p)$, so that $A^k = \mathrm{Id} + pB$ for some integer matrix B. If $n = km + r$, where $r \in \{0, 1, \dots, k-1\}$, then

$$x_n = \sum_{0 \le j \le m} \binom{m}{j} p^j \langle A^r B^j \mathbf{v}, \mathbf{e} \rangle.$$

11.138 (p-adically interpolating x_{km+r}). Continue with the above notation and assumptions but assume additionally that p is odd. For each fixed $r \in \{0, 1, \dots, k-1\}$, there is a Strassmann series $F_{k,r}(T)$ with $F_{k,r}(m) = x_{km+r}$ for every integer $m \ge 0$.

11.139. For each fixed $r \in \{0, 1, \dots, k-1\}$, either $x_n = 0$ for all nonnegative integers $n \equiv r \pmod{k}$, or $x_n = 0$ for only finitely many $n \equiv r \pmod{k}$.

Hence: The set of n with $x_n = 0$ is the union of a finite set and a finite collection of residue classes. **(Skolem's Theorem)**

11.140. Give an example of an integer linear recurrence sequence, not identically 0, with the property that $x_n = 0$ for infinitely many n.

11.141 (Mahler). Does Skolem's Theorem hold for recurrence sequences over $\mathbf{Q}$? ("Over $\mathbf{Q}$" means that $a_1, \dots, a_d$ and $x_0, \dots, x_{d-1}$ belong to $\mathbf{Q}$.) Over an arbitrary finite extension of $\mathbf{Q}$ (number field)?

p-Set #12

Strassmann Series

12.142. Let p be an odd prime and let $a \in p\mathbf{Z}_p$. The identity

$$\mathrm{Binom}(1+a;n) = (1+a)^n$$

proved in Exercise 11.134 for nonnegative integers n holds for all $n \in \mathbf{Z}$, since

$$(1+a)^n = \lim_{m\to\infty} (1+a)^{n+p^m} = \lim_{m\to\infty} \mathrm{Binom}(1+a;n+p^m) = \mathrm{Binom}(1+a;n).$$

12.143 (Skolem). Let p be an odd prime. Suppose $a_1, \ldots, a_m \in \mathbf{Z}_p$ and $\beta_1, \ldots, \beta_m \in 1 + p\mathbf{Z}_p$. Let $A \in \mathbf{Z}_p$. There is a Strassmann series $F(T)$ with

$$F(n) = a_1\beta_1^n + a_2\beta_2^n + \cdots + a_m\beta_m^n - A$$

for all integers n. Therefore: The equation $a_1\beta_1^n + a_2\beta_2^n + \cdots + a_m\beta_m^n = A$ is satisfied either for all $n \in \mathbf{Z}$ or for only finitely many integers n.

An Aside on Cubic Rings

Exercise 12.143 has a lovely application to a cubic analogue of Pell's equation. Before proceeding to that main course, we whet our appetites with some algebraic hors d'oeuvres.

Fix a cubefree integer $D > 1$. Let θ be the real cube root of D and let $K = \mathbf{Q}(\theta)$. (Thus, K is a subfield of $\mathbf{R}$.) Since $T^3 - D \in \mathbf{Q}[T]$ is irreducible over $\mathbf{Q}$ (a cubic polynomial with no roots in the ground field), each element of K has a unique representation in the form $x + y\theta + z\theta^2$ for rational x, y, and z.

Fix a complex primitive cube root of 1, say ω. Then $\theta' := \omega\theta$ and $\theta'' := \omega^2\theta$ are the nonreal complex roots of $T^3 - D$. The field K is isomorphic to both $K' = \mathbf{Q}(\theta')$ and $K'' = \mathbf{Q}(\theta'')$ — indeed, all three fields are isomorphic to $\mathbf{Q}[T]/(T^3 - D)$. We will decorate elements of K with $'$ and $''$ to indicate the images in K' and K'' under the isomorphisms sending θ to θ' and θ''. So $(x + y\theta + z\theta^2)' = x + y\theta' + z\theta'^2$ and similarly for $''$.

For each $\alpha \in K$, the norm $\mathrm{N}\alpha$ of α is defined by $\mathrm{N}\alpha = \alpha\alpha'\alpha''$. By a tedious but straightforward calculation,

$$\mathrm{N}(x + y\theta + z\theta^2) = x^3 + Dy^3 + D^2z^3 - 3Dxyz. \qquad (*)$$

As a consequence, $\mathrm{N}\alpha \in \mathbf{Q}$ for all $\alpha \in K$.

Since $'$ and $''$ are isomorphisms, $\mathrm{N}(\alpha\beta) = \mathrm{N}\alpha \cdot \mathrm{N}\beta$ for all $\alpha, \beta \in K$, and $\mathrm{N}\alpha \neq 0$ as long as $\alpha \neq 0$. Furthermore, since α' and α'' are a complex conjugate pair, $\mathrm{N}\alpha = \alpha\alpha'\alpha'' = \alpha|\alpha'|^2$ has the same sign as α.

Our application requires some understanding of the units in the pure cubic number ring

$$\mathbf{Z}[\theta] = \{x + y\theta + z\theta^2 : x, y, z \in \mathbf{Z}\}.$$

Clearly, $\mathbf{Z}[\theta]^\times = \langle -1 \rangle \times \mathcal{U}$, where $\mathcal{U} = \mathbf{Z}[\theta]^\times \cap \mathbf{R}^+$ is the collection of positive units in $\mathbf{Z}[\theta]$. Proceeding further requires characterizing $\mathcal{U}$ norm-theoretically.

The norm map is integer-valued on $\mathbf{Z}[\theta]$, as one sees from (*). Now if ε is a positive unit of $\mathbf{Z}[\theta]$, with inverse $\delta \in \mathbf{Z}[\theta]$, then

$$1 = \mathrm{N}(1) = \mathrm{N}(\varepsilon\delta) = \mathrm{N}\varepsilon \cdot \mathrm{N}\delta.$$

Since $\mathrm{N}\varepsilon, \mathrm{N}\delta \in \mathbf{Z}^+$, it must be that $\mathrm{N}\varepsilon = 1$ (and $\mathrm{N}\delta = 1$). Conversely, if $\varepsilon = x + y\theta + z\theta^2 \in \mathbf{Z}[\theta]$ with $\mathrm{N}\varepsilon = 1$, then $\varepsilon > 0$ and

$$\begin{aligned}\varepsilon^{-1} = \varepsilon'\varepsilon'' &= (x + y\theta' + z\theta'^2)(x + y\theta'' + z\theta''^2) \\ &= x^2 - Dyz + (Dz^2 - xy)\theta + (y^2 - xz)\theta^2 \in \mathbf{Z}[\theta].\end{aligned}$$

Hence, $\varepsilon \in \mathbf{Z}[\theta]^\times \cap \mathbf{R}^+ = \mathcal{U}$.

Summarizing: $\mathcal{U} = \{\varepsilon \in \mathbf{Z}[\theta] : \mathrm{N}\varepsilon = 1\}$.

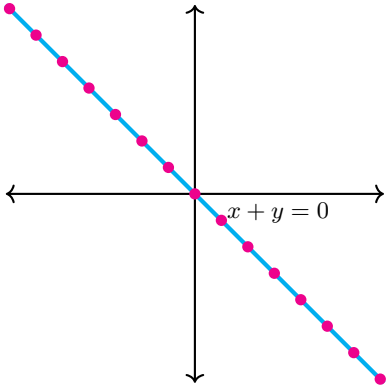
12.144. Let $\alpha = x + y\theta + z\theta^2$ with $x, y, z \in \mathbf{Q}$. Then

$$3x = \alpha + \alpha' + \alpha'', \quad 3y\theta = \alpha + \omega^2\alpha' + \omega\alpha'', \quad 3z\theta^2 = \alpha + \omega\alpha' + \omega^2\alpha''.$$

12.145. For each real number $R > 0$, there are finitely many $\alpha \in \mathbf{Z}[\theta]$ with $|\alpha|, |\alpha'| \leq R$. (Here and in Problem 12.146, $|\cdot|$ is the usual real/complex absolute value.)

12.146 (Dirichlet's logarithmic embedding). The map $\mathbf{L}\colon \mathcal{U} \to \mathbf{R}^2$ defined by $\mathbf{L}(\varepsilon) = (\log\varepsilon, 2\log|\varepsilon'|)$ is an injective group homomorphism with image $\mathbf{L}(\mathcal{U})$ contained in the subspace (line) $\{(x, y) \in \mathbf{R}^2 : x + y = 0\}$.

12.147. For every additive subgroup $\mathcal{G}$ of $\{(x, y) \in \mathbf{R}^2 : x + y = 0\}$, one of the following holds:



Subgroup, shown in pink, of $\{(x, y) \in \mathbf{R}^2 : x + y = 0\}$

(i) $\mathcal{G} = \{\mathbf{0}\}$,
(ii) $\mathcal{G}$ is infinite cyclic,
(iii) some (Euclidean) disc centered at $\mathbf{0}$ has infinite intersection with $\mathcal{G}$.

12.148. $\mathbf{L}(\mathcal{U}) = \{\mathbf{0}\}$ or $\mathbf{L}(\mathcal{U})$ is infinite cyclic.

Since $\mathbf{L}$ is an isomorphism from $\mathcal{U}$ onto $\mathbf{L}(\mathcal{U})$, we conclude from Problem 12.148 that $\mathcal{U} = \{1\}$ or $\mathcal{U}$ is infinite cyclic. With a bit more work, we could show that the second possibility always holds. (Look up the proof of Dirichlet's unit theorem in your favorite algebraic number theory textbook.) For our purposes, having $\mathcal{U} = \{1\}$ would only make life easier, so we do not worry about eliminating that (pseudo)possibility.

A Finiteness Theorem for a Cubic Analogue of Pell's Equation

The next two exercises outline a proof of the following theorem.

D	μ
2	$1 + \theta + \theta^2$
3	$4 + 3\theta + 2\theta^2$
4	$5 + 3\theta + 2\theta^2$
5	$41 + 24\theta + 14\theta^2$
6	$109 + 60\theta + 33\theta^2$

D	μ
7	$4 + 2\theta + \theta^2$
9	$4 + 2\theta + \theta^2$
10	$181 + 84\theta + 39\theta^2$
11	$89 + 40\theta + 18\theta^2$
12	$9073 + 3963\theta + 1731\theta^2$

Generators μ of $\mathcal{U}$ for the first several cubefree $D > 1$.

Theorem. Let D be a cubefree integer with $D > 1$. Then $x^3 - Dy^3 = 1$ has finitely many integer solutions x, y.

Restricting to cubefree $D > 1$ is not significant: Any $D \in \mathbf{Z}^+$ can be factored as $D = D_0 D_1^3$, where D_0, D_1 are positive integers with D_0 cubefree. Distinct solutions to $x^3 - Dy^3 = 1$ give rise to distinct solutions to $x'^3 - D_0 y'^3 = 1$ (take $x' = x$, $y' = D_1 y$). When $D_0 > 1$, the theorem applies to show that the latter equation has finitely many integer solutions; hence, so does the former. Finally, if $D_0 = 1$, then D is a cube and each solution to $x^3 - Dy^3 = 1$ yields a way of writing 1 as a difference of two cubes. But there is only one of these: $1 = 1^3 - 0^3$. (Why?) So the conclusion of the theorem actually holds for all $D \in \mathbf{Z}^+$.

This theorem, first shown by Thue in 1909, stands in sharp contrast with the situation for the classical (quadratic) Pell equation $x^2 - Dy^2 = 1$, which has infinitely many integer solutions for all nonsquare $D \in \mathbf{Z}^+$.

We continue with the notation of the last section. From our work there,

$$x^3 - Dy^3 = 1 \iff \mathrm{N}(x - y\theta) = 1 \iff x - y\theta \in \mathcal{U}. \qquad (\dagger)$$

If $\mathcal{U} = \{1\}$, the equation $x - y\theta \in \mathcal{U}$ forces $x = 1, y = 0$, and we are done proving the theorem already! That was too easy, so we suppose $\mathcal{U} = \langle \mu \rangle$, where μ has infinite order. We may assume that $\mu > 1$, by replacing μ with $1/\mu$ if necessary.

From (†), the solutions $x, y \in \mathbf{Z}$ to $x^3 - Dy^3 = 1$ are in one-to-one correspondence with integers n for which μ^n has vanishing θ^2-coefficient when written with respect to the basis $1, \theta, \theta^2$. From Problem 12.144, if $\mu^n = X + Y\theta + Z\theta^2$, then

$$3Z\theta^2 = \mu^n + \omega\mu'^n + \omega^2\mu''^n.$$

So we are looking for $n \in \mathbf{Z}$ where $\mu^n + \omega\mu'^n + \omega^2\mu''^n = 0$. This calls to mind Exercise 12.143.

12.149. Let $L = \mathbf{Q}(\theta, \omega)$ $(= \mathbf{Q}(\theta, \theta', \theta''))$. Fix an odd prime p for which L embeds into $\mathbf{Q}_p$. Then $|\theta|_p = |\omega|_p = |\mu|_p = |\mu'|_p = |\mu''|_p = 1$. That is, all of $\theta, \omega, \mu, \mu', \mu''$ belong to $\mathbf{Z}_p^\times$.

Here we abuse notation slightly, using the same symbols for elements of L and corresponding elements of $\mathbf{Q}_p$ under our embedding.

12.150. Let L and p be as in Exercise 12.149. We would like to apply Exercise 12.143 to detect the vanishing of $\mu^n + \omega\mu'^n + \omega^2\mu''^n$ but there is no reason to expect that $\mu, \mu', \mu'' \in 1 + p\mathbf{Z}_p$.

To deal with this, set $\nu := \mu^{p-1}, \nu' := \mu'^{p-1}, \nu'' := \mu''^{p-1}$. These belong to $1 + p\mathbf{Z}_p$ by Fermat's little theorem. Writing $n = (p-1)m + r$,

$$\mu^n + \omega\mu'^n + \omega^2\mu''^n = \mu^r\nu^m + \omega\mu'^r\nu'^m + \omega^2\mu''^r\nu''^m.$$

For each fixed r, there is some $m \in \mathbf{Z}$ where the right-hand side is nonzero (check this!). Hence, the RHS vanishes for only finitely many $m \in \mathbf{Z}$ (Exercise 12.143). The Theorem follows.

Much more is known. For instance, Delaunay and Nagell showed (independently) that $x^3 - Dy^3 = 1$ has at most one integer solution $\neq (1, 0)$.

12.151 (a striking corollary). Let $\mathcal{P}$ be a finite set of primes and let $\mathcal{D} = \{\prod_{p\in\mathcal{P}} p^{e_p} : \text{each } e_p = 0, 1, \text{ or } 2\}$. If $n \in \mathbf{Z}^+$ and $n^3 + 1$ has all prime factors from $\mathcal{P}$, then $(-n)^3 - Dy^3 = 1$ for some integer y and some $D \in \mathcal{D}\setminus\{1\}$.

Deduce: The largest prime factor of $n^3 + 1$ tends to infinity with n.

By more elaborate methods, Siegel showed that the largest prime factor of $f(n)$ tends to infinity whenever $f(T) \in \mathbf{Z}[T]$ is nonconstant with at least two distinct complex roots.

p-Set #13

NARRATOR: And so we come to the last chapter in which Christopher Robin and Pooh come to the enchanted place and we say goodbye.
WINNIE THE POOH: Goodbye? Oh no please can't we go back to page one and do it all over again?
NARRATOR: Sorry Pooh. But all stories have an ending you know.
WINNIE THE POOH: Oh bother.

The Many Adventures of Winnie the Pooh

Bern, Baby, Bern!

For each integer u not divisible by p, let $\omega(u)$ denote the $(p-1)$th root of unity in $\mathbf{Q}_p$ congruent to u modulo $p\mathbf{Z}_p$ (see Problem 8.102). Define $\vartheta(u) \in \mathbf{Z}_p$ by the equation $\omega(u) = u + p\vartheta(u)$.

13.152. For each $k \in \mathbf{Z}^+$: $\sum_{u=1}^{p-1} \omega(u)^k = \mathbf{1}_{p-1|k}(p-1)$.

13.153. Let $\beta_k = \frac{B_k}{k} - \frac{\mathbf{1}_{p-1|k}(p-1)}{pk}$. For each $k \in \mathbf{Z}^+$:

$$\beta_k + \sum_{0<j\le k} \binom{k-1}{j-1} B_{k-j} \frac{p^j}{j(j+1)} + \sum_{0<j\le k} \binom{k-1}{j-1} \frac{p^{j-1}}{j} \sum_{u=1}^{p-1} u^{k-j}\theta(u)^j = 0.$$

13.154. Assume p is odd. Then $\beta_k \in \mathbf{Z}_p$ for every $k \in \mathbf{Z}^+$. As a consequence, $\frac{B_k}{k} \in \mathbf{Z}_p$ whenever $p-1 \nmid k$ **(Adams)**.

13.155. Assume $p \ge 5$. Then $\beta_k + \sum_{u=1}^{p-1} u^{k-1}\vartheta(u) \in p\mathbf{Z}_p$ for each $k \in 2\mathbf{Z}^+$.

13.156 (Kummer). If k, k' are even positive integers with $k \equiv k' \pmod{p-1}$, and $p-1 \nmid k$, then $\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \pmod{p\mathbf{Z}_p}$.

For example, $\frac{B_4}{4} = -\frac{1}{120}$ and $\frac{B_{10}}{10} = \frac{1}{132}$ are congruent mod $7\mathbf{Z}_7$. In fact, $\frac{B_4}{4} - \frac{B_{10}}{10} = 7 \cdot -\frac{1}{440}$.

13.157 (Glaisher). Let $p \geq 5$, and put $k = \varphi(p^3) - 1$. Modulo $p^3\mathbf{Z}_p$,

$$H_{p-1} \equiv \sum_{n=1}^{p-1} n^k \equiv k\frac{p^2}{2}B_{k-1} \equiv -\frac{p^2}{3}B_{p-3}.$$

(Here, as usual, $H_{p-1} = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$.) Therefore: p^3 divides the numerator of $H_{p-1} \iff p$ divides the numerator of B_{p-3}. (Compare with Problem 1.11.)

Primes p dividing the numerator of B_{p-3} are known as Wolstenholme primes. The only examples not exceeding 10^{11} are 16 843 and 2 124 679.

Strassmann Series

Let $F(T) = \sum_{k\geq 0} a_k T^k \in \mathbf{Q}_p[[T]]$ be a Strassmann series where not all $a_k = 0$. Since $a_k \to 0$ in $\mathbf{Q}_p$, there is a largest nonnegative integer K with

$$a_K = \max_{k\geq 0} |a_k|_p.$$

We refer to K as the Strassmann degree of $F(T)$. For example, $p + T + \sum_{k\geq 2} p^{\lfloor\sqrt{k}\rfloor}T^k$ has Strassmann degree 1, while $\sum_{k\geq 0} k! \cdot T^k$ has Strassmann degree $p - 1$.

13.158. Let $F(T) = \sum_{k\geq 0} a_k T^k$ be a Strassmann series with a zero $r \in \mathbf{Z}_p$. For all $x \in \mathbf{Z}_p$, we have $F(x) = (x - r)G(x)$, where

$$G(T) = \sum_{j\geq 0} b_j T^j, \quad \text{with} \quad b_j := \sum_{k>j} a_k r^{k-1-j}.$$

Moreover, if $F(T)$ has Strassmann degree $K \geq 1$, then $G(T)$ is Strassmann with Strassmann degree $K - 1$.

13.159 (Strassmann's Theorem). Let $F(T)$ be a Strassmann series with Strassmann degree K. Then $F(x) = 0$ for at most K distinct values of $x \in \mathbf{Z}_p$.

Ramanujan's Conjecture Revisited

We finally return to the study of the equation $x^2 + 7 = 2^m$ initiated in Exercise 3.40. By that problem, to establish Ramanujan's conjecture it suffices to show that there are no $n > 13$ with $\frac{\alpha^n - \beta^n}{\alpha - \beta} = \pm 1$. Here $\alpha = \frac{1+\sqrt{-7}}{2}$ and $\beta = \frac{1-\sqrt{-7}}{2}$.

The quadratic field $\mathbf{Q}(\sqrt{-7})$ can be viewed as a subfield of $\mathbf{Q}_{11}$, identifying $\sqrt{-7}$ with the square root of -7 in $\mathbf{Z}_{11}$ that is congruent to 2 modulo $11\mathbf{Z}_{11}$. By hand, or with the aid of software such as PARI/GP, one computes that

$$\sqrt{-7} = 2 + 8 \cdot 11 + 8 \cdot 11^2 + 7 \cdot 11^3 + 10 \cdot 11^4 + 1 \cdot 11^5 + \ldots,$$

where $\ldots$ suppresses a quantity with 11-adic absolute value at most 11^{-6}. Then

$$\alpha = 7 + 9 \cdot 11 + 9 \cdot 11^2 + 3 \cdot 11^3 + 5 \cdot 11^4 + 6 \cdot 11^5 + \ldots,$$
$$\beta = 5 + 1 \cdot 11 + 1 \cdot 11^2 + 7 \cdot 11^3 + 5 \cdot 11^4 + 4 \cdot 11^5 + \ldots.$$

We study the equation $\frac{\alpha^n - \beta^n}{\alpha - \beta} = \pm 1$ by the method of Exercise 12.150. Put $A = \alpha^{10}$ and $B = \beta^{10}$, so that $A = 1 + a, B = 1 + b$ for

$$a = 7 \cdot 11 + 1 \cdot 11^2 + 1 \cdot 11^3 + 7 \cdot 11^4 + 5 \cdot 11^5 + \ldots,$$
$$b = 9 \cdot 11 + 9 \cdot 11^2 + 9 \cdot 11^3 + 3 \cdot 11^4 + 5 \cdot 11^5 + \ldots,$$

both of which belong to $11\mathbf{Z}_{11}$. Write $n = 10m + r$, where $r \in \{0, 1, \ldots, 9\}$. Then

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = \pm 1 \iff \alpha^n - \beta^n = \pm(\alpha - \beta)$$
$$\iff \alpha^r (1 + a)^m - \beta^r (1 + b)^m \mp (\alpha - \beta) = 0.$$

For each $r \in \{0, 1, \ldots, 9\}$ and each choice of $\pm$ sign, define

$$F_{r,\pm}(T) = \alpha^r \operatorname{Binom}(1 + a; T) - \beta^r \operatorname{Binom}(1 + b; T) \mp (\alpha - \beta),$$

so that $F_{r,\pm}(m) = \alpha^r (1 + a)^m - \beta^r (1 + b)^m \mp (\alpha - \beta)$ for all $m \in \mathbf{Z}$.

Each of our 20 power series $F_{r,\pm}(T)$ is a Strassmann series. For every one of these, we will apply Strassmann's Theorem (Exercise 13.159) to bound the number of zeros in $\mathbf{Z}_p$.

13.160. The constant term of $F_{r,\pm}(T)$ is $\alpha^r - \beta^r \mp (\alpha - \beta)$, which vanishes when

$$(r, \pm) \in \{(1, +), (2, +), (3, -), (5, -)\}$$

and is an 11-adic unit in the other sixteen cases. Every nonconstant coefficient of every $F_{r,\pm}(T)$ is a multiple of 11. Hence, $F_{r,\pm}(T)$ has no zero in $\mathbf{Z}_{11}$ except possibly for the four displayed values of $(r, \pm)$.

13.161. All of $F_{1,+}(T)$, $F_{2,+}(T)$, $F_{5,-}(T)$ have their T-coefficients multiples of 11 but not 11^2. Their Strassmann degrees are all 1.

13.162. $F_{3,-}(T)$ has a T-coefficient that vanishes mod 11^2. Its T^2-coefficient is a multiple of 11^2 but not 11^3. Its Strassmann degree is 2.

13.163. There are at most $3 \cdot 1 + 2 = 5$ integers n with $\frac{\alpha^n - \beta^n}{\alpha - \beta} = \pm 1$. We know five such integers — $n = 1, 2, 3, 5$, and 13 — so those must be all of them.

Remark. The choice to work in $\mathbf{Q}_p$ for $p = 11$ was fortuitous. The next prime after 11 for which -7 is a quadratic residue is $p = 23$. If we had elected to embed $\mathbf{Q}(\sqrt{-7})$ into $\mathbf{Q}_{23}$, we would have to bound the number of zeros of $2 \cdot 22 = 44$ Strassmann series. One of those would correspond to the equation $\frac{\alpha^{22m+12} - \beta^{22m+12}}{\alpha - \beta} = -1$. If you approximate the coefficients sufficiently to apply Strassmann's theorem, you'll find that this series has <u>at most one</u> zero $m \in \mathbf{Z}_p$; hence, $\frac{\alpha^{22m+12} - \beta^{22m+12}}{\alpha - \beta} = -1$ has at most one integer solution m. But in fact (as we know after Exercise 13.163), there are <u>zero</u> integers m satisfying the equation. So working in $\mathbf{Q}_{23}$, we fail to rule out an extraneous zero. What's going on in this instance is that there really *is* an $m \in \mathbf{Z}_{23}$ where the associated power series vanishes — but this m does not belong to $\mathbf{Z}$!

Part II

Solutions, Discussion, and Extra Explorations

Solutions to Set #1

1.1

(a) First off, $|1|^2 = |1 \cdot 1| = |1|$ and $|1| > 0$ (from (i)). Thus, $|1| = 1$. Next, $|-1|^2 = |(-1)(-1)| = |1| = 1$. As $|-1| > 0$, we conclude that $|-1| = 1$.
(b) The proof is the same for the "standard" absolute value: By the triangle inequality, $|x| = |(x-y)+y| \leq |x-y| + |y|$. Now rearrange.
(c) Since $|y^{-1}| \cdot |y| = |y^{-1} \cdot y| = |1| = 1$, we have $|y^{-1}| = |y|^{-1}$. So $|xy^{-1}| = |x||y^{-1}| = |x||y|^{-1}$, as claimed.

1.2 Property (i) in the absolute value definition is clear. Property (ii) is also easy: When $x + y = 0$, the inequality is obvious. Otherwise, either x or y is nonzero, so that $|x|$ or $|y|$ is 1. Hence, $1 = |x+y| \leq |x| + |y|$. To prove (iii), take cases: If x and y are nonzero, both sides are 1, otherwise both sides are 0. In this last step we use that fields are integral domains.

1.3 Property (i) is again clear. Of the remaining two properties, (iii) is quicker to dispense with: If x or y is zero, both sides of (iii) vanish. Otherwise, write $x = p^{v_p(x)}\frac{a}{b}$ and $y = p^{v_p(y)}\frac{c}{d}$, where p does not divide any of a, b, c, d. Then $xy = p^{v_p(x)+v_p(y)}\frac{ac}{bd}$, and p does not divide either of ac or bd. Hence, $v_p(xy) = v_p(x) + v_p(y)$ and $|xy|_p = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$.

To prove (ii) we have to work a bit harder. If x, y, or $x+y$ is zero, (ii) is trivial. Otherwise, write $x = p^{v_p(x)}\frac{a}{b}$ and $y = p^{v_p(y)}\frac{c}{d}$ as above. The symmetry of (ii) in x and y allows us to assume $v_p(x) \leq v_p(y)$. Then $x + y = p^{v_p(x)}\left(\frac{a}{b} + p^{v_p(y)-v_p(x)}\frac{c}{d}\right)$. Since $p^{v_p(y)-v_p(x)} \in \mathbf{Z}$, we can express $p^{v_p(y)-v_p(x)}\frac{c}{d}$ as a fraction with denominator d. Hence, $\frac{a}{b} + p^{v_p(y)-v_p(x)}\frac{c}{d} = \frac{N}{bd}$ for some nonzero $N \in \mathbf{Z}$. Write $N = p^w N'$, where w is a nonnegative integer and $N' \in \mathbf{Z}$ is not divisible by p. Then $x + y = p^{v_p(x)+w}\frac{N'}{bd}$, where neither N' nor bd is divisible by p. Hence, $v_p(x+y) = v_p(x) + w \geq v_p(x)$, and $|x+y|_p = p^{-v_p(x)}p^{-w} = |x|_p p^{-w} \leq |x|_p \leq |x|_p + |y|_p$.

1.4 This is implicit in our solution to Problem 1.3.

1.5 We may assume without loss of generality that $|x| > |y|$. A direct application of the strong triangle inequality gives $|x+y| \le \max\{|x|,|y|\} = |x|$. The strong triangle inequality also implies that $|x| = |(x+y)+(-y)| \le \max\{|x+y|,|-y|\} = \max\{|x+y|,|y|\}$. (We use in this last step that $|-y| = |y|$, which follows from $|-1| = 1$.) Since $|x| > |y|$, the maximum here cannot be $|y|$. So it must be $|x+y|$, yielding $|x| \le |x+y|$. Hence, $|x+y| = |x|$.

1.6 Since $|2| \le 1$, we see that $|2^{e_1}+\cdots+2^{e_n}| \le |2|^{e_1}+\cdots+|2|^{e_n} \le 1+\cdots+1 = n$. To conclude, notice that (a) every positive integer less than 2^n is a sum of at most n powers of 2 (e.g., use the binary representation), while (b) $\sum_{0\le k\le n}\binom{n}{k} = 2^n$, so that $\binom{n}{k} < 2^n$ for every k.

1.7 Write $x = \pm\frac{a}{b}$ where a and b are relatively prime positive integers. Since a and b share no prime factors,

$$\prod_{p \text{ prime}} |x|_p = \prod_{p \text{ prime}} \left(|a|_p|b|_p^{-1}\right) = \prod_{p|a} p^{-v_p(a)} \prod_{p|b} p^{v_p(b)} = |a|_\infty^{-1}|b|_\infty,$$

which is the multiplicative inverse of $|a|_\infty|b|_\infty^{-1} = |x|_\infty$.

Extra Exploration 1 (simultaneous approximation). The product formula suggests that $|\cdot|_\infty$, $|\cdot|_2$, $|\cdot|_3$, $|\cdot|_5$, ... "know about each other." The situation is very different if one considers only a finite subset of these absolute values. Make this precise by proving the following independence statement.

Let $\mathcal{P}$ be a finite set of primes. Choose rational numbers x_p for each prime $p \in \mathcal{P}$, alongside a rational number x_∞. For each $\epsilon > 0$, there is a rational number x satisfying

$$|x - x_p|_p < \epsilon \quad \text{for all } p \in \mathcal{P}, \quad \text{as well as} \quad |x - x_\infty|_\infty < \epsilon.$$

1.8 We begin by demonstrating a fabulously useful formula of Legendre: For each prime p and nonnegative integer n,

$$v_p(n!) = \sum_{1\le m\le n} v_p(m) = \sum_{1\le m\le n} \sum_{\substack{p^k|m \\ k\ge 1}} 1 = \sum_{k\ge 1} \sum_{\substack{1\le m\le n \\ p^k|m}} 1 = \sum_{k\ge 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

When $n > 0$, it follows that $v_p(n!) < \sum_{k\ge 1} \frac{n}{p^k} = \frac{n}{p-1}$. (The inequality is surely strict, as $\lfloor n/p^k \rfloor < n/p^k$ whenever $p^k > n$.) Therefore, $|n!|_p = p^{-v_p(n!)} > p^{-n/(p-1)}$.

Extra Exploration 2 (following up on Legendre's formula). Let p be a prime. For each nonnegative integer n, expand n in base p: write $n = n_0 + n_1 p + n_2 p^2 + \ldots$, where each $n_i \in \{0, 1, 2, \ldots, p-1\}$ and all but finitely many $n_i = 0$. Set $s_p(n) = n_0 + n_1 + n_2 + \ldots$.

(a) Show that $v_p(m) = \frac{1}{p-1}(s_p(m-1) - s_p(m) + 1)$ for every positive integer m. Deduce that $v_p(n!) = \frac{1}{p-1}(n - s_p(n))$ for all nonnegative integers n (an alternative form of Legendre's formula).

(b) Prove that $n!/(-p)^{v_p(n!)} \equiv n_0!n_1!n_2!n_3!\cdots \pmod{p}$ for all nonnegative $n \in \mathbf{Z}$. (Anton [1], Stickelberger [5, pp. 342–343], Hensel [2])

1.9 We interpret "grows faster" to mean that $n!/C^n$ tends to infinity. To prove that, we may (in fact, should!) assume that $C > 0$. A (canonical) application of the ratio test shows that $\sum_{n\geq 0} C^n/n!$ converges. (It converges to e^C but we do not need that here.) So its terms must tend to 0. Since $C^n/n!$ is positive for each n, we deduce that $n!/C^n \to \infty$.

On the other hand, if there are only finitely many primes, then $n! = |n!|_\infty = \prod_p |n!|_p^{-1} \leq \prod_p p^{n/(p-1)} = (\prod_p p^{1/(p-1)})^n$. That is, $n! \leq C^n$ with $C := \prod_p p^{1/(p-1)}$. Contradiction!

Extra Exploration 3 (Skolem [4]). Show that if p is prime and $n \in \mathbf{Z}^+$, either $|2^n - 1|_p = 1$ or $|2^n - 1|_p = |2^{p-1} - 1|_p |n|_p$. Deduce that if $\mathcal{P}$ is any fixed finite set of primes, then $2^n - 1$ has a prime factor outside of $\mathcal{P}$ for all sufficiently large n.

1.10 Given $n \in \mathbf{Z}^+$, let e be the largest nonnegative integer such that $2^e \leq n$. Then 2^e is the unique integer in $[1, n]$ divisible by 2^e. (The next smallest multiple of 2^e is 2^{e+1}, but this exceeds n.) It follows that $|1/m|_2 = 2^{v_2(m)}$ has a unique maximum, among $m \in [1, n]$, at $m = 2^e$. By "survival of the greatest" (Exercise 1.4), $|H_n|_2 = |\sum_{m\leq n} 1/m|_2 = |1/2^e|_2 = 2^e > \frac{1}{2}n$. So $|H_n|_2 \to \infty$.

Extra Exploration 4. Prove that in any nonempty set S of consecutive positive integers, one element of S has strictly smaller 2-adic absolute value than all the others. Conclude that if $S \neq \{1\}$, then $\sum_{n\in S} 1/n \notin \mathbf{Z}$ **(Kürschák [3])**.

1.11 The stated expression for H_{p-1} is immediate upon pairing the terms $\frac{1}{i}$ and $\frac{1}{p-i}$. To show $|H_{p-1}|_p \leq p^{-2}$, we must prove that $|S|_p \leq p^{-1}$, where $S := \sum_{0<i<p/2} \frac{1}{i(p-i)}$.

We would like to evaluate S modulo p by reducing term-by-term. This is essentially what we will do, but since it is not immediately clear what it means to reduce a rational number mod p, we premultiply by $(p-1)!$. In the field $\mathbf{F}_p = \mathbf{Z}/p$, we have $\frac{(p-1)!}{i(p-i)} = (p-1)!i^{-1}(p-i)^{-1} = -(p-1)!i^{-2*}$ whenever $0 < i < p/2$. Therefore (still working in $\mathbf{F}_p$),

$$(p-1)!S = -(p-1)! \sum_{0<i<p/2} i^{-2} = -\frac{1}{2}(p-1)! \sum_{i\in\mathbf{F}_p^\times} i^{-2} = -\frac{1}{2}(p-1)! \sum_{j\in\mathbf{F}_p^\times} j^2.$$

* The first equality is not a tautology! What is being claimed is that the integer on the left has its mod p reduction equal to the element of $\mathbf{F}_p$ on the right. The -1st powers indicate inverses in the field $\mathbf{F}_p$.

Here we use that $i^{-2} = (p-i)^{-2}$ and that as i runs over all the nonzero elements of $\mathbf{F}_p$, so does $j = i^{-1}$. To finish, observe that since $p > 3$, the group $\mathbf{F}_p^\times$ has an element other than ± 1. So there is an $r \in \mathbf{F}_p^\times$ with $r^2 \neq 1$. Since multiplication by r permutes $\mathbf{F}_p^\times$,

$$r^2 \sum_{j \in \mathbf{F}_p^\times} j^2 = \sum_{j \in \mathbf{F}_p^\times} (rj)^2 = \sum_{j \in \mathbf{F}_p^\times} j^2,$$

forcing $\sum_{j \in \mathbf{F}_p^\times} j^2 = 0$ (since $r^2 \neq 1$). It follows that $(p-1)!S = 0$ in $\mathbf{Z}/p$, and so $(p-1)!S$ is a multiple of p. Since $p \nmid (p-1)!$, we conclude that $|S|_p = |(p-1)!|_p |S|_p = |(p-1)!S|_p \leq p^{-1}$, as desired.

Remark. It is not really necessary to premultiply by $(p-1)!$. On the next problem set, we will introduce the ring $\mathbf{Z}_{(p)}$, whose elements are the rational numbers with denominators prime to p. $\mathbf{Z}_{(p)}$ is a local ring (in fact, domain) with unique maximal ideal $p\mathbf{Z}_{(p)}$, and $\mathbf{Z}_{(p)}/p\mathbf{Z}_{(p)} \cong \mathbf{Z}/p = \mathbf{F}_p$. The same argument we used to show $(p-1)!S = 0$ in $\mathbf{Z}/p$ will show directly that $S = 0$ in $\mathbf{Z}_{(p)}/p\mathbf{Z}_{(p)}$, and this is sufficient to conclude that $|S|_p \leq p^{-1}$.

References

1. H. Anton, *Die Elferprobe und die Proben für die Modul Neun, Dreizehn und Hunderteins. Für Volks- und Mittelschulen.* Archiv Math. Physik **49** (1869), 241–308.
2. K. Hensel, *Über die arithmetischen Eigenschaften der Faktoriellen.* Archiv Math. Physik (third series) **2** (1902), 293–294.
3. J. Kürschák, *A harmonikus sorról.* Mat. Fiz. Lapok **27** (1918), 299–300.
4. T. Skolem, *On certain exponential equations.* Norske Vid. Selsk. Forh. **18** (1945), 71–74.
5. L. Stickelberger, *Ueber eine Verallgemeinerung der Kreistheilung.* Math. Ann. **37** (1890), 321–367.

Solutions to Set #2

2.12 We have to show that for any $x, y, z \in K$, at least two of $|x-y|, |y-z|$, and $|z-x|$ coincide. This is a simple consequence of "survival of the greatest": If $|x-y| \neq |y-z|$, then $|z-x| = |x-z| = |(x-y)+(y-z)| = \max\{|x-y|, |y-z|\}$. This argument shows that the largest side length always appears at least twice.

2.13 Suppose to start with that $z \in \mathbf{D}_{<r}(x)$. Then $|z-x_0| = |(z-x)+(x-x_0)| \leq \max\{|z-x|, |x-x_0|\} < r$. Thus, $\mathbf{D}_{<r}(x) \subseteq \mathbf{D}_{<r}(x_0) = D$. Similarly, if $z \in D$, then $|z-x| = |(z-x_0)+(x_0-x)| \leq \max\{|z-x_0|, |x_0-x|\} < r$, proving that $D \subseteq \mathbf{D}_{<r}(x)$. So $D = \mathbf{D}_{<r}(x)$.

2.14 Suppose that $x \in K$ belongs to the intersection of the open discs $D_0 = \mathbf{D}_{<r_0}(x_0)$ and $D_1 = \mathbf{D}_{<r_1}(x_1)$. By Problem 2.13, $D_0 = \mathbf{D}_{<r_0}(x)$ and $D_1 = \mathbf{D}_{<r_1}(x)$. Then $D_0 \subseteq D_1$ or $D_1 \subseteq D_0$ according to whether $r_0 \leq r_1$ or vice versa.

2.15 Let $\mathcal{R} = \{p^v : v \in \mathbf{Z}\}$. If $r \notin \mathcal{R}$, then $\mathbf{D}_{<r}(x_0) = \mathbf{D}_{\leq r}(x_0)$, for any center x_0. If $r \in \mathcal{R}$, then $\mathbf{D}_{<r}(x_0) = \mathbf{D}_{\leq r/p}(x_0)$ while $\mathbf{D}_{\leq r}(x_0) = \mathbf{D}_{<pr}(x_0)$.

2.16 Suppose $|\cdot|$ is an absolute value on $F = \mathbf{F}_{2027}$. Let g be a generator of $F^\times$. Then $|g|^{2026} = |g^{2026}| = |1| = 1$, and so $|g| = 1$. Since g generates $F^\times$, it follows that $|x| = 1$ for all nonzero x in F. Therefore, the only absolute value on F is the trivial absolute value.

This argument works for any $\mathbf{F}_p$, or any finite field for that matter.

2.17 Applying the binomial theorem and the triangle inequality,

$$|x+y|^n = \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k |y|^{n-k}$$
$$\leq \max\{|x|, |y|\}^n \sum_{k=0}^{n} \left|\binom{n}{k}\right| \leq \max\{|x|, |y|\}^n \cdot (n+1) \max_{0 \leq k \leq n} \left|\binom{n}{k}\right|.$$

(Moving from the first to the second line, we used that $|x|^k|y|^{n-k} \leq \max\{|x|,|y|\}^k \cdot \max\{|x|,|y|\}^{n-k} = \max\{|x|,|y|\}^n$.) Take nth roots.

2.18 Every absolute value on $\mathbf{F}_p(T)$ restricts to an absolute value on $\mathbf{F}_p$, hence is trivial on $\mathbf{F}_p$ (Exercise 2.16). It follows that every binomial coefficient has absolute value at most 1. So by Exercise 2.17, for all $x, y \in \mathbf{F}_p(T)$,

$$|x+y| \leq (n+1)^{1/n} \max\{|x|,|y|\}.$$

Sending n to infinity, $|x+y| \leq \max\{|x|,|y|\}$. In other words, $|\cdot|$ is non-Archimedean.

2.19 We start by constructing a family of absolute values on $\mathbf{F}_p(T)$ parametrized by the monic irreducibles in $\mathbf{F}_p[T]$.

Fix a monic irreducible $\pi \in \mathbf{F}_p[T]$. Every $x \in \mathbf{F}_p(T)^\times$ can be written in the form $\pi^v \frac{a}{b}$ where a and b are elements of $\mathbf{F}_p[T]$ not divisible by π. Here the integer $v_\pi(x) := v$ is uniquely determined by x (a consequence of the unique factorization theorem for $\mathbf{F}_p[T]$). Fix your favorite constant $C_\pi > 1$. If we set $|x|_\pi = C_\pi^{-v_\pi(x)}$ for nonzero $x \in \mathbf{F}_p(T)$, and set $|0|_\pi = 0$, then $|\cdot|_\pi$ is a non-Archimedean absolute value on $\mathbf{F}_p(T)$. The proof is more or less identical to that for $|\cdot|_p$ (see Exercise 1.3).

If π and $\tilde{\pi}$ are distinct monic irreducibles in $\mathbf{F}_p[T]$, then $|\pi|_\pi = C_\pi^{-1} < 1$ while $|\tilde{\pi}|_\pi = C_\pi^0 = 1$. This settles the first half of the problem.

As for the concluding question: Yes, there is such an absolute value. Fix $C_\infty > 1$. For $x \in \mathbf{F}_p(T)^\times$, write $x = \frac{a}{b}$ with $a, b \in \mathbf{F}_p[T]$. While a and b are not uniquely determined by this representation, the difference $\deg a - \deg b$ is independent of the choice of a and b. We put $|x|_\infty = C_\infty^{\deg a - \deg b}$ for nonzero $x \in \mathbf{F}_p(T)$, taking $|0|_\infty = 0$. Since $|T|_\infty = C_\infty > 1$, we will be done if we show $|\cdot|_\infty$ is an absolute value on $\mathbf{F}_p(T)$.

Condition (i) in the absolute value definition (see Set #1) is obvious. Condition (iii) follows from $\deg uv = \deg u + \deg v$. To prove (ii), we may assume x, y, and $x+y$ are nonzero. Write $x = \frac{a}{b}$ and $y = \frac{c}{d}$. Then $x + y = \frac{ad+bc}{bd}$, and

$$\begin{aligned}
\deg(ad+bc) - \deg(bd) &\leq \max\{\deg(ad), \deg(bc)\} - \deg(bd) \\
&= \max\{\deg(ad) - \deg(bd), \deg(bc) - \deg(bd)\} \\
&= \max\{\deg(a) - \deg(b), \deg(c) - \deg(d)\}.
\end{aligned}$$

Since $C_\infty > 1$, the inequality is preserved upon raising C_∞ to both sides. This gives $|x+y|_\infty \leq \max\{|x|_\infty, |y|_\infty\}$, proving the strong triangle inequality.

2.20 To prove that $\mathbf{D}_{\leq 1}(0)$ is a subring it is enough to argue that $1 \in \mathbf{D}_{\leq 1}(0)$ and that $\mathbf{D}_{\leq 1}(0)$ is closed under multiplication and subtraction. The first

requirement is clear, since $|1| = 1$. Closure under multiplication follows from the multiplicative property of $|\cdot|$, as the interval $[0, 1]$ is closed under multiplication. Closure under subtraction is a consequence of the strong triangle inequality: If $|x|, |y| \leq 1$, then $|x - y| \leq \max\{|x|, |-y|\} = \max\{|x|, |y|\} \leq 1$.

By definition of the p-adic absolute value, $x \in \mathbf{Z}_{(p)}$ if and only if $x = p^v a/b$ for some nonnegative integer v and some $a, b \in \mathbf{Z}$ not divisible by p. This happens precisely when the denominator of x in lowest terms is not a multiple of p.

2.21 Write $x = a/b$ in lowest terms, with $b > 0$. By Problem 2.20, $x \in \bigcap_{p \text{ prime}} \mathbf{Z}_{(p)} \iff b$ has no prime factors $\iff b = 1 \iff x \in \mathbf{Z}$. So $\bigcap_{p \text{ prime}} \mathbf{Z}_{(p)} = \mathbf{Z}$.

2.22 Let $0 < k < p$. Working modulo p,

$$\begin{aligned}(k-1)!\binom{p-1}{k-1} &= (p-1)(p-2)\cdots(p-(k-1)) \\ &\equiv (-1)(-2)\cdots(-(k-1)) \\ &\equiv (-1)^{k-1}(k-1)!.\end{aligned}$$

Since $p \nmid (k-1)!$, we conclude that $\binom{p-1}{k-1} \equiv (-1)^{k-1} \pmod{p}$. Write $\binom{p-1}{k-1} = (-1)^{k-1} + pr$, where $r \in \mathbf{Z}$. Then $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1} = p\frac{(-1)^{k-1}}{k} + p^2\frac{r}{k}$. Hence, working in the ring $\mathbf{Z}_{(p)}$,

$$\binom{p}{k} \equiv p\frac{(-1)^{k-1}}{k} \pmod{p^2\mathbf{Z}_{(p)}}.$$

We have made sense of the claimed congruence mod p^2 by interpreting it — nay, proving it — as a congruence modulo the ideal $p^2\mathbf{Z}_{(p)}$ of the ring $\mathbf{Z}_{(p)}$.

2.23 Summing the congruence $\binom{p}{k} \equiv p\frac{(-1)^{k-1}}{k} \pmod{p^2\mathbf{Z}_{(p)}}$ over integers $0 < k < p$ yields $2^p - 2 \equiv p\sum_{0<k<p}(-1)^{k-1}/k \pmod{p^2\mathbf{Z}_{(p)}}$. Dividing by p,

$$\frac{2^p - 2}{p} \equiv 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{p-1} \pmod{p\mathbf{Z}_{(p)}}.$$

The left and right-hand sides of the displayed congruence have difference smaller than 1 in terms of p-adic absolute value. So by the strong triangle inequality, one side has absolute value < 1 if and only if the other does. The solution is concluded by observing that $|\frac{2^p-2}{p}|_p < 1 \iff p^2 \mid 2^p - 2$.

2.24 Since F has finitely many complex roots, we can fix $n_0 \in \mathbf{Z}$ with $F(n_0) \neq 0$. Replacing $F(T)$ with $F(T + n_0)$, we may assume that $F(T)$ has nonzero constant term a_0 (say). Then $F(a_0 T) = a_0 G(T)$ for some nonconstant $G(T) \in \mathbf{Z}[T]$ with $G(0) = 1$.

Let $\mathcal{P}$ be the set of primes dividing $G(n)$ for some integer n. Every prime dividing a value of G also divides a value of F, so it suffices to prove $\mathcal{P}$ is infinite.

We mimic Euclid. Suppose $p_1, \ldots, p_k$ is any finite list of primes in $\mathcal{P}$. We choose an integer m with $|G(mp_1 \cdots p_k)| > 1$. (Such an m surely exists, as the inequality excludes no more than $3 \deg G$ values of m.) Then $G(mp_1 \cdots p_k)$ is divisible by *some* prime p, but

$$G(mp_1 \cdots p_k) \equiv G(0) \equiv 1 \pmod{p_i}$$

for each $i = 1, 2, \ldots, k$. So there is a prime $p \in \mathcal{P}$ not on our list. As this is true no matter what finite list we start with, $\mathcal{P}$ is infinite.

Extra Exploration 5. Let $\mathcal{P}$ be a finite set of primes, say $\#\mathcal{P} = k$. Show that there are positive constants c and x_0 such that, for every real number $x \geq x_0$,

$$\#\{n \in \mathbf{Z} : |n| \leq x \text{ and } p \mid n \Rightarrow p \in \mathcal{P}\} \leq c(\log x)^k.$$

Use this to give another solution to Problem 2.24.

Extra Exploration 6 (Bauer [1]; see also Nagell [4, §49, pp. 168–169]). Let $F(T)$ be a nonconstant polynomial with integer coefficients. Suppose that F has a real root of odd multiplicity. Show that for each integer $m \geq 3$, there are infinitely many primes $p \not\equiv 1 \pmod{m}$ for which F has a root mod p.

2.25 Suppose p is odd. If $p \mid n^4 + 1$, then $n^4 \equiv -1 \pmod{p}$ and $n^8 \equiv 1 \pmod{p}$. Since $-1 \not\equiv 1 \pmod{p}$, the order of n modulo p divides 8 but does not divide 4 — so it must be precisely 8. As the order is always a divisor of $p - 1$, we conclude that $p \equiv 1 \pmod{8}$.

To obtain infinitely many primes $p \equiv 1 \pmod{8}$, apply Problem 2.24.

2.26 If $p \mid (2n + 1)^2 - 2$, then p is odd and 2 is a square modulo p. By elementary number theory, $p \equiv \pm 1 \pmod{8}$.

For each $n \in \mathbf{Z}^+$, the integer $(2n+1)^2 - 2$ is larger than 1 and thus factors as a product of positive primes. If each prime in this factorization is congruent to 1 (mod 8), then $(2n+1)^2 - 2$ is also congruent to 1 (mod 8). But $(2n+1)^2 - 2 \equiv 1 - 2 \equiv -1 \pmod{8}$. Thus, $(2n + 1)^2 - 2$ must be divisible by some prime congruent to $-1 \pmod{8}$.

Finally, suppose $p_1, \ldots, p_k$ is any finite list of primes congruent to $-1 \pmod{8}$. For each $i = 1, 2, \ldots, k$, there are two residue classes $n_i \bmod p_i$ for which $(2n_i + 1)^2 - 2 \equiv 0 \pmod{p_i}$. As each $p_i > 2$, the Chinese Remainder Theorem allows us to choose a positive integer n not congruent to any of the $n_i \pmod{p_i}$. Then $(2n+1)^2 - 2$ is divisible by some prime $p \equiv -1 \pmod{8}$ but not divisible by any of $p_1, \ldots, p_k$. Thus, there must be a prime congruent to $-1 \bmod 8$

that is not on the list $p_1, \ldots, p_k$. As our starting list was arbitrary, there are infinitely many primes $p \equiv -1 \pmod 8$.

2.27 Problem 2.25 handles the residue class 1 mod 8 while Problem 2.26 handles -1 mod 8. To take care of 5 mod 8, we argue as in Problem 2.26 with $(2n+1)^2+4$ replacing $(2n+1)^2-2$. Every odd prime p with -4 a square mod p is congruent to 1 or 5 $\pmod 8$. Since $(2n+1)^2+4 \equiv 1+4 \equiv 5 \pmod 8$, there must be some prime congruent to 5 $\pmod 8$ dividing $(2n+1)^2+4$. Following the solution to Problem 2.26, we obtain infinitely many primes $p \equiv 5 \pmod 8$ by varying n.

To deal with 3 mod 8, use $(2n+1)^2+2$. Every odd p with -2 a square mod p is congruent to 1 or 3 $\pmod 8$. As $(2n+1)^2+2 \equiv 1+2 \equiv 3 \pmod 8$, there is always some prime congruent to 3 $\pmod 8$ dividing $(2n+1)^2+2$. Varying n, we obtain infinitely many primes $p \equiv 3 \pmod 8$.

Remark. Dirichlet's general theorem is proved by moderately sophisticated analytic methods. By contrast, the proofs in the last few exercises are variants on Euclid's simple and familiar argument. This invites the question: Which other residue classes can be shown to contain infinitely many primes by a proof *in the style of Euclid's*? For one reasonable interpretation of "in the style of Euclid's" (which regrettably would take us too far afield to motivate here) an elegant answer has been given by Issai Schur and Ram Murty: *There is a Euclid-style proof of the infinitude of primes congruent to* $a \pmod m \iff a^2 \equiv 1 \pmod m$. See [2, 3, 5] for details.

References

1. M. Bauer, *Über die arithmetische Reihe*. J. Reine Angew. Math. **131** (1906), 265–267.
2. M. R. Murty, *Primes in certain arithmetic progressions*. J. Madras Univ., Section B, **51** (1988), 161–169.
3. M. R. Murty and N. Thain, *Prime numbers in certain arithmetic progressions*. Funct. Approx. Comment. Math. **35** (2006), 249–259.
4. T. Nagell, *Introduction to number theory*, Chelsea Publishing Co., New York, 1964.
5. I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*. Sitzungber. Berliner Math. Ges. **11** (1912), 40–50.

Solutions to Set #3

3.28 The proof is the same as in calculus: Suppose for a contradiction that $x_n \to x$ and $x_n \to x'$, where $x' \neq x$. Then $\epsilon := \frac{1}{2}|x' - x| > 0$. Since $x_n \to x$, we can choose $N \in \mathbf{Z}^+$ with $|x_n - x| < \epsilon$ for all $n \geq N$. Similarly, we can choose $N' \in \mathbf{Z}^+$ with $|x_n - x'| < \epsilon$ for all $n \geq N'$. Taking $n \geq \max\{N, N'\}$, we find that

$$|x' - x| = |(x' - x_n) + (x_n - x)| \leq |x' - x_n| + |x_n - x| < 2\epsilon = |x' - x|.$$

Contradiction!

3.29

(a) Let $\epsilon > 0$. Choose $N_1 = 1$. If $n \geq N_1$, then $|x_n - x| = 0 < \epsilon$.

(b) Let $\epsilon > 0$. Choose $N_1, N_2 \in \mathbf{Z}^+$ so that $|x_n - x| < \frac{1}{2}\epsilon$ whenever $n \geq N_1$ and $|y_n - y| < \frac{1}{2}\epsilon$ whenever $n \geq N_2$. For $n \geq \max\{N_1, N_2\}$,

$$|(x_n+y_n)-(x+y)| = |(x_n-x)+(y_n-y)| \leq |x_n-x|+|y_n-y| < \frac{1}{2}\epsilon+\frac{1}{2}\epsilon = \epsilon.$$

So $x_n + y_n \to x + y$.

(c) Here we must work a bit harder. When checking the definition of convergence, we can assume that $0 < \epsilon < 1$. (Larger values of ϵ only make life easier.) Given such an ϵ, choose $N_1, N_2 \in \mathbf{Z}^+$ with $|x_n - x| < \frac{1}{3(|y|+1)}\epsilon$ for all $n \geq N_1$ and $|y_n - y| < \frac{1}{3(|x|+1)}\epsilon$ for all $n \geq N_2$. Write $x_n = x + d_n$ and $y_n = y + e_n$, so that $x_n y_n = xy + xe_n + yd_n + d_n e_n$. For $n \geq \max\{N_1, N_2\}$,

$$|xe_n| \leq \frac{|x|}{3(|x|+1)}\epsilon < \frac{\epsilon}{3} \quad \text{and} \quad |yd_n| \leq \frac{|y|}{3(|y|+1)}\epsilon < \frac{\epsilon}{3}.$$

For these same values of n, we have $|d_n|, |e_n| < \frac{\epsilon}{3} < \frac{1}{3}$. So (estimating crudely) $|d_n e_n| \leq |d_n| < \frac{\epsilon}{3}$. Therefore,

$$|x_n y_n - xy| = |xe_n + yd_n + d_n e_n| \leq |xe_n| + |yd_n| + |d_n e_n| < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon.$$

3.30 Notice that $2x_n = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \cdots + 2 \cdot 3^n$, which is precisely the ternary expansion of $3^{n+1} - 1$. So $x_n = \frac{3^{n+1}-1}{2} = -\frac{1}{2} + \frac{1}{2}3^{n+1}$, and $|x_n - (-\frac{1}{2})|_3 = |\frac{1}{2}3^{n+1}|_3 = 3^{-(n+1)}$, which tends to 0. Therefore, $x_n \to -\frac{1}{2}$ in $(\mathbf{Q}, |\cdot|_3)$.

The series $\sum_{k=0}^{\infty} 3^k$ diverges in $\mathbf{Q}_p$ for each prime $p \neq 3$. To prove this, we appeal to a result possessing the air of the familiar.

Lemma (kth term test for a valued field). If $\sum_{k=1}^{\infty} a_k$ converges in $(K, |\cdot|)$, then $a_k \to 0$.

To apply this in our situation, observe that if $p \neq 3$, then $|3^k|_p = 1$ for every k, and 1 does not tend to 0 !*

Proof. Suppose $\sum_{k=1}^{\infty} a_k = x$ (where $x \in K$). This means that the sequence $\{s_n\}$ with nth term $s_n = \sum_{k=1}^{n} a_k$ converges to x. Let $\epsilon > 0$ and choose $N \in \mathbf{Z}^+$ with the property that $|s_n - x| < \frac{1}{2}\epsilon$ for all $n \geq N$. Then for every positive integer $n \geq N + 1$,

$$|a_n| = |s_n - s_{n-1}| = |(s_n - x) + (x - s_{n-1})| \leq |s_n - x| + |x - s_{n-1}| < 2 \cdot \frac{1}{2}\epsilon = \epsilon.$$

We have verified the definition of "$a_n \to 0$." ∎

3.31 Some experimentation suggests that $\sum_{n=0}^{N} n \cdot n! = (N+1)! - 1$, which is easily confirmed by induction. Hence, $|\sum_{n=0}^{N} n \cdot n! - (-1)|_2 = |(N+1)!|_2$. Since the power of 2 in $(N+1)!$ tends to infinity, $|(N+1)!|_2 \to 0$, and $\sum_{n=0}^{N} n \cdot n! \to -1$. That is, $\sum_{n=0}^{\infty} n \cdot n! = -1$.

Next, we look at $\sum_{n=0}^{N} n^2 \cdot 2^n$. Let $F(T) = \sum_{n=0}^{N} T^n$. Differentiating and multiplying by T gives $TF'(T) = \sum_{n=0}^{N} nT^n$. Another round of the same process yields

$$\sum_{n=0}^{N} n^2 T^n = T(TF'(T))' = T^2 F''(T) + TF'(T).$$

Substituting in $F(T) = \frac{1-T^{N+1}}{1-T} = \frac{1}{1-T} - T^{N+1}\frac{1}{1-T}$ and simplifying,

$$\sum_{n=0}^{N} n^2 T^n = \frac{T(T+1)}{(1-T)^3} + T^{N+1}\frac{G_N(T)}{(1-T)^3}$$

for some $G_N(T) \in \mathbf{Z}[T]$.

Plugging in $T = 2$, we deduce that

* Although it does tend to "0!"

$$\left|\sum_{n=0}^{N} n^2 2^n - (-6)\right|_2 = 2^{-N-1} \cdot |G_N(2)|_2 \le 2^{-N-1}.$$

We send N to infinity and conclude that $\sum_{n=0}^{\infty} n^2 2^n = -6$ in $(\mathbf{Q}, |\cdot|_2)$.

3.32 With $x_0 := \frac{11}{7} \in \mathbf{Z}_{(3)}$, each step of the displayed algorithm has the form $x_n = d_n + 3x_{n+1}$, where $d_n \in \{0, 1, 2\}$ and $x_{n+1} \in \mathbf{Z}_{(3)}$.

Repeated substitution reveals that for each nonnegative integer n,

$$\begin{aligned} x_0 &= d_0 + 3x_1 \\ &= d_0 + 3(d_1 + 3x_2) \\ &\vdots \\ &= d_0 + 3(d_1 + 3(d_2 + \cdots + 3(d_n + 3x_{n+1}))) \\ &= d_0 + 3d_1 + 3^2 d_2 + \cdots + 3^n d_n + 3^{n+1} x_{n+1}. \end{aligned}$$

Therefore,

$$\left|x_0 - \sum_{k=0}^{n} 3^k d_k\right|_3 = 3^{-n-1} |x_{n+1}|_3 \le 3^{-n-1}.$$

Sending n to infinity, $x_0 = \sum_{k=0}^{\infty} 3^k d_k$.

As shown in the problem statement, $x_1 = x_7$, implying that the "digits" d_i repeat in blocks of six starting from $i = 1$.

3.33 We modify the algorithm of Problem 3.32. This time $x_0 = \frac{2}{7} \in \mathbf{Q}_{(5)}$, and each $d_n \in \{0, 1, 2, 3, 4\}$ is chosen so that $x_n = d_n + 5x_{n+1}$ for an $x_{n+1} \in \mathbf{Q}_{(5)}$. Grinding this out,

$$\begin{aligned} \frac{2}{7} &= 1 + 5 \cdot \frac{-1}{7} & \qquad \frac{-6}{7} &= 2 + 5 \cdot \frac{-4}{7} \\ \frac{-1}{7} &= 2 + 5 \cdot \frac{-3}{7} & \qquad \frac{-4}{7} &= 3 + 5 \cdot \frac{-5}{7} \\ \frac{-3}{7} &= 1 + 5 \cdot \frac{-2}{7} & \qquad \frac{-5}{7} &= 0 + 5 \cdot \frac{-1}{7}. \\ \frac{-2}{7} &= 4 + 5 \cdot \frac{-6}{7} \end{aligned}$$

Replicating the logic of the solution to Problem 3.32, we conclude that in $(\mathbf{Q}, |\cdot|_5)$,

$$\frac{2}{7} = 1 + 2 \cdot 5 + 1 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 3 \cdot 5^5 + 0 \cdot 5^6 + 2 \cdot 5^7 + \ldots,$$

where the "digits" follow the eventually periodic pattern $1, \overline{2, 1, 4, 2, 3, 0}$.

Extra Exploration 7 (cf. Burger and Struppeck [1]). Show that there is a sequence of rational numbers $\{a_n\}$ with the property that $\sum_{n=1}^{\infty} a_n$ converges to 0 with respect to $|\cdot|_\infty$ and converges to $1/p$ with respect to $|\cdot|_p$ for every prime p.

3.34 If $|\cdot|$ is non-Archimedean, a straightforward induction shows that $|m| \le 1$ for *all* positive integers m. This handles the forward direction of the equivalence.

Turning to the reverse implication, suppose that $|2| \le 1$. If n is any positive integer, we get from Problem 1.6 that

$$\left|\binom{n}{k}\right| \le n \quad \text{whenever } 0 \le k \le n.$$

So by Exercise 2.17, $|x+y| \le (n(n+1))^{1/n} \max\{|x|,|y|\}$ for all $x, y \in K$. Sending n to infinity in this last inequality, $|x+y| \le \max\{|x|,|y|\}$: That is, $|\cdot|$ is non-Archimedean.

We can draw the same conclusion if 3 replaces 2. More generally, suppose $m \ge 2$ and $|m| \le 1$. Let n be a positive integer and write each associated binomial coefficient $\binom{n}{k}$ in base m: $\binom{n}{k} = \sum_{j \ge 0} d_j m^j$, where each $d_j \in \{0, 1, 2, \ldots, m-1\}$ and the d_j are eventually zero. If J is the largest index for which $d_j \ne 0$, then $2^n > \binom{n}{k} \ge m^j \ge 2^j$. Hence, $j < n$ and

$$\left|\binom{n}{k}\right| \le \sum_{0 \le j < n} |d_j||m|^j \le \sum_{0 \le j < n} |d_j| \le \max\{|0|, |1|, \ldots, |m-1|\} \cdot n.$$

This bound on $|\binom{n}{k}|$ is a suitable substitute for that of Problem 1.6 in the argument of the last paragraph.

In summary: If m is an integer with $m \ge 2$, and $|m| \le 1$, then $|\cdot|$ is non-Archimedean.

3.35 Let $|\cdot|$ be a nontrivial non-Archimedean absolute value on $\mathbf{Q}$. As noted in the solution to Problem 3.34, $|m| \le 1$ for all positive integers m. In particular, $|p| \le 1$ for all primes p. If equality holds for all p, then $|m| = 1$ for all $m \in \mathbf{Z}^+$ (apply the Fundamental Theorem of Arithmetic). But then Exercise 1.1(a,c) allows us to deduce $|x| = 1$ for all nonzero $x \in \mathbf{Q}$, contradicting that $|\cdot|$ is nontrivial.

3.36 Since $|\cdot|$ is non-Archimedean, $|k| \le 1$ for all integers k.

Given relatively prime integers m and n, write $1 = am + bn$ with $a, b \in \mathbf{Z}$ (Bézout). Then

$$1 = |am + bn| \le \max\{|a||m|, |b||n|\} \le \max\{|m|, |n|\} \le 1.$$

Hence, $\max\{|m|,|n|\} = 1$, so that either $|m| = 1$ or $|n| = 1$.

3.37 The units in $\mathcal{O}$ are precisely the $x \in K^\times$ satisfying both $|x| \leq 1$ and $|x^{-1}| \leq 1$. As $|x^{-1}| = |x|^{-1}$, the last two inequalities are satisfied simultaneously precisely when $|x| = 1$.

Let M be the collection of nonunits in $\mathcal{O}$, so that $M = \mathbf{D}_{<1}(0)$. Clearly $0 \in M$. If $x, y \in M$, then $|x+y| \leq \max\{|x|,|y|\} < 1$, and so $x + y \in M$. Moreover, if $x \in M$ and $r \in \mathcal{O}$, then $|rx| = |r||x| \leq |x| < 1$, so that $rx \in M$. Hence, M is an ideal of $\mathcal{O}$. Since $1 \notin M$, the ideal M is proper.

Let I be any proper ideal of $\mathcal{O}$. If $x \in I$, then x cannot be a unit in $\mathcal{O}$: Otherwise $I \supseteq x\mathcal{O} = \mathcal{O}$. Thus, $x \in M$. Since this holds for all $x \in I$, we conclude that $I \subseteq M$.

Thus, M is a proper ideal of $\mathcal{O}$ containing all proper ideals of $\mathcal{O}$. So M cannot itself be properly contained in a proper ideal of $\mathcal{O}$; that is, M is maximal.

3.38 Each nonzero $x \in \mathbf{Z}_{(p)}$ has the form $\frac{a}{b}$ where $a, b \in \mathbf{Z}$ and $p \nmid b$. If we factor $a = p^{v_p(a)}a'$, then $x = p^{v_p(a)}\frac{a'}{b}$. Here $v_p(a) \geq 0$ and $\frac{a'}{b} \in \mathbf{Z}_{(p)}^\times$. So we have at least one decomposition of the desired form.

Uniqueness is easy: Suppose $x = p^v u = p^{v'}u'$ with v, v' nonnegative integers and $u, u' \in \mathbf{Z}_{(p)}^\times$. Then $|u|_p = |u'|_p = 1$, so that $p^{-v} = |x|_p = p^{-v'}$. Hence, $v = v'$. But then $p^v u = p^v u'$, and $u = u'$.

3.39 Let I be any nonzero ideal of $\mathbf{Z}_{(p)}$ and choose a nonzero $x \in I$ with $v_p(x)$ minimal among nonzero elements of I. Set $v = v_p(x)$.

Claim: $I = p^v\mathbf{Z}_{(p)}$.

Since $x = p^v u$ for some $u \in \mathbf{Z}_{(p)}^\times$, it is immediate that $I \supseteq x\mathbf{Z}_{(p)} = p^v u\mathbf{Z}_{(p)} = p^v\mathbf{Z}_{(p)}$. To prove the reverse containment, we take an arbitrary $y \in I$ and show that $y \in p^v\mathbf{Z}_{(p)}$. Clearly $y = 0$ belongs to $p^v\mathbf{Z}_{(p)}$. If $y \neq 0$, write $y = p^{v_p(y)}w$ where $w \in \mathbf{Z}_{(p)}^\times$. Then $v_p(y) \geq v$, and $y = p^v(p^{v_p(y)-v}w) \in p^v\mathbf{Z}_{(p)}$, finishing the proof of the Claim.

It follows that $\mathbf{Z}_{(p)}$ is a principal ideal domain (PID), with each of its ideals somewhere in the infinite chain

$$(0) \subsetneq \cdots \subsetneq p^n\mathbf{Z}_{(p)} \subsetneq \cdots \subsetneq p^3\mathbf{Z}_{(p)} \subsetneq p^2\mathbf{Z}_{(p)} \subsetneq p\mathbf{Z}_{(p)} \subsetneq \mathbf{Z}_{(p)}.$$

(The containments are strict since p is a nonzero, nonunit element of the domain $\mathbf{Z}_{(p)}$.) It is clear from this linear ordering that $p\mathbf{Z}_{(p)}$ is the unique maximal ideal of $\mathbf{Z}_{(p)}$.*

* We could also have proved that $p\mathbf{Z}_{(p)}$ is the unique maximal ideal of $\mathbf{Z}_{(p)}$ by invoking Problem 3.37: $p\mathbf{Z}_{(p)} = \{x \in \mathbf{Z}_{(p)} : |x|_p < 1\}$.

3.40 Since $x^2 + 7 = 2^m$, the integer x must be odd. Hence, $8 \mid x^2 + 7 = 2^m$ and $m \geq 3$.

Since x is an odd number, $\frac{x \pm \sqrt{-7}}{2} \in R$ for both choices of sign. Furthermore, recalling that $\alpha = \frac{1+\sqrt{-7}}{2}$ and $\beta = \frac{1-\sqrt{-7}}{2}$,

$$\begin{aligned} \frac{x + \sqrt{-7}}{2} \cdot \frac{x - \sqrt{-7}}{2} = 2^{m-2} &= (\alpha\beta)^{m-2} \\ &= \alpha^{m-2} \cdot \beta^{m-2}. \end{aligned} \tag{*}$$

We proceed by analyzing prime factorizations. First we show that α and β are prime in R. Since $R = \mathbf{Z}[\alpha]$, it is plain that every residue class mod αR has a representative from $\mathbf{Z}$. In fact, since $2 = \alpha\beta = 0$ in $R/\alpha R$, every class mod αR is represented by 0 or 1. If every class is represented by 0, then $R = \alpha R$, forcing α to be a unit and contradicting that $R^\times = \{\pm 1\}$. So $R/\alpha R$ is (isomorphic to) $\mathbf{Z}/2$. Since $\mathbf{Z}/2$ is a domain, αR is a prime ideal of R, and α is a prime element of R. An identical argument shows that β is prime in R.

Continuing, we argue that neither α nor β is a common divisor of the left-hand factors in (*). If α is common divisor, then $\alpha \mid \frac{x+\sqrt{-7}}{2} - \frac{x-\sqrt{-7}}{2} = \sqrt{-7}$. But $\sqrt{-7} = 2\alpha - 1 = -1$ in $R/\alpha R$, rather than 0. A similar argument shows that β is not a common divisor.

The two left-hand factors in (*) are nonunits. By unique factorization, each is a (nonempty) product of the primes α and β (up to units). We also know, from our work in the last paragraph, that α appears in the prime factorization of only one of $\frac{x+\sqrt{-7}}{2}$ and $\frac{x-\sqrt{-7}}{2}$, and similarly for β.

How can this be? $\frac{x+\sqrt{-7}}{2}$ and $\frac{x-\sqrt{-7}}{2}$ must match up with α^{m-2} and β^{m-2}, up to order and associates. That is, for some $\epsilon = \pm 1$ and some units η, η' of R,

$$\frac{x + \epsilon\sqrt{-7}}{2} = \eta\alpha^{m-2}, \quad \frac{x - \epsilon\sqrt{-7}}{2} = \eta'\beta^{m-2}.$$

Multiplying the last two equations, $x^2 + 7 = \eta\eta' 2^{m-2}$, and so $\eta\eta' = 1$. Since $\eta, \eta' \in \{-1, 1\}$, in fact $\eta = \eta'$, and

$$\eta(\alpha^{m-2} - \beta^{m-2}) = \frac{x + \epsilon\sqrt{-7}}{2} - \frac{x - \epsilon\sqrt{-7}}{2} = \epsilon\sqrt{-7} = \epsilon(\alpha - \beta).$$

Therefore,

$$u_{m-2} = \frac{\alpha^{m-2} - \beta^{m-2}}{\alpha - \beta} = \epsilon\eta^{-1} \in \{\pm 1\}.$$

The converse also holds: Every m with $u_{m-2} = \pm 1$ gives rise to an x with $x^2 + 7 = 2^m$. If $u_{m-2} = \pm 1$, then $\alpha^{m-2} - \beta^{m-2} = \pm(\alpha - \beta) = \pm\sqrt{-7}$. On the other

hand, if we write $\alpha^{m-2} = \frac{x+y\sqrt{-7}}{2}$ for integers x and y, then (applying complex conjugation) $\beta^{m-2} = \frac{x-y\sqrt{-7}}{2}$, so that $\alpha^{m-2} - \beta^{m-2} = y\sqrt{-7}$. Comparing expressions, $y = \pm 1$. Therefore, $2^{m-2} = \alpha^{m-2}\beta^{m-2} = \frac{x^2+7y^2}{4} = \frac{x^2+7}{4}$, and $x^2 + 7 = 2^m$.

Remarks.

(i) We didn't need to know R was a UFD to execute our solution. After proving that α and β are prime, we could have appealed to the following result, valid in *every* integral domain: If a product UV factors as $\pi_1 \cdots \pi_k$, with all π_i prime*, then $U = \eta \prod_{i\in S} \pi_i$ and $V = \eta' \prod_{i\in S'} \pi_i$ for some units η, η' and some partition of $\{1, 2, \ldots, k\}$ into sets S and S'. (We allow S or S' to be empty.) Try to prove this if you haven't seen it before!

(ii) For completeness, we include a proof that $R^\times = \{\pm 1\}$. It is obvious that $\pm 1 \in R^\times$. What requires proof is that ± 1 are the *only* elements of $R^\times$.
For each $\mu \in R$, we define the norm of μ by $\mathrm{N}\mu = \mu\bar{\mu}$, where the bar denotes complex conjugation. Thus, if $\mu = \frac{1}{2}(a+b\sqrt{-7})$, then $\mathrm{N}\mu = \frac{1}{4}(a^2+7b^2)$. Recalling that $a \equiv b \pmod 2$, we deduce that (a) $\mathrm{N}\mu$ is a nonnegative integer for every $\mu \in R$, with $\mathrm{N}\mu = 0$ only when $\mu = 0$. Furthermore, (b) for every $\mu, \nu \in R$, $\mathrm{N}(\mu\nu) = \mu\nu \cdot \overline{\mu\nu} = \mu\bar{\mu} \cdot \nu\bar{\nu} = \mathrm{N}\mu \cdot \mathrm{N}\nu$.
Suppose ε is a unit in R with inverse ε'. Using (b), $1 = \mathrm{N}(1) = \mathrm{N}(\varepsilon\varepsilon') = \mathrm{N}\varepsilon \cdot \mathrm{N}\varepsilon'$. From (a), $\mathrm{N}\varepsilon = \mathrm{N}\varepsilon' = 1$. Writing $\varepsilon = \frac{1}{2}(e + f\sqrt{-7})$, the equation $\mathrm{N}\varepsilon = 1$ translates into $e^2 + 7f^2 = 4$. This forces $f = 0$ and $e = \pm 2$, so that $\varepsilon = \frac{1}{2}(\pm 2 + 0\sqrt{-7}) = \pm 1$.

References

1. E. B. Burger and T. Struppeck, *Does* $\sum_{n=0}^{\infty} \frac{1}{n!}$ *really converge? Infinite series and p-adic analysis.* Amer. Math. Monthly **103** (1996), 565–577.

* we really do mean *prime*, not merely irreducible!

Solutions to Set #4

4.41 We have $1 + \mathrm{e}^T + \mathrm{e}^{2T} + \cdots + \mathrm{e}^{(n-1)T} = \sum_{0\le j<n}\sum_{k\ge 0}\frac{(jT)^k}{k!} = \sum_{k\ge 0}\left(\sum_{0\le j<n} j^k\right)\frac{T^k}{k!} = \sum_{k\ge 0} S_k(n)\frac{T^k}{k!}$.

4.42 Summing the finite geometric series,

$$\sum_{0\le j<n} \mathrm{e}^{jT} = \sum_{0\le j<n} (\mathrm{e}^T)^j = \frac{\mathrm{e}^{nT}-1}{\mathrm{e}^T-1} = \frac{\mathrm{e}^{nT}-1}{T}\cdot\frac{T}{\mathrm{e}^T-1}.$$

Therefore, by Problem 4.41,

$$\begin{aligned}\sum_{k\ge 0} S_k(n)\frac{T^k}{k!} &= \frac{\mathrm{e}^{nT}-1}{T}\cdot\frac{T}{\mathrm{e}^T-1}\\ &= \left(\sum_{r\ge 0}\frac{n^{r+1}T^r}{(r+1)!}\right)\left(\sum_{s\ge 0} B_s\frac{T^s}{s!}\right)\\ &= \sum_{k\ge 0}\frac{T^k}{k!}\sum_{\substack{r+s=k\\ r,s\ge 0}} B_s\frac{(r+s)!}{(r+1)!s!}n^{r+1}.\end{aligned}$$

Comparing coefficients of $\frac{T^k}{k!}$ gives

$$S_k(n) = \sum_{\substack{r+s=k\\ r,s\ge 0}} B_s\frac{(r+s)!}{(r+1)!s!}n^{r+1} = \sum_{0\le r\le k}\frac{B_{k-r}}{r+1}\binom{k}{r}n^{r+1}.$$

Remark. If you stare carefully, you will notice this argument takes for granted the identities $\mathrm{e}^{jT} = (\mathrm{e}^T)^j$ (for $j = 0, 1, 2, 3\ldots$). Here what is important is not that these identities hold for real numbers T (which is familiar from calculus), but that they hold as identities of formal power series in the indeterminate T.

To effect a proof, write

$$(\mathrm{e}^T)^j = \sum_{k_1,\ldots,k_j\ge 0}\frac{1}{k_1!\cdots k_j!}T^{k_1+\cdots+k_j} = \sum_{k\ge 0}\frac{T^k}{k!}\sum_{k_1+\cdots+k_j=k}\binom{k}{k_1,k_2,\ldots,k_j}.$$

By the multinomial theorem, $\sum_{k_1+\cdots+k_j=k} \binom{k}{k_1,k_2,\ldots,k_j} = j^k$. Therefore, $(\mathrm{e}^T)^j = \sum_{k\geq 0} \frac{(jT)^k}{k!} = \mathrm{e}^{jT}$.

We could also have proved the required identities by leveraging our prior knowledge of the "real world." Expand (formally) $\mathrm{e}^{jT} - (\mathrm{e}^T)^j = \sum_{k\geq 0} c_k T^k$ for some coefficients c_k. The exact same transformations you use to put the left side into the form of the right will show that

$$(\mathrm{e}^x)^j - \mathrm{e}^{jx} = \sum_{k\geq 0} c_k x^k \quad \text{for all } \underline{\text{real}} \text{ numbers } x.$$

Here all manipulations with real numbers can be justified by citing absolute convergence of the relevant series. (Operations on formal power series are *defined* to mirror operations that can be performed on numerical series in the presence of sufficiently good convergence.) Since $(\mathrm{e}^x)^j - \mathrm{e}^{jx} = 0$ for all real numbers x, the series $\sum_{k\geq 0} c_k x^k$ converges everywhere to 0. This forces each $c_k = 0$, which in turn shows that $\mathrm{e}^{jT} = (\mathrm{e}^T)^j$ formally. While gratuitous in this instance, the principle that an identity of real numbers can (often) be transmogrified into an identity of formal power series is frequently useful.

4.43 All of the claimed equalities are straightforward to verify, including the invariance of $T\coth T$ under the substitution $T \mapsto -T$ (provided we accept that $\mathrm{e}^{2T}\mathrm{e}^{-2T} = 1$, which can be proved by the method of the preceding Remark). Writing down the power series for $-T\coth(-T)$ and $T\coth(T)$, we conclude that

$$-T + \sum_{k\geq 0} B_k \frac{(-2T)^k}{k!} = T + \sum_{k\geq 0} B_k \frac{(2T)^k}{k!}.$$

When k is odd and larger than 1, comparing coefficients of T^k on both sides shows that $B_k = 0$. When $k = 1$, the same reasoning gives $-1 - 2B_1 = 1 + 2B_1$, leading to $B_1 = -\frac{1}{2}$ (as asserted in our table).

4.44 Starting from $T\coth T = T + \sum_{k\geq 0} B_k \frac{(2T)^k}{k!}$, divide by T and substitute $B_0 = 1$, $B_1 = -\frac{1}{2}$ and $B_k = 0$ for odd $k > 1$. This provides the expansion claimed for $\coth T$. That $\frac{\mathrm{d}}{\mathrm{d}T}\coth T = 1 - \coth^2 T$ can be checked directly.

To ease notation, write

$$\coth T = \frac{1}{T} + \sum_{k\geq 1} c_k T^{2k-1}.$$

As c_k and B_{2k} share the same sign, we will be done if we show that $(-1)^{k+1}c_k > 0$ for each $k \in \mathbf{Z}^+$. Assuming this claim fails, let K be the minimal counterexample. For later use, note that $K > 1$ (since $c_1 = 2B_2 = \frac{1}{3} > 0$). Differentiating the last displayed equation,

$$\frac{\mathrm{d}}{\mathrm{d}T}\coth T = -\frac{1}{T^2} + \sum_{k\geq 1}(2k-1)c_k T^{2k-2}.$$

The right-hand Laurent series has T^{2K-2} appearing with coefficient $(2K-1)c_K$. On the other hand, the coefficient of T^{2K-2} in $\frac{\mathrm{d}}{\mathrm{d}T}\coth T$ is the same as its coefficient in $-\coth^2 T$, since $\frac{\mathrm{d}}{\mathrm{d}T}\coth T = 1 - \coth^2 T$ and $K > 1$. That coefficient is $-(2c_K + \sum_{i+j=K,\ i,j\geq 1} c_i c_j)$. Therefore, $(2K+1)c_K = -\sum_{i+j=K,\ i,j\geq 1} c_i c_j$, and

$$(-1)^{K+1}c_K = \frac{(-1)^K}{2K+1}\sum_{\substack{i+j=K\\ i,j\geq 1}} c_i c_j = \frac{1}{2K+1}\sum_{\substack{i+j=K\\ i,j\geq 1}} (-1)^{i+1}c_i \cdot (-1)^{j+1}c_j > 0.$$

We use in the last step that $(-1)^{i+1}c_i > 0$ and $(-1)^{j+1}c_j > 0$, since i and j are positive integers smaller than K.

Remark. A more satisfying explanation for why the even-indexed Bernoulli numbers alternate in sign is found in Euler's formula

$$B_{2k} = (-1)^{k+1}2\zeta(2k)\cdot\frac{(2m)!}{(2\pi)^{2m}},$$

where $\zeta(s) := \sum_{n\geq 1}\frac{1}{n^s}$ is the Euler–Riemann zeta function. This remarkable relation pins down B_{2k} rather precisely as a real number. Indeed, when conjoined to Stirling's estimate on factorials, it implies that

$$\lim_{k\to\infty}\frac{|B_{2k}|}{4\sqrt{\pi k}(\frac{k}{\pi \mathrm{e}})^{2k}} = 1.$$

Unfortunately, Euler's formula does not contain any obvious information about the *number-theoretic* properties of B_{2k}.

We will not prove Euler's result here. Interested readers are referred to the exquisitely written textbook of Ireland and Rosen for a characteristically elegant treatment [2, pp. 231–232].

4.45 Information on the first ten partial sums is collected below.

n	$\sum_{1\leq k\leq n} 2^k/k$
1	2
2	2^2
3	$2^2\cdot 5/3$
4	$2^2\cdot 8/3$
5	$2^8\cdot 1/15$
6	$2^5\cdot 13/15$
7	$2^5\cdot 151/105$
8	$2^{13}\cdot 1/105$
9	$2^9\cdot 83/315$
10	$2^{10}\cdot 73/315$

Already this limited data suggests that $v_2(\sum_{1\le k\le n} 2^k/k)$ tends to infinity with n (equivalently, that $\sum_{k=1}^{\infty} 2^k/k = 0$ in $(\mathbf{Q}, |\cdot|_2)$). Being a bit bolder, we might conjecture that $v_2(\sum_{1\le k\le n} 2^k/k)$ is bounded below by a function ever-so-slightly smaller than n. For the resolution of both conjectures, see the solution to Problem 11.130.

4.46 We need the following lemma.

Lemma. For each $x \in \mathbf{Z}_{(p)}$, there is a $d \in \{0, 1, 2, \ldots, p-1\}$ with $x - d \in p\mathbf{Z}_{(p)}$.

Proof. Write $x = a/b$ where $a, b \in \mathbf{Z}$ and $p \nmid b$. Choose $B \in \mathbf{Z}$ with $Bb \equiv 1 \pmod p$, and select $d \in \{0, 1, \ldots, p-1\}$ with $d \equiv aB \pmod p$. Then $db \equiv aBb \equiv a \pmod p$, and $x - d = p\frac{(a-db)/p}{b} \in p\mathbf{Z}_{(p)}$. ∎

With the lemma in hand, we can express r in the desired form by the algorithm of Problems 3.32 and 3.33. Specifically, let $x_0 = r$, and for $n = 0, 1, 2, 3, \ldots$, select $d_n \in \{0, 1, 2, \ldots, p-1\}$ so that $x_n = d_n + px_{n+1}$ for some $x_{n+1} \in \mathbf{Z}_{(p)}$. Then $r = \sum_{k\ge 0} d_k p^k$.

Having shown existence we turn to uniqueness. Suppose $r = \sum_{k\ge 0} d_k p^k = \sum_{k\ge 0} d'_k p^k$ with all $d_k, d'_k \in \{0, 1, \ldots, p-1\}$. Assume $\{d_k\}$ and $\{d'_k\}$ do not coincide, and let k_0 be the smallest nonnegative integer with $d_{k_0} \ne d'_{k_0}$. Then $0 = r - r' = \sum_{k\ge k_0}(d_k - d'_k)p^k$, and

$$(d'_{k_0} - d_{k_0})p^{k_0} = \sum_{k>k_0} (d_k - d'_k)p^k.$$

So if we set $s_n = \sum_{k_0<k\le n}(d_k - d'_k)p^k$, then $s_n \to (d'_{k_0} - d_{k_0})p^{k_0}$ in $(\mathbf{Q}, |\cdot|_p)$. That is,

$$|s_n - (d'_{k_0} - d_{k_0})p^{k_0}|_p \to 0. \qquad (*)$$

However, $|s_n|_p \le \max_{k_0<k\le n} |(d_k - d'_k)p^k|_p \le p^{-k_0-1}$, while $|(d'_{k_0} - d_{k_0})p^{k_0}|_p = p^{-k_0}$. So by "survival of the greatest,"

$$|s_n - (d'_{k_0} - d_{k_0})p^{k_0}|_p = p^{-k_0}$$

for every $n > k_0$, contradicting (*).

Finally we prove $\{d_k\}$ is eventually periodic. It suffices to show that in the algorithm of Problems 3.32 and 3.33, there will always be nonnegative integers $m < n$ with $x_m = x_n$. In that case $\{d_k\}$ repeats, from $k = m$ onwards, with (not necessarily minimal) period $n - m$.

Write $r = a/b$ where $p \nmid b$. We will base our proof on two claims:

(a) each $x_n \in \frac{1}{b}\mathbf{Z}$,

(b) each $|x_n|_\infty \le M$, where $M := \max\{2, |r|_\infty\}$.

Claim (a) is obvious when $n = 0$, since $x_0 = r = a/b$. Suppose that $x_n \in \frac{1}{b}\mathbf{Z}$. Then $bpx_{n+1} = bx_n - bd_n \in \mathbf{Z}$. As $x_{n+1} \in \mathbf{Z}_{(p)}$, we also have $|bpx_{n+1}|_p = |bp|_p|x_{n+1}|_p \le p^{-1}$. So in fact $bpx_{n+1} \in p\mathbf{Z}$, and $x_{n+1} \in \frac{1}{bp}(p\mathbf{Z}) = \frac{1}{b}\mathbf{Z}$. This gives (a). Since $x_0 = r$, (b) is trivial when $n = 0$. If $|x_n|_\infty \le M$, then

$$|x_{n+1}|_\infty = \frac{1}{p}|x_n - d_n|_\infty < \frac{1}{p}(|x_n|_\infty + p) \le \frac{1}{2}|x_n|_\infty + 1 \le \frac{1}{2}M + 1 \le M.$$

So we have (b) as well. From (a) and (b) it is easy to conclude: $[-M, M]$ has finite intersection with $\frac{1}{b}\mathbf{Z}$, so the x_n cannot all be distinct.

4.47 Observe that

$$|x_n| - |x_n - x| \le |x_n - (x_n - x)| = |x| = |x_n + (x - x_n)| \le |x_n| + |x - x_n|.$$

Hence,

$$-|x - x_n| \le |x| - |x_n| \le |x - x_n|.$$

Since $|x_n - x| \to 0$, the squeeze theorem implies that $|x| - |x_n| \to 0$. Therefore, $|x_n|$ converges to $|x|$.

Suppose now that $|\cdot|$ is non-Archimedean and that $x_n \to x$, where $x \ne 0$. The limit definition guarantees that $|x_n - x| < |x|$ for all sufficiently large n. For these n, "survival of the greatest" yields $|x_n| = |(x_n - x) + x| = |x|$.

4.48 By Problem 3.34 we can choose a prime p with $|p| < 1$. Then whenever n is an integer not divisible by p, the integers p and n are relatively prime and Problem 3.35 tells us that $|n|_p = 1$.

Write $|p| = p^{-c}$ with $c > 0$. Given $x \in \mathbf{Q}^\times$, we can express $x = p^{v_p(x)}a/b$ where a and b are integers not divisible by p. Then

$$|x| = |p|^{v_p(x)}|a||b|^{-1} = |p|^{v_p(x)} = p^{-cv_p(x)} = (p^{-v_p(x)})^c = |x|_p^c.$$

Of course, we also have $|0| = 0 = |0|_p^c$. So $|\cdot| = |\cdot|_p^c$.

4.49 From Exercise 4.45, $|r| > 1$ for each integer $r \ge 2$. So there are indeed real numbers $c, d > 0$ with $|2| = 2^c$ and $|3| = 3^d$.

If we write $2^n = \sum_{i=0}^m \epsilon_i 3^i$, with each $\epsilon_i \in \{0, 1, 2\}$ and $\epsilon_m > 0$, then

$$\begin{aligned} 2^{cn} = |2|^n = |2^n| &\le \sum_{i=0}^m |\epsilon_i||3|^i \le \max\{|1|, |2|\}\frac{|3|^{m+1} - 1}{|3| - 1} \\ &\le \frac{\max\{|1|, |2|\}|3|}{|3| - 1} \cdot |3|^m = \frac{|2| \cdot |3|}{|3| - 1}3^{dm}, \end{aligned}$$

proving the claimed inequality with $B := \frac{|2|\cdot|3|}{|3|-1}$. As $\epsilon_m > 0$, we have $2^n \geq 3^m$, and thus $3^{dm} \leq 2^{dn}$. Therefore, $2^{cn} \leq B \cdot 2^{dn}$, and $2^{(c-d)n} \leq B$. Since n may be taken arbitrarily large, it follows that $c \leq d$.

We could have run the argument with the roles of 2 and 3 reversed. Writing 3^n in base 2 and reasoning analogously would lead to the inequality $3^{dn} \leq B' 3^{cn}$, where $B' = \frac{|2|}{|2|-1}$. We would then conclude that $d \leq c$. Thus, $c = d$.

4.50 The arguments of Problem 4.49 apply equally well with 3 replaced by an arbitrary integer $r \geq 3$. Writing $|2| = 2^c$ and $|r| = r^d$, we find that for each positive integer n,

$$2^{cn} \leq B \cdot 2^{dn} \quad \text{while} \quad r^{dn} \leq B' \cdot r^{cn}$$

for the constants $B = \frac{\max\{|2|,\ldots,|r-1|\}|r|}{|r|-1}$ and $B' = \frac{|2|}{|2|-1}$. These two inequalities imply $c \leq d$ and $d \leq c$ (respectively), yielding $c = d$.

It follows that $|r| = r^c$ for every integer $r > 1$. That equality holds trivially when $r = 1$, and so $|\cdot| = |\cdot|^c$ on all of $\mathbf{Z}^+$. Writing each $x \in \mathbf{Q}^\times$ in the form $x = \pm\frac{a}{b}$ where $a, b \in \mathbf{Z}^+$, we deduce that

$$|x| = |a| \cdot |b|^{-1} = a^c b^{-c} = (ab^{-1})^c = |x|_\infty^c.$$

Of course $|0| = 0 = |0|_\infty^c$ as well, and so $|\cdot| = |\cdot|_\infty^c$.

Extra Exploration 8. For which positive real numbers c is $|\cdot|_\infty^c$ an absolute value on $\mathbf{Q}$? Now let p be prime. For which positive real numbers c is $|\cdot|_p^c$ an absolute value on $\mathbf{Q}$?

4.51 We begin with a simple but useful observation: If $(K, |\cdot|)$ is any valued field, and $x \in K$, then

$$x^n \to 0 \text{ in } K \iff |x^n - 0| \to 0 \text{ in } \mathbf{R} \iff |x| < 1.$$

Now suppose for a contradiction that $|\cdot|$ and $|\cdot|'$ are equivalent absolute values on K with $|\cdot|$ Archimedean and $|\cdot|'$ non-Archimedean. By Problem 3.34, $|2| > 1$, and so $|\frac{1}{2}| < 1$. Hence, $(\frac{1}{2})^n \to 0$ in $(K, |\cdot|)$. Since $|\cdot|$ and $|\cdot|'$ are equivalent, $(\frac{1}{2})^n \to 0$ in $(K, |\cdot|')$ as well, so that $|\frac{1}{2}|' < 1$. But then $|2|' > 1$, contradicting that $|2|' = |1+1|' \leq \max\{|1|', |1|'\} = 1$.

4.52 Let $|\cdot|$ be a nontrivial absolute value on $\mathbf{Q}$. If $|\cdot|$ is Archimedean, then $|\cdot| = |\cdot|_\infty^c$ for some $c > 0$ (Problem 4.50). In this case, $|\cdot|$ is equivalent to $|\cdot|_\infty$, since

$$\begin{aligned} x_n \to x \text{ in } (\mathbf{Q}, |\cdot|) &\iff |x_n - x| \to 0 \\ &\iff |x_n - x|_\infty \to 0 \iff x_n \to x \text{ in } (\mathbf{Q}, |\cdot|_\infty). \end{aligned}$$

If $|\cdot|$ is non-Archimedean, then $|\cdot| = |\cdot|_p^c$ for some prime p and some $c > 0$. In this case $|\cdot|$ is equivalent to $|\cdot|_p$ (same reasoning as displayed above).

It remains to show that none of $|\cdot|_\infty, |\cdot|_2, |\cdot|_3, |\cdot|_5 \ldots$ are equivalent. From Exercise 4.51, $|\cdot|_\infty$ is not equivalent to any of the others, since $|\cdot|_\infty$ is Archimedean while $|\cdot|_p$ is non-Archimedean. If p and q are distinct primes, then $p^n \to 0$ in $(\mathbf{Q}, |\cdot|_p)$ but $p^n \not\to 0$ in $(\mathbf{Q}, |\cdot|_q)$. So $|\cdot|_p$ and $|\cdot|_q$ are inequivalent.

Extra Exploration 9 (classifying absolute values on $\mathbf{F}_p(T)$). Fix a prime p, and let $\mathbf{\Pi}$ denote the collection of all monic irreducible polynomials $\pi \in \mathbf{F}_p[T]$. Let $|\cdot|$ be an absolute value on $\mathbf{F}_p(T)$.

(a) Suppose that $|T| > 1$. Prove that $|F| = |T|^{\deg a - \deg b}$ for all $F = \frac{a}{b} \in \mathbf{F}_p(T)^\times$.
(b) Now assume that $|T| \leq 1$. Prove that $|F| \leq 1$ for all $F \in \mathbf{F}_p[T]$. Assuming $|\cdot|$ is nontrivial, show that there is a unique $\pi \in \mathbf{\Pi}$ with $|\pi| < 1$. Furthermore, $|F| = |\pi|^{v_\pi(F)}$ for all $F \in \mathbf{F}_p(T)^\times$. (Recall that when $F = \pi^v \frac{a}{b}$ for $a, b \in \mathbf{F}_p[T]$ coprime to π, we are setting $v_\pi(F) := v$.)
(c) State and prove an $\mathbf{F}_p(T)$-analogue of the assertion in Problem 4.52.

4.53 NO. Suppose $x_0, \ldots, x_p$ are $p+1$ (distinct) equidistant rational numbers. Translating each by $-x_0$, we can assume $x_0 = 0$. Next, scaling the x_i by the same power of p, we can assume that each $x_i \in \mathbf{Z}_{(p)}$ and that at least one of them, say x_1, is not in $p\mathbf{Z}_{(p)}$. Then $|x_1 - x_0|_p = |x_1|_p = 1$.

Each of $x_1, \ldots, x_p$ is congruent modulo $p\mathbf{Z}_{(p)}$ to one of $0, 1, 2, 3, \ldots, p-1$ (see the solution to Problem 4.46). Since the x_i are equidistant from one another,

$$|x_j|_p = |x_j - x_0|_p = |x_1 - x_0|_p = 1$$

for all $j = 1, 2, \ldots, p$. Therefore, each of $x_1, \ldots, x_p$ is congruent to one of $1, 2, \ldots, p-1 \pmod{p\mathbf{Z}_{(p)}}$. But then two of $x_1, \ldots, x_p$, say x_i and x_j, coincide modulo $p\mathbf{Z}_{(p)}$ (Pigeonhole Principle). For these two,

$$|x_i - x_j|_p \leq \frac{1}{p} < 1 = |x_1 - x_0|_p.$$

Contradiction!

4.54 Notice that $H_n - \frac{1}{p}H_m = \sum_{1 \leq k \leq n} \frac{1}{k} - \sum_{1 \leq r \leq m} \frac{1}{pr} = \sum_{1 \leq k \leq n,\ p \nmid k} \frac{1}{k} \in \mathbf{Z}_{(p)}$. Hence, $|H_n - \frac{1}{p}H_m|_p \leq 1 \leq |H_m|_p < p|H_m|_p = |\frac{1}{p}H_m|_p$. Now "survival of the greatest" gives us

$$|H_n|_p = \left|\frac{1}{p}H_m + \left(H_n - \frac{1}{p}H_m\right)\right|_p = \left|\frac{1}{p}H_m\right|_p = p|H_m|_p$$

4.55 Let p be a prime. Suppose we happen to have in hand a nonnegative integer k with $|H_m|_p \geq 1$ for all m in the range $p^k \leq m < p^{k+1}$. Problem 4.54

allows us to conclude that $|H_n|_p \geq p$ whenever $p^{k+1} \leq n < p^{k+2}$. Repeating the reasoning, $|H_n|_p \geq p^2$ whenever $p^{k+2} \leq n < p^{k+3}$. In general, $|H_n|_p \geq p^j$ for all $n \geq p^{k+j}$ (for $j = 0, 1, 2, 3, \ldots$). Therefore, $|H_n|_p \to \infty$.

One can check with a simple computer program that $k = 2$ satisfies our hypothesis both when $p = 3$ and when $p = 5$. So $|H_n|_3 \to \infty$ and $|H_n|_5 \to \infty$.

Remark. For an in-depth examination of $|H_n|_p$, see [1].

Several open questions persist regarding the numerators and denominators of the harmonic numbers. Here is one that appears deceptively simple: Are there infinitely many n for which the denominator of H_n (in lowest terms) is the least common multiple of $1, 2, 3, \ldots, n$?

References

1. D. W. Boyd, *A p-adic study of the partial sums of the harmonic series*. Experiment. Math. **3** (1994), 287–302.
2. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

Solutions to Set #5

5.56 We check that $\mathbf{Z}_p$ contains the multiplicative identity $1 = (1 \bmod p, 1 \bmod p^2, 1 \bmod p^3, \dots)$ of the ambient ring $\prod_{k=1}^{\infty} \mathbf{Z}/p^k$ and that $\mathbf{Z}_p$ is closed under subtraction and multiplication. The first requirement is clear. To prove the second and third, suppose $x, y \in \mathbf{Z}_p$. Write $x = (a_1 \bmod p, a_2 \bmod p^2, \dots)$ and $y = (b_1 \bmod p, b_2 \bmod p^2, \dots)$, where $a_k \equiv a_{k+1} \pmod{p^k}$ and $b_k \equiv b_{k+1} \pmod{p^k}$ for all $k = 1, 2, 3, \dots$. Then $a_k - b_k \equiv a_{k+1} - b_{k+1} \pmod{p^k}$ and $a_k b_k \equiv a_{k+1} b_{k+1} \pmod{p^k}$, for all $k = 1, 2, 3, \dots$, These congruences imply that $x - y = (a_1 - b_1 \bmod p, a_2 - b_2 \bmod p^2, \dots)$ and $xy = (a_1 b_1 \bmod p, a_2 b_2 \bmod p^2, \dots)$ also belong to $\mathbf{Z}_p$, as desired.

5.57 Suppose $x = (a_1 \bmod p, a_2 \bmod p^2, \dots)$ and $y = (b_1 \bmod p, b_2 \bmod p^2, \dots)$ are nonzero elements of $\mathbf{Z}_p$. Since $x \neq 0$, there is an i for which $p^i \nmid a_i$. Similarly, there is a j for which $p^j \nmid b_j$. We will prove $xy \neq 0$ by showing that the mod p^{i+j} component of xy is nonzero, i.e., that $p^{i+j} \nmid a_{i+j} b_{i+j}$.

The compatibility condition in the definition of $\mathbf{Z}_p$ assures us that $a_{i+j} \equiv a_i \not\equiv 0 \pmod{p^i}$. Similarly, $b_{i+j} \equiv b_j \not\equiv 0 \pmod{p^j}$. Therefore,

$$v_p(a_{i+j} b_{i+j}) = v_p(a_{i+j}) + v_p(b_{i+j}) < i + j,$$

and $p^{i+j} \nmid a_{i+j} b_{i+j}$.

5.58 For each $n \in \mathbf{Z}^+$, the element $n \cdot 1$ of $\mathbf{Z}_p$ has a nonzero mod p^k component whenever $p^k > n$. In particular, $n \cdot 1 \neq 0$. Thus, $\mathbf{Z}_p$ has characteristic 0, so that we can (and henceforth will!) view $\mathbf{Z}$ as a subring of $\mathbf{Z}_p$, identifying each integer n with $n \cdot 1 = (n \bmod p, n \bmod p^2, n \bmod p^3, \dots)$.

The rest of the problem asks (essentially) for a description of $\mathbf{Q} \cap \mathbf{Z}_p$. It may not be clear that this task even makes sense: To take this intersection, both $\mathbf{Q}$ and $\mathbf{Z}_p$ have to be viewed as sitting inside a common superset. What is that set?

Fortunately, this question has an easy answer: Both $\mathbf{Q}$ and $\mathbf{Z}_p$ are contained in the fraction field of $\mathbf{Z}_p$. Taking this interpretation, if $a, b \in \mathbf{Z}$ with b nonzero,

$\frac{a}{b} \in \mathbf{Q} \cap \mathbf{Z}_p$ precisely when there is a $y \in \mathbf{Z}_p$ with $by = a$. When does this happen?

We can assume, without loss of generality, that $\gcd(a, b) = 1$. If $p \mid b$, there is no hope of finding a y with $by = a$: The mod p component of by is 0 for every $y \in \mathbf{Z}_p$, while the mod p component of a is nonzero (remember that $\gcd(a, b) = 1$, so that p cannot divide a). Suppose instead that $p \nmid b$. In this case, we can choose integers B_k with $bB_k \equiv 1 \pmod{p^k}$, for $k = 1, 2, 3, \ldots$. Observing that $bB_{k+1} \equiv 1 \pmod{p^{k+1}}$, we find that

$$bB_{k+1} \equiv 1 \equiv bB_k \pmod{p^k}, \quad \text{and thus} \quad B_{k+1} \equiv B_k \pmod{p^k}.$$

Therefore $y_0 := (B_1 \bmod p, B_2 \bmod p^2, B_3 \bmod p^3, \ldots) \in \mathbf{Z}_p$. Furthermore, $by_0 = (bB_1 \bmod p, bB_2 \bmod p^2, \ldots) = (1 \bmod p, 1 \bmod p^2, \ldots) = 1$, so that $y = ay_0$ satisfies $by = a$.

We conclude that $\mathbf{Q} \cap \mathbf{Z}_p$ is the set of rational numbers whose denominators, in lowest terms, are not multiples of p. This is precisely our faithful and familiar companion $\mathbf{Z}_{(p)}$. (Incidentally, this explains the term p-integral for elements of $\mathbf{Z}_{(p)}$; the p-integral rationals are the rational numbers that are also p-adic integers.)

As for the final question: Yes, $(4 \bmod 5, 34 \bmod 5^2, 334 \bmod 5^3, \ldots) \in \mathbf{Q} \cap \mathbf{Z}_5$. In fact, $3 \cdot (4 \bmod 5, 34 \bmod 5^2, 334 \bmod 5^3, \ldots) = (12 \bmod 5, 102 \bmod 5^2, 1002 \bmod 5^3, \ldots) = (2 \bmod 5, 2 \bmod 5^2, 2 \bmod 5^3, \ldots) = 2$.

5.59 Let $u = (a_1 \bmod p, , a_2 \bmod p, \ldots) \in \mathbf{Z}_p$. If $u \in \mathbf{Z}_p^\times$ with inverse $v = (b_1 \bmod p, b_2 \bmod p^2, \ldots)$, then $uv = 1 = (1 \bmod p, 1 \bmod p^2, \ldots)$. Comparing mod p components, $a_1 b_1 \equiv 1 \pmod{p}$. Thus, a_1 is invertible mod p, which implies that $p \nmid a_1$.

Conversely, suppose that $p \nmid a_1$. Since each $a_k \equiv a_{k-1} \equiv \cdots \equiv a_1 \pmod{p}$, all of the a_k are coprime to p. Choose integers b_k with $a_k b_k \equiv 1 \pmod{p^k}$, for $k = 1, 2, 3, \ldots$. Working modulo p^{k+1},

$$a_{k+1} b_{k+1} \equiv 1 \equiv a_k b_k \equiv a_{k+1} b_k,$$

so that $b_{k+1} \equiv b_k \pmod{p^k}$. Hence, $v := (b_1 \bmod p, b_2 \bmod p^2, \ldots) \in \mathbf{Z}_p$. It is now straightforward to check that $uv = 1$, so that $u \in \mathbf{Z}_p^\times$ (with $v = u^{-1}$).

It remains to prove that $p \mid a_1$ (in $\mathbf{Z}$) $\iff p \mid u$ (in $\mathbf{Z}_p$). Suppose $p \mid u$ and write $u = pv$, where $v = (v_1 \bmod p, v_2 \bmod p^2, \ldots) \in \mathbf{Z}_p$. Then $a_1 \equiv pv_1 \equiv 0 \pmod{p}$, and $p \mid a_1$.

Conversely, suppose $p \mid a_1$. Since each $a_k \equiv a_1 \pmod{p}$, p divides every a_k. Put $v_k = a_{k+1}/p$ for $k = 1, 2, 3, \ldots$. Dividing the congruence $a_{k+2} \equiv a_{k+1} \pmod{p^{k+1}}$ through by p gives $v_{k+1} \equiv v_k \pmod{p^k}$, and so $v := (v_1 \bmod p, v_2 \bmod p^2, \ldots) \in \mathbf{Z}_p$. Moreover,

$$pv = (a_2 \bmod p, a_3 \bmod p^2, \dots) = (a_1 \bmod p, a_2 \bmod p^2, \dots) = u.$$

(We use here that $a_{k+1} \equiv a_k \pmod{p^k}$ for each k.) Thus, $p \mid u$.

5.60 Let $x = (a_1 \bmod p, a_2 \bmod p^2, \dots)$ be a nonzero element of $\mathbf{Z}_p$ and choose the nonnegative integer v minimally with $a_{v+1} \not\equiv 0 \pmod{p^{v+1}}$. For each integer $j > v$,

$$a_j \equiv a_{j-1} \equiv \cdots \equiv a_{v+1} \equiv 0 \pmod{p^v}.$$

(Consider two cases, $v = 0$ or $v > 0$.) So $b_k := p^{-v} a_{v+k} \in \mathbf{Z}$ for each $k = 1, 2, 3, \dots$. The congruences $a_{v+k+1} \equiv a_{v+k} \pmod{p^{v+k}}$ imply that $b_{k+1} \equiv b_k \pmod{p^k}$. Therefore, $u := (b_1 \bmod p, b_2 \bmod p^2, \dots) \in \mathbf{Z}_p$.

By the choice of v, we have that $p \nmid \frac{a_{v+1}}{p^v} = b_1$. Thus, $u \in \mathbf{Z}_p^\times$ (Exercise 5.59). Furthermore,

$$\begin{aligned} p^v u &= (0 \bmod p, \dots, 0 \bmod p^v, a_{2v+1} \bmod p^{v+1}, a_{2v+2} \bmod p^{v+2}, \dots) \\ &= (0 \bmod p, \dots, 0 \bmod p^v, a_{v+1} \bmod p^{v+1}, a_{v+2} \bmod p^{v+2}, \dots) = x. \end{aligned}$$

(Here we use that $a_{2v+i} \equiv a_{2v+i-1} \equiv \cdots \equiv a_{v+i} \pmod{p^{v+i}}$.) So we have produced a representation $x = p^v u$ with $u \in \mathbf{Z}_p^\times$.

To prove uniqueness, suppose $x = p^v u = p^{v'} u'$ with v, v' nonnegative integers and $u, u' \in \mathbf{Z}_{(p)}^\times$. Assume $v \le v'$. Canceling p^v from both sides, $u = p^{v'-v} u'$. Since $u \in \mathbf{Z}_p^\times$, to avoid a contradiction with Exercise 5.59 we must have $v' - v = 0$, i.e., $v = v'$. Then $p^v u = p^v u'$, leading to $u = u'$.

5.61 For each nonzero $x \in \mathbf{Z}_p$, define $v_p(x)$ as the integer v appearing in the representation of x described in Problem 5.60. Then proceed as in the solution to Problem 3.39.

5.62 We preface the solution with some philosophical comments. With the definition we have given of $\mathbf{Z}_p$, there is an obvious *informal* way to reduce x modulo powers of p: Write $x = (a_1 \bmod p, a_2 \bmod p^2, \dots)$ and reduce mod p^n by extracting the nth component, i.e., singling out $a_n \bmod p^n$. This defines the reduction of x mod p^n as an element of $\mathbf{Z}/p^n$. Since $\mathbf{Z}_p$ is a ring, there is also a *canonical* way to reduce x modulo p^n: Take the image of x in $\mathbf{Z}_p/p^n\mathbf{Z}_p$. It would be reassuring if these two ways of reducing mod p^n were somehow the same. As we will see shortly, this turns out to be the case! The isomorphism between $\mathbf{Z}/p^n$ and $\mathbf{Z}_p/p^n\mathbf{Z}_p$ induced by the inclusion $\mathbf{Z} \hookrightarrow \mathbf{Z}_p$ matches up $a_n \bmod p^n$ and $x \bmod p^n\mathbf{Z}_p$. Equivalently: $x \bmod p^n\mathbf{Z}_p = a_n \bmod p^n\mathbf{Z}_p$.

There is no justice in Heaven or Earth,
but there is certainly justice in
MATHEMATICS!

Paul Erdős

We proceed to the proof proper. Let ϕ denote the homomorphism from $\mathbf{Z}$ to $\mathbf{Z}_p/p^n\mathbf{Z}_p$ induced by the inclusion $\mathbf{Z} \hookrightarrow \mathbf{Z}_p$. We start by computing the kernel of ϕ. For $x \in \mathbf{Z}$,

$$x \in \ker(\phi) \iff x \in p^n\mathbf{Z}_p \iff x/p^n \in \mathbf{Z}_p \cap \mathbf{Q} \iff x/p^n \in \mathbf{Z}_{(p)} \iff x \in p^n\mathbf{Z}.$$

(Here we have recalled that $\mathbf{Q} \cap \mathbf{Z}_p = \mathbf{Z}_{(p)}$.) So $\ker(\phi) = p^n\mathbf{Z}$, and ϕ induces an embedding $\tilde{\phi}\colon \mathbf{Z}/p^n \hookrightarrow \mathbf{Z}_p/p^n\mathbf{Z}_p$.

Next we show that ϕ, and hence also $\tilde{\phi}$, is surjective. Let $x = (a_1 \bmod p, a_2 \bmod p^2, \dots) \in \mathbf{Z}_p$. The mod p^j-component of $a_n - x$ is $a_n - a_j \bmod p^j$, which vanishes for all $j \leq n$ (by the compatibility condition in the definition of $\mathbf{Z}_p$). So by our solution to Problem 5.60, either $a_n - x = 0$ or $a_n - x = p^k u$ for an integer $k \geq n$ and a unit $u \in \mathbf{Z}_p^\times$. In either case, $a_n - x \in p^n\mathbf{Z}_p$, so that $\phi(a_n) = a_n \bmod p^n\mathbf{Z}_p = x \bmod p^n\mathbf{Z}_p$. This proves ϕ is surjective, and so $\tilde{\phi}$ is an isomorphism.

The isomorphism $\tilde{\phi}$ carries $a_n \bmod p^n$ to $\phi(a_n) = x \bmod p^n\mathbf{Z}_p$, as we promised in our initial remarks.

5.63 Keeping in mind the Chinese Remainder Theorem, it is straightforward to check that $\mathbf{Z}_g \cong \prod_{p|g} \mathbf{Z}_{p^{v_p(g)}}$, via the map sending

$$(a_1 \bmod g, a_2 \bmod g^2, a_3 \bmod g^3, \dots) \mapsto ((a_1 \bmod p^{v_p(g)}, a_2 \bmod p^{2v_p(g)}, a_3 \bmod p^{3v_p(g)}, \dots))_{p|g}.$$

"Straightforward" means that the tedium of writing out the proof outweighs the enlightenment gained from doing so. (Please walk through the argument in your head and decide if you agree!)

To complete the problem, it suffices to show that if p is prime and $v \in \mathbf{Z}^+$, then $\mathbf{Z}_{p^v} \cong \mathbf{Z}_p$. Here we can map $(b_1 \bmod p^v, b_2 \bmod p^{2v}, b_3 \bmod p^{3v}, \dots)$ to $(b_1 \bmod p, \dots, b_1 \bmod p^v, b_2 \bmod p^{v+1}, \dots, b_2 \bmod p^{2v}, \dots)$, each b_i repeated v times. (Again, that this work is "straightforward." Verify!)

5.64 The outer, red disc represents the entirety of $\mathbf{Z}_3$. The salmon-colored discs partition $\mathbf{Z}_3$ into three parts, based on the mod 3 component. Once the mod 3 component is fixed, there are 3 possibilities for the mod 3^2 component, depicted by the green discs. Finally, having fixed the mod 3^2 component, there are three possibilities for the mod 3^3 component, illustrated by the purple

discs. In theory this partitioning process could continue indefinitely, but at some point our eyes would ask for a break!

5.65 Who am I to tell you how to appreciate art?

Remark. For further discussions around visualizing $\mathbf{Z}_p$, see [3], [9], [10, Chapter 2], and [11, Chapter 1, §2].

5.66 Let f be any function from $\mathbf{Z}^+$ to $\mathbf{Z}_p$. We will show f cannot be onto by adapting Cantor's famous diagonal argument. Choose a residue class $a_1 \bmod p$ different from the mod p component of $f(1)$. The class $a_1 \bmod p$ lifts to p residue class mod p^2; choose one, say $a_2 \bmod p^2$, different from the mod p^2 component of $f(2)$. This in turn lifts to p classes mod p^3; choose one, say $a_3 \bmod p^3$, different from the mod p^3 component of $f(3)$. Continue. At the end of the (very long) day, we find that $(a_1 \bmod p, a_2 \bmod p^2, a_3 \bmod p^3, \dots)$ is an element of $\mathbf{Z}_p$ that cannot belong to the image of f, since it has a different mod p^n component from $f(n)$ for each $n = 1, 2, 3, \dots$.

Extra Exploration 10. Show that $\mathbf{Z}_p$ has the same cardinality as $\mathbf{R}$. A useful tool for this kind of proof is the Cantor–Schröder–Bernstein theorem: *If there are injections from A to B and from B to A, then there is a bijection between A and B.*[*]

5.67 Let (x_r, y_r), (x_b, y_b), and (x_g, y_g) be the coordinates of the red, blue, and green vertices of Δ. Then, by a formula well-known to those who know it well,

$$2 \cdot \text{Area}(\Delta) = \pm \begin{vmatrix} x_b & y_b & 1 \\ x_g & y_g & 1 \\ x_r & y_r & 1 \end{vmatrix} = \pm(x_b y_g + x_r y_b + x_g y_r - x_g y_b - x_b y_r - x_r y_g).$$

We claim that $x_b y_g$ has 2-adic absolute value strictly larger than the other five terms. By definition of the coloring, $|x_b y_g|_2 = |x_b|_2 |y_g|_2 \geq 1 \cdot 1 = 1$. Next, we observe that

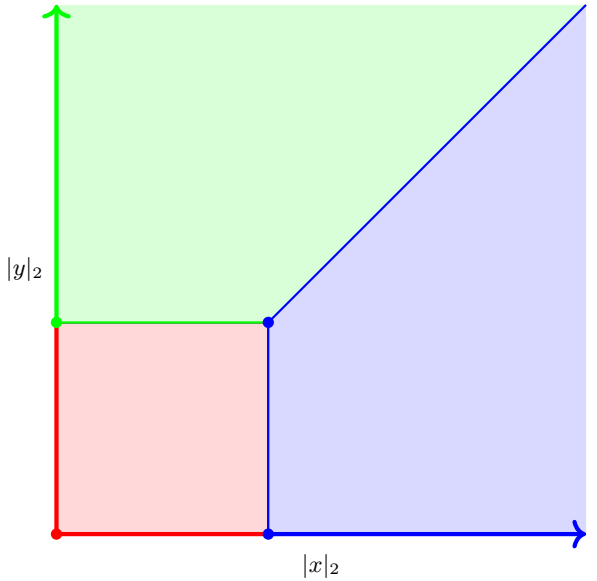
$$|x_r|_2 |y_b|_2 \leq |x_r|_2 |x_b|_2 < |x_b|_2 \leq |x_b|_2 |y_g|_2.$$

If $y_r = 0$, then $|x_g y_r|_2 = 0 < |x_b y_g|_2$; otherwise,

$$|x_g|_2 |y_r|_2 < |y_g|_2 |y_r|_2 < |y_g|_2 \leq |x_b|_2 |y_g|_2.$$

If $y_b = 0$, then $|x_g y_b|_2 = 0 < |x_b y_g|_2$; otherwise,

[*] The author cannot resist outlining Cox's straightforward-to-verify proof of the Cantor–Schröder–Bernstein result [2]. First, reduce to showing that if f is an injection from a set X to a subset $Y \subseteq X$, then there is a bijection between X and Y. To tackle this new claim, put $S = \bigcup_{n=0}^{\infty} f^{(n)}(X \setminus Y) = (X \setminus Y) \cup f(X \setminus Y) \cup f(f(X \setminus Y)) \cup \dots$. Define $g\colon X \to Y$ by letting $g(x) = f(x)$ for $x \in S$ and $g(x) = x$ for $x \notin S$. Argue directly that g is well-defined, injective, and surjective.



Coloring of $\mathbf{Q}^2$ in Problem 5.67.

$$|x_g|_2|y_b|_2 < |y_g|_2|y_b|_2 \leq |x_b|_2|y_g|_2.$$

Next,

$$|x_b|_2|y_r|_2 < |x_b|_2 \leq |x_b|_2|y_g|_2.$$

Finally,

$$|x_r|_2|y_g|_2 < |y_g|_2 \leq |x_b|_2|y_g|_2.$$

Phew!

Falling back on "survival of the greatest," we conclude that $|2 \cdot \text{Area}(\Delta)|_2 = |x_b y_g|_2 \geq 1$, so that $|\text{Area}(\Delta)|_2 \geq |2|_2^{-1} > 1$.

Remark. Here is a quick sketch of Monsky's proof. We can assume the square we are trying to dissect is $S = [0,1] \times [0,1] \subseteq \mathbf{R}^2$.

Color $\mathbf{Q}^2$ as described in Problem 5.67. A triangle with vertices from $\mathbf{Q}^2$ will be called a rainbow triangle if each vertex receives a different color.

Suppose S has been dissected into finitely many triangles. So that we can bring the coloring of $\mathbf{Q}^2$ into the picture, let's suppose that the vertices of all triangles appearing in the dissection have rational coordinates.

Using a version of Sperner's lemma from combinatorial geometry, along with basic properties of our coloring, Monsky argues that the dissection must contain an *odd* number of rainbow triangles. In particular, there is always at least one rainbow triangle Δ involved. As we showed above, $|\text{Area}(\Delta)|_2 > 1$. So if we assume there are

n triangles involved in the dissection, each with the same area, then $|1/n|_2 > 1$; that is, n is even.

This is all well and good, but we are interested in arbitrary (real) dissections of S, not merely "rational" ones. Well, here is the astounding part: The same argument applies in the general case! At first glance this claim doesn't seem to make sense: Our initial coloring was defined in terms of $|\cdot|_2$, and $|\cdot|_2$ has domain $\mathbf{Q}$, not $\mathbf{R}$. It turns out, however, that it is possible to extend $|\cdot|_2$ to an absolute value on $\mathbf{R}$. (This is far from obvious!) With this extension in hand, everything else in the argument goes through with zero change.

A complete proof of Monsky's theorem can be found in [1, Chapter 22]. The discussion in [1] sidesteps extending $|\cdot|_2$ to an absolute value on $\mathbf{R}$; the reader interested in seeing such an extension constructed can consult §14 of [12].

Extra Exploration 11 (cf. Hales and Straus [4]). Let K be an infinite field that can be endowed with a nontrivial, non-Archimedean absolute value. Show that it is possible to 3-color the affine plane K^2, using all three colors in an interesting way, so that every line receives points of at most two colors. In an interesting way means that each color is assigned to three non-collinear points. (If we remove "in an interesting way," this can be done for every infinite field. Can you see why?)

Extra Exploration 12 (Hensel's definition of the p-adic integers). Let $\phi\colon \mathbf{Z}[[T]] \to \prod_{k=1}^{\infty} \mathbf{Z}/p^k$ be the map sending $a_0 + a_1T + a_2T^2 + \dots$ to $(a_0 \bmod p, a_0 + a_1p \bmod p^2, a_0 + a_1p + a_2p^2 \bmod p^3, \dots)$. Here the kth component of the output is $a_0 + a_1p + \cdots + a_{k-1}p^{k-1} \bmod p^k$.

(a) Check that ϕ is a ring homomorphism.

(b) Show that $\phi(\mathbf{Z}[[T]]) = \mathbf{Z}_p$.

If you squint just right, you can see Hensel defining the p-adic integers in [8] as the quotient $\mathbf{Z}[[T]]/\ker(\phi)$. This claim must be taken *cum grano salis*; even the notion of a "ring" was still up in the air when [8] was written. Nevertheless, it gets at the essence of Hensel's description.

(c) Show that $\ker(\phi) = (T - p)\mathbf{Z}[[T]]$.

Remark. It seems that neither the definition in [8], nor Hensel's earlier descriptions in [6, 7] (similar but less refined), were viewed by Hensel's contemporaries as entirely rigorous. In his obituary [5] for Hensel, Hasse describes the p-adic numbers as "a genuine creation driven by intuition and imagination, which, initially, like every revolutionary idea, was thrown down bluntly and in raw form and which, similar to Leibniz's differential calculus, initially lacked a solid logical foundation." Apprehensions about the logical standing of p-adic numbers were dispelled only after Kürschák and Ostrowski's papers on valuation theory, which began to appear around the same time as [8].

References

1. M. Aigner and G. M. Ziegler, *Proofs from The Book*, sixth edition, Springer, Berlin, 2018.

2. R. H. Cox, *A proof of the Schroeder-Bernstein theorem*. Amer. Math. Monthly **75** (1968), 508.
3. A. A. Cuoco, *Visualizing the p-adic integers*. Amer. Math. Monthly **98** (1991), 355–36.
4. A. W. Hales and E. G. Straus, *Projective colorings*. Pacific J. Math. **99** (1982), 31–43.
5. H. Hasse, *Kurt Hensel zum Gedächtnis*. J. Reine Angew. Math. **187** (1949), 1–13.
6. K. Hensel, *Neue Grundlagen der Arithmetik*. J. Reine Angew. Math. **127** (1904), 51–84.
7. ———, *Theorie der algebraischen Zahlen*, B. G. Teubner, Leipzig and Berlin, 1908.
8. ———, *Zahlentheorie*, G. J. Göschen, Berlin and Leipzig, 1913.
9. J. E. Holly, *Pictures of ultrametric spaces, the p-adic numbers, and valued fields*. Amer. Math. Monthly **108** (2001), 721–728.
10. S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37, American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007.
11. A. M. Robert, *A course in p-adic analysis*, Grad. Texts in Math., vol. 198, Springer-Verlag, New York, 2000.
12. W. H. Schikhof, *Ultrametric calculus: An introduction to p-adic analysis*, Cambridge Studies in Advanced Mathematics, vol. 4, Cambridge University Press, Cambridge, 2006.

Solutions to Set #6

6.68 Suppose $\{x_n\}$ is Cauchy. To prove that $|x_{n+1} - x_n| \to 0$, let $\epsilon > 0$ be given, and select $N \in \mathbf{Z}^+$ so that $|x_n - x_m| < \epsilon$ for all positive integers $n, m \geq N$. Then $|x_{n+1} - x_n| < \epsilon$ whenever $n \geq N$. (This direction of the proof does not use that $|\cdot|$ is non-Archimedean.)

Conversely, suppose that $|x_{n+1} - x_n| \to 0$. To prove $\{x_n\}$ is Cauchy, let $\epsilon > 0$, and choose $N \in \mathbf{Z}^+$ with $|x_{n+1} - x_n| < \epsilon$ whenever $n \geq N$. If we assume that $n > m \geq N$, the strong triangle inequality yields

$$\begin{aligned} |x_n - x_m| &= |(x_n - x_{n-1}) + (x_{n-1} + x_{n-2}) + \cdots + (x_{m+1} - x_m)| \\ &\leq \max\{|x_n - x_{n-1}|, \ldots, |x_{m+1} - x_m|\} < \epsilon. \end{aligned}$$

The cases where $m > n \geq N$ are interchangeable with these, since $|x_n - x_m| = |x_m - x_n|$. Finally, the inequality $|x_n - x_m| < \epsilon$ is trivial for $n = m$.

6.69 Let $x_n = 2^{5^n}$. By Euler's theorem, $x_{n+1} - x_n = x_n \cdot (2^{5^{n+1}-5^n} - 1) = x_n \cdot (2^{\varphi(5^{n+1})} - 1) \equiv x_n \cdot 0 \equiv 0 \pmod{5^{n+1}}$. Thus, $|x_{n+1} - x_n|_5 \leq 5^{-n-1}$, which tends to 0, and $\{x_n\}$ is a Cauchy sequence by Exercise 6.68.

6.70 Choose $N \in \mathbf{Z}^+$ so that $|x_n - x_m| < 1$ whenever $n, m \geq N$. Then for all $n \geq N$, we have $|x_n - x_N| < 1$, so that

$$|x_n| = |(x_n - x_N) + x_N| \leq |x_n - x_N| + |x_N| \leq 1 + |x_N|.$$

As a consequence, each $|x_n| \leq \max\{|x_1|, |x_2|, \ldots, |x_{N-1}|, 1 + |x_N|\}$.

6.71 The argument is the same as in calculus. Suppose $\{x_n\}$ is Cauchy and that the subsequence $\{x_{n_k}\}$ converges to x.

Given $\epsilon > 0$, choose $N_1 \in \mathbf{Z}^+$ with the property that $|x_k - x_\ell| < \frac{1}{2}\epsilon$ whenever $k, \ell \geq N_1$. Choose $N_2 \in \mathbf{Z}^+$ so that $|x_{n_k} - x| < \epsilon$ for all $k \geq N_2$. If $k \geq \max\{N_1, N_2\}$, then

$$|x_k - x| = |(x_k - x_{n_k}) + (x_{n_k} - x)| \leq |x_k - x_{n_k}| + |x_{n_k} - x| < \frac{1}{2}\epsilon + \frac{1}{2}\epsilon = \epsilon.$$

(We use here that $n_k \geq k \geq N_1$.) Hence, $x_k \to x$.

6.72 Since $p^{-1} \in \mathbf{Q}_p$, both $\bigcup_{n\geq 0} p^{-n}\mathbf{Z}_p$ and $\mathbf{Z}_p[1/p]$ are contained in $\mathbf{Q}_p$. Both also contain 0, so we will be done if we show that both contain $\mathbf{Q}_p^\times$.

By Exercise 5.60, each $x \in \mathbf{Q}_p^\times$ can be written as $\frac{p^v u}{p^{v'}u'}$ for some nonnegative integers v, v' and some $u, u' \in \mathbf{Z}_p^\times$. Then $x = p^{v-v'}uu'^{-1} \in p^{v-v'}\mathbf{Z}_p$. Since $p^{v-v'}\mathbf{Z}_p$ is a subset of both $\bigcup_{n\geq 0} p^{-n}\mathbf{Z}_p$ and $\mathbf{Z}_p[1/p]$, it follows that x is contained in both sets.

6.73 That x has such a representation is implicit in our solution to Problem 6.72. To prove uniqueness, suppose $x = p^v u = p^{v'}u'$, with $v, v' \in \mathbf{Z}$ and $u, u' \in \mathbf{Z}_p^\times$. Choose $w \in \mathbf{Z}$ large enough that both $v + w$ and $v' + w$ are nonnegative, and apply the already-known uniqueness statement from Problem 5.60 to $p^w x = p^{v+w}u = p^{v'+w}u'$.

6.74 Both definitions assign $v_p(0) = \infty$, so it is enough to prove our two definitions of $v_p(x)$ agree for $x \in \mathbf{Q}^\times$. Write $x = p^v \frac{a}{b}$ where a and b are integers not divisible by p. Then $v_p(x) = v$ if we go by the Set #1 definition. To show $v_p(x) = v$ with our new definition, it suffices to prove that $\frac{a}{b}$ is a unit in $\mathbf{Z}_p$. Thankfully, this is easy: Since $p \nmid ab$, we have both $\frac{a}{b} \in \mathbf{Z}_{(p)} \subseteq \mathbf{Z}_p$ and $(\frac{a}{b})^{-1} = \frac{b}{a} \in \mathbf{Z}_{(p)} \subseteq \mathbf{Z}_p$. (See Problem 5.58 for the containment $\mathbf{Z}_{(p)} \subseteq \mathbf{Z}_p$.) Thus, $\frac{a}{b} \in \mathbf{Z}_p^\times$.

It remains to show that $|\cdot|_p$ is a non-Archimedean absolute value on $\mathbf{Q}_p$. Property (i) in the absolute value definition (see Set #1) is clear. Property (iii) is straightforward: We can assume x, y are nonzero. Write $x = p^{v_p(x)}u$ and $y = p^{v_p(y)}u'$, where $u, u' \in \mathbf{Z}_p^\times$. Then $xy = p^{v_p(x)+v_p(y)}uu'$, and $uu' \in \mathbf{Z}_p^\times$. Hence, $v_p(xy) = v_p(x)+v_p(y)$, so that $|xy|_p = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$. Finally, we turn our attention to the strong triangle inequality: $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. For the proof we may assume that x, y, and $x + y$ are all nonzero. As above, write $x = p^{v_p(x)}u$ and $y = p^{v_p(y)}u'$. Assuming (as we may) that $v_p(x) \leq v_p(y)$, we find that $x + y = p^{v_p(x)}w$ for some $w \in \mathbf{Z}_p$. Furthermore, w is nonzero by our assumption that $x + y \neq 0$. Write $w = p^{v_p(w)}u''$. Then $x + y = p^{v_p(x)+v_p(w)}u''$, and $|x + y|_p = p^{-v_p(x)-v_p(w)} \leq p^{-v_p(x)} = \max\{p^{-v_p(x)}, p^{-v_p(y)}\} = \max\{|x|_p, |y|_p\}$.

6.75 First, we argue that for $x \in \mathbf{Q}_p$: $\quad x \in \mathbf{Z}_p \iff |x|_p \leq 1$.

We may assume that $x \in \mathbf{Q}_p^\times$. Write $x = p^{v_p(x)}u$ where $u \in \mathbf{Z}_p^\times$. When $v_p(x) \geq 0$, it is clear that $x \in \mathbf{Z}_p$, as both $p^{v_p(x)}$ and u belong to $\mathbf{Z}_p$. On the other hand, Problem 5.60 gives $v_p(x) \geq 0$ for all nonzero $x \in \mathbf{Z}_p$. Therefore,

$$x \in \mathbf{Z}_p \iff v_p(x) \geq 0 \iff p^{-v_p(x)} \leq 1 \iff |x|_p \leq 1,$$

and $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x|_p \leq 1\}$.

Next, observe that for each nonzero $x \in \mathbf{Q}_p$,

$$x \in \mathbf{Z}_p^\times \iff v_p(x) = 0 \iff p^{-v_p(x)} = 1 \iff |x|_p = 1.$$

Hence, $\mathbf{Z}_p^\times = \{x \in \mathbf{Q}_p : |x|_p = 1\}$.

6.76 We address only the part after "thus"; the earlier claims in the problem are consequences of the Pigeonhole Principle. By construction, $a_{k+1} \equiv a_k \pmod{p^k}$ for every k, so that $x := (a_1 \bmod p, a_2 \bmod p^2, \dots) \in \mathbf{Z}_p$. Furthermore, for each k, there are infinitely many $n \in \mathbf{Z}^+$ where the mod p^k component of x_n is $a_k \bmod p^k$.

Choose $n_1 \in \mathbf{Z}^+$ so that the mod p component of x_{n_1} is $a_1 \bmod p$. Then choose $n_2 > n_1$ where the mod p^2 component of x_{n_2} is $a_2 \bmod p^2$, then $n_3 > n_2$ where the mod p^3 component of x_{n_3} is $a_3 \bmod p^3$, etc.

We argue that $x_{n_k} \to x$ in $(\mathbf{Q}_p, |\cdot|_p)$. Let $k \in \mathbf{Z}^+$. By construction, the mod p^k component of $x_{n_k} - x$ vanishes. By the compatibility condition baked into the definition of $\mathbf{Z}_p$, the mod p, mod p^2, ..., mod p^{k-1} components also vanish. Therefore (see the solution to Problem 5.60), either $x_{n_k} - x = 0$ or $x_{n_k} - x = p^v u$ for an integer $v \geq k$ and a $u \in \mathbf{Z}_p^\times$. In either case, $v_p(x_{n_k} - x) \geq k$, and $|x_{n_k} - x|_p \leq p^{-k}$. Since $p^{-k} \to 0$, we conclude that $x_{n_k} \to x$, as required.

Remark. Grouchy experts may complain that Problem 6.76 establishes the *sequential* compactness of $\mathbf{Z}_p$, not compactness with today's accepted meaning in general topology (cf. [1]). But those same experts will know that for metric spaces — such as $\mathbf{Z}_p$ — the two concepts coincide. So what exactly are they complaining about?

Such grumblers may find the following Extra Exploration more to their tastes.

Extra Exploration 13 ($\mathbf{Z}_p$ is compact, take two).

(a) A (possibly infinite) number of Ross Program counselors are stationed at points of $\mathbf{Z}_p$. Each counselor is responsible for the campers within a certain positive radius of their position, as measured by $|\cdot|_p$. Presently, all of $\mathbf{Z}_p$ is monitored: each point of $\mathbf{Z}_p$ lies within the assigned radius of some counselor. Show that all but finitely many of the counselors can leave to purchase talent show supplies while $\mathbf{Z}_p$ remains fully monitored (without the need to relocate the remaining counselors).

(b) What happens if we replace every occurrence of $\mathbf{Z}_p$ by $\mathbf{Z}$? Assume distances are still measured by $|\cdot|_p$ for some prime p.

6.77 Let's accept for the time being the identity $\prod_{j \geq 1} e^{T^j/j} = \frac{1}{1-T}$ in $\mathbf{Q}[[T]]$.

The series for $\frac{1}{1-T}$ has T^p-coefficient (in fact, every coefficient) equal to 1. To see what the coefficient of T^p looks like on the left side of our identity, we expand

$$\prod_{j=1}^{\infty}\left(1+\frac{T^j}{j}+\frac{1}{2!}\frac{T^{2j}}{j^2}+\frac{1}{3!}\frac{T^{3j}}{j^3}+\dots\right)$$
$$=\sum_{k\ge 0}T^k\sum_{\substack{e_1+2e_2+3e_3+\cdots=k\\ \text{all } e_i\ge 0}}\frac{1}{e_1!e_2!e_3!\cdots}\frac{1}{1^{e_1}2^{e_2}3^{e_3}\dots}.$$

All but two of the tuples $e_1, e_2, \dots$ with $e_1 + 2e_2 + 3e_3 + \cdots = p$ have $\frac{1}{e_1!e_2!e_3!\cdots}\frac{1}{1^{e_1}2^{e_2}3^{e_3}\dots} \in \mathbf{Z}_{(p)}$. The two exceptions are (1) the tuple with $e_1 = p$ and all other $e_i = 0$ and (2) the tuple with $e_p = 1$ and all other $e_i = 0$, which make respective contributions of $\frac{1}{p!}$ and $\frac{1}{p}$. Equating coefficients of T^p leads to the conclusion that $1 - (\frac{1}{p!} + \frac{1}{p}) \in \mathbf{Z}_{(p)}$, as claimed.

Since 1 also belongs to the ring $\mathbf{Z}_{(p)}$, we infer that $\frac{1}{p!} + \frac{1}{p} \in \mathbf{Z}_{(p)}$. But

$$\left|\frac{1}{p!}+\frac{1}{p}\right|_p = \left|\frac{(p-1)!+1}{p!}\right|_p = p|(p-1)!+1|_p.$$

Consequently, $|(p-1)!+1|_p \le 1/p$. This translates to $p \mid (p-1)!+1$, or $(p-1)! \equiv -1 \pmod p$.

Remark. It is a little tricky to write down a rigorous proof of the formal identity $\prod_{j\ge1} \mathrm{e}^{T^j/j} = \frac{1}{1-T}$. We sketch one argument, which, however, involves some 'cheating'; specifically we draw on the theory of complex variables, which is not a prerequisite for the rest of the text.

For each $J \in \mathbf{Z}^+$, let $F_J(T) = \prod_{1\le j\le J} \mathrm{e}^{T^j/j}$ (as a formal power series). Reasoning as in the Remark to Problem 4.42, $F_J(z) = \prod_{1\le j\le J} \mathrm{e}^{z^j/j}$ for all complex z. As $J \to \infty$, the functions $F_J(z)$ converge uniformly to $\frac{1}{1-z}$ on every compact subset of the open unit disc $|z| < 1$. So by Cauchy's integral formula, if we write $F_J(T) = \sum_{k\ge0} a_{k,J}T^k$, then for each fixed k,

$$a_{k,J} = \frac{1}{2\pi\mathrm{i}}\int_{|z|=9/10} F_J(z)z^{-k-1}\,\mathrm{d}z \xrightarrow{J\to\infty} \frac{1}{2\pi i}\int_{|z|=9/10}\frac{1}{1-z}z^{-k-1}\,\mathrm{d}z = 1.$$

(Here we recognized the final integral as the coefficient of T^k in $\frac{1}{1-T} = 1+T+T^2+\dots$.) Since $a_{k,J} = a_{k,k}$ for all $J \ge k$, we conclude that $a_{k,J} = 1$ for all $J \ge k$. In particular: For each fixed k, the kth coefficient of $F_J(T)$ eventually stabilizes at the kth coefficient of $\frac{1}{1-T}$. This is precisely what it means to say that $\prod_{j\ge1} \mathrm{e}^{T^j/j} = \frac{1}{1-T}$ as formal power series.

6.78 Write $a^{p-1} = 1 + pq_p(a)$, $b^{p-1} = 1 + pq_p(b)$. Multiplying, $(ab)^{p-1} = 1 + p(q_p(a)q_p(b) + pq_p(a)q_p(b))$, so that

$$q_p(ab) = \frac{(ab)^{p-1}-1}{p} = q_p(a)+q_p(b)+pq_p(a)q_p(b) \equiv q_p(a)+q_p(b) \pmod p.$$

References

1. M. Raman-Sundström, *A pedagogical history of compactness*. Amer. Math. Monthly **122** (2015), 619–635.

Solutions to Set #7

7.79 Let $\{x_n\}$ be a Cauchy sequence in $\mathbf{Z}_p$. By Problem 6.76, $\{x_n\}$ has a subsequence $\{x_{n_k}\}$ converging to some $x \in \mathbf{Z}_p$. By Problem 6.71, $x_n \to x$.

7.80 Let $\{x_n\}$ be a Cauchy sequence in $\mathbf{Q}_p$. We know from Exercise 6.70 that $\{|x_n|\}$ is bounded. Hence, if k is sufficiently large, then each $|p^k x_n| \leq 1$, i.e., $\{p^k x_n\}$ is a sequence in $\mathbf{Z}_p$. Since $\{x_n\}$ is Cauchy, so is $\{p^k x_n\}$. By Problem 7.79, $p^k x_n \to x$ for some $x \in \mathbf{Z}_p$. Then $x_n \to p^{-k} x$.

7.81 Let $x_n = 2^{5^n}$. By Problem 6.69, $\{x_n\}$ is a Cauchy sequence in $\mathbf{Z}_5$. Invoking Exercise 7.79, $x_n \to x$ for some $x \in \mathbf{Z}_p$.

By the product rule for limits, $\lim x_n^5 = (\lim x_n)^5 = x^5$. On the other hand, $x_n^5 = x_{n+1}$, so that $\lim x_n^5 = \lim x_{n+1} = x$. Hence, $x = x^5$.

As shown in the solution to Problem 6.69, $x_n = 2^{5^n} \equiv 2^{5^1} \equiv 2 \pmod 5$ for all n. Therefore, $|x_n - 2|_5 \leq \frac{1}{5}$ for all n, and (see Problem 4.47)

$$|x - 2|_5 = |\lim (x_n - 2)|_5 = \lim |x_n - 2|_5 \leq \frac{1}{5}.$$

Thus, $x \equiv 2 \pmod{5\mathbf{Z}_5}$. In particular, $x \neq 0$, and $x = x^5$ tells us $1 = x^4$. That is, x is a 4th root of 1, as claimed.

The only 4th roots of 1 belonging to $\mathbf{Q}$ are 1 and -1. Neither is congruent to 2 modulo $5\mathbf{Z}_5$. Therefore, $x \notin \mathbf{Q}$.

7.82 Let $x \in \mathbf{Z}_p$. For each $k \in \mathbf{Z}^+$, there is an integer a_k with $x \equiv a_k \pmod{p^k \mathbf{Z}_p}$. (If we view x as an infinite tuple, we can take for a_k any integer representing the mod p^k component of x; see the solution to Problem 5.62.) Then $|a_k - x|_p \leq p^{-k}$, which tends to 0 as $k \to \infty$. So $\{a_k\}$ is a sequence of integers converging to x.

7.83 Let $x \in \mathbf{Q}_p$. Choose $k \in \mathbf{Z}$ with $p^k x \in \mathbf{Z}_p$. By Problem 7.82, we can find a sequence of integers a_k converging to $p^k x$. Then $p^{-k} a_k$ is a sequence of rational numbers converging to x.

7.84 We define a candidate isomorphism $\phi\colon L \to L'$ as follows. Since K is dense in L, for each $x \in L$ there is a sequence $\{x_n\}$ in K such that $x_n \to x$ in L. Since $\{x_n\}$ converges in L, $\{x_n\}$ is Cauchy in L. Then $\{x_n\}$ is also Cauchy in L', as each $x_n \in K$ and $|\cdot|$ and $|\cdot|'$ extend the same absolute value on K. Since $(L', |\cdot|')$ is complete, $\{x_n\}$ converges in L'. We define $\phi(x) = \lim^{(L')} x_n$, where the superscript indicates that the limit is taken in L'.

Honor demands we check that $\phi(x)$ depends only on x and not on the particular $\{x_n\}$. Suppose $\{x_n\}$ and $\{\tilde{x}_n\}$ are two sequences in K both converging to x in L. Then $x_n - \tilde{x}_n \to 0$ in L. As each $x_n - \tilde{x}_n \in K$, and $|\cdot|$ and $|\cdot|'$ extend the same absolute value on K, it must be that $x_n - \tilde{x}_n \to 0$ in L'. Consequently, $\lim^{(L')} x_n = \lim^{(L')} \tilde{x}_n$. Vindication!

If $x \in K$, we can compute $\phi(x)$ by taking each $x_n = x$. This shows that $\phi(x) = \lim^{(L')} x = x$. So ϕ fixes K.

Let $x, y \in L$ and choose sequences $\{x_n\}$, $\{y_n\}$ in K such that $x_n \to x$ in L and $y_n \to y$ in L. Then $x_n + y_n \to x + y$ in L, and

$$\phi(x+y) = \lim^{(L')}(x_n + y_n) = \lim^{(L')} x_n + \lim^{(L')} y_n = \phi(x) + \phi(y).$$

Similarly, $\phi(xy) = \phi(x)\phi(y)$, confirming that ϕ is a homomorphism.

A homomorphism between fields is always injective. To establish surjectivity, take any $x' \in L'$. Since K is dense in L', there is a sequence $\{x_n\}$ in K converging to x' in L'. Since $\{x_n\}$ converges in L', it is Cauchy in L' and hence in L as well. Define $x \in L$ by $x = \lim^{(L)} x_n$. Then $\phi(x) = \lim^{(L')} x_n = x'$.

Thus far we have shown ϕ is an isomorphism. To prove ϕ is isometric, let $x \in L$, and consider a sequence $\{x_n\}$ in K converging to x in L. Then $\{x_n\}$ converges to $\phi(x)$ in L'. Given $\epsilon > 0$, we choose $N \in \mathbf{Z}^+$ such that, for all $n \geq N$,

$$|x_n - x| < \epsilon \quad \text{and} \quad |x_n - \phi(x)|' < \epsilon.$$

Then, for $n \geq N$,

$$|x| \leq |x_n| + \epsilon = |x_n|' + \epsilon < |\phi(x)|' + 2\epsilon,$$

and

$$|x| \geq |x_n| - \epsilon = |x_n|' - \epsilon \geq |\phi(x)|' - 2\epsilon.$$

Hence $|x|$ and $|\phi(x)|'$ are within 2ϵ of each other. Since this holds for each $\epsilon > 0$, it must be that $|x| = |\phi(x)|'$.

Extra Exploration 14. Show that the map ϕ described above is the *unique* isometric isomorphism from L to L'.

Remark. Every valued field $(K, |\cdot|)$ admits a completion (which we have just seen is then unique up to isometric isomorphism). The usual way to show a completion exists is to mimic one of the standard constructions of $\mathbf{R}$ from $\mathbf{Q}$, due to Cantor and Méray: Take the ring of Cauchy sequences in K and quotient by the maximal ideal of sequences tending to 0. For details, see for instance [3, §1.3]. Those with more exotic tastes might enjoy a recent, very different argument by Kionke [4].

7.85 Let $s_n = \sum_{k=0}^{n} c_k p^k$. Then $|s_{n+1} - s_n|_p = |c_{n+1}p^{n+1}|_p \leq p^{-n-1}$. As $p^{-n-1} \to 0$, the sequence $\{s_n\}$ is Cauchy (see Exercise 6.68). By Problem 7.79, s_n has a limit in $\mathbf{Z}_p$. This is precisely what it means to say that $\sum_{k=0}^{\infty} c_k p^k$ converges to an element of $\mathbf{Z}_p$.

7.86 Our selection process guarantees that $x_{k+1} \equiv x \equiv x_k \pmod{p^k \mathbf{Z}_p}$ and thus $x_{k+1} \equiv x_k \pmod{p^k}$ (this last congruence holding in $\mathbf{Z}$). It also ensures that x_k is the least nonnegative representative of its residue class mod p^k. Therefore, $x_{k+1} \geq x_k$, and $c_k = \frac{1}{p^k}(x_{k+1} - x_k) \geq 0$. Since $x_{k+1} < p^{k+1}$, we also have $c_k < p^{k+1}/p^k = p$. Hence, $c_k \in \{0, 1, \ldots, p-1\}$.

Clearly, $x_k \to x$, since $|x_k - x|_p \leq p^{-k}$. Moreover,

$$c_0 + c_1 p + \cdots + c_{k-1}p^{k-1} = (x_1 - x_0) + (x_2 - x_1) + \cdots + (x_k - x_1) = x_k - x_0 = x_k$$

for every $k \in \mathbf{Z}^+$. Sending k to infinity, $c_0 + c_1 p + c_2 p^2 + \cdots = \lim x_k = x$.

Extra Exploration 15. Show that if p is an odd prime, then every $x \in \mathbf{Z}_p$ has a unique representation in the form $\sum_{k=0}^{\infty} d_k p^k$, where the d_k are integers from the interval $(-p/2, p/2)$. For which x is this expansion terminating? For which x is it eventually periodic?

Extra Exploration 16 (Knopfmacher and Knopfmacher [5]). Prove that every $x \in 1 + p\mathbf{Z}_p$ has a unique product representation $x = (1+p)^{e_1}(1+p^2)^{e_2}(1+p^3)^{e_3}\cdots$, where $e_1, e_2, e_3, \ldots \in \{0, 1, 2, \ldots, p-1\}$.

Extra Exploration 17 (Pigeons hard at work; Mahler [6]). Let $x \in \mathbf{Z}_p$. In this problem we look for prescribed patterns of digits in the base p expansions of the integer multiples of x.

(a) Let $m, n \in \mathbf{Z}^+$. Prove that there are integers A, B with $A \neq 0$, $-p^m \leq A \leq p^m$, and $0 \leq B < p^n$ satisfying $Ax \equiv B \pmod{p^{m+n}\mathbf{Z}_p}$.
Suggestion. Consider $Ax - B \bmod p^{m+n}\mathbf{Z}_p$ for $1 \leq A \leq p^m$ and $0 \leq B < p^n$. If $0 \bmod p^{m+n}\mathbf{Z}_p$ is represented, you are done. Otherwise, start stuffing pigeons in holes.

(b) Taking $m = 1$ in (a), show that one of the $2p$ p-adic integers $\pm x, \pm 2x, \ldots, \pm px$ has infinitely many '0' digits in its base p expansion. More generally, for each $m \in \mathbf{Z}^+$, one of the $2p^m$ p-adic integers $\pm x, \pm 2x, \ldots, \pm p^m x$ has infinitely many runs of m consecutive zeros in its base p expansion.

(c) Assume x is an irrational element of $\mathbf{Z}_p$. (That is, $x \in \mathbf{Z}_p \setminus \mathbf{Z}_{(p)}$.) Let $m \in \mathbf{Z}^+$, and let $d_0, d_1, d_2, \ldots, d_{m-1} \in \{0, 1, \ldots, p-1\}$. Show that there is a nonzero

integer k such that the following holds: The digits $d_0, d_1, \ldots, d_{m-1}$ appear, in that order, infinitely often in the base p expansion of kx.

The last bit means that if we expand $kx = \sum_{j \geq 0} c_j p^j$, then $c_j = d_0, c_{j+1} = d_1, \ldots, c_{j+m-1} = d_{m-1}$ for infinitely many nonnegative integers j. For the proof, consider multiples of $k_0 x$, where $k_0 x$ has long runs of zeros as in (b).

(d) Assume x is an irrational element of $\mathbf{Z}_p$. Let $m \in \mathbf{Z}^+$. Show that there is a *positive* integer k' such that *every* sequence of m base p digits appears infinitely often in the base p expansion of $k'x$.

Hint. Can you do this with a not-necessarily-positive (but nonzero) k'? If so, what happens when you replace k' with $-k'$?

7.87 Start with any $x \in \mathbf{Q}_p$ and select $k \in \mathbf{Z}$ with $p^k x \in \mathbf{Z}_p$. Take the infinite base p expansion of $p^k x$ constructed in Problem 7.86 and scale by p^{-k} to obtain an expansion of x satisfying (i)–(iii).

If there were two expansions of x possessing properties (i)—(iii), scaling both by the same sufficiently large power of p would produce an element of $\mathbf{Z}_p$ with two different base p expansions.

7.88 The forward direction is clear. Now suppose $x = 0$ or $x \in \mathbf{Q}^+$ with denominator a power of p. Write $x = a/p^k$, where a and k are nonnegative integers. Then the canonical expansion of x is obtained by taking the usual base p expansion of a and scaling by p^{-k}; this is obviously terminating.

7.89 We record a simple observation for later use: For each $\ell \in \mathbf{Z}^+$, the series $1 + p^\ell + p^{2\ell} + \ldots$ converges to $1/(1 - p^\ell)$ in $(\mathbf{Q}_p, |\cdot|)$. We omit the straightforward proof (compare with Exercise 3.30).

Suppose x has an eventually periodic canonical expansion with (not necessarily minimal) period ℓ. Scaling x by a suitable power of p (which does not affect rationality), we can assume $x = \sum_{k \geq 0} c_k p^k$ where $c_k = c_{k+\ell}$ for all $k \geq k_0$. Then $x = \sum_{0 \leq k < k_0} c_k p^k + \sum_{k \geq k_0} c_k p^k$. Clearly, $\sum_{0 \leq k < k_0} c_k p^k \in \mathbf{Q}$. Less trivially,

$$\begin{aligned}
\sum_{k \geq k_0} c_k p^k &= \lim_{m \to \infty} \sum_{k_0 \leq k < k_0 + m\ell} c_k p^k \\
&= \lim_{m \to \infty} \sum_{k_0 \leq k < k_0 + \ell} c_k p^k (1 + p^\ell + \cdots + p^{(m-1)\ell}) \\
&= \sum_{k_0 \leq k < k_0 + \ell} c_k p^k (1 + p^\ell + p^{2\ell} + \ldots) \\
&= \sum_{k_0 \leq k < k_0 + \ell} c_k \frac{p^k}{1 - p^\ell} \in \mathbf{Q}.
\end{aligned}$$

Therefore, $x \in \mathbf{Q}$.

Turning to the converse: We have already shown that each $x \in \mathbf{Z}_{(p)}$ has an eventually periodic base p expansion. To obtain an eventually periodic canonical expansion for an arbitrary $x \in \mathbf{Q}$, scale x by p^k to place $p^k x \in \mathbf{Z}_{(p)}$, then rescale by p^{-k}.

Open problem: Is the p-adic number $\sum_{k=0}^{\infty} k!$ rational for some prime p?

Extra Exploration 18 (Casacuberta [1]). Show that the p-adic number $\sum_{k=0}^{\infty} p^{v_p(k!)}$ has a canonical expansion containing arbitrarily long (but finite) runs of zeros, for every prime p. Deduce that $\sum_{k=0}^{\infty} p^{v_p(k!)} \notin \mathbf{Q}$.

Extra Exploration 19 (Dragovich [2]). Disprove: $\sum_{k=0}^{\infty} k!$ converges to the same rational number in $\mathbf{Q}_p$ for all primes p.

7.90 By Problem 6.78, $\sum_{a=1}^{p-1} q_p(a) \equiv q_p((p-1)!) \equiv \frac{(p-1)!^{p-1}-1}{p} \pmod{p}$. So the claimed congruence is equivalent to $\frac{(p-1)!^{p-1}-(p-1)!-2}{p} \equiv 0 \pmod{p}$, or $(p-1)!^{p-1} - (p-1)! \equiv 2 \pmod{p^2}$. Using Wilson's theorem, write $(p-1)! = -1 + pr$ with $r \in \mathbf{Z}$. Then, working modulo p^2,

$$(p-1)!^{p-1} = \sum_{j=0}^{p-1} \binom{p-1}{j} (-1)^{p-1-j} (pr)^j \equiv 1 + (p-1)(-1)pr \equiv 1 + pr,$$

so that $(p-1)!^{p-1} - (p-1)! \equiv (1+pr) - (-1+pr) \equiv 2$, as desired.

7.91 Let us argue that whenever we have a solution to $x^2 = 2$ in $\mathbf{Z}/7^k$, say $a_k \bmod 7^k$, we can lift it uniquely — by the process described — to a solution $a_{k+1} \bmod 7^{k+1}$ in $\mathbf{Z}/7^{k+1}$. Expanding, $(a_k + 7^k q)^2 \equiv a_k^2 + 2 \cdot 7^k a_k q \pmod{7^{k+1}}$. This last expression is congruent to 2 modulo 7^{k+1} precisely when

$$2 \cdot 7^k a_k q \equiv 2 - a_k^2 \pmod{7^{k+1}}.$$

By assumption, $7^k \mid 2 - a_k^2$. So the preceding congruence is equivalent to

$$2 a_k q \equiv \frac{2 - a_k^2}{7^k} \pmod{7}.$$

Both 2 and a_k are coprime to 7. (Since $a_k^2 \equiv 2 \pmod{7}$, we cannot have $a_k \equiv 0 \pmod{7}$.) Thus, the last displayed congruence uniquely determines the residue class of q modulo 7. Picking any q from this class and defining $a_{k+1} = a_k + 7^k q$ yields our desired lift. Note that since q is uniquely determined mod 7, our lift is uniquely determined as a residue class mod 7^{k+1}.

Assume now that $a_1 \bmod 7, a_2 \bmod 7^2, a_3 \bmod 7^3, \ldots$ have been determined by the above procedure. Let $x = (a_1 \bmod 7, a_2 \bmod 7^2, a_3 \bmod 7^3, \ldots)$. Then

$x \in \mathbf{Z}_7$ as each a_{k+1} is a lift of a_k. By construction, $x^2 = (2 \bmod 7, 2 \bmod 7^2, 2 \bmod 7^3, \dots) = 2$.

We still need to verify that the canonical expansion of x is as stated. The initial steps of the algorithm, starting with $3 \bmod 7$, are described in the problem statement. We lifted $3 \bmod 7$ to $3 + 1 \cdot 7 \bmod 7^2$, and we lifted *that* to $3 + 1 \cdot 7 + 2 \cdot 7^2 \bmod 7^3$. If we run the algorithm one more round, we arrive at $3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 \bmod 7^4$ (check this!). We can read off from here that the 7-adic expansion of x starts as $3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \dots$.

Remark. Gauss left us in 1855, four decades before Hensel's first publication on the p-adic numbers. It is therefore rather remarkable that one finds in his Nachlass (manuscripts left behind at death) the claim that

$$\sqrt{5} \pmod{11^\infty} = 9.0.4.10.4.4.$$

This seems to be Gauss's way of expressing that in $\mathbf{Z}_{11}$,

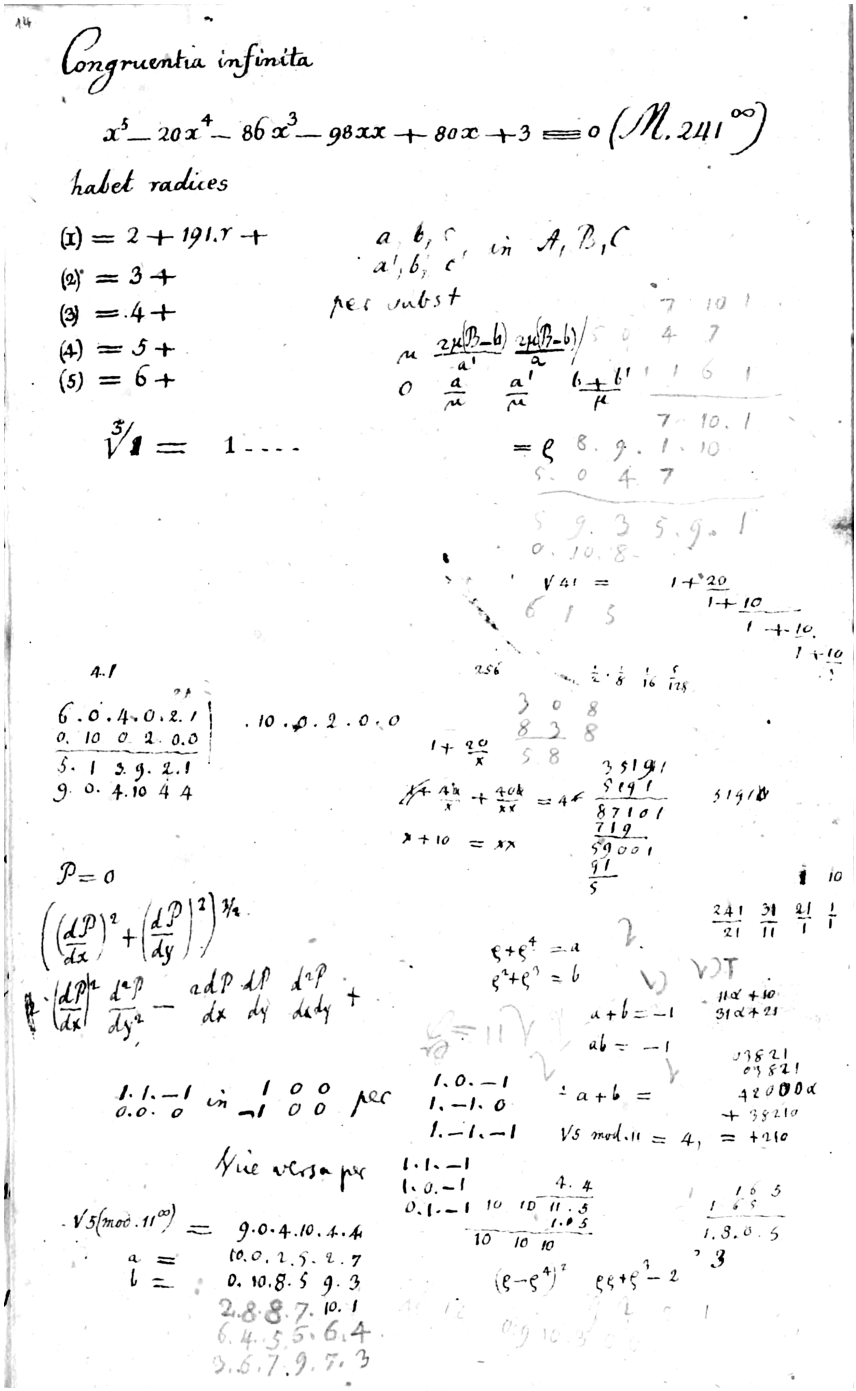
$$\sqrt{5} = 4 + 4 \cdot 11 + 10 \cdot 11^2 + 4 \cdot 11^3 + 0 \cdot 11^4 + 9 \cdot 11^5 + \dots.$$

I owe this historical nugget to math StackExchange user `user2554`.*

References

1. S. Casacuberta, *Irrationality of the sum of a p-adic series*. Unpublished. `arXiv:1710.11484 [math.NT]`
2. B. Dragovich, *On p-adic power series*. In: p-adic functional analysis (Poznań, 1998), Lecture Notes in Pure and Appl. Math., vol. 207, Dekker, New York, 1999, pp. 65–75.
3. S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37, American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007.
4. S. Kionke, *Constructing the completion of a field using Quasimorphisms*, p-Adic Numbers Ultrametric Anal. Appl. **11** (2019), 335–337.
5. A. Knopfmacher and J. Knopfmacher, *A binomial product representation for p-adic numbers*, Arch. Math. (Basel) **52** (1989), 333–336.
6. K. Mahler, *On the digits of the multiples of an irrational p-adic number*. Proc. Cambridge Philos. Soc. **76** (1974), 417–422.

* `https://math.stackexchange.com/a/4877205`



Page from Gauss's Nachlass; originally scanned by the Göttinger Digitalisierungszentrum.

Solutions to Set #8

8.92

(a) In any complete valued field, a sequence $\{s_n\}$ converges $\iff$ $\{s_n\}$ is Cauchy. The forward implication was noted on Set #6 (for every valued field, not necessarily complete). The backward implication is the definition of completeness.
Let $\sum_{k=1}^{\infty} a_k$ be a series in K, a field assumed to be complete with respect to a non-Archimedean absolute value. Put $s_n = \sum_{k=1}^{n} a_k$. Then $\sum_{k=1}^{\infty} a_k$ converges $\iff$ $\{s_n\}$ converges $\iff$ $\{s_n\}$ is Cauchy $\iff$ $s_{n+1} - s_n \to 0$ $\iff$ $a_{n+1} \to 0 \iff a_n \to 0$.

(b) If we assume $\sum_{k=1}^{\infty} a_k$ converges to s, then $|s_n| \to |s|$ (see Problem 4.47). By the strong inequality, each $|s_n| \leq \max\{|a_1|, |a_2|, \ldots, |a_n|\} \leq \max_{k=1,2,3,\ldots} |a_k|$. (That the last max exists is ensured by $|a_k|$ tending to 0.) Hence, $|s| = \lim |s_n| \leq \max_{k=1,2,3,\ldots} |a_k|$.

Extra Exploration 20 (convergence of infinite products). Let K be a field complete with respect to a non-Archimedean absolute value. Let $\{a_k\}$ be a sequence in K.

(a) Suppose that $a_k \to 0$. Show that $\prod_{k=1}^{\infty}(1 + a_k)$ is a well-defined element of K (meaning that that the partial products have a limit in K). Furthermore, $\prod_{k=1}^{\infty}(1 + a_k) = 0$ if and only if some $a_k = -1$.

(b) Conversely, prove that if $\prod_{k=1}^{\infty}(1 + a_k)$ defines a *nonzero* element of K, then $a_k \to 0$.

8.93 Let $\sum_{k=1}^{\infty} b_k$ be any rearrangement of $\sum_{k=1}^{\infty} a_k$; say $b_k = a_{\sigma(k)}$ for all $k = 1, 2, 3, \ldots$, where $\sigma \in \mathrm{Sym}(\mathbf{Z}^+)$. Put $s_n = \sum_{k=1}^{n} a_k$ and $t_n = \sum_{k=1}^{n} b_k$. By assumption, $s_n \to s$, while our task is to prove that $t_n \to s$.

Given $\epsilon > 0$, select $N_0 \in \mathbf{Z}^+$ with $|a_n| < \epsilon$ whenever $n > N_0$. Then choose $N \in \mathbf{Z}^+$ as the maximum of $\sigma^{-1}(1), \ldots, \sigma^{-1}(N_0)$. Let us argue that $|t_n - s| < \epsilon$ whenever $n \geq N$.

Let $n \geq N$. By our choice of N, all of $a_1, a_2, \ldots, a_{N_0}$ appear among $b_1, b_2, \ldots, b_N$, so that

$$t_n - s_{N_0} = \sum_{1\le k\le n} b_k - \sum_{1\le k\le N_0} a_k = \sum_{1\le k\le n,\ \sigma(k)>N_0} a_{\sigma(k)},$$

and

$$|t_n - s_{N_0}| \le \max\{|a_{\sigma(k)}| : 1 \le k \le n, \sigma(k) > N_0\} < \epsilon.$$

Moreover,

$$|s - s_{N_0}| = \left|\sum_{k>N_0} a_k\right| \le \max_{k>N_0} |a_k| < \epsilon.$$

Hence,

$$|t_n - s| = |(t_n - s_{N_0}) - (s - s_{N_0})| \le \max\{|t_n - s_{N_0}|, |s - s_{N_0}|\} < \epsilon,$$

as desired.

8.94 Put $s_n = \sum_{k=0}^n a_k, t_n = \sum_{k=0}^n b_k$, and $u_n = \sum_{k=0}^n c_k$. Let $s = \lim s_n$ and $t = \lim t_n$ be the infinite sums of the a_k and b_k, respectively. We must show that $u_n \to st$.

Observe that

$$s_n t_n = \sum_{\substack{0\le k,\ell\le n\\ k+\ell\le n}} a_k b_\ell + \sum_{\substack{0\le k,\ell\le n\\ k+\ell>n}} a_k b_\ell$$

and that the first of the two right-hand sums satisfies

$$\sum_{\substack{0\le k,\ell\le n\\ k+\ell\le n}} a_k b_\ell = \sum_{0\le r\le n} \sum_{\substack{k+\ell=r\\ k,\ell\ge 0}} a_k b_\ell = \sum_{0\le r\le n} \sum_{0\le k\le r} a_k b_{r-k} = \sum_{0\le r\le n} c_r = u_n.$$

Let e_n be the previously neglected sum, $e_n = \sum_{0<k,\ell\le n,\ k+\ell>n} a_k b_\ell$. Using A and B to denote upper bounds on $\{|a_k|\}$ and $\{|b_k|\}$ respectively (which certainly exist, since $a_k, b_k \to 0$), we find that

$$|e_n| \le \max_{0\le k,\ell\le n,\ k+\ell>n} |a_k b_\ell| \le B \max_{n/2<k\le n} |a_k| + A \max_{n/2<\ell\le n} |b_k|,$$

which tends to 0. Hence, $e_n \to 0$, and $u_n = s_n t_n - e_n \to st$, as desired.

8.95 For each fixed i, the series $\sum_j a_{i,j}$ converges, since $|a_{i,j}| \le \epsilon_j$ and $\epsilon_j \to 0$ as $j \to \infty$. Put $s_i = \sum_j a_{i,j}$. Then $\sum_i s_i$ also converges, since $|s_i| \le \max\{|a_{i,j}| : j \ge 0\} \le \epsilon_i$, and $\epsilon_i \to 0$ as $i \to \infty$. Thus, we have obtained convergence of the double series $\sum_i \sum_j a_{i,j}$. A symmetric argument demonstrates the convergence of $\sum_j \sum_i a_{i,j}$.

8.96 We start by noting that all of the double series appearing here converge or involve finitely many terms. This follows from Problem 8.95. To take one example (the others are similar), $\sum_{i=0}^N \sum_j a_{i,j}$ can be rewritten as $\sum_i \sum_j a_{i,j} \mathbf{1}_{i\le N}$.

Since $|a_{i,j}\mathbf{1}_{i\le N}| \le |a_{i,j}|$, the sufficient condition for convergence furnished by Problem 8.95 is satisfied with the same sequence $\{\epsilon_N\}$.

We can now establish our four inequalities. To attack the first of these, notice that

$$\left|\sum_i\sum_j a_{i,j} - \sum_{i=0}^{N}\sum_j a_{i,j}\right| = \left|\sum_{i=N+1}^{\infty}\sum_j a_{i,j}\right| \le \max_{i\ge N+1}\left|\sum_j a_{i,j}\right|.$$

Each term $a_{i,j}$ appearing in the final sum on j has $i \ge N+1$, and thus $|a_{i,j}| \le \epsilon_{N+1}$. Hence, $|\sum_j a_{i,j}| \le \max_j |a_{i,j}| \le \epsilon_{N+1}$ for each $i \ge N+1$, and $\max_{i\ge N+1}|\sum_j a_{i,j}| \le \epsilon_{N+1}$. So we have the first inequality.

Analogous reasoning shows that

$$\left|\sum_j\sum_i a_{i,j} - \sum_j\sum_{i=0}^{N} a_{i,j}\right| = \left|\sum_j\sum_{i=N+1}^{\infty} a_{i,j}\right| \le \max_j\left|\sum_{i=N+1}^{\infty} a_{i,j}\right| \le \epsilon_{N+1},$$

$$\left|\sum_{i=0}^{N}\sum_j a_{i,j} - \sum_{i=0}^{N}\sum_{j=0}^{N} a_{i,j}\right| = \left|\sum_{i=0}^{N}\sum_{j=N+1}^{\infty} a_{i,j}\right| \le \max_{0\le i\le N}\left|\sum_{j=N+1}^{\infty} a_{i,j}\right| \le \epsilon_{N+1},$$

and

$$\left|\sum_j\sum_{i=0}^{N} a_{i,j} - \sum_{j=0}^{N}\sum_{i=0}^{N} a_{i,j}\right| = \left|\sum_{j=N+1}^{\infty}\sum_{i=0}^{N} a_{i,j}\right| \le \max_{j\ge N+1}\left|\sum_{i=0}^{N} a_{i,j}\right| \le \epsilon_{N+1}.$$

Now look at the first column of inequalities in the problem statement. These inequalities, in conjunction with the strong triangle inequality, imply that

$$\left|\sum_i\sum_j a_{i,j} - \sum_{i=0}^{N}\sum_{j=0}^{N} a_{i,j}\right| \le \epsilon_{N+1}.$$

Similarly, we obtain from the second column of inequalities that

$$\left|\sum_j\sum_i a_{i,j} - \sum_{j=0}^{N}\sum_{i=0}^{N} a_{i,j}\right| \le \epsilon_{N+1}.$$

Since $\sum_{i=0}^{N}\sum_{j=0}^{N} a_{i,j} = \sum_{j=0}^{N}\sum_{i=0}^{N} a_{i,j}$ (it is always OK to swap finite sums!), a final application of the strong triangle inequality yields

$$\left|\sum_i\sum_j a_{i,j} - \sum_j\sum_i a_{i,j}\right| \le \epsilon_{N+1}.$$

Send N to infinity to conclude that $\sum_i \sum_j a_{i,j} = \sum_j \sum_i a_{i,j}$.

8.97 If $p-1 \mid k$, then $n^k \equiv 1 \pmod{p}$ for all of $n = 1, 2, \ldots, p-1$, so that $S_k(p) \equiv p-1 \pmod{p}$. Thus, $p \mid S_k(p)+1 = S_k(p) + \mathbf{1}_{p-1|k}$.

If $p-1 \nmid k$, choose an integer g that generates the multiplicative group mod p. Working modulo p,

$$g^k S_k(p) = g^k \sum_{0 \le n < p} n^k \equiv \sum_{0 \le n < p} (gn)^k \equiv \sum_{m \bmod p} m^k \equiv S_k(p),$$

using that multiplication by g permutes the residue classes modulo p. As $g^k \not\equiv 1 \pmod{p}$, we infer that $S_k(p) \equiv 0 \pmod{p}$. Therefore, $p \mid S_k(p) = S_k(p) + \mathbf{1}_{p-1|k}$.

8.98 By Faulhaber's formula, $\frac{S_k(p)}{p} = \frac{p^k}{k+1} + B_k + \sum_{0<j<k} \binom{k}{j} B_{k-j} \frac{p^j}{j+1}$. Rearranging,

$$B_k + \frac{\mathbf{1}_{p-1|k}}{p} + \sum_{0<j<k} \binom{k}{j} B_{k-j} \frac{p^j}{j+1} = \frac{S_k(p) + \mathbf{1}_{p-1|k}}{p} - \frac{p^k}{k+1}.$$

It will suffice to argue that both right-hand terms belong to $\mathbf{Z}_{(p)}$.

The first is in $\mathbf{Z}$ (Problem 8.97), so certainly also in $\mathbf{Z}_{(p)}$. To handle the second, notice that $p^k \ge 2^k \ge k+1$ for each $k \in \mathbf{Z}^+$. Therefore, $v_p(k+1) \le k$, and $v_p(\frac{p^k}{k+1}) = k - v_p(k+1) \ge 0$. That is, $\frac{p^k}{k+1} \in \mathbf{Z}_p$.

8.99 Suppose the claim is false and let k be the smallest positive integer for which $B_k + p^{-1}\mathbf{1}_{p-1|k} \notin \mathbf{Z}_{(p)}$. Let S be the sum on j appearing in Problem 8.98, so that $B_k + p^{-1}\mathbf{1}_{p-1|k} + S \in \mathbf{Z}_{(p)}$. For use momentarily, we rewrite

$$S = \sum_{0<j<k} \binom{k}{j} p B_{k-j} \frac{p^{j-1}}{j+1}.$$

By the minimality of k, we have $B_{k-j} + p^{-1}\mathbf{1}_{p-1|k-j} \in \mathbf{Z}_{(p)}$ for all j in the range $0 < j < k$. Hence, $pB_{k-j} \in \mathbf{Z}_{(p)}$ for all these j. Furthermore, $\frac{p^{j-1}}{j+1} \in \mathbf{Z}_{(p)}$ in this same range of j: To see why, note that $p^j \ge 3^j > j+1$, so that $v_p(j+1) < j$. Since $v_p(j+1)$ is an integer, $v_p(j+1) \le j-1$, and $v_p(\frac{p^{j-1}}{j+1}) \ge 0$. It follows that each term in our rewritten expression for S belongs to $\mathbf{Z}_{(p)}$, so that S itself belongs to $\mathbf{Z}_{(p)}$. But if $S \in \mathbf{Z}_{(p)}$ and $B_k + p^{-1}\mathbf{1}_{p-1|k} + S \in \mathbf{Z}_{(p)}$, then $B_k + p^{-1}\mathbf{1}_{p-1|k} \in \mathbf{Z}_{(p)}$. This contradicts the choice of k.

8.100 This is similar to Problem 8.99. Assuming the claim fails, let k be the smallest even positive integer for which $B_k + \frac{1}{2} \notin \mathbf{Z}_{(2)}$. From Exercise 8.98, $B_k + \frac{1}{2} + S \in \mathbf{Z}_{(2)}$, where

$$S = \sum_{0<j<k} \binom{k}{j} 2B_{k-j} \frac{2^{j-1}}{j+1}.$$

Let us argue that each term in this expression for S is in $\mathbf{Z}_{(2)}$ (and thus, $S \in \mathbf{Z}_2$). Let $0 < j < k$. If j is odd, then $B_{k-j} = 0$ unless $j = k-1$. The $j = k-1$ term of S is $\binom{k}{k-1} 2B_1 \frac{2^{k-2}}{k} = -2^{k-2}$, which is indeed in $\mathbf{Z}_{(2)}$. (We recalled here that $B_1 = -\frac{1}{2}$.) If j is even, the minimality of k ensures that $2B_{k-j} \in \mathbf{Z}_{(2)}$. As $\frac{2^{j-1}}{j+1}$ is also in $\mathbf{Z}_{(2)}$ (clear, as $j+1$ is odd), the jth term is 2-integral in the even case as well.

Since $S \in \mathbf{Z}_{(2)}$ and $B_k + \frac{1}{2} + S \in \mathbf{Z}_{(2)}$, we are forced to have $B_k + \frac{1}{2} \in \mathbf{Z}_{(2)}$. This contradicts the choice of k.

8.101 Let k be a positive even integer. From the last two problems we have that for every prime p,

$$B_k + \frac{\mathbf{1}_{p-1|k}}{p} \in \mathbf{Z}_{(p)}.$$

Put

$$\hat{B}_k := B_k + \sum_{p:\ p-1|k} \frac{1}{p}.$$

Then for every prime p,

$$\hat{B}_k = \left(B_k + \frac{\mathbf{1}_{p-1|k}}{p} \right) + \sum_{\substack{\ell \text{ prime},\ \ell \neq p \\ \ell - 1 | k}} \frac{1}{\ell} \in \mathbf{Z}_{(p)}.$$

Hence, $\hat{B}_k \in \bigcap_p \mathbf{Z}_{(p)} = \mathbf{Z}$.

Remark. Let D_k denote the denominator of B_k in lowest terms. The Clausen–von Staudt theorem implies that when k is a positive even integer, D_k is the product of the primes p for which $p - 1 \mid k$. (So in particular D_k is a multiple of 6 for all even $k > 0$.) It was realized by Erdős and Wagstaff [2] that this characterization of D_k allows one to establish strong statistical results. For example, enlisting methods from analytic number theory — specifically, the field known as the "anatomy of integers" — they showed that if $D = D_k$ for some positive even k, then the limit

$$p_D := \lim_{x \to \infty} \frac{\#\{\text{even positive } n \leq x \colon D_n = D\}}{\#\{\text{even positive } n \leq x\}}$$

exists and is positive. That is, any D appearing as a denominator of an even-indexed Bernoulli number actually appears with a well-defined, positive limiting frequency. Furthermore,

$$\sum_{D \geq 1} p_D = 1.$$

More recent work on the distribution of the p_D can be found in the article [3] of Pomerance and Wagstaff; among other things, they re-prove (in stronger form) a

theorem of Sunseri that 6 is the most popular denominator among even-indexed Bernoulli numbers.

8.102 Since u is a unit in $\mathbf{Z}_p$, it is also a unit modulo every power of $p\mathbf{Z}_p$. Setting $x_n = u^{p^n}$, Euler's theorem yields

$$x_{n+1} - x_n = x_n(u^{p^{n+1}-p^n} - 1) = x_n(u^{\varphi(p^{n+1})} - 1) \equiv 0 \pmod{p^{n+1}\mathbf{Z}_p},$$

for each $n = 1, 2, 3, \ldots$. (We may appeal to Euler's theorem here since the unit groups of $\mathbf{Z}_p$ mod powers of $p\mathbf{Z}_p$ are "the same" as the unit groups of $\mathbf{Z}$ mod powers of p, by Problem 5.62.) Hence, $|x_{n+1} - x_n|_p \le p^{-n-1}$ for each n, and $\{x_n\}$ is a Cauchy sequence in $\mathbf{Z}_p$.

Let $x = \lim x_n$. Since $\lim x_{n+1} = \lim x_n^p = (\lim x_n)^p = x^p$, and $\lim x_{n+1} = \lim x_n = x$, it follows that $x^p = x$.

By Fermat's little theorem, each $x_n = u^{p^n} \equiv u^{p^{n-1}} \equiv \cdots \equiv u^p \equiv u \pmod{p\mathbf{Z}_p}$, Therefore, $x \equiv u \pmod{p\mathbf{Z}_p}$ (cf. the solution to Problem 7.81), and in particular, $x \neq 0$. Thus, we have shown that $\omega(u) := x$ is a solution to $\omega(u)^{p-1} = 1$ with $\omega(u) \equiv u \bmod p\mathbf{Z}_p$.

To prove $\omega(u)$ is the *unique* $(p-1)$th root of unity congruent to u mod $p\mathbf{Z}_p$, it is enough to argue that no residue class mod $p\mathbf{Z}_p$ contains two different $(p-1)$th roots of unity. This is easy: The $(p-1)$th roots of unity $\omega(1), \ldots, \omega(p-1)$ belong to different residue classes mod $p\mathbf{Z}_p$. And these are all of the $(p-1)$th roots of unity, since the degree $p-1$ polynomial $x^{p-1} - 1$ cannot have more than $p-1$ roots in $\mathbf{Q}_p$.

8.103 In $\mathbf{Q}_3$, the element -1 is a $(3-1)$th root of unity congruent to 2 modulo $3\mathbf{Z}_3$. Therefore, $\omega(2) = -1$.

Let $p = 7$. As seen in the solution to Problem 8.102, $2^{7^{n+1}} \equiv 2^{7^n} \pmod{7^{n+1}\mathbf{Z}_7}$ for each $n \in \mathbf{Z}^+$. Hence, for all integers $k \ge 3$,

$$2^{7^k} \equiv 2^{7^{k-1}} \equiv \cdots \equiv 2^{7^2} \pmod{7^3\mathbf{Z}_7},$$

from which it follows that

$$\omega(2) = \lim 2^{7^k} \equiv 2^{7^2} \pmod{7^3\mathbf{Z}_7}.$$

This information is enough to compute c_0, c_1, and c_2, provided we are willing to get our hands (or computing devices) a little dirty: $2^7 \equiv 128 \pmod{7^3}$, and $2^{7^2} \equiv 128^7 \equiv 324 \pmod{7^3}$. So the base 7 expansion of $\omega(2)$ begins the same way as that of $324 = 2 + 4 \cdot 7 + 6 \cdot 7^2$. In other words, the desired digits are $c_0 = 2, c_1 = 4$, and $c_2 = 6$.

8.104 We begin with a lemma valid over an arbitrary field of characteristic not equal to 2.

Lemma. Let F be a field of characteristic not equal to 2. If ζ is an element of order 3 in $F^\times$, then $1+\zeta$ is an element of order 6.

Proof. By assumption, ζ is a zero of T^3-1 but not $T-1$. Hence, ζ is a root of $\frac{T^3-1}{T-1} = T^2+T+1 \in F[T]$, and $1+\zeta = -\zeta^2$. Since $\mathrm{char}(F) \neq 2$, the element $-1 \in F^\times$ has order 2, while ζ^2 has order 3. Since 2 and 3 are relatively prime, $1+\zeta = (-1)\cdot\zeta^2$ has order $2\cdot 3 = 6$. ∎

Now assume that $u \in \mathbf{Z}$ has order 3 mod p. There are no elements of order 3 in $\mathbf{F}_2^\times$. Hence, p is odd, and we can invoke our lemma to deduce that $1+u$ has order 6 in $\mathbf{F}_p^\times$. In particular, $p \equiv 1 \pmod 6$, as the order of each element in $\mathbf{F}_p^\times$ necessarily divides $p-1$; this congruence will be needed shortly.

Continuing, observe that

$$\omega(u)^3 = (\lim_{n\to\infty} u^{p^n})^3 = \lim_{n\to\infty} (u^3)^{p^n} = \omega(u^3).$$

Here $\omega(u^3)$ is the unique $(p-1)$th root of unity congruent to u^3 mod $p\mathbf{Z}_p$. But 1 is a $(p-1)$th root of unity, and $1 \equiv u^3 \pmod{p\mathbf{Z}_p}$. Thus, $1 = \omega(u^3) = \omega(u)^3$. If $\omega(u) = 1$, then $u \equiv \omega(u) \equiv 1 \pmod{p\mathbf{Z}_p}$, contradicting that u has order 3 modulo p. So $\omega(u)$ is an element of order 3 in $\mathbf{Q}_p^\times$ and, applying the lemma a second time, $1+\omega(u)$ is an element of order 6.

In particular, $1+\omega(u)$ is a $(p-1)$th root of unity (since $6 \mid p-1$). Furthermore, $1+\omega(u) \equiv 1+u \pmod{p\mathbf{Z}_p}$. Therefore, $1+\omega(u) = \omega(1+u)$.

Extra Exploration 21 ($(\mathbf{Z}/p)^\times$ is cyclic, revisited, or *sledgehammer swats fly*). For this exercise (only), you are asked to "forget" the general result that finite subgroups of multiplicative groups of fields are always cyclic.*

(a) Show that the mapping $u \bmod p \mapsto \omega(u)$ sets up an isomorphism between $(\mathbf{Z}/p)^\times$ and the group μ_{p-1} of $(p-1)$th roots of unity in $\mathbf{Q}_p$. This map is known as the Teichmüller lift.

(b) Let $\zeta = \mathrm{e}^{2\pi\mathrm{i}/(p-1)} \in \mathbf{C}$. Explain why the minimal polynomial of ζ over $\mathbf{Q}$ divides $T^{p-1}-1$. Then deduce from (a) that said minimal polynomial splits over $\mathbf{Q}_p$. Conclude that $\mathbf{Q}(\zeta)$ embeds into $\mathbf{Q}_p$.

(c) Prove that the image of ζ under any of the embeddings in (b) generates μ_{p-1}. Hence, μ_{p-1} and $(\mathbf{Z}/p)^\times$ are cyclic.

This unusual argument is due to Matt Baker [1].

* "Please forget everything you have learned at school, because you haven't learned it. Please keep in mind everywhere the corresponding portions of your school work, because you haven't actually forgotten them." — Edmund Landau

References

1. M. Baker, *Primitive roots, discrete logarithms, and p-adic numbers.* URL: `https://mattbaker.blog/2013/11/07/primitive-roots-discrete-logarithms-and-the-interplay-between-p-adic-and-complex-numbers/`
2. P. Erdős and S. S. Wagstaff, Jr., *The fractional parts of the Bernoulli numbers.* Illinois J. Math. **24** (1980), 104—112.
3. C. Pomerance and S. S. Wagstaff, Jr., *The denominators of the Bernoulli numbers.* Acta Arith. **209** (2023), 1–15.

Solutions to Set #9

9.105 Let $a \in \mathbf{Z}_p^\times$. If $a = x^2$ for some $x \in \mathbf{Q}_p$, then $|x|_p^2 = |a|_p = 1$. Therefore, $|x|_p = 1$; in particular, $x \in \mathbf{Z}_p$. Reducing the equation $x^2 = a$ modulo the ideal $p\mathbf{Z}_p$ shows that $a \bmod p\mathbf{Z}_p$ is a square in $\mathbf{Z}_p/p\mathbf{Z}_p$. Now recall from Exercise 5.62 that the inclusion of $\mathbf{Z}$ into $\mathbf{Z}_p$ induces an isomorphism between $\mathbf{Z}/p$ and $\mathbf{Z}_p/p\mathbf{Z}_p$ and that this isomorphism identifies $a_1 \bmod p$ with $a \bmod p\mathbf{Z}_p$. Since $a \bmod p\mathbf{Z}_p$ is a square in $\mathbf{Z}_p/p\mathbf{Z}_p$, it follows that $a_1 \bmod p$ is a square in $\mathbf{Z}/p$.

Conversely, suppose $a \in \mathbf{Z}_p^\times$ and that $a_1 \bmod p$ is a square in $\mathbf{Z}/p$. Then $a \bmod p\mathbf{Z}_p$ is a square in $\mathbf{Z}_p/p\mathbf{Z}_p$ and we can choose $r_1 \in \mathbf{Z}_p$ with $r_1^2 \equiv a \pmod{p\mathbf{Z}_p}$. We construct a $\mathbf{Z}_p$-solution to $x^2 = a$ following the iterative procedure of Problem 7.91.

Let $k \in \mathbf{Z}^+$. Suppose we have a mod $p^k\mathbf{Z}_p$-solution $r_k \bmod p^k\mathbf{Z}_p$ to $x^2 = a$; we lift this to a mod $p^{k+1}\mathbf{Z}_p$ solution. Expanding, $(r_k + p^k q)^2 \equiv r_k^2 + 2p^k r_k q \pmod{p^{k+1}\mathbf{Z}_p}$. The right-hand side is congruent to $a \bmod p^{k+1}\mathbf{Z}_p$ precisely when

$$2p^k r_k q \equiv a - r_k^2 \pmod{p^{k+1}\mathbf{Z}_p}.$$

By construction, $a - r_k^2 \in p^k\mathbf{Z}_p$, so we can rewrite the last congruence as

$$2r_k q \equiv \frac{a - r_k^2}{p^k} \pmod{p\mathbf{Z}_p}.$$

Since p is odd, 2 is invertible in $\mathbf{Z}_p$. As $r_k^2 \equiv a \pmod{p\mathbf{Z}_p}$ and $a \notin p\mathbf{Z}_p$, we have $r_k \notin p\mathbf{Z}_p$. So r_k is invertible in $\mathbf{Z}_p$, and the last displayed congruence is equivalent to

$$q \equiv \frac{a - r_k^2}{2p^k r_k} \bmod p\mathbf{Z}_p.$$

So if we put $r_{k+1} = r_k + p^k \frac{a-r_k^2}{2p^k r_k} = r_k + \frac{a-r_k^2}{2r_k}$, then $r_{k+1} \bmod p^{k+1}\mathbf{Z}_p$ is a lift of $r_k \bmod p^k\mathbf{Z}_p$ to a mod $p^{k+1}\mathbf{Z}_p$ solution of $x^2 = a$.

Assume $r_1, r_2, r_3, \ldots$ have been determined by the above procedure. Since $r_{k+1} \bmod p^{k+1}\mathbf{Z}_p$ is a lift of $r_k \bmod p^k\mathbf{Z}_p$, we have $|r_{k+1} - r_k|_p \leq p^{-k}$. Thus, $\{r_k\}$ is a Cauchy sequence of elements of $\mathbf{Z}_p$. Let $x = \lim r_k$, which belongs to

$\mathbf{Z}_p$. By construction, $|r_k^2 - a|_p \leq p^{-k}$. Thus, $r_k^2 \to a$. Since r_k^2 also tends to x^2, we conclude that $x^2 = a$.

Remark. By a small modification of the argument, we can choose our mod $p^k\mathbf{Z}_p$ solutions r_k to all be rational integers. Then their limit x is simply $(r_1 \bmod p, r_2 \bmod p^2, r_3 \bmod p^3, \dots) \in \mathbf{Z}_p$.

9.106 By Problem 9.105, the map $\phi\colon \mathbf{Z}_p^\times \to \{\pm 1\}$ that sends a to $\left(\frac{a_1}{p}\right)$ is a homomorphism with kernel $(\mathbf{Z}_p^\times)^2$. This homomorphism is onto, as 1 is sent to 1 and any $n \in \mathbf{Z}$ with $\left(\frac{n}{p}\right) = -1$ is sent to -1. Therefore, the two cosets of $(\mathbf{Z}_p^\times)^2$ in $\mathbf{Z}_p^\times$ are $\phi^{-1}(1) = (\mathbf{Z}_p^\times)^2$ and $\phi^{-1}(-1) = n(\mathbf{Z}_p^\times)^2$, establishing the first claim.

Every $x \in \mathbf{Q}_p^\times$ has a unique representation in the form $p^v u$ where $v \in \mathbf{Z}$ and $u \in \mathbf{Z}_p^\times$. Identifying $p^v u$ with (v, u) sets up an isomorphism $\mathbf{Q}_p^\times \cong \mathbf{Z} \times \mathbf{Z}_p^\times$, which after quotienting by squares becomes $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2 \cong \mathbf{Z}/2 \times \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^2$. In this last isomorphism, $1, p, n, np$ are sent to the four distinct elements of $\mathbf{Z}/2 \times \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^2$. Hence, $1, p, n$, and np are coset representatives for $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$.

9.107 Assume $a \in \mathbf{Z}_2^\times$. Then a is a square in $\mathbf{Q}_2 \iff a$ is a square in $\mathbf{Z}_2$ (cf. the solution to Problem 9.105).

If $a = x^2$ with $x \in \mathbf{Z}_2$, and $a \in \mathbf{Z}_2^\times$, then $x \in \mathbf{Z}_2^\times$. Hence, $x \equiv 1, 3, 5,$ or $7 \pmod{8\mathbf{Z}_2}$. In each of these cases, $x^2 \equiv 1 \pmod{8\mathbf{Z}_2}$, and so $a \equiv 1 \pmod{8\mathbf{Z}_2}$.

Conversely, suppose that $a \equiv 1 \pmod{8\mathbf{Z}_2}$ and write $a = 1 + 8b$. Any square root of a in $\mathbf{Z}_2$ must have the form $1 + 2y$, for some $y \in \mathbf{Z}_2$. As $(1 + 2y)^2 = a \iff y^2 + y = 2b$, it suffices to prove that $y^2 + y = 2b$ has a solution $y \in \mathbf{Z}_2$. This we do following the method of Problem 9.105.

To get started, the residue class 0 mod $2\mathbf{Z}_2$ is a mod $2\mathbf{Z}_2$-solution to $y^2 + y = 2b$. Suppose we have already found a mod $2^k\mathbf{Z}_2$ solution $r_k \bmod 2^k\mathbf{Z}_2$ to $y^2 + y = 2b$, where $k \in \mathbf{Z}^+$. We proceed to lift this to a mod $2^{k+1}\mathbf{Z}_2$ solution. Expanding, $(r_k + 2^k q)^2 + (r_k + 2^k q) \equiv r_k^2 + r_k + 2^k q \pmod{2^{k+1}\mathbf{Z}_2}$. The right-hand side is congruent to $2b$ modulo $2^{k+1}\mathbf{Z}_2$ precisely when

$$2^k q \equiv 2b - (r_k^2 + r_k).$$

By construction, $2b - (r_k^2 + r_k) \in 2^k\mathbf{Z}_2$, and so this last congruence can be rewritten as

$$q \equiv \frac{2b - (r_k^2 + r_k)}{2^k} \pmod{2\mathbf{Z}_2}.$$

So if we put $r_{k+1} = r_k + 2^k \frac{2b - (r_k^2 + r_k)}{2^k} = 2b - r_k^2$, then $r_{k+1} \pmod{2^{k+1}\mathbf{Z}_2}$ is a suitable lift.

The rest of the solution is essentially the same as that of Problem 9.105.

9.108 By Problem 9.107, the homomorphism from $\mathbf{Z}_2^\times$ to $(\mathbf{Z}_2/8\mathbf{Z}_2)^\times$ sending a to $a \bmod 8\mathbf{Z}_2$ has kernel $(\mathbf{Z}_2^\times)^2$. As this homomorphism is easily seen to be surjective, $\mathbf{Z}_2^\times/(\mathbf{Z}_2^\times)^2 \cong (\mathbf{Z}_2/8\mathbf{Z}_2)^\times = \{1 \bmod 8\mathbf{Z}_2, 3 \bmod 8\mathbf{Z}_2, 5 \bmod 8\mathbf{Z}_2, 7 \bmod 8\mathbf{Z}_2\}$. Hence, $1, 3, 5$, and 7 are coset representatives for $(\mathbf{Z}_2/8\mathbf{Z}_2)^\times$. Noting that each element of $\mathbf{Q}_2^\times$ has a unique representation in the form $2^v u$, with $v \in \mathbf{Z}$ and $u \in \mathbf{Z}_2^\times$, we conclude that

$$1,\ \ 3,\ \ 5,\ \ 7,\ \ 2\cdot 1,\ \ 2\cdot 3,\ \ 2\cdot 5,\ \ 2\cdot 7$$

are coset representatives for $\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2$. (See the solution to Problem 9.106 for further details on this last step.)

Extra Exploration 22. Characterize the elements of $\mathbf{Z}_p$ that can be written as $x^2 - y^2$ for $x, y \in \mathbf{Z}_p$. Then do the same for $x^2 + y^2$ (harder). For the latter problem, start by showing that every element of $\mathbf{Z}/p$ is a sum of two squares.

9.109 Let $a \in \mathbf{Q}_p^\times$ and write $a = p^v u$ with $u \in \mathbf{Z}_p^\times$. If $a = x^n$ for some $x \in \mathbf{Q}_p$, then $n \mid nv_p(x) = v_p(a) = v$. For this to hold for infinitely many n requires $v = 0$, so that $a = p^v u = u \in \mathbf{Z}_p^\times$. This proves the "$\Longleftarrow$" implication: If $\sqrt[n]{a} \in \mathbf{Q}_p$ for infinitely many n, then $a \in \mathbf{Z}_p^\times$.

Now suppose that $a \in \mathbf{Z}_p^\times$. It suffices to show that if ℓ is any prime not dividing $p(p-1)$, then a is an ℓth power in $\mathbf{Q}_p$.

Since $\ell \nmid p - 1 = \#(\mathbf{Z}_p/p\mathbf{Z}_p)^\times$, the ℓth power map is an automorphism of $(\mathbf{Z}_p/p\mathbf{Z}_p)^\times$. So we can find an $r_1 \in \mathbf{Z}_p^\times$ with $r_1^\ell \equiv a \bmod p\mathbf{Z}_p$. We take $r_1 \bmod p\mathbf{Z}_p$ as our starting point in the method of successive approximation.

Assume we know a $\bmod p^k\mathbf{Z}_p$-solution to $x^\ell = a$, say $r_k \bmod p^k\mathbf{Z}_p$. We seek a $\bmod p^{k+1}\mathbf{Z}_p$-solution $r_{k+1} \bmod p^{k+1}\mathbf{Z}_p$. Expanding, $(r_k + p^k q)^\ell \equiv r_k^\ell + \ell r_k^{\ell-1} p^k q \pmod{p^{k+1}\mathbf{Z}_p}$. For the right-hand expression to agree with $a \bmod p^{k+1}$, we require that $\ell r_k^{\ell-1} p^k q \equiv a - r_k^\ell \pmod{p^{k+1}\mathbf{Z}_p}$, or equivalently

$$\ell r_k^{\ell-1} q \equiv \frac{a - r_k^\ell}{p^k} \pmod{p\mathbf{Z}_p}.$$

Both r_k and ℓ belong to $\mathbf{Z}_p^\times$. (We use here that $a \in \mathbf{Z}_p^\times$ and that ℓ is a prime distinct from p.) So we can satisfy this congruence with any $q \equiv \frac{a - r_k^\ell}{p^k \ell r_k^{\ell-1}}$ modulo $p\mathbf{Z}_p$. In particular, $r_{k+1} = r_k + p^k \frac{a - r_k^\ell}{p^k \ell r_k^{\ell-1}} = r_k + \frac{a - r_k^\ell}{\ell r_k^{\ell-1}}$ yields a suitable lift.

Assume $r_1, r_2, r_3, \ldots$ are chosen according to the above procedure. Each $|r_{k+1} - r_k| \le p^{-k-1}$, so that the $\{r_k\}$ form a Cauchy sequence in $\mathbf{Z}_p$ with a limit $x \in \mathbf{Z}_p$. Since $r_k \to x$, and taking ℓth powers preserves limits, $r_k^\ell \to x^\ell$. On the other hand, each $|r_k^\ell - a| \le p^{-k}$, so that $r_k^\ell \to a$. Therefore, $x^\ell = a$.

9.110 Let R be any commutative ring. If $F(T) \in R[T]$, then

$$F(X) - F(Y) \equiv F(Y) - F(Y) \equiv 0 \pmod{(X-Y)R[X,Y]}.$$

So we can write $F(X) - F(Y) = (X-Y)G(X,Y)$ for some $G(X,Y) \in R[X,Y]$.

If $G(X,Y) \in \mathbf{Z}[X,Y]$ is the polynomial corresponding to our $F(T) \in \mathbf{Z}[T]$, then

$$|F(n) - F(\alpha)|_p = |(n-\alpha)G(n,\alpha)|_p \le |n-\alpha|_p.$$

(To make the last estimate we use that G has $\mathbf{Z}_p$-coefficients and that both $n, \alpha \in \mathbf{Z}_p$.) This establishes the first claim of the problem.

Since α is a root of F, it is clear that $|F(n) - F(\alpha)|_p = |F(n)|_p$.

As F has no integer zeros, $F(n) \neq 0$, so that by the product formula, $|F(n)|_p = |F(n)|_\infty^{-1} \prod_{\text{prime } \ell \neq p} |F(n)|_\ell^{-1} \ge |F(n)|_\infty^{-1}$.

Write $F(T) = \sum_{k=0}^{d} a_k T^k$. Then

$$|F(n)|_\infty = \left| \sum_{k=0}^{d} a_k n^k \right|_\infty \le \left(\sum_{k=0}^{d} |a_k|_\infty \right) |n|_\infty^d.$$

Therefore, $|F(n)|_\infty^{-1} \ge c|n|_\infty^{-d}$ for $c := (\sum_k |a_k|_\infty)^{-1}$. (The definition of c makes sense since the a_k are not all zero.)

Remark. When $d \ge 2$ our inequality $|n-\alpha|_p \ge c|n|_\infty^{-d}$ can be improved substantially. A theorem of Mahler [3, Theorem (5,I), p. 159] allows us to replace $-d$ with $-1-\epsilon$, for any fixed $\epsilon > 0$. In this new statement, the coefficient c in front of $|n|_\infty^{-1-\epsilon}$ is now allowed to depend on both F and ϵ. Mahler's theorem is a p-adic variant of a deep result of Klaus Roth, for which Roth was awarded the Fields Medal in 1958.

The exponent $-1-\epsilon$ in Mahler's theorem is essentially best possible, since approximations to within $|n|_\infty^{-1}$ are thick on the ground. Indeed, each $\alpha \in \mathbf{Z}_p$ has a canonical expansion of the form $c_0 + c_1 p + c_2 p^2 + \dots$. If we choose $n = c_0 + c_1 p + \dots + c_{k-1} p^{k-1}$, then $|n-\alpha|_p \le p^{-k} < |n|_\infty^{-1}$ (if $n \neq 0$). Provided that α is not a nonnegative integer, varying k yields infinitely many distinct positive integers n. By a similar argument, as long as α is not a nonpositive integer, $|n-\alpha|_p < |n|_\infty^{-1}$ has infinitely many solutions in negative integers n. Therefore, $|n-\alpha|_p < |n|_\infty^{-1}$ has infinitely many integer solutions n whenever α is a nonzero element of $\mathbf{Z}_p$.

Extra Exploration 23. Let $A(T) = \sum_{k=0}^{d} a_k T^k \in \mathbf{Z}_p[T]$. It is easy to prove (and we essentially did this in our solution to Problem 9.110) that $|A(x+h) - A(x)|_p \le |h|_p$ whenever $x, h \in \mathbf{Z}_p$. Show that for $x \in \mathbf{Z}_p$ and $h \in p\mathbf{Z}_p$, this bound can be refined to

$$|A(x+h) - A(x)|_p \le K|h|_p,$$

where $K = \max_{k \ge 0} |k a_k|_p$ is the largest absolute value of any coefficient of $A'(T)$. This is a p-adic cousin of the usual mean value theorem (cf. Robert [4]).

9.111 That $\alpha := \sum_{k\geq 1} p^{k!} \in \mathbf{Z}_p$ follows from Problem 8.92. Suppose for a contradiction that α is a root of the nonconstant polynomial $F(T) \in \mathbf{Q}[T]$. We can assume $F(T)$ is irreducible over $\mathbf{Q}$ and, by clearing denominators, that $F(T) \in \mathbf{Z}[T]$.

If F has an integer root n_0, irreducibility over $\mathbf{Q}$ forces F to be linear with n_0 as its only root. In that case, $\alpha = n_0 \in \mathbf{Z}$. But this is absurd: α's canonical expansion is not eventually periodic, so that α is not even rational, let alone a rational integer.

We can therefore apply the result of Exercise 9.110. Let c be the constant associated with F in that problem. For each n, let $r_n = \sum_{k=1}^{n} p^{k!} \in \mathbf{Z}$. Then $|r_n - \alpha|_p = |\sum_{k>n} p^{k!}|_p \leq p^{-(n+1)!}$. Also, $|r_n|_\infty \leq 2p^{n!}$; here we use that the largest term in the sum defining r_n is $p^{n!}$ and that each term in that sum is at least twice the preceding one. Therefore,

$$p^{-(n+1)!} \geq |r_n - \alpha|_p \geq c|r_n|_\infty^{-d} \geq c \cdot 2^{-d} p^{-dn!}.$$

Rearranging,

$$p^{n!(d-(n+1))} \geq c \cdot 2^{-d}.$$

But the right-hand side is a positive quantity independent of n, while the left-hand side tends to 0 as n tends to infinity. Contradiction!

9.112 Given $x \in \mathbf{Z}_{10}$, define the $\mathbf{Z}_2$ and $\mathbf{Z}_5$-reductions of x as the first and second components of the image of x under the isomorphism $\mathbf{Z}_{10} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$ described in the solution to Problem 5.63. Concretely, if $x = (a_1 \bmod 10, a_2 \bmod 10^2, \dots)$, its $\mathbf{Z}_2$-reduction is $(a_1 \bmod 2, a_2 \bmod 2^2, \dots)$, and its $\mathbf{Z}_5$-reduction is $(a_1 \bmod 5, a_1 \bmod 5^2, \dots)$.

Convergence in $\mathbf{Z}_{10}$ can then be defined in terms of convergence in $\mathbf{Q}_2$ and $\mathbf{Q}_5$. If $\{x_n\}$ is a sequence of elements of $\mathbf{Z}_{10}$, and $x \in \mathbf{Z}_{10}$, we say $x_n \to x$ in $\mathbf{Z}_{10}$ if the $\mathbf{Z}_2$ and $\mathbf{Z}_5$-reductions of the x_n converge to the $\mathbf{Z}_2$ and $\mathbf{Z}_5$-reductions of x (in $\mathbf{Q}_2$ and $\mathbf{Q}_5$).

With this definition of convergence in place, your work on Set #7 can be adapted to show that every element of $\mathbf{Z}_{10}$ has a unique, convergent 10-adic expansion $\sum_{k\geq 0} d_k \cdot 10^k$ with each $d_k \in \{0, 1, 2, \dots, 9\}$. (Check this!)

Clearly, $2^{4 \cdot 5^n} \to 0$ in $\mathbf{Z}_2$. By Exercise 7.81, $2^{4 \cdot 5^n} \to 1$ in $\mathbf{Z}_5$. So the $\mathbf{Z}_{10}$ limit x of $2^{4 \cdot 5^n}$ corresponds, under our isomorphism, to $(0, 1) \in \mathbf{Z}_2 \times \mathbf{Z}_5$. Write the 10-adic expansion of x as $\sum_{k\geq 0} d_k \cdot 10^k$ and assume for a contradiction that the sequence $\{d_k\}$ is eventually periodic, say $d_k = d_{k+\ell}$ for all $k \geq k_0$. Working in $\mathbf{Z}_2$, we find that the $\mathbf{Z}_2$-reduction of x is

$$\sum_{0\le k<k_0} 10^k + \sum_{k_0\le k<k_0+\ell} d_k\cdot 10^k(1+10^\ell+10^{2\ell}+\dots)$$
$$= \sum_{0\le k<k_0} 10^k + \sum_{k_0\le k<k_0+\ell} \frac{d_k\cdot 10^k}{1-10^\ell}.$$

Let r be the rational number defined by the right-hand side. The exact same calculation shows that the $\mathbf{Z}_5$-reduction of x is also r. It follows that $x=\sum_{k\ge 0} d_k\cdot 10^k$ is the element of $\mathbf{Z}_{10}$ corresponding under our isomorphism to $(r,r)\in \mathbf{Z}_2\times\mathbf{Z}_5$. But we saw already that x corresponds to $(0,1)$. Contradiction!

Extra Exploration 24. Say that the infinite sequence of decimal digits d_0, d_1, d_2, $d_3,\dots$ is self-squaring if, for every $k\in\mathbf{Z}^+$,

$$(d_0+d_1\cdot 10+\cdots+d_{k-1}\cdot 10^{k-1})^2 \equiv d_0+d_1\cdot 10+\cdots+d_{k-1}\cdot 10^{k-1} \pmod{10^k}.$$

For example, the two sequences $0,0,0,0,\dots$ (all zeros) and $1,0,0,0,\dots$ (all zeros past the first term) are trivially self-squaring.

(a) Prove that there is a unique self-squaring sequence starting with $d_0=6$.
(b) Show that the sequence in (a) begins 6, 7, 3, 9, 0, 1, 7, 8, 7, 1. (As a spot check, $76^2=5\underline{776}$, while $109376^2=11963\underline{109376}$.)
(c) How many self-squaring sequences are there?

Extra Exploration 25 (Shapiro and Shapiro [6]). Let $a_1,a_2,a_3,\dots$ be an arbitrary sequence of positive integers. Show that for every $g\in\mathbf{Z}^+$, the sequence $a_1, a_1^{a_2}, a_1^{a_2^{a_3}},\dots$ stabilizes modulo g. Deduce that for each $g>1$, this same sequence converges in $\mathbf{Z}_g$. (Define convergence in $\mathbf{Z}_g$ by mimicking what we did for $\mathbf{Z}_{10}$ above.)

Extra Exploration 26 (continuation). Let a be a positive integer not divisible by 10. By Extra Exploration 25, for each $k\in\mathbf{Z}^+$ the residue class mod 10^k of $a, a^a, a^{a^a},\dots$ eventually stabilizes. Let x_k be the least nonnegative integer in the limiting residue class mod 10^k, so that $0\le x_k<10^k$.

(a) Show that for each $k\ge 2$, we have $a^{x_k}\equiv x_k \pmod{10^k}$.
(b) Let $a=73$. Compute x_{33}, by hook or by crook, and thereby show that

$$73^{990485815519399724778909194186633} = \dots 990485815519399724778909194186633.$$

For more on this theme, see the papers of Jiménez Urroz & Yebra [2] and Germain [1].

9.113 The first equivalence is immediate from Problem 8.92.

Turning to the second: If $x\in\mathbf{Z}_p$, then $|a_nx^n|_p\le |a_n|_p$ for all n. So if $|a_n|_p\to 0$, then $\sum_{n\ge 0} a_nx^n$ converges for all $x\in\mathbf{Z}_p$.

Conversely, suppose that $\sum_{n\ge 0} a_nx^n$ converges for all $x\in\mathbf{Z}_p$. Then $\sum_{n\ge 0} a_n$ converges (the case $x=1$), so that $|a_n|_p\to 0$.

Extra Exploration 27. Check that the Strassmann series form a subring of $\mathbf{Q}_p[[T]]$. This ring is commonly denoted $\mathbf{Q}_p\langle T\rangle$ and referred to as the Tate algebra in one variable over $\mathbf{Q}_p$. Show that for each $z \in \mathbf{Z}_p$, the evaluation map $\mathrm{eval}_z \colon \mathbf{Q}_p\langle T\rangle \to \mathbf{Q}_p$ sending $F(T)$ to $F(z)$ is a ring homomorphism.

9.114 Since $F(T)$ is a Strassmann series, its coefficients a_n tend to 0. In particular, $\{|a_n|_p\}$ is bounded, and $p^k F(T) \in \mathbf{Z}_p[[T]]$ for a certain integer k. Since F and $p^k F$ have the same zeros, we can (and will) assume that $F(T) \in \mathbf{Z}_p[[T]]$ to start with.

Let m be the smallest nonnegative integer for which $a_m \neq 0$ and let $\delta = |a_m|_p$. Note that $\delta \leq 1$, since $F(T) \in \mathbf{Z}_p[[T]]$. If $0 < |x|_p < \delta$, then

$$\left| \sum_{n>m} a_n x^n \right|_p \leq \max_{n>m} |a_n x^n|_p \leq |x|_p^{m+1} < \delta |x|_p^m = |a_m x^m|_p = \left| \sum_{n=0}^{m} a_n x^n \right|_p.$$

Therefore,

$$|F(x)|_p = \left| \sum_{n=0}^{m} a_n x^n + \sum_{n>m} a_n x^n \right|_p \geq \left| \sum_{n=0}^{m} a_n x^n \right|_p - \left| \sum_{n>m} a_n x^n \right|_p > 0,$$

so that $F(x) \neq 0$.

As a consequence, if $F(T)$ is Strassmann and not the zero series in $\mathbf{Q}_p[[T]]$, then $F(p^m)$ is nonzero for all sufficiently large m (specifically, for any m with $p^{-m} < \delta$). Hence, a Strassmann series that vanishes everywhere on $\mathbf{Z}_p$ must be the zero series.

9.115 Substituting and applying the binomial theorem, we find that whenever $x, x_0 \in \mathbf{Z}_p$,

$$F(x + x_0) = \sum_{k \geq 0} a_k (x + x_0)^k = \sum_{k \geq 0} \sum_{j \geq 0} \mathbf{1}_{k \geq j} a_k \binom{k}{j} x^j x_0^{k-j}.$$

We would like to reverse the order of summation. To justify this we appeal to the criterion of Exercise 8.96. Put $u_{k,j} = \mathbf{1}_{k \geq j} a_k \binom{k}{j} x^j x_0^{k-j}$. If we set $\epsilon_N = \max_{k \geq N} |a_k|_p$, then $|u_{k,j}|_p \leq \epsilon_N$ whenever $k \geq N$ or $j \geq N$. Since $F(T)$ is a Strassmann series, $\epsilon_N \to 0$ as $N \to \infty$, and so the conditions of Exercise 8.96 are satisfied. Therefore,

$$F(x + x_0) = \sum_k \sum_j u_{k,j} = \sum_j \sum_k u_{k,j} = \sum_{j \geq 0} \left(\sum_{k \geq j} a_k \binom{k}{j} x_0^{k-j} \right) x^j.$$

Here the coefficient of x^j is precisely the claimed coefficient b_j.

Since $\sum_{j\geq 0} b_j x^j$ converges for all $x \in \mathbf{Z}_p$ (to $F(x+x_0)$), $\sum_{j\geq 0} b_j T^j$ is a Strassmann series.

9.116 Let $F(T)$ be a Strassmann series, $F(T) \neq 0$. Suppose for a contradiction that F has an infinite number of zeros in $\mathbf{Z}_p$, and let $x_1, x_2, x_3, \ldots$ be a sequence of distinct zeros. As $\mathbf{Z}_p$ is compact (Problem 6.76), there is an $x_0 \in \mathbf{Z}_p$ such that some subsequence of $\{x_n\}$ converges to x_0.

Problem 9.115 describes how to construct a Strassmann series $G(T)$ with $G(x) = F(x+x_0)$ for every $x \in \mathbf{Z}_p$. By the choice of x_0, every open disc centered at x_0 contains infinitely many zeros of F. Hence, every open disc centered at 0 contains infinitely many zeros of G. This contradicts Exercise 9.114 unless $G(T) = 0$ in $\mathbf{Q}_p[[T]]$. But that's impossible: If $G(T) = 0$, then $F(x) = G(x - x_0) = 0$ for all $x \in \mathbf{Z}_p$. But a nonzero Strassmann series such as $F(T)$ cannot vanish on all of $\mathbf{Z}_p$ (Exercise 9.115).

Extra Exploration 28. We assume familiarity with infinite products, as defined in Extra Exploration 20. Let $c_1, c_2, c_3, \ldots$ be a sequence of elements of $\mathbf{Q}_p$ tending to 0. By Extra Exploration 20, the infinite product $\prod_{j=1}^{\infty}(1 - c_j x)$ determines a well-defined element of $\mathbf{Q}_p$ for all $x \in \mathbf{Q}_p$. Write down a power series $F(T) \in \mathbf{Q}_p[[T]]$ with the property that $F(x) = \prod_{j=1}^{\infty}(1 - c_j x)$ for all $x \in \mathbf{Q}_p$.

Extra Exploration 29 (continuation; Schöbe [5, p. 38]). Let $e_1, e_2, e_3, \ldots$ be a sequence of positive integers. For each $x \in \mathbf{Q}_p$, let $A(x) = \prod_{j=1}^{\infty}(1 - (p^j x)^{p-1})^{e_j}$.

(a) Prove that $A(x)$ is a well-defined function from $\mathbf{Q}_p$ to $\mathbf{Q}_p$ and that $A(x)$ can be represented by an everywhere convergent power series with $\mathbf{Q}_p$-coefficients.

(b) Show that $|A(x)|_p = 1$ if $x \in \mathbf{Z}_p$.

(c) Suppose $|x|_p = p^r$, where r is a positive integer. Show that $|A(x)|_p \leq p^{-e_r} \prod_{j=1}^{r-1} p^{(r-j)(p-1)e_j}$.

(d) Describe a method of choosing $e_1, e_2, e_3, \ldots$ that guarantees $|A(x)|_p \leq |x|_p^{-1}$ whenever $x \in \mathbf{Q}_p \setminus \mathbf{Z}_p$.

(e) Deduce from (a)–(d) that there is an power series over $\mathbf{Q}_p$ that converges everywhere and induces a bounded but nonconstant function from $\mathbf{Q}_p$ to $\mathbf{Q}_p$. For those who have taken a complex variables course: Explain how this suggests $\mathbf{Q}_p$ is more analogous to $\mathbf{R}$ than to $\mathbf{C}$.

9.117 When $p = 2$, neither statement holds. So assume p is odd.

By Problem 7.90, $\frac{(p-1)!+1}{p} \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p}$. So it suffices to show that $\sum_{a=1}^{p-1} q_p(a) - (B_{p-1} + \frac{1}{p} - 1) \in p\mathbf{Z}_{(p)}$.

By Faulhaber's formula,

$$\sum_{a=1}^{p-1} q_p(a) = \frac{S_{p-1}(p)}{p} - \frac{p-1}{p} = B_{p-1} + \frac{1}{p} - 1 + \sum_{j=1}^{p-1} \binom{p-1}{j} B_{p-1-j} \frac{p^j}{j+1}.$$

For each $j = 1, 2, 3, \ldots, p-1$, the Bernoulli number $B_{p-1-j} \in \mathbf{Z}_{(p)}$; this is clear for $j = p-1$ (recall that $B_0 = 1$) and for $j < p-1$ it follows from Exercise 8.99. In this same range of j, we have $p^j \geq 3^j > j+1$. Thus, $v_p(j+1) < j$, and $v_p(\frac{p^j}{j+1}) = j - v_p(j+1) > 0$. Consequently, each term in our sum on j belongs to $p\mathbf{Z}_{(p)}$, implying that the sum itself belongs to $p\mathbf{Z}_{(p)}$. But that sum is precisely $\sum_{a=1}^{p-1} q_p(a) - (B_{p-1} + \frac{1}{p} - 1)$.

9.118 By Problem 8.104 and its solution, $p \equiv 1 \pmod 6$ and $\omega(1+u) = 1 + \omega(u)$. Write $v = \omega(u) + p^k q$, where $q \in \mathbf{Z}_p$. Since p is odd and $p \mid \binom{p}{k}$ for all k between 0 and p,

$$\begin{aligned} v^p = (\omega(u) + p^k q)^p &\equiv \omega(u)^p + \omega(u)^{p-1} p^{k+1} q \pmod{p^{2k+1} p\mathbf{Z}_p} \\ &\equiv \omega(u) + p^{k+1} q \pmod{p^{2k+1} p\mathbf{Z}_p}. \end{aligned}$$

On the other hand, $1 + v = 1 + \omega(u) + p^k q = \omega(u+1) + p^k q$, and (by analogous reasoning to what is displayed above)

$$(1+v)^p \equiv \omega(u+1) + p^{k+1} q \pmod{p^{2k+1} p\mathbf{Z}_p}.$$

Using once more that $1 + \omega(u) = \omega(u+1)$, we deduce that $(1+v)^p \equiv 1 + v^p \pmod{p^{2k+1}\mathbf{Z}_p}$. Since both $(1+v)^p$ and $1 + v^p$ lie in $\mathbf{Z}$, this last congruence in fact holds modulo $(p^{2k+1}\mathbf{Z}_p) \cap \mathbf{Z} = p^{2k+1}\mathbf{Z}$.

Let $p = 7$. In the course of solving Problem 8.103, we computed that $\omega(2) \equiv 324 \pmod{7^3\mathbf{Z}_7}$. Taking $v = 324$ and $k = 3$ in the result of the last paragraph "explains" the given example.

References

1. J. Germain, *On the equation $a^x \equiv x \pmod b$*. Integers **9** (2009), A47, 629–638.
2. J. Jiménez Urroz and J. L. A. Yebra, *On the equation $a^x \equiv x \pmod{b^n}$*. J. Integer Seq. **12** (2009), Article 09.8.8, 8 pp.
3. K. Mahler, *Lectures on Diophantine approximations. Part I: g-adic numbers and Roth's theorem*, Notre Dame Mathematical Lectures, vol. 7, University of Notre Dame Press, Notre Dame, 1961.
4. A. Robert, *A note on the numerators of the Bernoulli numbers*. Exposition. Math. **9** (1991), 189–191.
5. W. Schöbe, *Beiträge zur Funktionentheorie in nichtarchimedisch bewerteten Körpern*. Münster: Diss. Math. Univ. Münster, Universitas-Archiv **42**, Math. Abteilung Nr. 2 (1930), 61 pp.
6. D. B. Shapiro and S. D. Shapiro, *Iterated exponents in number theory*. Integers **7** (2007), A23, 19 pp.

Solutions to Set #10

10.119 We begin by establishing some useful arithmetic properties of the generalized binomial coefficients $\binom{\frac{1}{2}}{k}$ for nonnegative integers k.

Fix k. Let ℓ be an odd prime, and let A be a nonnegative integer with $\frac{1}{2} \equiv A \pmod{\ell^{v_\ell(k!)}\mathbf{Z}_\ell}$; e.g., $A = \frac{1}{2}(\ell^{v_\ell(k!)} + 1)$. Since $\binom{A}{k} \in \mathbf{Z}$,

$$\ell^{v_\ell(k!)} \mid k! \mid \binom{A}{k} k! = A(A-1)(A-2)\cdots(A-(k-1)),$$

where the divisibility relations are being asserted in the ring $\mathbf{Z}$. Naturally, these same relations also hold in $\mathbf{Z}_\ell$, so that working in $\mathbf{Z}_\ell$ modulo $\ell^{v_\ell(k!)}\mathbf{Z}_\ell$,

$$\frac{1}{2}\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-(k-1)\right) \equiv A(A-1)\cdots(A-(k-1)) \equiv 0.$$

It follows that $v_\ell(\frac{1}{2}(\frac{1}{2}-1)\cdots(\frac{1}{2}-(k-1))) \geq v_\ell(k!)$, so that $v_\ell(\binom{\frac{1}{2}}{k}) \geq 0$. As this holds for all odd primes ℓ, the rational number $\binom{\frac{1}{2}}{k}$ has denominator a power of 2.

To determine which power of 2, we look 2-adically. Expanding out,

$$\binom{\frac{1}{2}}{k} = \frac{1 \cdot (1-2) \cdot (1-2\cdot 2)\cdots(1-2(k-1))}{2^k k!}.$$

The numerator on the right is odd, and so the power of 2 in the denominator of $\binom{\frac{1}{2}}{k}$ is $2^{k+v_2(k!)}$.

Collecting what we know so far: $\binom{\frac{1}{2}}{k}$ is a rational number with denominator $2^{k+v_2(k!)}$.

We are now well-positioned to decide when $B_{\frac{1}{2}}(x)$ converges — equivalently, when $|\binom{\frac{1}{2}}{k}x^k|_p \to 0$ (as $k \to \infty$). For use momentarily, we recall that $v_2(k!) \leq k$, so that $k + v_2(k!) \leq 2k$.

Suppose p is odd. Then $|\binom{\frac{1}{2}}{k}|_p \le 1$, and $|\binom{\frac{1}{2}}{k}x^k|_p \le |x|_p^k$. If $|x|_p \le 1/p$, then $|x|_p^k \to 0$ as $k \to \infty$. Thus, $B_{\frac{1}{2}}(x)$ converges for these x.

Suppose instead that $p = 2$. If $x \in \mathbf{Q}_2$, then $|\binom{\frac{1}{2}}{k}x^k|_2 = 2^{k+v_2(k!)}|x|_2^k \le 2^{2k}|x|_2^k$. This last expression tends to 0 if $|x|_2 \le 1/2^3$.

These conditions on x turn out to be necessary for convergence.

Lemma. Let $F(T) \in \mathbf{Q}_p[[T]]$. If $F(x_0)$ converges ($x_0 \in \mathbf{Q}_p$), then $F(x)$ converges for all $x \in \mathbf{Q}_p$ with $|x|_p \le |x_0|_p$.

Proof. Write $F(T) = \sum_{k\ge 0} a_k T^k$. If $|a_k x_0^k|_p \to 0$, and $|x|_p \le |x_0|_p$, then $|a_k x^k|_p \to 0$. ∎

Seeking a contradiction, suppose p is odd and that $B_{\frac{1}{2}}(x_0)$ converges for a value of x_0 with $|x_0|_p > 1/p$. Then $|x_0|_p \ge 1$. Invoking the lemma, $B_{\frac{1}{2}}(x)$ converges whenever $|x|_p \le 1$, i.e., on all of $\mathbf{Z}_p$. But whenever $B_{\frac{1}{2}}(x)$ converges, it converges to a square root of $1 + x$. We infer that that every element of $\mathbf{Z}_p$ has a square root in $\mathbf{Q}_p$ — absurd!

Similarly, if $B_{\frac{1}{2}}(x)$ converges for an $x_0 \in \mathbf{Q}_2$ with $|x_0|_2 > 1/2^3$, then it converges whenever $|x|_2 \le 1/2^2$. But then $B_{\frac{1}{2}}(4)$ converges to a square root of 5 in $\mathbf{Q}_2$, whereas $5 \notin (\mathbf{Q}_2^\times)^2$!

Extra Exploration 30. Establish the following claims.

(a) If $x \in \mathbf{Z}_p$ and k is a nonnegative integer, then $\binom{x}{k} := \frac{x(x-1)\cdots(x-(k-1))}{k!} \in \mathbf{Z}_p$.
(b) If $x \in \mathbf{Q}$ and k is a positive integer, then every prime appearing in the denominator of $\binom{x}{k}$ appears in the denominator of x, and vice versa.

Extra Exploration 31. (continuation of Extra Exploration 30) Let $m \in \mathbf{Z}^+$.

(a) Show that if p is a prime not dividing m and $x \in p\mathbf{Z}_p$, then $\sum_{k\ge 0}\binom{\frac{1}{m}}{k}x^k$ converges to (one value of) $\sqrt[m]{1+x}$ in $\mathbf{Q}_p$.
(b) Now assume $p \mid m$. Show that the conclusion of (a) holds if either p is odd and $v_p(x) \ge v_p(m) + 1$, or $p = 2$ and $v_2(x) \ge v_2(m) + 2$.

10.120 When x is real and $|x| < 1$, the series $B_{\frac{1}{2}}(x)$ converges to the positive square root of $1 + x$. So over the real numbers, $B_{\frac{1}{2}}(\frac{9}{16}) = \frac{5}{4}$.

Suppose now that p is an odd prime and that $x \in p\mathbf{Z}_p$. Recalling that $\binom{\frac{1}{2}}{k} \in \mathbf{Z}_p$ for each $k = 0, 1, 2, \ldots$, we find that $|B_{\frac{1}{2}}(x) - 1|_p \le \max_{k\ge 1}|\binom{\frac{1}{2}}{k}x^k|_p \le 1/p$. Thus, $B_{\frac{1}{2}}(x) \in 1 + p\mathbf{Z}_p$.

When $p = 3$ and $x = \frac{9}{16}$, the (unique) square root of $1 + x$ belonging to $1 + 3\mathbf{Z}_3$ is $-\frac{5}{4}$.

10.121 These results are not particular to $\mathbf{Z}_p$ and $\mathbf{Q}_p$. Let D be any domain of characteristic 0 with fraction field K. (For example, we could take $D = \mathbf{Z}_p$ and $K = \mathbf{Q}_p$.) Then Taylor's formula holds for polynomials over K: If $F(T) \in K[T]$ and $a \in K$, then

$$F(a+T) = \sum_{j \geq 0} \frac{F^{(j)}(a)}{j!} T^j.$$

For the proof, fix $a \in K$. Consider $K[T]$ as a K-vector space and observe that both sides of the claimed equation represent K-linear functions of $F(T) \in K[T]$. So the identity will be established if it is shown for $F(T) = 1, T, T^2, \ldots$ (a K-basis for $K[T]$). When $F(T) = T^n$, the left-hand side is $(a+T)^n$ while the right is

$$\sum_{j \geq 0} \mathbf{1}_{n \geq j} \frac{n(n-1)(n-2)\ldots(n-(j-1))}{j!} a^{n-j} T^j = \sum_{0 \leq j \leq n} \binom{n}{j} a^{n-j} T^j.$$

This last expression is of course the binomial expansion of $(a+T)^n$.

Next, we show that if $F(T) \in D[T]$, then $\frac{1}{j!} F^{(j)}(T) \in D[T]$ for each non-negative integer j. We fix j and check the claim for $F(T) = 1, T, T^2, \ldots$ (a D-basis for $D[T]$). This is straightforward: If $F(T) = T^n$, then $\frac{1}{j!} F^{(j)}(T) = \mathbf{1}_{n \geq j} \binom{n}{j} T^{n-j} \in \mathbf{Z}[T] \subseteq D[T]$.

10.122 Taylor's formula gives $F(\tilde{x}) = \sum_{j \geq 0} \frac{1}{j!} F^{(j)}(x)(-F(x)/F'(x))^j$. The terms of the sum corresponding to $j = 0$ and $j = 1$ cancel each other out (being $F(x)$ and $-F(x)$, respectively), so that

$$|F(\tilde{x})|_p = \left| \sum_{j \geq 2} \frac{F^{(j)}(x)}{j!} \left(-\frac{F(x)}{F'(x)} \right)^j \right|_p \leq \max_{j \geq 2} \left| \frac{F^{(j)}(x)}{j!} \left(-\frac{F(x)}{F'(x)} \right)^j \right|_p.$$

Viewing $F^{(j)}(x)/j!$ as the evaluation of the polynomial $F^{(j)}(T)/j! \in \mathbf{Z}_p[T]$ at the point $x \in \mathbf{Z}_p$, it is clear that $|F^{(j)}(x)/j!|_p \leq 1$ for every j. Furthermore, $|F'(x)|_p = 1$ while $|F(x)|_p \leq 1$, so that $|(-F(x)/F'(x))^j|_p = |F(x)|_p^j \leq |F(x)|_p^2$ for each $j \geq 2$. Hence, the above maximum does not exceed $|F(x)|_p^2$.

10.123 We iteratively apply Exercise 10.122 in order to construct a Cauchy sequence of elements of $\mathbf{Z}_p$ converging to a root of F.

Let $n \in \mathbf{Z}^+$. Suppose that $x_n \in \mathbf{Z}_p$ satisfies both

$$|F(x_n)|_p < 1 \quad \text{and} \quad |F'(x_n)|_p = 1.$$

Let $x_{n+1} = x_n - \frac{F(x_n)}{F'(x_n)}$. By Exercise 10.122,

$$|F(x_{n+1})|_p \leq |F(x_n)|_p^2 < 1.$$

Furthermore, $x_{n+1} \equiv x_n \pmod{p\mathbf{Z}_p}$, implying $F'(x_{n+1}) \equiv F'(x_n) \not\equiv 0 \pmod{p\mathbf{Z}_p}$, so that

$$|F'(x_{n+1})|_p = 1.$$

Thus, the hypotheses we originally assumed for x_n hold for x_{n+1}, allowing us to reboot the procedure with x_{n+1} replacing x_n.

Starting from the given x_1, we produce in this way a sequence $\{x_n\}$ of elements of $\mathbf{Z}_p$ satisfying

$$|F(x_n)|_p \leq |F(x_{n-1})|_p^2 \leq \cdots \leq |F(x_1)|_p^{2^{n-1}} \qquad (*)$$

for each $n = 1, 2, 3, \ldots$. As $|F(x_1)|_p < 1$, (*) guarantees that $F(x_n)$ converges (rapidly!) to 0.

Observe that $|x_{n+1} - x_n|_p = |F(x_n)/F'(x_n)|_p = |F(x_n)|_p$, for every n. Therefore, $\{x_n\}$ is Cauchy, and $x_n \to x$ for some $x \in \mathbf{Z}_p$. Hence, $F(x) = F(\lim x_n) = \lim F(x_n) = 0$. (We use here that polynomials preserve limits, which follows from Exercise 3.29.)

It remains only to argue that $x \equiv x_1 \pmod{p\mathbf{Z}_p}$. This is immediate from the identity $x - x_1 = \sum_{k \geq 1}(x_{k+1} - x_k)$ expressing $x - x_1$ as a sum of terms from $p\mathbf{Z}_p$.

Extra Exploration 32 (a stronger version of Hensel's Lemma). Let $F(T) \in \mathbf{Z}_p[T]$, and suppose that $a \in \mathbf{Z}_p$ satisfies $|F(a)|_p < |F'(a)|_p^2$. Prove that starting from a, Newton's method converges to a root x of F with $|x - a|_p = |\frac{F(a)}{F'(a)}|_p < |F'(a)|_p$.

10.124 Express the $\mathbf{Q}[T]$-ideal $F(T)\mathbf{Q}[T] + F'(T)\mathbf{Q}[T]$ as $D(T)\mathbf{Q}[T]$, where $D(T) \in \mathbf{Q}[T]$. Since $F(T), F'(T) \in D(T)\mathbf{Q}[T]$, each complex root of $D(T)$ is a common zero of $F(T)$ and $F'(T)$ — in other words, a multiple root of $F(T)$.

We are given that $F(T)$ has distinct complex roots. Therefore, $D(T)$ has no complex roots, meaning that $D(T)$ is a nonzero constant. As a result, $F(T)\mathbf{Q}[T] + F'(T)\mathbf{Q}[T] = D(T)\mathbf{Q}[T] = \mathbf{Q}[T]$, and there are $X(T), Y(T) \in \mathbf{Q}[T]$ with $F(T)X(T) + F'(T)Y(T) = 1$. Choose $R \in \mathbf{Z}^+$ so that $\hat{X}(T) := RX(T), \hat{Y}(T) := RY(T) \in \mathbf{Z}[T]$. Then

$$F(T)\hat{X}(T) + F'(T)\hat{Y}(T) = R.$$

Taking this last equation mod p, we find that the mod p reductions of $F(T)$ and $F'(T)$ generate the unit ideal in $(\mathbf{Z}/p)[T]$ whenever $p \nmid R$. Hence, $F(T)$ and $F'(T)$ are coprime in $(\mathbf{Z}/p)[T]$ for each prime p not dividing R.

10.125 According to Problem 2.24, there are infinitely many primes p for which F has a root in $\mathbf{F}_p$. By Problem 10.124, there are only finitely many

primes p for which F and F' have a common root in $\mathbf{F}_p$. So for infinitely many p, we can find an $x_1 \in \mathbf{Z}$ with $F(x_1) \equiv 0 \pmod{p}$ and $F'(x_1) \not\equiv 0 \pmod{p}$. For each of these primes, F has a root in $\mathbf{Z}_p$ by Problem 10.123.

Extra Exploration 33 (bounding the number of modular roots of a polynomial). Suppose $F(T) \in \mathbf{Z}[T]$ is a nonconstant polynomial with distinct complex roots, and let R be a nonzero integer belonging to $F(T)\mathbf{Z}[T] + F'(T)\mathbf{Z}[T]$ (as in Problem 10.124).

(a) Show that if $K \geq 2v_p(R)+1$, and a is an integer with $F(a) \equiv 0 \pmod{p^K}$, then there is a root $x \in \mathbf{Z}_p$ of F with $x \equiv a \pmod{p^{K-v_p(R)}\mathbf{Z}_p}$.

(b) Continue to assume $K \geq 2v_p(R)+1$. Deduce from F having at most $\deg F$ roots in (the domain) $\mathbf{Z}_p$ that F has at most $(\deg F)p^{v_p(R)}$ roots in $\mathbf{Z}/p^K$.

(c) Finally, show that for every $m \in \mathbf{Z}^+$, the number of roots of F in $\mathbf{Z}/m$ is at most $(\deg F)^{\nu(m)}R^2$, where $\nu(m)$ is the count of distinct primes dividing m.

This bound, which finds many applications in analytic number theory, was proved independently by Nagell [2] and Ore [3] in 1921.

10.126 If F has a root $\theta' \in \mathbf{Q}_p$, let $K' = \mathbf{Q}(\theta')$ be the field generated by θ' over the copy of $\mathbf{Q}$ within $\mathbf{Q}_p$. By standard field theory, both K and K' are isomorphic to $\mathbf{Q}[T]/(F(T))$, via isomorphisms identifying θ and θ' with the class of T mod $F(T)$. Daisy chain the isomorphism $K \xrightarrow{\sim} \mathbf{Q}[T]/(F(T))$ with the isomorphism $\mathbf{Q}[T]/(F(T)) \xrightarrow{\sim} K'$ to determine an embedding of K into $\mathbf{Q}_p$.

Such a θ' exists for infinitely many p by Exercise 10.125.

10.127 Let $\phi\colon \mathbf{Q}_p \to \mathbf{Q}_p$ be a homomorphism. As every ring homomorphism sends $n \cdot 1$ to $n \cdot 1$ (for all $n \in \mathbf{Z}$), it is immediate that ϕ fixes $\mathbf{Z}$. Furthermore, for any $a, b \in \mathbf{Z}$ with $b \neq 0$, we have

$$\phi\left(\frac{a}{b}\right) b = \phi\left(\frac{a}{b}\right)\phi(b) = \phi(a) = a.$$

Thus, $\phi\left(\frac{a}{b}\right) = \frac{a}{b}$, meaning that ϕ in fact fixes all of $\mathbf{Q}$.

Now let x be an arbitrary element of $\mathbf{Q}_p$. Since $\mathbf{Q}$ is dense in $\mathbf{Q}_p$, there is a sequence of rational numbers $\{x_n\}$ for which $x_n \to x$. We will show that $\phi(x_n) \to \phi(x)$. Since each $\phi(x_n) = x_n$, and $x_n \to x$, it must be that $\phi(x) = x$. As x was arbitrary, ϕ is the identity map.

The algebraic characterization of $\mathbf{Z}_p^\times$ from Exercise 9.109 implies that ϕ maps $\mathbf{Z}_p^\times$ into $\mathbf{Z}_p^\times$. To use this, suppose $x_n - x \neq 0$ (where n is a positive integer index). Then $x_n - x = p^{v_p(x_n - x)}u_n$ for some $u_n \in \mathbf{Z}_p^\times$, and

$$\phi(x_n) - \phi(x) = \phi(x_n - x) = \phi(p^{v_p(x_n-x)})\phi(u_n) = p^{v_p(x_n-x)}u_n'$$

for some $u_n' \in \mathbf{Z}_p^\times$. Hence,

$$|\phi(x_n) - \phi(x)|_p = p^{-v_p(x_n - x)} = |x_n - x|_p.$$

Of course, the equation $|\phi(x_n) - \phi(x)|_p = |x_n - x|_p$ also holds when $x_n - x = 0$.

We are assuming $x_n \to x$. Therefore, $|\phi(x_n) - \phi(x)|_p = |x_n - x|_p \to 0$. Hence, $\phi(x_n) \to \phi(x)$, as desired.

10.128 Suppose first that p and q are odd primes with $q \neq p$. Select $n \in \mathbf{Z}$ with $\left(\frac{n}{q}\right) = -1$, and choose $a \in \mathbf{Z}$ with $a \equiv 1 \pmod{p}$ and $a \equiv n \pmod{q}$. Then a is a square in $\mathbf{Q}_p$ but not a square in $\mathbf{Q}_q$ (see Problem 9.105). Since $a \in \mathbf{Z}$, any homomorphism from $\mathbf{Q}_p$ to $\mathbf{Q}_q$ must send a to a. However, homomorphisms always send squares to squares, so no homomorphism from $\mathbf{Q}_p$ to $\mathbf{Q}_q$ can exist. If $p = 2$ and q is odd, the same argument works if we select $a \equiv 1 \pmod{8}$ and $a \equiv n \pmod{q}$ (see Problem 9.107). If p is odd and $q = 2$, choose $a \equiv 1 \pmod{p}$ and $a \equiv 3 \pmod{8}$.

The same argument works to demonstrate the impossibility of a homomorphism from $\mathbf{Q}_p$ to $\mathbf{R}$. If p is odd, select a with $a \equiv 1 \pmod{p}$ and $a < 0$. If $p = 2$, pick $a \equiv 1 \pmod{8}$ with $a < 0$.

10.129 Suppose for a contradiction that $\alpha := 0.2481632\cdots \in \mathbf{Q}$. Then the decimal expansion of α is eventually periodic with period ℓ, say.

Let $\beta \in \mathbf{Z}_{10}$ be the 10-adic limit of $2^{4\cdot 5^n}$ (see Problem 9.112). Write the 10-adic expansion of β as $(\ldots d_5 d_4 d_3 d_2 d_1 d_0)_{10}$, representing $d_0 + d_1 \cdot 10 + d_2 \cdot 10^2 + \ldots$. For each fixed N and all large n, the decimal expansion of $2^{4\cdot 5^n}$ terminates with the string $d_N d_{N-1} \ldots d_1 d_0$. Therefore, this digit string appears infinitely often in the expansion of α. Fixing any nonnegative integer n_0, and choosing $N \geq n_0 + \ell$, we deduce from the periodicity of α's expansion that $d_{n_0} = d_{n_0+\ell}$. Since this holds for each n_0, the 10-adic expansion of β is (purely) periodic with period ℓ, contradicting the result of Problem 9.112.

Extra Exploration 34 (Mahler [1]). Let g be an integer at least 2. Show that the real number $0.(g)(g^2)(g^3)\ldots$ obtained by concatenating the decimal expansions of $g, g^2, g^3, \ldots$ is irrational.

References

1. K. Mahler, *On some irrational decimal fractions.* J. Number Theory **13** (1981), 268–269.
2. T. Nagell, *Généralisation d'un théorème de Tchebycheff.* J. Math. Pures Appl. **8** (1921), 343–356.
3. O. Ore, *Anzahl der Wurzeln höherer Kongruenzen.* Norsk Mat. Tidsskr. **3** (1921), 63–66.

Solutions to Set #11

11.130 We assume $|x-1|_p < 1$ and argue that the terms of the series defining $\log_p x$ tend to 0. For each positive integer k, the product formula yields $|k|_p^{-1} = |k|_\infty \prod_{\text{prime } q \neq p} |k|_q \leq |k|_\infty = k$. Therefore,

$$\left|(-1)^{k-1}\frac{(x-1)^k}{k}\right|_p = |x-1|_p^k \cdot |k|_p^{-1} \leq k \cdot |x-1|_p^k,$$

which tends to 0 as k tends to infinity.

11.131 We start by noting that if $x \in 1+p\mathbf{Z}_p$, then $x^{-1} \in 1+p\mathbf{Z}_p$. This is not difficult to prove directly, futzing about with absolute values, but a more elegant approach is to observe that $(1+rp)^{-1} = 1-rp+r^2p^2-\cdots \in 1+p\mathbf{Z}_p$ whenever $r \in \mathbf{Z}_p$. Utilizing the addition rule (†), we deduce that for all $x \in 1+p\mathbf{Z}_p$,

$$\log_p x + \log_p \frac{1}{x} = \log_p 1 = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k}(1-1)^k = 0.$$

(That $\log_p x + \log_p \frac{1}{x} = 0$ should not be surprising, but it ought to be comforting!)

If $j \in \{1, 2, \ldots, p-1\}$, then

$$\sum_{k=1}^{\infty} \frac{1}{j^k}\frac{p^k}{k} = -\log_p\left(1-\frac{p}{j}\right) = \log_p\left(\left(1-\frac{p}{j}\right)^{-1}\right) = \log_p \frac{j}{j-p}.$$

Therefore,

$$\begin{aligned}\sum_{k=1}^{\infty}\left(\sum_{j=1}^{p-1}\frac{1}{j^k}\right)\frac{p^k}{k} &= \sum_{j=1}^{p-1}\left(\sum_{k=1}^{\infty}\frac{1}{j^k}\frac{p^k}{k}\right) = \sum_{j=1}^{p-1}\log_p\frac{j}{j-p} \\ &= \log_p \prod_{0<j<p}\frac{j}{j-p} = \log_p((-1)^{p-1}).\end{aligned}$$

Here the interchange of the sums on j and k is routine to justify, for example by setting $a_{k,j} = \mathbf{1}_{0<j<p} j^{-k} p^k k^{-1}$ and applying the result of Problem 8.96.

If p is odd, then $(-1)^{p-1} = 1$, and $\log_p 1 = 0$ gives the desired result. To finish off, we must show $\log_2(-1) = 0$. But this is easy: $\log_2(-1) + \log_2(-1) = \log_2((-1)^2) = \log_2(1) = 0$.

Remarks.

(i) You may have conjectured in Problem 4.45 that $v_2(\sum_{k=1}^n 2^k/k)$ is bounded below by $n -$ (something small). Once we know that $\sum_{k=1}^n 2^k/k = 0$, this becomes easy to show. Indeed,

$$\left|\sum_{k=1}^{n} \frac{2^k}{k}\right|_2 = \left|-\sum_{k=n+1}^{\infty} \frac{2^k}{k}\right|_2 \le \max_{k\ge n+1} \left|\frac{2^k}{k}\right|_2 \le \max_{k\ge n+1} \frac{k}{2^k} = \frac{n+1}{2^{n+1}}.$$

(To estimate $|2^k/k|_2$ we used the displayed inequality in the solution to Problem 11.130, for $x = -1$.) Converting this from a statement about absolute values to one about valuations, $v_2(\sum_{k=1}^n 2^k/k) \ge (n+1) - \frac{\log(n+1)}{\log 2}$. A slight modification of this argument will show that equality holds when $n+1$ is a power of 2.

(ii) In the next Extra Exploration, we outline one proof of the addition law (†). Arguments for (†) based on different principles can be found in the books of Gouvêa [2, §5.7] and Robert [10, Chapter 5, §4].
Our proof of (†) is motivated by the following formula from (real) calculus: For each real number $x > 0$,

$$\log x = \lim_{k\to\infty} k(\sqrt[k]{x} - 1).$$

(Check this yourself, possibly starting from $\frac{\mathrm{d}}{\mathrm{d}t} x^t\big|_{t=0} = \log x$.) This identity is surprisingly powerful; Landau shows in [5] that all of the familiar theory of the natural logarithm can be developed taking the right-hand side as the *definition* of $\log x$. We will establish and apply a p-adic analogue of this relation.

Extra Exploration 35 (Leopoldt [6]). Fix a prime number p. For $x \in 1+p\mathbf{Z}_p$ and $m \in \mathbf{Z}^+$, put

$$L_{p,m}(x) = \frac{x^{p^m} - 1}{p^m}.$$

Justify each of the following assertions.

(a) For $x \in 1 + p\mathbf{Z}_p$ and $m \in \mathbf{Z}^+$: $|L_{p,m+1}(x) - L_{p,m}(x)|_p \le p^{-m-2}$.
(b) For each $x \in 1 + p\mathbf{Z}_p$, the limit $L_p(x) := \lim_{m\to\infty} L_{p,m}(x)$ exists in $\mathbf{Q}_p$.
(c) For all $x, y \in 1 + p\mathbf{Z}_p$, and all $m \in \mathbf{Z}^+$: $|L_{p,m}(xy) - (L_{p,m}(x) + L_{p,m}(y))|_p \le p^{-m-2}$. Hence, $L_p(xy) = L_p(x) + L_p(y)$.

The rest of this problem is devoted to showing that L_p and $\log_p$ coincide; once this is known, (†) follows from (c).

(d) For $x \in 1 + p\mathbf{Z}_p$ and $m \in \mathbf{Z}^+$: $L_{p,m}(x) = \sum_{k\ge 1} \frac{1}{p^m} \binom{p^m}{k} (x-1)^k$.

(e) For $m, k \in \mathbf{Z}^+$: $\frac{1}{p^m}\binom{p^m}{k} = \frac{(-1)^{k-1}}{k}\prod_{1\le j<k}\left(1-\frac{p^m}{j}\right)$. Therefore, $L_{p,m}(x) = \log_p(x) + e_{p,m}(x)$, where

$$e_{p,m}(x) = \sum_{k\ge 2}\frac{(-1)^{k-1}}{k}\left(\prod_{1\le j<k}\left(1-\frac{p^m}{j}\right)-1\right)(x-1)^k.$$

(f) For each $x \in 1 + p\mathbf{Z}_p$, we have $\lim_{m\to\infty} e_{p,m}(x) = 0$. Thus, $L_p(x) = \log_p x$.
Hint. If k is small in terms of m, then $\prod_{1\le j<k}(1-p^m/j)$ is congruent to 1 modulo a large power of $p\mathbf{Z}_p$. On the other hand, when k is large, $v_p((x-1)^k/k)$ is also large.

11.132 Quite a lot of what is claimed here is true — just none of the important bits!

Let p be an odd prime and define $\sin_p(T) = \sum_{k\ge 0}(-1)^k\frac{T^{2k+1}}{(2k+1)!} \in \mathbf{Q}_p[[T]]$. It is straightforward to check that $\sin_p x$ converges when $|x|_p \le 1/p$; consequently, $\sin_p(pa)$ is a well-defined element of $\mathbf{Q}_p$ for all $a \in \mathbf{Z}$. It is also true that if a is an integer not divisible by p, then $\sin_p(ap) \ne 0$. Otherwise the display following "Therefore" indeed lays out a contradiction.

Unfortunately, none of this has much to do with the real number π! Let's assume $\pi = \frac{a}{b}$, with $a, b \in \mathbf{Z}$, $b \ne 0$. Choose an odd prime p not dividing a, Then the series $\sum_{k\ge 0}(-1)^k(ap)^k/(2k+1)!$ converges to $\sin(pb\pi) = 0$ in $\mathbf{R}$. So far, so good. But the fact that a series converges to 0 in $\mathbf{R}$ and converges to *something* in $\mathbf{Q}_p$ — something that could (misleadingly?) be labeled $\sin_p(pb\pi)$ — doesn't imply it converges to 0 in $\mathbf{Q}_p$. (Cf. Exercise 10.120.)

Remark. An error of a similar nature crept into the work of Hensel himself. In 1905, Hensel claimed to prove that $[\mathbf{Q}_p(\mathrm{e}) : \mathbf{Q}] = p$ for each odd prime p, from which he derived the corollary that e is transcendental over $\mathbf{Q}$ [3]. While the transcendence of e had already been shown by Hermite in 1873, Hensel's reasoning was much shorter and simpler; his proof has an unmistakable air of elegance. Unfortunately, it is also fundamentally flawed.* See [12] and [9, §5.6] for discussion (and compare with [4, Exercise 9, p. 84]).

11.133 We apply again the method of successive approximation. If $x_1 = -1$, then $F(x_1) \equiv 0 \pmod p$. Suppose we have found $x_k \in \mathbf{Z}_p$ with $F(x_k) \equiv 0 \pmod{p^k}$; we demonstrate how to find $x_{k+1} \in \mathbf{Z}_p$ with $x_{k+1} \equiv x_k \bmod p^k\mathbf{Z}_p$ and $F(x_{k+1}) \equiv 0 \pmod{p^{k+1}\mathbf{Z}_p}$.

To enforce the congruence $x_{k+1} \equiv x_k \pmod{p^k\mathbf{Z}_p}$, we look for x_{k+1} of the form $x_{k+1} = x_k + p^k h$, with $h \in \mathbf{Z}_p$. For each $h \in \mathbf{Z}_p$,

$$F(x_k + p^k h) - F(x_k) = p^k h + \sum_{j\ge 1} p^{2^j}\left((x_k + p^k h)^{2^j} - x_k^{2^j}\right).$$

* "For every complex problem there is an answer that is clear, simple, and wrong." — H. L. Mencken

Since $p^k \mid ((x_k + p^k h)^{2^j} - x_k^{2^j})$ and $p \mid p^{2^j}$, the sum on j belongs to $p^{k+1}\mathbf{Z}_p$. Hence, $F(x_k + p^k h) \equiv F(x_k) + p^k h \pmod{p^{k+1}}$, and $F(x_k + p^k h) \equiv 0 \pmod{p^{k+1}}$ provided we choose $h \equiv -F(x_k)/p^k \pmod{p\mathbf{Z}p}$.

If $x_1, x_2, x_3, \ldots$ are constructed as above, then the $\{x_n\}$ form a Cauchy sequence in $\mathbf{Z}_p$, so that $x_n \to x$ for some $x \in \mathbf{Z}_p$. For each n,

$$|F(x)|_p \le |F(x) - F(x_n)|_p + |F(x_n)|_p.$$

By construction, $|F(x_n)|_p \to 0$. Moreover, $F(x) - F(x_n) = (x - x_n)(1 + \sum_{j\ge 1} p^{2^j}(x^{2^j-1} + \cdots + x_n^{2^j-1}))$. Thus, $|F(x) - F(x_n)|_p \le |x - x_n|_p$, a quantity that also tends to 0. So taking n to infinity, we deduce that $F(x) = 0$.

We could prove uniqueness similarly, showing that if $x \in \mathbf{Z}_p$ is any zero of F, then x is uniquely determined mod $p\mathbf{Z}_p$, then mod $p^2\mathbf{Z}_p$, mod $p^3\mathbf{Z}_p$, etc. We choose a different path. We will show that F assumes *every* value at most once; that is, F is injective as a function from $\mathbf{Z}_p$ to $\mathbf{Z}_p$. Suppose $x, x' \in \mathbf{Z}_p$ with $F(x') = F(x)$. Rearranging,

$$x' - x = -(x' - x) \sum_{j\ge 1} p^{2^j}(x'^{2^j-1} + \cdots + x^{2^j-1}).$$

Since the right-hand sum is divisible by p, the only way the p-adic absolute values of both sides can agree is if $x' - x = 0$, so that $x' = x$.

11.133 (yes, déjà vu all over again!) We will factor $F(T)$ so as to make obvious that $F(x) = 0$ for a unique $x \in \mathbf{Z}_p$. The factors are constructed by a variant of the method of successive approximation.

The only property of $F(T)$ we will use is that $F(T) = 1 + T + pG(T)$, where $G(T) \in \mathbf{Z}_p[[T]]$ is a Strassmann series. Since $G(T)$ is Strassmann, for any $k \in \mathbf{Z}^+$ the power series $F(T) \in \mathbf{Z}_p[[T]]$ is congruent modulo $p^k\mathbf{Z}_p[[T]]$ to a *polynomial* with $\mathbf{Z}_p$ coefficients. This will be crucial.

We begin by locating $r_1 \in \mathbf{Z}_p$ and $q_1(T) \in \mathbf{Z}_p[T]$ with

$$(1 + T + p \cdot r_1)(1 + p \cdot q_1(T)) \equiv F(T) \pmod{p^2\mathbf{Z}_p[[T]]}.$$

The left-hand side is congruent to $(1 + T) + p((1 + T)q_1(T) + r_1)$ modulo $p^2\mathbf{Z}_p[[T]]$, and this matches the right mod $p^2\mathbf{Z}_p[[T]]$ if

$$(1 + T)q_1(T) + r_1 \equiv \frac{F(T) - (1 + T)}{p} \pmod{p\mathbf{Z}_p[[T]]}. \qquad (*)$$

Choose $F_1(T) \in \mathbf{Z}_p[T]$ with $\frac{F(T)-(1+T)}{p} \equiv F_1(T) \pmod{p\mathbf{Z}_p[[T]]}$. We can find $q_1(T)$ and $r_1(T)$ satisfying (*) by performing long division in the ring $(\mathbf{Z}_p/p\mathbf{Z}_p)[T]$. Specifically, if $\tilde{F}_1(T)$ is the mod $p\mathbf{Z}_p$-reduction of $F_1(T)$, long division furnishes us with $\tilde{q}_1(T) \in (\mathbf{Z}_p/p\mathbf{Z}_p)[T]$ and $\tilde{r}_1 \in \mathbf{Z}_p/p\mathbf{Z}_p$ with $\tilde{F}_1(T) =$

$(1+T)\tilde{q}_1(T) + \tilde{r}_1$ in $(\mathbf{Z}_p/p\mathbf{Z}_p)[T]$. Then (*) holds if we choose $q_1(T) \in \mathbf{Z}_p[T]$ and $r_1 \in \mathbf{Z}_p$ to lift $\tilde{q}_1(T)$ and $\tilde{r}_1$.

Continuing, suppose we have already found $r_1, r_2, \ldots, r_k \in \mathbf{Z}_p$ and $q_1(T)$, $q_2(T), \ldots, q_k(T) \in \mathbf{Z}_p[T]$ with

$$\left(1 + T + \sum_{j=1}^{k} p^j r_j\right)\left(1 + \sum_{j=1}^{k} p^j q_j(T)\right) \equiv F(T) \pmod{p^{k+1}\mathbf{Z}_p[[T]]}.$$

We determine $r_{k+1} \in \mathbf{Z}_p$ and $q_{k+1}(T) \in \mathbf{Z}_p[T]$ such that the analogous congruence holds with k replaced everywhere by $k+1$. To ease notation, put $U_k(T) = 1 + T + \sum_{j=1}^{k} p^j r_j$ and $V_k(T) = 1 + \sum_{j=1}^{k} p^j q_j(T)$. (Thus, $U_k(T)V_k(T) \equiv F(T) \pmod{p^{k+1}\mathbf{Z}_p[[T]]}$.) Then

$$\begin{aligned}&(U_k(T) + p^{k+1}r_{k+1})(V_k(T) + p^{k+1}q_{k+1}(T)) \\ &\equiv U_k(T)V_k(T) + p^{k+1}(U_k(T)q_{k+1}(T) + r_{k+1}V_k(T)) \pmod{p^{k+2}\mathbf{Z}_p[[T]]}.\end{aligned}$$

Hence, we would like to choose $q_{k+1}(T)$ and r_{k+1} to satisfy

$$U_k(T)q_{k+1}(T) + r_{k+1}V_k(T) \equiv \frac{F(T) - U_k(T)V_k(T)}{p^{k+1}} \pmod{p\mathbf{Z}_p[[T]]}.$$

Equivalently, as $U_k(T) \equiv 1+T \pmod{p\mathbf{Z}_p[[T]]}$ and $V_k(T) \equiv 1 \pmod{p\mathbf{Z}_p[[T]]}$, we want

$$(1+T)q_{k+1}(T) + r_{k+1} \equiv \frac{F(T) - U_k(T)V_k(T)}{p^{k+1}} \pmod{p\mathbf{Z}_p[[T]]}.$$

The right-hand side is congruent to a polynomial mod $p\mathbf{Z}_p[[T]]$ and so we are in a similar situation as before; we can find $q_{k+1}(T)$ and r_{k+1} by performing long division in $(\mathbf{Z}_p/p\mathbf{Z}_p)[T]$ and taking lifts.

Suppose we have chosen $r_1, r_2, r_3, \ldots \in \mathbf{Z}_p$ and $q_1(T), q_2(T), q_3(T), \ldots \in \mathbf{Z}_p[T]$ by the above procedure. We might then expect that

$$F(T) = U(T)V(T),$$
$$\text{where} \quad U(T) := 1 + T + \sum_{j=1}^{\infty} p^j r_j, \ V(T) := 1 + \sum_{j=1}^{\infty} p^j q_j(T).$$

There's one problem with this proposal. While $\sum_{j=1}^{\infty} p^j r_j$ is a well-defined element of $\mathbf{Z}_p$ (the sum being obviously convergent), it is not clear what is meant by $\sum_{j=1}^{\infty} p^j q_j(T)$, an infinite sum of elements of $\mathbf{Z}_p[T]$.* Fortunately

* This *should* be a power series over $\mathbf{Z}_p$. But its precise interpretation requires some care: Convergence in power series rings is usually defined by the requirement that the coefficient on each fixed power of T stabilizes, i.e., is eventually constant. But that is *not* the intended meaning here.

this difficulty is not so serious: For each fixed nonnegative integer r, the sum of the T^r coefficients of $p^j q_j(T)$ converges, to $\gamma_r \in \mathbf{Z}_p$ (say), and we simply define $\sum_{j=1}^{\infty} p^j q_j(T)$ to *mean* $\sum_{r\geq 0} \gamma_r T^r$. Having made this definition, the factorization $F(T) = U(T)V(T)$ follows easily (check that the two sides are congruent modulo $p^k \mathbf{Z}_p[[T]]$, for every k, and convince yourself that this implies equality in $\mathbf{Z}_p[[T]]$).

So far we have shown $F(T) = U(T)V(T)$, as formal power series. As each $q_j(T)$ is a polynomial, a moment's thought shows that $V(T) = 1 + \sum_{j=1}^{\infty} p^j q_j(T)$ is a Strassmann series. Invoking Problem 8.94, $F(x) = U(x)V(x)$ for all $x \in \mathbf{Z}_p$. Since $V(x) \in 1 + p\mathbf{Z}_p$ for each $x \in \mathbf{Z}_p$, the $\mathbf{Z}_p$-zeros of F are precisely the same as those of U. But it is obvious $U(x) = 0$ for a unique $x \in \mathbf{Z}_p$, namely $x = -1 - \sum_{j=1}^{\infty} p^j r_j$.

Remark. This took quite a bit longer than our first approach! However, if you understand this argument, you are well on your way to proving (one form of) the Weierstrass preparation theorem for $\mathbf{Q}_p$. See the remark after the solution to Problem 13.159.

Extra Exploration 36. Let $F(T)$ be a Strassmann series with $\mathbf{Z}_p$-coefficients. Reducing the coefficients of $F(T)$ modulo $p\mathbf{Z}_p$ yields a *polynomial* $\tilde{F}(T) \in (\mathbf{Z}_p/p\mathbf{Z}_p)[T]$. Show that if $\tilde{F}(T)$ has degree 1, then there is exactly one $x \in \mathbf{Z}_p$ with $F(x) = 0$.

Extra Exploration 37. Let p be an odd prime.

(a) Show that $\log_p$ defines a group isomorphism between $1 + p\mathbf{Z}_p$ (under multiplication) and $p\mathbf{Z}_p$ (under addition). This is analogous to how the usual log map sets up an isomorphism between $\mathbf{R}^+$ and $\mathbf{R}$.

Hint. One proof of injectivity goes by establishing $|\log_p x - \log_p y|_p = |x - y|_p$ for all $x, y \in 1 + p\mathbf{Z}_p$. For surjectivity, change variables and apply Extra Exploration 36.

(b) Prove that every element of $\mathbf{Z}_p^\times$ has a unique representation in the form ζu, where ζ is a $(p-1)$th root of unity and $u \in 1 + p\mathbf{Z}_p$.

(c) Let μ_{p-1} denote the group of $(p-1)$th roots of unity in $\mathbf{Q}_p$. Deduce that $\mathbf{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbf{Z}_p) \cong \mathbf{Z}/(p-1) \times \mathbf{Z}_p$ and that $\mathbf{Q}_p^\times \cong \mathbf{Z} \times \mathbf{Z}/(p-1) \times \mathbf{Z}_p$.

Extra Exploration 38 (the p-adic exponential). We assume familiarity with Extra Explorations 35 and 37. Let p be an odd prime. For $y \in p\mathbf{Z}_p$, define $\exp_p(y) = \sum_{k\geq 0} \frac{1}{k!} y^k$. Show that $\exp_p$ maps $p\mathbf{Z}_p$ into $1 + p\mathbf{Z}_p$, and that in fact $\exp_p : p\mathbf{Z}_p \to 1 + p\mathbf{Z}_p$ is the inverse of the isomorphism $\log_p : 1 + p\mathbf{Z}_p \xrightarrow{\sim} p\mathbf{Z}_p$.

One approach is to introduce $E_p(y) := \lim_{m\to\infty}(1 + p^m y)^{1/p^m}$. (Here raising to the power $1/p^m$ is defined by the Newton binomial expansion, as in Extra Exploration 31.) Show that E_p maps $p\mathbf{Z}_p$ into $1+p\mathbf{Z}_p$ and is actually the inverse of $L_p : 1+p\mathbf{Z}_p \to p\mathbf{Z}_p$. Then argue that $E_p(y) = \exp_p(y)$. The identity $E_p(y) = \exp_p(y)$ is the p-adic analogue of the well-known formula $\exp(x) = \lim_{n\to\infty}(1 + \frac{1}{n}x)^n$.

11.134 We explain how to transform the double sum on k and j into the claimed sum on j. Put $u_{k,j} = \mathbf{1}_{k\geq j} s(k,j) n^j \frac{a^k}{k!}$. Since p is odd and $|a|_p \leq 1/p$,

$$\left|\mathbf{1}_{k\geq j}s(k,j)n^j\frac{a^k}{k!}\right|_p \leq \mathbf{1}_{k\geq j}p^{-k}|k!|_p^{-1} \leq \mathbf{1}_{k\geq j}p^{-k}p^{k/(p-1)} \leq \mathbf{1}_{k\geq j}p^{-k/2}.$$

So if we set $\epsilon_N := p^{-N/2}$, then $|\mathbf{1}_{k\geq j}s(k,j)\frac{a^k}{k!}|_p \leq \epsilon_N$ whenever $k \geq N$ or $j \geq N$. By Problem 8.96,

$$\begin{aligned}\sum_{k=0}^{\infty}\left(\sum_{j=0}^{k}s(k,j)n^j\right)\frac{a^k}{k!} &= \sum_{k=0}^{\infty}\sum_{j=0}^{\infty}u_{k,j} = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty}u_{k,j} \\ &= \sum_{j=0}^{\infty}n^j\left(\sum_{k\geq j}s(k,j)\frac{a^k}{k!}\right) = \sum_{j=0}^{\infty}C_{a,j}n^j.\end{aligned}$$

When $n = 1$, this argument shows that $\sum_{j=0}^{\infty}C_{a,j} = 1 + a$. Since $\sum_{j=0}^{\infty}C_{a,j}$ converges, $|C_{a,j}|_p \to 0$ as $j \to \infty$.

11.135 Put $\mathbf{v}_n = [x_n, x_{n+1}, \ldots, x_{n+d-1}]^T$, so that $\mathbf{v} = \mathbf{v}_0$. According to our recurrence relation, $x_{n+d} = a_1x_{n+d-1} + a_2x_{n+d-2} + \cdots + a_dx_n$, and so

$$A\mathbf{v}_n = \begin{bmatrix}0 & 1 & 0 & \ldots & 0\\ 0 & 0 & 1 & \ldots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \ldots & 1\\ a_d & a_{d-1} & a_{d-2} & \ldots & a_1\end{bmatrix}\begin{bmatrix}x_n\\ x_{n+1}\\ x_{n+2}\\ \vdots\\ x_{n+d-1}\end{bmatrix} = \begin{bmatrix}x_{n+1}\\ x_{n+2}\\ x_{n+3}\\ \vdots\\ x_{n+d}\end{bmatrix} = \mathbf{v}_{n+1}$$

for each nonnegative integer n. Iterating, $A^n\mathbf{v} = A^n\mathbf{v}_0 = \mathbf{v}_n$, and $\langle A^n\mathbf{v}, \mathbf{e}\rangle = \langle \mathbf{v}_n, \mathbf{e}\rangle = x_n$.

11.136 Computing the determinant by expanding along the first column gives $\det(A) = \pm a_d$. Therefore, A is invertible over any ring in which a_d^{-1} exists, such as $\mathbf{F}_p$ when $p \nmid a_d$.

11.137 We have

$$\begin{aligned}x_n &= \langle A^n\mathbf{v}, \mathbf{e}\rangle = \langle A^r(A^k)^m\mathbf{v}, \mathbf{e}\rangle = \langle A^r(\mathrm{Id} + pB)^m\mathbf{v}, \mathbf{e}\rangle \\ &= \langle A^r\sum_{j=0}^{m}\binom{m}{j}p^jB^j\mathbf{v}, \mathbf{e}\rangle = \sum_{j=0}^{m}\binom{m}{j}p^j\langle A^rB^j\mathbf{v}, \mathbf{e}\rangle.\end{aligned}$$

11.138 Let $s(N, K)$ be the Stirling numbers of the first kind. For each nonnegative integer m, Problem 11.137 gives

$$x_{km+r} = \sum_{j=0}^{\infty} \frac{m(m-1)(m-2)\cdots(m-(j-1))}{j!} p^j \langle A^r B^j \mathbf{v}, \mathbf{e}\rangle$$
$$= \sum_{j=0}^{\infty} \frac{p^j}{j!} \left(\sum_{\ell=0}^{j} s(j,\ell) m^\ell \right) \langle A^r B^j \mathbf{v}, \mathbf{e}\rangle.$$

If we put $u_{j,\ell} = \mathbf{1}_{\ell \le j} \frac{p^j}{j!} s(j,\ell) m^\ell \langle A^r B^j \mathbf{v}, \mathbf{e}\rangle$, then $|u_{j,\ell}|_p \le \mathbf{1}_{\ell \le j} |j!|_p^{-1} \cdot p^{-j} \le \mathbf{1}_{\ell \le j} p^{j/(p-1)} p^{-j} \le \mathbf{1}_{\ell \le j} p^{-j/2}$. Hence, if $\epsilon_N := p^{-N/2}$, then $|u_{j,\ell}|_p \le \epsilon_N$ whenever $j \ge N$ or $\ell \ge N$. Because $\epsilon_N \to 0$ as $N \to \infty$, Exercise 8.96 allows us to write

$$x_{km+r} = \sum_{j=0}^{\infty} \sum_{\ell=0}^{\infty} u_{j,\ell} = \sum_{\ell=0}^{\infty} \sum_{j=0}^{\infty} u_{j,\ell} = \sum_{\ell=0}^{\infty} m^\ell \sum_{j \ge \ell} \frac{p^j}{j!} s(j,\ell) \langle A^r B^j \mathbf{v}, \mathbf{e}\rangle.$$

So if we define

$$F_{k,r}(T) = \sum_{\ell=0}^{\infty} \left(\sum_{j \ge \ell} \frac{p^j}{j!} s(j,\ell) \langle A^r B^j \mathbf{v}, \mathbf{e}\rangle \right) T^\ell,$$

then $F_{k,r}(m)$ converges to x_{km+r} for every nonnegative integer m. In particular, $F_{k,r}(1)$ converges, so that the coefficients of T^ℓ tend to 0 as $\ell \to \infty$. Thus, $F_{k,r}(T)$ is a Strassmann series.

11.139 Let $r \in \{0, 1, \ldots, k-1\}$. Suppose $x_n \ne 0$ for some nonnegative integer $n \equiv r \pmod{k}$. If we write $n = km + r$, then $F_{k,r}(m) = x_{km+r} = x_n \ne 0$. Therefore, $F_{k,r}(T)$ is not the zero series. Since $F_{k,r}(T)$ is Strassmann, Exercise 9.116 shows that $F_{k,r}$ has finitely many zeros in $\mathbf{Z}_p$. Consequently, there are finitely many nonnegative integers m with $F_{k,r}(m) = 0$. Equivalently, there are finitely many nonnegative integers $n \equiv r \pmod{k}$ with $x_n = 0$.

Summarizing: Either x_n vanishes for all nonnegative integers $n \equiv r \pmod{k}$ or x_n vanishes for only finitely many nonnegative integers $n \equiv r \pmod{k}$. The final claim of the problem ("Hence, ...") follows immediately.

Remarks.

(i) Imagine you are presented with an integer linear recurrence sequence, specified by a list of coefficients $a_1, \ldots, a_d \in \mathbf{Z}$ (where $a_d \ne 0$) and a collection of initial values $x_0, \ldots, x_{d-1} \in \mathbf{Z}$. The Skolem problem asks whether $x_n = 0$ for some nonnegative integer n. Frustratingly, while we have algorithms to decide this for any sequence with $d \le 4$ ("algorithm" here meaning a procedure that is proven to always terminate), no general algorithm is known for $d \ge 5$. See [8] for a discussion.

(ii) The *Monthly* article [7] of Myerson and Van der Poorten provides a highly entertaining account of the Skolem–Mahler–Lech theorem, addressing several aspects not discussed here.

Extra Exploration 39 (Shapiro [11], Myerson and Van der Poorten [7]). Let $\{x_n\}_{n\geq 0}$ be an integer linear recurrence sequence. Call $m \in \mathbf{Z}$ a repeat offender (relative to $\{x_n\}$) if $x_n = m$ for infinitely many nonnegative integers n. Show that each integer linear recurrence sequence is associated with only finitely many repeat offenders.

11.140 These are easy to find once you go looking. For instance, let $x_0 = 0$, $x_1 = 1$, and set $x_n = -x_{n-2}$ for all $n \geq 2$. Then $x_n = 0$ precisely when n is even.

Here is a more compelling example, yoinked from [7]. Consider the integer recurrence sequence $\{x_n\}$ satisfying

$$x_n = 6x_{n-2} - 12x_{n-4} + 8x_{n-6} \quad \text{for all } n \geq 6,$$

with initial conditions $x_0 = 8$, $x_1 = 0$, $x_2 = 9$, $x_3 = 0$, $x_4 = 8$, and $x_5 = 0$. Then $x_n = 0$ when n is odd, while $x_n = (n-8)^2 2^{(n-6)/2}$ when n is even. Hence, $x_n = 0 \iff n$ is odd or $n = 8$.

11.141 Yes, the same result holds for recurrence sequences defined over an arbitrary number field K.

The proof is almost the same as that given for integer recurrences. An obvious complication is that when $K \neq \mathbf{Q}$, a general element of K does not carry a preassigned meaning as an element of $\mathbf{Q}_p$. This obstacle is by no means insurmountable; it is resolved by embedding K into $\mathbf{Q}_p$, which we know is possible for infinitely many primes p (Exercise 10.126). Let's suppose we have not just an embedding but an EMBEDDING$^+$ (TM), meaning an embedding of K into $\mathbf{Q}_p$, p *odd*, where (identifying elements of K with their images in $\mathbf{Q}_p$) $a_1, \ldots, a_d, x_0, \ldots, x_{d-1} \in \mathbf{Z}_p$, and $a_d \in \mathbf{Z}_p^\times$. Then it is not hard to convince yourself that our proof of Skolem's theorem goes through nearly verbatim. (Check this!)

We know there are always embeddings, but is there always an EMBEDDING$^+$? Yes! Since K embeds into $\mathbf{Q}_p$ for infinitely many p, it will suffice to prove the following lemma.

Lemma. Let K be a number field and let α be a nonzero element of K. There are only finitely many primes p for which there exists an embedding of K into $\mathbf{Q}_p$ with $|\alpha|_p \neq 1$.

(As usual, we abuse notation and identify α with its image in $\mathbf{Q}_p$.)

Proof. Let $m(T)$ be the minimal polynomial of α over $\mathbf{Q}$, scaled to have integer coefficients. Write $m(T) = c_d T^d + c_{d-1} T^{d-1} + \cdots + c_1 T + c_0$. If $c_0 = 0$, then T divides $m(T)$, and the irreducibility of $m(T)$ over $\mathbf{Q}$ forces $m(T)$ to be a constant multiple of T. But then $\alpha = 0$, contrary to hypothesis. So $c_0 \neq 0$.

Assume now that K has been embedded into $\mathbf{Q}_p$, where p is a prime not dividing $c_d c_0$. We will show that $|\alpha|_p = 1$. Since only finitely many primes divide $c_d c_0$, the lemma follows.

Suppose instead that $|\alpha|_p > 1$. Since $m(\alpha) = 0$, we have $c_d\alpha^d = -(c_{d-1}\alpha^{d-1} + \cdots + c_0)$. However (keeping in mind that $p \nmid c_d$),

$$\begin{aligned} |c_d\alpha^d|_p = |\alpha|_p^d > |\alpha|_p^{d-1} &\geq \max\{|c_{d-1}\alpha^{d-1}|_p, \ldots, |c_1\alpha|_p, |c_0|_p\} \\ &\geq \left|\sum_{j=0}^{d-1} c_j\alpha^j\right|_p. \end{aligned}$$

If $|\alpha|_p < 1$, we argue similarly, exploiting that $1/\alpha$ is a root of the reciprocal polynomial $T^d m(T^{-1}) = c_0T^d + c_1T^{d-1} + \cdots + c_{d-1}T + c_d$. In this situation, $c_0(1/\alpha)^d = -(c_1(1/\alpha)^{d-1} + \cdots + c_{d-1}(1/\alpha) + c_d)$, and (keeping in mind that $p \nmid c_0$)

$$\begin{aligned} \left|c_0\left(\frac{1}{\alpha}\right)^d\right|_p = \left|\frac{1}{\alpha}\right|_p^d > \left|\frac{1}{\alpha}\right|_p^{d-1} &\geq \max\left\{|c_1(1/\alpha)^{d-1}|_p, \ldots, |c_{d-1}(1/\alpha)|_p, |c_d|_p\right\} \\ &\geq \left|\sum_{j=0}^{d-1} c_{d-j}\left(\frac{1}{\alpha}\right)^j\right|_p. \end{aligned}$$

Again we have a contradiction. ∎

Remark. Lech has shown that Skolem's theorem holds for recurrence sequences defined over *arbitrary* fields of characteristic 0. Today one usually refers to this general statement as the Skolem–Mahler–Lech theorem. In this setting the embedding required to make the proof work is guaranteed by a lemma of Cassels (see [1, Chapter 5]): *Let K be a finitely generated extension of $\mathbf{Q}$ and let S be a finite set of nonzero elements of K. For infinitely many primes p, there is an embedding of K into $\mathbf{Q}_p$ with the property that $|x|_p = 1$ for all $x \in S$.* To prove the Skolem–Mahler–Lech Theorem, apply this with $K = \mathbf{Q}(a_1, \ldots, a_d, x_0, \ldots, x_{d-1})$ (details left to you!).

References

1. J. W. S. Cassels, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986.
2. F. Q. Gouvêa, *p-adic numbers: An introduction*, third ed., Universitext, Springer, Cham, 2020.
3. K. Hensel, *Über die arithmetischen Eigenschaften der algebraischen und transzendenten Zahlen.* Jahresber. Dtsch. Math.-Ver. **14** (1905), 545–558.
4. N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984.
5. E. Landau, *Differential and integral calculus*, third ed., AMS Chelsea Publishing, Providence, RI, 2001.

6. H.-W. Leopoldt, *Zur Approximation des p-adischen Logarithmus*. Abh. Math. Sem. Univ. Hamburg **25** (1961), 77–81.
7. G. Myerson and A. van der Poorten, *Some problems concerning recurrence sequences*. Amer. Math. Monthly **102** (1995), 698–705.
8. J. Ouaknine and J. Worrell, *Decision problems for linear recurrence sequences*. In: Reachability Problems, Lecture Notes in Comput. Sci., vol. 7550, Springer, Heidelberg, 2012, pp. 21–28.
9. B. Petri, *Perioden, Elementarteiler, Transzendenz. Kurt Hensels Weg zu den p-adischen Zahlen*, Dr. Hut, München, 2011. URL: `http://tuprints.ulb.tu-darmstadt.de/2785/1/DissPetri.pdf`
10. A. M. Robert, *A course in p-adic analysis*, Grad. Texts in Math., vol. 198, Springer-Verlag, New York, 2000.
11. H. N. Shapiro, *On a theorem concerning exponential polynomials*. Comm. Pure Appl. Math. **12** (1959), 487–500.
12. P. Ullrich, *Der Henselsche Beweisversuch für die Transzendenz von e*, in: Mathematik im Wandel, bd. 1, Franzbecker, Hildesheim, 1998, pp. 320–330.

Solutions to Set #12

12.142 We begin with a simple lemma.

Lemma. If $x \in 1 + p^k\mathbf{Z}_p$, where $k \in \mathbf{Z}^+$, then $x^p \in 1 + p^{k+1}\mathbf{Z}_p$.

Proof. Write $x = 1+p^k r$, where $r \in \mathbf{Z}_p$. Then $x^p = 1+p^{k+1}r+\sum_{j\geq 2}\binom{p}{j}p^{jk}r^j \equiv 1 \pmod{p^{k+1}\mathbf{Z}_p}$, as desired. ∎

Now we return to the problem at hand. Since $a \in p\mathbf{Z}_p$, applying the lemma m times will show $(1+a)^{p^m} \in 1 + p^{m+1}\mathbf{Z}_p$. Hence, $|(1+a)^{p^m} - 1|_p \leq p^{-m-1}$, so that $(1+a)^{p^m} \to 1$. Therefore, for any $n \in \mathbf{Z}$,

$$(1+a)^n = (1+a)^n \lim_{m\to\infty}(1+a)^{p^m} = \lim_{m\to\infty}(1+a)^{n+p^m}.$$

This proves the first equality claimed in the problem.

Whenever $n + p^m \geq 0$, we have $(1+a)^{n+p^m} = \mathrm{Binom}(1+a; n+p^m)$, by Exercise 11.134. This explains the second equality.

Write $\mathrm{Binom}(1+a; n+p^m) - \mathrm{Binom}(1+a; n) = \sum_{j\geq 0} C_{a,j}((n+p^m)^j - n^j)$. Then

$$\begin{aligned}|\mathrm{Binom}(1+a; n+p^m) - \mathrm{Binom}(1+a; n)|_p &\leq \max_{j\geq 0}|C_{a,j}|_p|(n+p^m)^j - n^j|_p \\ &\leq p^{-m}\max_{j\geq 0}|C_{a,j}|_p,\end{aligned}$$

which tends to 0 as $m \to \infty$. This yields the final equality.

Extra Exploration 40. Let p be an odd prime, and let $a \in p\mathbf{Z}_p$. You have just demonstrated one way to extend $(1+a)^x$ from a function of x defined on $\mathbf{Z}$ to one defined on $\mathbf{Z}_p$: Set $(1+a)^x := \mathrm{Binom}(1+a; x)$. But there is another approach you could take to extend the domain of $(1+a)^x$ to $\mathbf{Z}_p$. Namely, you might define $(1+a)^x$ as the limit of $(1+a)^{x_n}$, where x_n is any sequence of integers converging to x in $\mathbf{Q}_p$. This should remind you of how exponentiation of real numbers is defined when the exponent is irrational.

Check that this idea works (i.e., leads to a well-defined value of $(1+a)^x$, independent of the particular sequence x_n) but doesn't give anything new: $(1+a)^x = \mathrm{Binom}(1+a;x)$, again. What happens when $p = 2$?

12.143 Put $F(T) = \sum_{i=1}^m a_i \cdot \mathrm{Binom}(\beta_i; T) - A$. The results of Problems 11.134 and 12.142 imply that $F(T)$ is a Strassmann series with $F(n) = \sum_{i=1}^m a_i \beta_i^n - A$ for every $n \in \mathbf{Z}$.

Every $n \in \mathbf{Z}$ satisfying $a_1\beta_1^n + \cdots + a_m\beta_m^n = A$ is a zero of F in $\mathbf{Z}_p$. So if this equation has infinitely many integer solutions, then F has infinitely many zeros in $\mathbf{Z}_p$. In that case, $F(T) = 0$ in $\mathbf{Q}_p[[T]]$ (by Exercise 9.116). Then $A = F(n) + A = a_1\beta_1^n + \cdots + a_m\beta_m^n$ for all $n \in \mathbf{Z}$.

Remark. It is often easy to rule out that $\sum_{i=1}^m a_i\beta_i^n = A$ for all $n \in \mathbf{Z}$. Let's assume, as is natural to do, that no $a_i = 0$.

Suppose to start off that $A = 0$. If $\sum_{i=1}^m a_i\beta_i^n = 0$ for all $n \in \mathbf{Z}$ (or even just the nonnegative $n \in \mathbf{Z}$), then we have a formal identity

$$0 = \sum_{n\geq 0} \left(\sum_{i=1}^m a_i \beta_i^n \right) T^n = \sum_{i=1}^m a_i \sum_{n \geq 0} (\beta_i T)^n = \sum_{i=1}^m \frac{a_i}{1-\beta_i T}.$$

Multiplying through by $\prod_{j=1}^m (1-\beta_j T)$ and replacing T with $1/\beta_1$ shows that $0 = a_1 \prod_{j=2}^m (1 - \beta_j/\beta_1)$. Hence, $\beta_1 = \beta_j$ for some $j = 2, 3, \ldots, m$. That is, the term β_1 is repeated in the list $\beta_1, \ldots, \beta_m$. But our setup is symmetric, and so *every* β_i must appear at least twice in that list. Turning things around, if some β_i appears only once, then we cannot have $\sum_{i=1}^n a_i\beta_i^n = 0$ for all $n \in \mathbf{Z}$. For an application, see the Remark following the solution of Problem 12.150.

Similar reasoning can be applied when $A \neq 0$. If $\sum_{i=1}^m a_i\beta_i^n = A$ for all nonnegative integers n, we find that $\frac{A}{1-T} = \sum_{i=1}^m \frac{a_i}{1-\beta_i T}$. This leads to the conclusion that every element in the list $1, \beta_1, \ldots, \beta_m$ is repeated.

12.144 If $\alpha = x + y\theta + z\theta^2$, then $\alpha' = x + y\theta' + z\theta'^2 = x + y\omega\theta + z\omega^2\theta^2$, and $\alpha'' = x + y\theta'' + z\theta''^2 = x + y\omega^2\theta + z\omega\theta^2$. Hence,

$$\alpha + \alpha' + \alpha'' = 3x + y\theta(1 + \omega + \omega^2) + z\theta^2(1 + \omega^2 + \omega) = 3x.$$

Similarly,

$$\begin{aligned} \alpha + \omega^2\alpha' + \omega\alpha'' &= (x + y\theta + z\theta^2) + (x\omega^2 + y\theta + z\omega\theta^2) + (x\omega + y\theta + z\omega^2\theta^2) \\ &= x(1 + \omega^2 + \omega) + 3y\theta + z\theta^2(1 + \omega + \omega^2) \\ &= 3y\theta, \end{aligned}$$

and

$$\begin{aligned} \alpha + \omega\alpha' + \omega^2\alpha'' &= (x + y\theta + z\theta^2) + (x\omega + y\omega^2\theta + z\theta^2) + (x\omega^2 + y\omega\theta + z\theta^2) \\ &= x(1 + \omega + \omega^2) + y\theta(1 + \omega^2 + \omega) + 3z\theta^2 \\ &= 3z\theta^2. \end{aligned}$$

12.145 Suppose $|\alpha|, |\alpha'| \leq R$. Since α'' is the complex conjugate of α', we also have $|\alpha''| \leq R$. By Exercise 12.144, $|x| \leq \frac{1}{3}(|\alpha| + |\alpha'| + |\alpha''|) \leq R$, $|y| \leq \frac{1}{3|\theta|}(|\alpha| + |\omega^2\alpha'| + |\omega\alpha''|) \leq \frac{R}{|\theta|}$, and $|z| \leq \frac{1}{3|\theta|^2}(|\alpha| + |\omega\alpha'| + |\omega^2\alpha''|) \leq \frac{R}{|\theta|^2}$. So there are finitely many possibilities for the integers x, y, and z, and therefore finitely many possibilities for $\alpha = x + y\theta + z\theta^2$.

12.146 For all $\varepsilon_1, \varepsilon_2 \in \mathcal{U}$,

$$\begin{aligned}\mathbf{L}(\varepsilon_1\varepsilon_2) &= (\log \varepsilon_1\varepsilon_2, 2\log|(\varepsilon_1\varepsilon_2)'|) \\ &= (\log \varepsilon_1, 2\log|\varepsilon_1'|) + (\log \varepsilon_2, 2\log|\varepsilon_2'|) = \mathbf{L}(\varepsilon_1) + \mathbf{L}(\varepsilon_2).\end{aligned}$$

So $\mathbf{L}$ is a homomorphism. If $\mathbf{L}(\varepsilon) = 0$, then $\log \varepsilon = 0$, which implies $\varepsilon = 1$. Therefore, $\ker(\mathbf{L})$ is trivial and $\mathbf{L}$ is injective. Finally, summing the x and y coordinates of $\mathbf{L}(\varepsilon)$ gives $\log \varepsilon + 2\log|\varepsilon'| = \log(\varepsilon|\varepsilon'|^2) = \log \mathrm{N}\varepsilon = \log 1 = 0$. So the image of $\mathbf{L}$ is contained in the subspace $x + y = 0$.

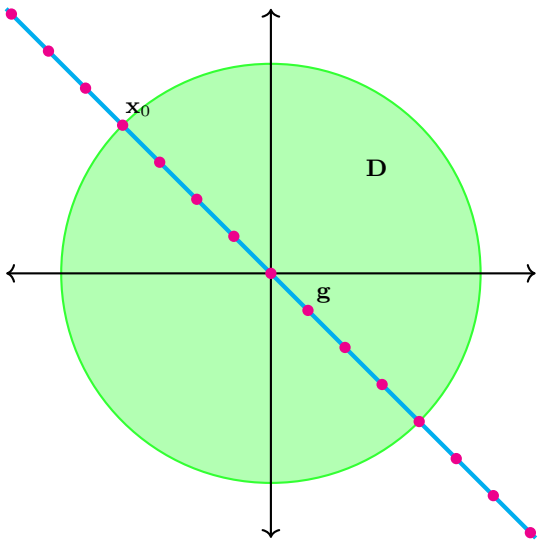


Figure corresponding to the solution of Problem 12.147.

12.147 We show that if (i) and (iii) both fail, then (ii) must hold. Since (i) fails, we may choose an $\mathbf{x}_0 \in \mathcal{G}$ with $\mathbf{x}_0 \neq \mathbf{0}$. Let $\mathbf{D}$ denote the closed disc about $\mathbf{0}$ passing through $\mathbf{x}_0$. The set $(\mathcal{G} \setminus \{\mathbf{0}\}) \cap \mathbf{D}$ is nonempty (containing, for example, $\mathbf{x}_0$). Since (iii) fails, this set is also finite. Let $\mathbf{g}$ be any element of $(\mathcal{G} \setminus \{\mathbf{0}\}) \cap \mathbf{D}$ minimizing the Euclidean distance to $\mathbf{0}$ (among elements of $(\mathcal{G} \setminus \{\mathbf{0}\}) \cap \mathbf{D}$).

As $\mathbf{g}$ is a nonzero vector belonging to the one-dimensional subspace $V := \{(x, y) : x + y = 0\}$ of $\mathbf{R}^2$, we have that $V = \mathbf{R}\mathbf{g}$. We leverage this observation to show that $\mathbf{g}$ generates $\mathcal{G}$. (Hence, (ii) holds!) It is enough to show that an arbitrarily chosen $\mathbf{x} \in \mathcal{G}$ belongs to $\langle \mathbf{g} \rangle$. Since $\mathcal{G} \subseteq V$, we may write $\mathbf{x} = t\mathbf{g}$, where $t \in \mathbf{R}$. Then $\{t\}\mathbf{g} = \mathbf{x} - \lfloor t \rfloor \mathbf{g} \in \mathcal{G}$. (Here $\{t\} = t - \lfloor t \rfloor$ denotes the fractional part of t.) Since $0 \leq \{t\} < 1$, the vector $\{t\}\mathbf{g}$ is an element of $\mathcal{G}$ closer to the origin than $\mathbf{g}$. This contradicts the choice of $\mathbf{g}$ unless $\mathbf{x} - \lfloor t \rfloor \mathbf{g} = \mathbf{0}$. But then $\mathbf{x} = \lfloor t \rfloor \mathbf{g} \in \langle \mathbf{g} \rangle$.

12.148 In view of Problem 12.147, it is enough to show that each closed disc about $\mathbf{0}$ intersects $\mathbf{L}(\mathcal{U})$ in a finite set.

Let $\mathbf{D}$ be the closed disc of radius R centered at $\mathbf{0}$. Every element of $\mathbf{D} \cap \mathbf{L}(\mathcal{U})$ can be written as $\mathbf{L}(\varepsilon)$ where $1 \leq \varepsilon \leq e^R$ and $|\varepsilon'| \leq e^{R/2}$. As a consequence of Problem 12.145, there are only finitely many possibilities for ε and hence only finitely many possibilities for $\mathbf{L}(\varepsilon)$.

12.149 Since $\theta^3 = D$ and D is cubefree, $0 \leq 3v_p(\theta) = v_p(D) < 3$. Hence, $v_p(\theta) = 0$ and $|\theta|_p = 1$. Also, $|\omega|_p^3 = |\omega^3|_p = |1|_p = 1_p$, so that $|\omega|_p = 1$.

Each of $\mu, \mu', \mu'' \in \mathbf{Z}[\theta, \omega]$. Since $\mathbf{Z} \subseteq \mathbf{Z}_p$ and $\theta, \omega \in \mathbf{Z}_p^\times$, we have $\mathbf{Z}[\theta, \omega] \subseteq \mathbf{Z}_p$. Hence, $|\mu|_p, |\mu'|_p, |\mu''|_p \leq 1$. But $|\mu|_p|\mu'|_p|\mu''|_p = |\mu\mu'\mu''|_p = |1|_p = 1$. So it must be that $|\mu|_p, |\mu'|_p, |\mu''|_p = 1$.

12.150 Fix $r \in \mathbf{Z}$. For each $m \in \mathbf{Z}$, set $E(m) = \mu^r\nu^m + \omega\mu'^r\nu'^m + \omega^2\mu''^r\nu''^m$. The equation $E(m) = 0$ is an equation involving only elements of L and field operations in L. At present, our attention is fixed on the embedded copy of L inside $\mathbf{Q}_p$, but if $E(m) = 0$ holds in that copy of L, it holds in the OG* version of L, which is a subfield of $\mathbf{C}$.

Back in the complex numbers, $|\mu| = \mu > 1$. (Here and below $|\cdot|$ is the usual complex absolute value.) Moreover, $1 = \mu|\mu'\mu''| = \mu|\mu'|^2$, so that $|\mu'| = |\mu''| = 1/\mu < 1$. It follows that $|\nu| = \nu > 1$ while $|\nu'| = |\nu''| < 1$. As a consequence,

$$|\omega\mu'^r\nu'^m + \omega^2\mu''^r\nu''^m| \leq |\mu'^r| \cdot |\nu'|^m + |\mu''^r| \cdot |\nu''|^m < 1$$

for all large enough positive integers m, and

$$|E(m)| \geq |\mu^r\nu^m| - |\omega\mu'^r\nu'^m + \omega^2\mu''^r\nu''^m| \geq |\mu^r|\nu^m - 1 > 0$$

for all sufficiently large m.

Therefore, if we pick m as a large enough positive integer, then $E(m) \neq 0$ (and this holds whether we are thinking of L as inside $\mathbf{C}$ or inside $\mathbf{Q}_p$). So from the Strassmann series machinery that we have built up, $E(m) = 0$ for only finitely many integers m. (Note that this finiteness does *not* follow from the

* Original Gauss

bounds over $\mathbf{C}$ that we derived above. Those bounds imply that $E(m) = 0$ for only finitely many positive integers m, but they say nothing useful about negative integers m.) Finally, letting r range from 0 to $p-1$, we see that $\mu^n + \omega\mu'^n + \omega^2\mu''^n = 0$ for only finitely many $n \in \mathbf{Z}$.

Remark. We can shorten the argument using the Remark following the solution to Problem 12.143. If $E(m) = 0$ for all $m \in \mathbf{Z}$, then each term in the list ν, ν', ν'' is repeated. But, working again in $\mathbf{C}$,

$$|\nu| = \nu > 1 > |\nu'| = |\nu''|,$$

and so ν is not repeated.

12.151 Suppose n^3+1 has all prime factors from $\mathcal{P}$. Then $n^3+1 = \prod_{p\in\mathcal{P}} p^{v_p}$ for some nonnegative integers v_p. Writing each $v_p = 3e_p + r_p$, where $r_p \in \{0, 1, 2\}$,

$$n^3 + 1 = (-D)y^3 \qquad \text{for} \qquad D = \prod_{p\in\mathcal{P}} p^{r_p}, \quad y = -\prod_{p\in\mathcal{P}} p^{e_p}.$$

Hence, $(-n, y)$ is an integer solution to $X^3 - DY^3 = 1$.

By construction, $D \in \mathcal{D}$. If $D = 1$, then n^3 and $n^3 + 1$ are positive perfect cubes differing by 1. But the smallest difference between positive perfect cubes is $2^3 - 1^3 = 7$. Thus, $D \in \mathcal{D} \setminus \{1\}$.

By Problem 12.150, each equation $X^3 - DY^3 = 1$, with $D \in \mathcal{D} \setminus \{1\}$, has finitely many integer solutions. Since $\#\mathcal{D}$ is finite, we conclude that there are finitely many n for which $n^3 + 1$ has all prime factors from $\mathcal{P}$. To deduce that the largest prime factor of $n^3 + 1$ tends to infinity, choose $\mathcal{P}$ as the set of primes up to an arbitrarily prescribed bound.

Extra Exploration 41. Keep the same assumptions and notation from the proof of the theorem. In this exercise, you will show that for each nonzero integer k, the equation $x^3 - Dy^3 = k$ has finitely many integer solutions x, y. Equivalently, there are finitely many pairs of integers x, y with $\mathrm{N}(x - y\theta) = k$.

(a) Show that the ring $\mathbf{Z}[\theta]/k\mathbf{Z}[\theta]$ is finite, and that in fact $\#\mathbf{Z}[\theta]/k\mathbf{Z}[\theta] = |k|_\infty^3$.
(b) Prove that if $\kappa \in \mathbf{Z}[\theta]$ has $\mathrm{N}\kappa = k$, then $\kappa\mathbf{Z}[\theta] \supseteq k\mathbf{Z}[\theta]$. Deduce from (a) that there are finitely many possibilities for κ, up to associates.
(c) Suppose $\kappa \in \mathbf{Z}[\theta]$ has $\mathrm{N}\kappa = k$. Prove that there are finitely many $u \in \mathcal{U}$ (same meaning as above — positive units in $\mathbf{Z}[\theta]$) for which $u\kappa$ has the form $x - y\theta$ for some $x, y \in \mathbf{Z}$. Conclude!

Extra Exploration 42 (continuation). Fix a finite set of primes $\mathcal{P}$ and a nonzero integer d. Show that there are finitely many $n \in \mathbf{Z}$ such that both n and $n + d$ have all of their prime factors belonging to $\mathcal{P}$.

Remark. As stated on Set #12, Delaunay and Nagell showed that $x^3 - Dy^3 = 1$ has at most one integer solution with $y \neq 0$. It was discovered by Skolem [2] that their theorem can be established by p-adic methods. Skolem's proof uses arithmetic in extensions of $\mathbf{Q}_3$; a more elementary p-adic proof can be found in lecture notes of Ljunggren [1].

References

1. W. Ljunggren, *Diophantine equations: a p-adic approach*. Notes by R. R. Laxton from a 1968 lecture course at the University of Nottingham.
2. T. Skolem, *Anvendelse av 3-adisk analyse og „bikropper" til bevis for noen satser angående visse kubiske ubestemte ligninger*. Norsk Mat. Tidsskr. **34** (1952), 45–51.

Solutions to Set #13

13.152 When $p-1 \mid k$, every term in the sum is 1, and $\sum_{u=1}^{p-1} \omega(u)^k = p-1 = \mathbf{1}_{p-1|k}(p-1)$.

Now suppose that $p-1 \nmid k$. Recall that every finite subgroup of the multiplicative group of a field is cyclic. Thus, we may choose a generator ζ for the group $\mu_{p-1} = \{\omega(1), \ldots, \omega(p-1)\}$ of $(p-1)$th roots of unity in $\mathbf{Q}_p$. Since $\zeta^{(p-1)k} = 1$ and $\zeta^k \neq 1$,

$$\begin{aligned}\sum_{u=1}^{p-1} \omega(u)^k &= \sum_{j=1}^{p-1} (\zeta^j)^k = \sum_{j=1}^{p-1} (\zeta^k)^j \\ &= \zeta^k(1 + \zeta^k + \cdots + \zeta^{(p-2)k}) = \zeta^k \frac{1-\zeta^{(p-1)k}}{1-\zeta^k} = 0,\end{aligned}$$

which agrees with $\mathbf{1}_{p-1|k}(p-1)$ in this case.

13.153 By Faulhaber's formula and Exercise 13.152,

$$\begin{aligned}\mathbf{1}_{p-1|k}(p-1) &= \sum_{u=1}^{p-1} (u + p\vartheta(u))^k \\ &= \sum_{u=1}^{p-1} u^k + \sum_{0<j\leq k} \binom{k}{j} p^j \sum_{u=1}^{p-1} u^{k-j}\vartheta(u)^j \\ &= B_k p + \sum_{0<j\leq k} \binom{k}{j} B_{k-j} \frac{p^{j+1}}{j+1} + \sum_{0<j\leq k} \binom{k}{j} p^j \sum_{u=1}^{p-1} u^{k-j}\vartheta(u)^j.\end{aligned}$$

Shifting $\mathbf{1}_{p-1|k}(p-1)$ to the right-hand side and dividing by pk,

$$\beta_k + \sum_{0<j\leq k} \frac{1}{k}\binom{k}{j} B_{k-j} \frac{p^j}{j+1} + \sum_{0<j\leq k} \frac{1}{k}\binom{k}{j} p^{j-1} \sum_{u=1}^{p-1} u^{k-j}\vartheta(u)^j = 0.$$

This becomes the relation claimed in the problem statement after the substitution $\binom{k}{j} = \frac{k}{j}\binom{k-1}{j-1}$.

13.154 Suppose the claim is false and let k be the smallest positive integer with $\beta_k \notin \mathbf{Z}_p$. We will derive a contradiction from the relation

$$\beta_k + \sum_{0<j\le k} \binom{k-1}{j-1} B_{k-j} \frac{p^j}{j(j+1)} + \sum_{0<j\le k} \binom{k-1}{j-1} \frac{p^{j-1}}{j} \sum_{u=1}^{p-1} u^{k-j} \vartheta(u)^j = 0 \ (*)$$

established in Problem 13.153.

Let j be an integer in the range $0 < j \le k$. We argue below that the jth term in both of the above sums is p-adically integral. It is then immediate from (*) that $\beta_k \in \mathbf{Z}_p$, contrary to our choice of k.

We start with the first of the two sums. Observe that

$$\begin{aligned} v_p\left(\frac{p^j}{j(j+1)}\right) &= j - v_p(j(j+1)) \ge j - v_p((j+1)!) \\ &> j - \frac{j+1}{p-1} \ge j - \frac{j+1}{2} = \frac{j-1}{2} \ge 0. \end{aligned}$$

Hence, $p^j/j(j+1) \in p\mathbf{Z}_p$. Since $\binom{k-1}{j-1} \in \mathbf{Z}$, to complete the proof that $\binom{k-1}{j-1} B_{k-j} p^j/j(j+1) \in \mathbf{Z}_p$ it is enough to establish that $pB_{k-j} \in \mathbf{Z}_p$. But this follows from our choice of k: If $0 < j < k$, then $k-j$ is a positive integer smaller than k, so that $\beta_{k-j} \in \mathbf{Z}_p$. Hence, $pB_{k-j} - \mathbf{1}_{p-1|k-j}(p-1) = p(k-j)\beta_{k-j} \in p\mathbf{Z}_p$, and $pB_{k-j} \in \mathbf{Z}_p$. If $j = k$, then $pB_{k-j} = pB_0 = p$, which is also in $\mathbf{Z}_p$.

The second sum is easier. There it is clear that the jth term lies in $\mathbf{Z}_p$ as long as p^{j-1}/j is p-adically integral. Integrality is obvious when $j = 1$. When $j \ge 2$, we can argue as follows: $v_p\left(\frac{p^{j-1}}{j}\right) = j - 1 - v_p(j) \ge j - 1 - v_p(j!) > j - 1 - \frac{j}{p-1} \ge j - 1 - \frac{j}{2} \ge 0$. (This argument actually shows a bit more: If $j \ge 2$, then $p^{j-1}/j \in p\mathbf{Z}_p$.)

Remark. Note that $k\beta_k = B_k - \frac{\mathbf{1}_{p-1|k}(p-1)}{p} = B_k + \frac{\mathbf{1}_{p-1|k}}{p} - \mathbf{1}_{p-1|k}$. Thus, $\beta_k \in \mathbf{Z}_p$ implies $B_k + \frac{\mathbf{1}_{p-1|k}}{p} \in \mathbf{Z}_p$, recovering the result of Exercise 8.99.

13.155 Let $p \ge 5$ and let $k \in 2\mathbf{Z}^+$. We refine the analysis appearing in the solution to Problem 13.154. Label the two sums in (*) as $\sum_1$ and $\sum_2$.

We will show that the jth term of $\sum_1$ lies in $p\mathbf{Z}_p$ whenever $0 < j \le k$ and that the jth term of $\sum_2$ belongs to $p\mathbf{Z}_p$ whenever $1 < j \le k$. Taking (*) modulo $p\mathbf{Z}_p$, we deduce that $\beta_k + \sum_{u=1}^{p-1} u^{k-1}\vartheta(u) \in p\mathbf{Z}_p$, as required.

For the second sum there is almost nothing to do. We noted at the end of the solution to Problem 13.154 that $\frac{p^{j-1}}{j} \in p\mathbf{Z}_p$ once $j \ge 2$. (There we only needed $p \ge 3$.) As the other factors in the terms of $\sum_2$ are p-adic integers, our claim for $\sum_2$ follows.

Since k is even, the only odd integer j which contributes to $\sum_1$ is $j = k-1$. For this j, we have $\binom{k-1}{j-1} B_{k-j} \frac{p^j}{j(j+1)} = (k-1) B_1 \frac{p^{k-1}}{k(k-1)} = -\frac{1}{2}\frac{p^{k-1}}{k}$. We already observed that $\frac{p^{k-1}}{k} \in p\mathbf{Z}_p$, while clearly $-\frac{1}{2} \in \mathbf{Z}_p$ (p is odd). Hence, the term of $\sum_1$ corresponding to $j = k-1$ belongs to $p\mathbf{Z}_p$. Suppose now that j is even and $0 < j \leq k$. If $0 < j < k$, the p-integrality of β_{k-j} established in Problem 13.154 implies that

$$pB_{k-j} = p(k-j)\beta_{k-j} + \mathbf{1}_{p-1|k-j}(p-1) \in \mathbf{Z}_p.$$

If $j = k$, then $pB_{k-j} = pB_0 = p$, and this also belongs to $\mathbf{Z}_p$. Thus, it will suffice to show that $\frac{p^{j-1}}{j(j+1)} \in p\mathbf{Z}_p$. This follows upon observing that

$$\begin{aligned} v_p\left(\frac{p^{j-1}}{j(j+1)}\right) &= j - 1 - v_p(j(j+1)) \geq j - 1 - v_p((j+1)!) \\ &> j - 1 - \frac{j+1}{p-1} \geq j - 1 - \frac{j+1}{4} > 0, \end{aligned}$$

keeping in mind for the last step that $j \geq 2$.

13.156 We are assuming that $p-1$ does not divide the even integer k, so that $p \geq 5$. Since k and k' are congruent mod $p-1$, the integer k' is also not divisible by $p-1$. By Problem 13.155,

$$\begin{aligned} \frac{B_k}{k} = \beta_k &\equiv -\sum_{u=1}^{p-1} u^{k-1}\vartheta(u) \pmod{p\mathbf{Z}_p}, \\ \frac{B_{k'}}{k'} = \beta_{k'} &\equiv -\sum_{u=1}^{p-1} u^{k'-1}\vartheta(u) \pmod{p\mathbf{Z}_p}. \end{aligned}$$

Suppose without loss of generality that $k' \geq k$ and write $k' = k + (p-1)q$. Then $u^{k'-1} = u^{k-1}u^{(p-1)q} \equiv u^{k-1} \pmod{p\mathbf{Z}_p}$, by Fermat's little theorem. (To apply Fermat, we identify $\mathbf{Z}_p/p\mathbf{Z}_p$ with $\mathbf{Z}/p$, invoking Problem 5.62.) Substituting above, $\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \pmod{p\mathbf{Z}_p}$.

Remark. Call an odd prime p regular if p does not divide the numerator of any of $B_2, B_4, \ldots, B_{p-3}$. In the middle of the 19th century, Kummer showed that Fermat's last theorem for the exponent p holds for all regular primes p. That is, if p is a regular prime, then $x^p + y^p = z^p$ has no solutions in integers x, y, z with $xyz \neq 0$ (see the books of Ribenboim [8] and Washington [12] for accounts of this work).

All primes smaller than 37 are regular, while 37 is not: $B_{32} = -37 \cdot \frac{683 \cdot 305065927}{2 \cdot 3 \cdot 5 \cdot 17}$. Via Kummer's congruence (the result of Problem 13.156), it is possible to show that there are infinitely many irregular primes (odd primes that are not regular). We sketch an argument for this due to Carlitz [2], which nicely illustrates how the facts we have built up about Bernoulli numbers can be put to use.

Looking at the Remark following the solution to Problem 4.44, we see that $|B_{2m}|_\infty$ tends to infinity faster than any power of m. In particular, as we will use momentarily, $|\frac{B_{2m}}{2m}|_\infty > 1$ for all large values of m.

Let $p_1, \ldots, p_r$ be any finite list of irregular primes, and let

$$N = 2\,\mathrm{lcm}[p_1 - 1, \ldots, p_r - 1].$$

We let k run over the positive multiples of N and consider the ratios B_k/k. From the last paragraph, we can choose k with $|B_k/k|_\infty > 1$. Then there is a prime p dividing the numerator of B_k/k. Since $p_i - 1$ divides k for each $i = 1, 2, \ldots, r$, each of our primes p_i appears in the denominator of B_k, and so also in the denominator of B_k/k (by the Clausen–von Staudt theorem, Exercise 8.101). Thus, p is not any of $p_1, \ldots, p_r$. A similar argument shows that $p - 1$ does not divide k (note that this implies $p \neq 2$). If we let k' denote the reduction of k modulo $p - 1$, then $k' \in \{2, 4, 6, \ldots, p - 3\}$, and by Kummer's congruence,

$$\frac{B_{k'}}{k'} \equiv \frac{B_k}{k} \equiv 0 \pmod{p\mathbf{Z}_p}.$$

Therefore, p divides the numerator of $B_{k'}$, implying that p is an irregular prime not on our initial list. At this point in the proof Euclid is smiling down from heaven.

From the perspective of progress towards Fermat's Last Theorem, it would certainly be more encouraging to know that there are infinitely many *regular* primes. Unfortunately, this question remains wide open! Of course, the urgency of the problem has diminished somewhat in the wake of the full proof of Fermat's Last Theorem by Wiles and Taylor–Wiles.*

13.157 Let $p \geq 5$ be prime, and let $k = \varphi(p^3) - 1$.

The group $(\mathbf{Z}_p/p^3\mathbf{Z}_p)^\times$ can be identified with $(\mathbf{Z}/p^3)^\times$, which has order $\varphi(p^3)$. Hence, each $x \in \mathbf{Z}_p^\times$ satisfies $x^{\varphi(p^3)} \equiv 1 \pmod{p^3\mathbf{Z}_p}$, and $x^k \equiv \frac{1}{x} \pmod{p^3\mathbf{Z}_p}$. Therefore, working in $\mathbf{Z}_p$ modulo $p^3\mathbf{Z}_p$,

$$H_{p-1} = \sum_{n=1}^{p-1} \frac{1}{n} \equiv \sum_{n=1}^{p-1} n^k = k\frac{p^2}{2}B_{k-1} + \sum_{2 \leq j \leq k} \binom{k}{j} B_{k-j} \frac{p^{j+1}}{j+1}.$$

In this last expression, the term pB_k has been dropped from Faulhaber's formula, which is harmless as k is odd and larger than 1.

Continuing, we argue that every term of the sum on j belongs to $p^3\mathbf{Z}_p$. Suppose $j \geq 3$. Since $pB_{k-j} \in \mathbf{Z}_p$ (as follows from Problem 8.99 or 13.154),

$$\begin{aligned} v_p\left(\binom{k}{j} B_{k-j} \frac{p^{j+1}}{j+1}\right) &= v_p\left(\binom{k}{j} pB_{k-j} \frac{p^j}{j+1}\right) \geq j - v_p(j+1) \\ &\geq j - v_p((j+1)!) > j - \frac{j+1}{p-1} \geq j - \frac{j+1}{4} \geq 2. \end{aligned}$$

* The story of which is gloriously recounted in Joshua Rosenblum and Joanne Sydney Lessner's 2000 musical *Fermat's Last Tango*.

This shows that each term with $j \geq 3$ belongs to $p^3\mathbf{Z}_p$. The remaining term, corresponding to $j = 2$, is $\binom{k}{2} B_{k-2} \frac{p^3}{3}$. As $k - 2 \equiv p - 4 \not\equiv 0 \pmod{p-1}$, we have that $B_{k-2} \in \mathbf{Z}_p$. Hence, $\binom{k}{2} B_{k-2} \frac{p^3}{3} \in p^3\mathbf{Z}_p$.

Collecting our results so far, $H_{p-1} \equiv k\frac{p^2}{2} B_{k-1} \pmod{p^3\mathbf{Z}_p}$. Kummer, as incarnated in Problem 13.156, now steps in to tell us that

$$\frac{B_{k-1}}{k-1} \equiv \frac{B_{p-3}}{p-3} \pmod{p\mathbf{Z}_p}.$$

Therefore,

$$B_{k-1} \equiv (k-1)\frac{B_{p-3}}{p-3} \equiv \frac{2}{3} B_{p-3} \pmod{p\mathbf{Z}_p},$$

and

$$H_{p-1} \equiv k\frac{p^2}{2} B_{k-1} \equiv k\frac{p^2}{3} B_{p-3} \equiv -\frac{p^2}{3} B_{p-3} \pmod{p^3\mathbf{Z}_p}.$$

From this last congruence for H_{p-1}, we have $H_{p-1} \in p^3\mathbf{Z}_p \iff B_{p-3} \in p\mathbf{Z}_p$. This equivalence is the concluding assertion of the problem statement.

Remark. This problem brings to a close our study of the Bernoulli numbers. For everything you ever wanted to know about this subject but were afraid to ask, see Chapter 15 in the book of Ireland and Rosen [6], Chapter 9 in Cohen's volume [4], and the recent book [1] by T. Arakawa, T. Ibukiyama, and M. Kaneko. A bibliography with ≈ 3000 books and papers related to Bernoulli numbers has been compiled by Karl Dilcher, Ladislav Skula, and Ilja Sh. Slavutskii [5].

13.158 Since $F(r) = 0$, we have $F(x) = F(x) - F(r) = \sum_{k\geq 0} a_k(x^k - r^k) = \sum_{k\geq 0} a_k(x-r)\sum_{j=0}^{k-1} x^j r^{k-1-j}$.

Let $u_{k,j} = \mathbf{1}_{0\leq j<k} \cdot a_k x^j r^{k-1-j}$. If we put $\epsilon_N := \max_{n\geq N} |a_n|_p$, then

$$|u_{k,j}|_p \leq \mathbf{1}_{0\leq j<k}|a_k|_p \leq \epsilon_N \qquad \text{whenever } j \geq N \text{ or } k \geq N.$$

Moreover, $\epsilon_N \to 0$ (as F is a Strassmann series). So by Exercises 8.95 and 8.96, $\sum_k \sum_j u_{k,j}$ and $\sum_j \sum_k u_{k,j}$ both converge, and to the same value. Hence,

$$\begin{aligned} F(x) = (x-r)\sum_k \sum_j u_{k,j} &= (x-r)\sum_j \sum_k u_{k,j} \\ &= (x-r)\sum_{j\geq 0} x^j \sum_{k>j} a_k r^{k-1-j}. \end{aligned}$$

Here the final sum on k is exactly what we called b_j. Therefore, if we set $G(T) = \sum_{j\geq 0} b_j T^j$, we have shown that $G(x)$ converges for all $x \in \mathbf{Z}_p$ (i.e., $G(T)$ is Strassmann) and that $F(x) = (x-r)G(x)$ for all such x.

Now we suppose that the Strassmann degree K of $F(T)$ is at least 1 and prove that the Strassmann degree of $G(T)$ is $K-1$. If $j < K-1$, then

$$|b_j|_p \leq \max_{k>j} |a_k r^{k-1-j}|_p \leq \max_k |a_k|_p = |a_K|_p.$$

When $j = K-1$,

$$|b_{K-1}|_p = \left| a_K + \sum_{k>K} a_k r^{k-K} \right|_p.$$

This last sum on k satisfies

$$\left| \sum_{k>K} a_k r^{k-K} \right|_p \leq \max_{k>K} |a_k r^{k-K}|_p \leq \max_{k>K} |a_k|_p < |a_K|_p.$$

So by survival of the greatest, $|b_{K-1}|_p = |a_K|_p$. Finally, when $j \geq K$,

$$|b_j|_p \leq \max_{k>K} |a_k r^{k-1-j}|_p \leq \max_{k>K} |a_k|_p < |a_K|_p.$$

Hence, the maximum value of $|b_j|_p$ is $|a_K|_p$, and this maximum is attained for the last time at $j = K-1$. Therefore, $G(T)$ has Strassmann degree $K-1$.

Extra Exploration 43. Recall our notation $\mathbf{Q}_p\langle T\rangle$ for the ring of Strassmann series. Problem 13.158 establishes a version of the Root-Factor theorem for Strassmann series viewed as functions on $\mathbf{Z}_p$. Show that the Root-Factor theorem is also valid at the level of formal power series. More precisely, show that if $r \in \mathbf{Z}_p$ is a root of $F(T) \in \mathbf{Q}_p\langle T\rangle$, then $F(T) = (T-r)G(T)$, where $G(T) \in \mathbf{Q}_p\langle T\rangle$ is the power series constructed in the preceding solution.

Extra Exploration 44.

(a) Prove that if $F(T), G(T)$ are nonzero elements of $\mathbf{Q}_p\langle T\rangle$, then the Strassmann degree of FG is the sum of the Strassmann degrees of F and G.
(b) Show that if $X(T)$ is a Strassmann series with all coefficients from $\mathbf{Z}_p$, then $1 + pT \cdot X(T)$ is a unit in $\mathbf{Q}_p\langle T\rangle$, with inverse $1 - pT \cdot X(T) + p^2T^2 \cdot X(T)^2 - p^3T^3 \cdot X(T)^3 + \ldots$, for an appropriate interpretation of the infinite series.
(c) Establish that the units in $\mathbf{Q}_p\langle T\rangle$ are precisely the elements of Strassmann degree 0.

13.159 Suppose to start off that $F(T) = \sum_{k\geq 0} a_k T^k$ has Strassmann degree $K = 0$. Then $|a_0|_p > |a_k|_p$ for every $k \geq 1$. Hence, for every $x \in \mathbf{Z}_p$, we have $|\sum_{k\geq 1} a_k x^k|_p \leq \max_{k\geq 1} |a_k|_p < |a_0|_p$ and

$$|F(x)|_p = \left| a_0 + \sum_{k\geq 1} a_k x^k \right|_p \geq |a_0|_p - \left| \sum_{k\geq 1} a_k x^k \right|_p > 0.$$

Therefore, F has no zeros in $\mathbf{Z}_p$ (and no zeros is "at most $K = 0$ zeros"),

Assuming the general claim fails, choose a counterexample $F(T)$ whose Strassmann degree K is as small as possible. Then $K \geq 1$. By assumption, F has more than K distinct zeros in $\mathbf{Z}_p$; pick one of these and call it r. By Exercise 13.158, we can find a Strassmann series $G(T)$ of Strassmann degree $K-1$ with $F(x) = (x-r)G(x)$ for all $x \in \mathbf{Z}_p$. As $K-1 < K$, we know that G has at most $K-1$ distinct zeros in $\mathbf{Z}_p$. But each zero of F, other than (possibly) r, is a zero of G. Thus, there are at most $1 + (K-1) = K$ zeros of F in $\mathbf{Z}_p$, contradicting the choice of $F(T)$.

Remark. It is enlightening to view Strassmann's theorem through the lens of the Weierstrass preparation theorem for $\mathbf{Q}_p$: *Every Strassmann series $F(T)$ with Strassmann degree K admits a factorization $F(T) = U(T)V(T)$ where $U(T) \in \mathbf{Q}_p[T]$ is polynomial whose degree and Strassmann degree are both K and $V(T) = 1 + p\tilde{V}(T)$ for a Strassmann series $\tilde{V}(T) \in \mathbf{Z}_p[[T]]$.* You might try to prove this theorem yourself by imitating our second solution to Problem 11.133. If you get stuck, look at [7, pp. 54–55] or [9, pp. 166–167].

Suppose we have factored $F(T) = U(T)V(T)$ as in the Weierstrass preparation theorem. Then $V(x) \in 1 + p\mathbf{Z}_p$ for all $x \in \mathbf{Z}_p$; in particular, $V(x) \neq 0$. Since $F(x) = U(x)V(x)$ for all $x \in \mathbf{Z}_p$, we deduce that F and U have the same zeros in $\mathbf{Z}_p$. But U, as a polynomial of degree K, has at most K zeros in $\mathbf{Q}_p$, and a fortiori at most K zeros in $\mathbf{Z}_p$.* Thus, the Weierstrass preparation theorem can be viewed as "explaining" Strassmann's theorem. This reasoning is very close to Strassmann's original proof; the Weierstrass preparation theorem as stated here follows from the assertions "1", "1′", and "3" appearing on page 21 of [11].

13.160 Referring back to Set #11, for each $A \in p\mathbf{Z}_p$ the constant term $C_{A,0}$ of $\mathrm{Binom}(1+A, T)$ is

$$C_{A,0} = \sum_{k \geq 0} s(k,0)\frac{A^k}{k!} = s(0,0)\frac{A^0}{0!} = 1.$$

Therefore, the constant term of

$$F_{r,\pm}(T) = \alpha^r \,\mathrm{Binom}(1+a;T) - \beta^r \,\mathrm{Binom}(1+b;T) \mp (\alpha - \beta)$$

is $\alpha^r - \beta^r \mp (\alpha - \beta)$. This vanishes precisely when $\frac{\alpha^r - \beta^r}{\alpha - \beta} = \pm 1$. Inspecting the table on Set #3, we see that when $0 \leq r \leq 9$, we have $\frac{\alpha^r - \beta^r}{\alpha - \beta} = \pm 1$ if and only if $(r, \pm) \in \{(1,+), (2,+), (3,-), (5,-)\}$.

For all other values of $(r, \pm)$ one computes directly (see the tables at the top of this page) that $F_{r,\pm}(0)$ is an 11-adic unit.

* Actually, each of its $\mathbf{Q}_p$-zeros is a $\mathbf{Z}_p$-zero. Since U has the same degree as Strassmann degree, scaling by an appropriate power of p turns U into a polynomial with $\mathbf{Z}_p$-coefficients and leading coefficient a p-adic unit. Each $\mathbf{Q}_p$-root of such a polynomial belongs to $\mathbf{Z}_p$. Cf. the proof of the Lemma in the solution to Problem 11.141.

r	0	1	2	3	4	5	6	7	8	9
$F_{r,+}(0) \bmod 11\mathbf{Z}_{11}$	9	0	0	7	3	7	8	1	3	8
r	0	1	2	3	4	5	6	7	8	9
$F_{r,-}(0) \bmod 11\mathbf{Z}_{11}$	2	4	4	0	7	0	1	5	7	1

Constant terms of $F_{r,\pm}(T)$ modulo $11\mathbf{Z}_{11}$.

Now let $j \geq 1$. The T^j-coefficient of $F_{r,\pm}(T)$ is given by

$$\alpha^r C_{a,j} - \beta^r C_{b,j} = \sum_{k \geq j} s(k,j) \left(\alpha^r \frac{a^k}{k!} - \beta^r \frac{b^k}{k!} \right).$$

For each $k \geq j$, we have $v_{11}(a^k/k!), v_{11}(b^k/k!) \geq k - v_{11}(k!) > k - \frac{k}{10} = 0.9k \geq 0.9j$. Therefore,

$$|\alpha^r C_{a,j} - \beta^r C_{b,j}|_{11} \leq \max_{k \geq j} \left| s(k,j) \left(\alpha^r \frac{a^k}{k!} - \beta^r \frac{b^k}{k!} \right) \right|_{11} \leq 11^{-0.9j}.$$

In particular, every nonconstant coefficient of $F_{r,\pm}(T)$ has 11-adic absolute value less than 1.

We conclude that, apart from the four specified values of $(r, \pm)$, the series $F_{r,\pm}(T)$ has constant term an 11-adic unit and all other terms belonging to $11\mathbf{Z}_{11}$. Hence, $F_{r,\pm}(T)$ has Strassmann degree 0 and no zeros in $\mathbf{Z}_p$ (by Exercise 13.159).

13.161 The T-coefficient of $F_{r,\pm}(T)$ is

$$\alpha^r C_{a,1} - \beta^r C_{b,1} = \sum_{k \geq 1} s(k,1) \left(\alpha^r \frac{a^k}{k!} - \beta^r \frac{b^k}{k!} \right).$$

Reasoning as in the solution to Problem 13.160, the terms of the right-hand sum with $k \geq 2$ make a contribution bounded in 11-adic absolute value by $11^{-0.9 \cdot 2}$, and hence also bounded by 11^{-2} (since no absolute value is strictly between 11^{-1} and 11^{-2}). Keeping in mind that $s(1,1) = 1$, we conclude that

$$\alpha^r C_{a,1} - \beta^r C_{b,1} \equiv \alpha^r a - \beta^r b \pmod{11^2 \mathbf{Z}_{11}}. \qquad (*)$$

Plugging our approximations of α and a into (*), we find that the T-coefficient

$$\begin{aligned}
&\text{of } F_{1,+} \text{ is } \equiv 4 \cdot 11 \pmod{11^2\mathbf{Z}_{11}}, \\
&\text{of } F_{2,+} \text{ is } \equiv 8 \cdot 11 \pmod{11^2\mathbf{Z}_{11}}, \\
&\text{of } F_{3,-} \text{ is } \equiv 0 \pmod{11^2\mathbf{Z}_{11}}, \textit{ and} \\
&\text{of } F_{5,-} \text{ is } \equiv 6 \cdot 11 \pmod{11^2\mathbf{Z}_{11}}.
\end{aligned}$$

So the T-coefficients are divisible by 11 but not 11^2 for $(r,\pm) = (1,+)$, $(2,+)$, and $(5,-)$.

Let's take stock of what we've shown in this exercise and the last. If $(r,\pm)$ is any of $(1,+),(2,+),(5,-)$, then the constant term of $F_{r,\pm}(T)$ is 0. The T-coefficient has 11-adic absolute value 11^{-1}. And the T^j coefficient has 11-adic absolute value at most $11^{-0.9\cdot 2} < 11^{-1}$, for each $j \geq 2$. It follows that $F_{r,\pm}(T)$ has Strassmann degree 1.

13.162 We saw already in the solution to Problem 13.161 that $F_{3,-}(T)$ has T-coefficient divisible by 11^2.

The T^2-coefficient of $F_{3,-}(T)$ is given by

$$\alpha^3 C_{a,2} - \beta^3 C_{b,2} = \sum_{k\geq 2} s(k,2)\left(\alpha^3 \frac{a^k}{k!} - \beta^3 \frac{b^k}{k!}\right).$$

Here the terms of the right-hand sum corresponding to $k \geq 3$ make a contribution bounded in 11-adic absolute value by $11^{-0.9\cdot 3}$, and hence also by 11^{-3}. Since $s(2,2) = 1$ ($s(2,2)$ is the coefficient of T^2 in $T(T-1)$),

$$\alpha^3 C_{a,2} - \beta^3 C_{b,2} \equiv \alpha^3 \frac{a^2}{2} - \beta^3 \frac{b^2}{2} \pmod{11^3 \mathbf{Z}_{11}}.$$

Working with the right-hand side, we find that

$$\alpha^3 C_{a,2} - \beta^3 C_{b,2} \equiv 8 \cdot 11^2 \pmod{11^3 \mathbf{Z}_{11}}.$$

Hence, the T^2-coefficient of $F_{3,-}(T)$ is divisible by 11^2 but not 11^3.

For every $j \geq 3$, the T^j coefficient of $F_{3,-}(T)$ is bounded in absolute value by $11^{-0.9\cdot 3} < 11^{-2}$.

Summing up: $F_{3,-}(T)$ has vanishing constant term, T-coefficient bounded in absolute value by 11^{-2}, T^2-coefficient with absolute value equal to 11^{-2}, and T^j coefficients with absolute value strictly smaller than 11^{-2} for $j \geq 3$. Therefore, $F_{3,-}(T)$ has Strassmann degree 2.

13.163 If $\frac{\alpha^n - \beta^n}{\alpha - \beta} = \pm 1$, then $F_{r,\pm}(n) = 0$, where r is the remainder when n is divided by 10. In Exercise 13.160, we found that $F_{r,\pm}$ has no zeros in $\mathbf{Z}_p$ (let alone in $\mathbf{Z}$!) except possibly if $(r,\pm) \in \{(1,+),(2,+),(3,-),(5,-)\}$.

In Exercise 13.161, we showed that $F_{r,\pm}(T)$ has Strassmann degree 1 for each of $(r,\pm) = (1,+)$, $(2,+)$, and $(5,-)$. By Strassmann's Theorem (Exercise 13.159), each corresponding series $F_{r,\pm}(T)$ has at most one zero in $\mathbf{Z}_p$. Similarly, the result of Exercise 13.162 shows that $F_{3,-}(T)$ has at most 2 zeros in $\mathbf{Z}_p$.

Consequently, there are at most $1+1+1+2 = 5$ integers n for which $\frac{\alpha^n - \beta^n}{\alpha - \beta} = \pm 1$. We know five such integers already: $n = 1, 2, 3, 5, 13$. (See the table on Set #3.) Thus, there can be no others.

Extra Exploration 45 (Skolem, Chowla, and Lewis [10]). Prove that each integer appears at most three times in the sequence $\{\frac{\alpha^n-\beta^n}{\alpha-\beta}\}_{n\geq 0}$ (for the same α, β as above).

Extra Exploration 46 (Cohen and Ljunggren [3]). Find all integer solutions to $x^2 + 11 = 3^m$.

Extra Exploration 47. What are all of the positive integer solutions to $2x^2+1 = 3^m$? Equivalently: Which squares have ternary expansions consisting entirely of the digit 1?

References

1. T. Arakawa, T. Ibukiyama, and M. Kaneko, *Bernoulli numbers and zeta functions*, Springer Monogr. Math., Springer, Tokyo, 2014.
2. L. Carlitz, *Note on irregular primes.* Proc. Amer. Math. Soc. **5** (1954), 329–331.
3. E. L. Cohen, *Sur l'équation diophantienne* $x^2 + 11 = 3^k$. C. R. Acad. Sci. Paris Sér. A-B 275 (1972), A5–A7.
4. H. Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007.
5. K. Dilcher, L. Skula, and I. Sh. Slavutskii, *A bibliography of Bernoulli numbers.* Online resource. URL: `https://www.mscs.dal.ca/~dilcher/bernoulli.html`
6. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.
7. D. J. Lewis, *Diophantine equations: p-adic methods.* In: Studies in Number Theory, MAA Stud. Math., vol. 6, pp. 25–75. Math. Assoc. America, Buffalo, NY, 1969.
8. P. Ribenboim, *13 lectures on Fermat's last theorem*, Springer-Verlag, New York-Heidelberg, 1979.
9. T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen.* Comptes Rendus Congr. Math. Scand. (Stockholm, 1934), 163–188.
10. T. Skolem, S. Chowla, and D. J. Lewis, *The diophantine equation* $2^{n+2} - 7 = x^2$ *and related problems.* Proc. Amer. Math. Soc. **10** (1959), 663–669.
11. R. Strassmann, *Über den Wertevorrat von Potenzreihen im Gebiet der* `p`*-adischen Zahlen.* J. Reine Angew. Math. **159** (1928), 13–28.
12. L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

Index