Modular Arithmetic

Chaang Tze Shen Tristan

May 19, 2018

1 Congruence

Two integers are said to be congruent mod m if their remainders are equal when divided by m, we write this as

$$a \equiv b \pmod{m}$$

For example the following holds:

$$16 \equiv 9 \equiv 2 \equiv -5 \equiv -12 \pmod{7}$$

Note that congruence expressions are linear and multiplicative. Also, if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for any positive integer n.

2 Multiplicative Inverses

We want to solve $7x \equiv 3 \pmod{9}$. Then we write $x \equiv \frac{3}{7} \pmod{9}$ (Note that here $\frac{3}{7}$ is not really a fraction! It is just a convention to write x in a neater manner.)

$$x \equiv \frac{3}{7} \equiv \frac{12}{28} \equiv \frac{12}{1} \equiv 12 \pmod{9}$$

3 The Base-eliminating Method

When solving congruences with large powers, we need to find a way to eliminate it.

Example 1. Find the remainder of 2^{10000} when divided by 127.

Solution. Note that $2^7 \equiv 1 \pmod{127}$. Therefore we can do this:

$$\begin{aligned} 2^{10000} &\equiv (2^7)^{1428} \times 2^4 \\ &\equiv 1^{1428} \times 2^4 \\ &\equiv 16 \pmod{127} \end{aligned}$$

We need to be smart to find the order, which is when will it be congruent to 1 (or anything that would be easy to evaluate under large powers)

3.1 Problems

1. Find the remainder of 3^{2000} when divided by 13.
2. Find the remainder of $2019^{2019^{2019}}$ when divided by 7.
3. Find the units digit of $163^{163^{163}}$.

4 The Chinese Remainder Theorem (CRT)

If given a system of ANY number of expressions

$$x \equiv a_i \pmod{m_i}$$

where m_i are all pairwise coprime, then there is a unique solution mod $m_1 m_2 ... m_i$

$$x \equiv A \pmod{m_1 m_2 ... m_i}$$

Example 2. Find the last two digits of $7^{7^{7^7}}$.

Solution. We can first split 100 into two coprime numbers 4 and 25.
For mod 4,

$$7^{7^{7^7}} \equiv (-1)^{2k+1} \equiv -1 \equiv 3 \pmod 4$$

For mod 25, note that $7^2 \equiv -1 \pmod{25}$, so $7^4 \equiv 1 \pmod{25}$.

$$7^{7^{7^7}} \equiv 7^{4k+3} \equiv 7^3 \equiv 343 \equiv 18 \pmod{25}$$

Therefore $7^{7^{7^7}} \equiv 43 \pmod{100}$.

Example 3. Given n, is it always possible to have n consecutive integers, each divisible by a square greater than 1?

Solution. Yes. Consider n pairwise coprime perfect squares $X_1, X_2, X_3, ..., X_n$. Let

$$\begin{aligned} x + i &\equiv 0 \pmod{X_i} & \qquad (i = 1, 2, 3, ..., n) \\ x &\equiv -i \pmod{X_i} & \qquad (i = 1, 2, 3, ..., n) \end{aligned}$$

x is solvable by CRT. Thus $x+1, x+2, x+3, ...x+n$ is the desired sequence. (Q.E.D)

4.1 Real Problems

1. Find the last two digits of $17^{17^{17^{17}}}$
2. (1987/IMO) Prove that there 1000 consecutive integers such that none is a power of a prime.
3. (2017/ChenJingRun) How many positive integers $n < 1000$ are there such that $n^n + 1$ can be divisible by 66?

5 Perfect Squares

Here are some extremely important perfect-square properties.

$$x^2 \equiv 0, 1 \pmod 3$$
$$x^2 \equiv 0, 1 \pmod 4$$
$$x^2 \equiv 0, 1, 4, 5, 6, 9 \pmod{10}$$

5.1 Problems

1. How many $n \in \mathbb{N}$ are there such that $2007 + 4^n$ is a perfect square?
2. Prove that there are no $\overline{abc}$ such that $\overline{abc} + \overline{bca} + \overline{cab}$ is not a perfect square.
3. Prove that there are infinitely primes which cannot be expressed as a sum of two squares.
4. Let $2001m^2 + m = 2002n^2 + n$ and m, n positive integers. Prove that $m - n$ is a perfect square.