MAT315 (Summer 2022) Notes

Zhongmang Cheng

August 18, 2022

Fundamentals

Definition (divides): $a \mid b$ if and only if $b = k \cdot a$ for some integer k.
$a \mid 0, a \mid a, a \mid -a, 1 \mid a$ for every a.

Definition (fully divides): $p^e \mid\mid a$ if $p^e \mid a$ but $p^{e+1} \nmid a$.
$p^\alpha \mid\mid a$ and $p^\beta \mid\mid b \implies p^{\alpha+\beta} \mid\mid ab$, $p^{\alpha-\beta} \mid\mid \frac{a}{b}$

Division Algorithm: If $b \neq 0$, then there are unique integers k and r such that:
$a = k \cdot b + r$ and $0 \leq r < |b|$.

Fundamental Theorem of Arithmetic: Every $n \geq 2$ has a prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where p_i are distinct primes and a_i are positive integers. This factorization is unique up to re-ordering.

Dirichlet's Theorem: There are infinitely many primes of the form $ak + b$ if and only if $(a, b) = 1$.

Diophantine Equation: $ax + by = c$ has solution if and only if $(a, b) \mid c$.
The set of all solution is:

$$\{x \in \mathbb{Z} : x_0 + t \cdot \tfrac{m}{(m,a)}\} \text{ or } \{x \in \mathbb{Z} : x = x_0 \pmod{\tfrac{m}{(m,a)}}\}$$

Modular Arithmetic's

If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then:

- $a + b \equiv c + d \pmod{n}$
- $ab \equiv cd \pmod{n}$
- $a^k \equiv c^k \pmod{n}$ where $k \in \mathbb{N}$

Suppose $d \geq 1$ and $d \mid m$, then $a \equiv b \pmod{m} \implies a \equiv b \pmod{d}$
Suppose $c \geq 0$, then $a \equiv b \pmod{m} \implies ac \equiv bc \pmod{mc}$
$ax \equiv ay \pmod{m} \implies x \equiv y \pmod{\frac{m}{(m,a)}}$

CRT and related conclusions

Chinese Remainder Theorem: $x \equiv a_1 \pmod m)_1, x \equiv a_2 \pmod m)_2 \cdots x \equiv a_k \pmod m)_k$ with $(m_i, m_j) = 1$ for all $i \neq j$ has a unique solution $x \equiv a \pmod{m_1 m_2 \cdots m_k}$ in $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ for some a.

$x \equiv a \pmod{m_1 m_2} \implies x \equiv a \pmod{m_1}, x \equiv a \pmod{m_2}$
$x \equiv a \pmod{m_1}, x \equiv a \pmod{m_2} \implies x \equiv a \pmod{[m_1, m_2]}$

$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2} \implies x$ has 0 or 1 solution in $\mathbb{Z}_{[m_1, m_2]}$
$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, (m_1, m_2) = 1 \implies x$ has unique solution in $\mathbb{Z}_{m_1 m_2}$

x has n_1 possible values mod m_1, n_2 possible values mod m_2, $(m_1, m_2) = 1$
$\implies$ x has $n_1 n_2$ possible values in $\mathbb{Z}_{m_1 m_2}$

FLT and related applications

Fermat Little Theorem: if a is not divisible by p, then $a^{p-1} \equiv 1 \pmod p$.
$a^{p-1} \equiv 1 \pmod p$ for $(a, p) = 1$ where p is a prime.
$a^p \equiv a \pmod p$ for all a where p is a prime.

Wilson's Theorem: $n \geq 2$ is a prime if and only if $(n-1)! \equiv -1 \pmod n$.

Primality Test: "n passes base a test" if $a^n \equiv a \pmod n$

Definition (pseudo-prime): a composite number n such that $2^n \equiv 2 \pmod n$.
If p is an odd prime, then $x^2 + 1 \equiv 0 \pmod p$ has a solution if and only if $p \equiv 1 \pmod 4$.

Polynomials

Let $p(x)$ be a polynomial with integer coefficients, then:
$a \equiv b \pmod n \implies p(a) \equiv p(b) \pmod n$

Lagrange Theorem: $f(x) = a_d x^d + a_{d-1} x^{d-1} \cdots a_1 x + a_0$ is a polynomial with integer coefficients such that $a_i \not\equiv 0 \pmod p$ for at least one i. Then, $f(x) \equiv 0 \pmod p$ has at most d solutions mod p. (If $f(x) = a_d x^d + a_{d-1} x^{d-1} \cdots a_1 x + a_0$ has more than d solutions mod p, then $a_i \equiv 0 \pmod p$ for all i.)

Remark: $f(a) \equiv 0 \pmod p \implies f(x) \equiv (x - a) g(x) \pmod p$

$x^a - 1 = (x-1)(x^{a-1} + x^{a-2} \cdots + x + 1)$
$x^{2a+1} + 1 = (x+1)(x^{2a} - x^{2a-1} + x^{2a-2} \cdots - x + 1)$
If $2^m + 1$ is prime, then $m = 2^n$ for some n
If $2^m - 1$ is prime, then m must be prime

Hensel's Lemma: Suppose $f(a) = 0 \pmod{p}$, then:

- if $f'(a) \neq 0 \pmod{p}$, then a can be lifted uniquely to p^2.
- if $f'(a) \equiv 0 \pmod{p}$ and $\frac{f(a)}{p} \neq 0 \pmod{p}$, then a cannot be lifted uniquely to p^2.
- if $f'(a) \equiv 0 \pmod{p}$ and $\frac{f(a)}{p} \equiv 0 \pmod{p}$, then a can be lifted to p solutions in p^2.

Euler Function and Primitive Roots

Definition (unit): u is a unit mod n if it has an inverse.
u has an inverse u^{-1} such that $u \cdot u^{-1} \equiv 1 \pmod{n}$ only if $(u, n) = 1$.

Definition (Euler Function): $\phi(n)$ represent the number of units in $\mathbb{Z}_n$.

Euler's Theorem: Suppose $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

$\phi(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k})$ and $\phi(p^k) = p^k \cdot (1 - \frac{1}{p})$ for p prime, $k \geq 1$.
$\phi(mn) = \phi(m)\phi(n)$ for $(m, n) = 1$.

Definition (primitive root):
g is a primitive root if $\{1, 2 \cdots, p-1\} \equiv \{g, g^2 \cdots, g^{p-1}\}$ in $\mathbb{Z}_p$ (generator for $(\mathbb{Z}_n)^\times$).

Definition (order):
The smallest postive integer k such that $u^k \equiv 1 \pmod{n}$, denoted by $ord_n(u)$.

Remark: $u^k \equiv 1 \pmod{n} \iff ord_n(u) \mid k$

A unit u is a primitive root (generates the complete set of $(\mathbb{Z}_p)^\times$) $\iff ord_n(u) = \phi(p)$.
If g is a primitive root modulo p, then $g^k \equiv 1 \pmod{p} \iff p - 1 \mid \phi(p)$.
If g is a primitive root modulo p, then $ord_n(g^a) = \frac{\phi(n)}{\phi(n),a)}$

Let $d \mid p - 1$ be positive, then there are exactly $\phi(d)$ units mod p of order d.
The sum of all $\phi(m)$ such that $m \mid n$ equals to n

There are $\phi(d)$ units of order d mod p when $d \mid p - 1$.

Existence and related lemmas: Z_n has a primitive root if and only if $n = 1, 2, 4$ or $n = p^m$ or $n = 2 \cdot p^m$ where $p \neq 2$ is prime.

- Let $m \geq 2$, if g is a primitive root mod p^m, then g is a primitive root mod p^{m+1}.
- Let n be odd, if g is a primitive root mod n and g is odd, then g is a primitive root mod $2n$.
- If $n = a \cdot b$ with $(a, b) = 1$ and $a, b > 2$, then $\mathbb{Z}_n$ has no primitive root.

Theorem: $ord_{2^n}(5) = 2^{n-2}$
Theorem: Units of $\mathbb{Z}_{2^n}$ can be generated by two units: 5 and -1.

Applications in Cryptography

In the following context, we assume that x is the message we would like to encode, and m is the message we would like to decode. Also, we assume that finding the modulo inverse is an easy computation using Euclidean Algorithm.

Modular Exponential Cipher

Public information: p large prime
Secret information: e where $(e, p-1) = 1$ (Here e is the key)

To encode: compute $m \equiv x^e \pmod{p}$, send m.
To decode: find the inverse f such that $e \cdot f \equiv 1 \pmod{p-1}$, computes $m^f \pmod{p}$.

Remark: $m^f \equiv (x^e)^f \equiv x^{ef} \equiv x^{(p-1)k+1} \equiv x \pmod{p}$

Diffie-Hellman Key Exchange

Public information: p large prime, g such that $1 < g < p$, and g^a, g^b
Secret information: a only known by A, b only known by B (Here g^{ab} is the key)

A computes $g^a \pmod{p}$ and send it to B. B computes $g^b \pmod{p}$ and send it to A. A and B compute $(g^b)^a \pmod{p}$ and $(g^a)^b \pmod{p}$, where g^{ab} is the key. Then encode and decode as the previous method using the key.

RSA Public Key

Public information: e such that $(e, (p-1)(q-1)) = 1$, $N = p \cdot q$
Secret information: p and q large prime

To encode: compute $m \equiv x^e \pmod{pq}$, send m.
To decode: find the inverse f such that $e \cdot f \equiv 1 \pmod{(p-1)(q-1)}$, computes $m^f \pmod{pq}$.

Remark: $m^f \equiv (x^e)^f \equiv x^{ef} \equiv x^{(p-1)(q-1)k+1} \equiv x^{\phi(pq)k+1} \equiv x \pmod{p}$

Quadratic Residue

Definition (Quadratic Residue): n is a positive integer, a is a unit in $\mathbb{Z}_n$.
If $x^2 \equiv a \pmod{n}$ has a solution, then it's a quadratic residue (QR). Otherwise, it's a quadratic non-residue (QNR).

Legendre Symbol and related properties
Let p be an odd prime. $(\frac{a}{p}) = 1$ if a is QR, $(\frac{a}{p}) = -1$ if a is NQR, $(\frac{a}{p}) = 0$ if $a = 0 \pmod p$.

- $(\frac{1}{p}) = 1$, $(\frac{a}{p}) = (\frac{a^{-1}}{p})$, $(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$
- If g is a primitive root, then $(\frac{g^k}{p}) = (-1)^k$.
- If a is a unit, then $(\frac{a^2}{p}) = 1$, $(\frac{a^2 b}{p}) = (\frac{b}{p})$.
- There are $\frac{p-1}{2}$ QR, and $\frac{p-1}{2}$ QNR.

$p \equiv 1 \pmod 4 \implies$ -1 is a QR
$p \equiv 3 \pmod 4 \implies$ -1 is a QNR

Euler's Criterion: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod p$

Gauss' Lemma and conclusions Suppose a is a unit mod p, write each of $a, 2a \cdots, \frac{p-1}{2}a$ between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$ mod p. Let n be the number of negative signs. Then $(\frac{a}{p}) = (-1)^n$.

$(\frac{2}{p}) = 1$ if $p \equiv 1, 7 \pmod 8$
$(\frac{2}{p}) = -1$ if $p \equiv 3, 5 \pmod 8$

$(\frac{3}{p}) = 1$ if $p = 1, 11 \pmod{12}$
$(\frac{3}{p}) = -1$ if $p = 5, 7 \pmod{12}$

Law of Quadratic Reciprocity: Suppose $p \neq q$ are odd primes, then:

$$(\frac{p}{q}) = (\frac{q}{p}) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Let $k \geq 3$, then a is a QR mod 2^k if and only if $a \equiv 1 \pmod 8$.