Number Theory Definitions

Based on lectures by Professor Henri Johnston

Notes taken by James Arthur

Contents

Theorem (Division Algorithm)**.** Given a $a \in \mathbb{Z}$ and a $b \in \mathbb{N}_1$ there exists unique integers q and r satisfying $a = bq + r$ and $0 \leq r < b$.

Theorem. Let $a, b \in \mathbb{Z}$, $\exists\, d \in \mathbb{N}_0$ and non-unique $x, y \in \mathbb{Z}$ such that,

1. $d \mid a$ and $d \mid b$
2. and if $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$, then $e \mid d$
3. $d = ax + by$

Theorem (Solubility of linear equations in $\mathbb{Z}$)**.** Let $a, b, c \in \mathbb{Z}$. The equation,

$$ax + by = c$$

is soluble with $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b) \mid c$

Theorem (Euclids Algorithm)**.** Let $a, b \in \mathbb{N}_1$ with $a > b > 0$ and $b \nmid a$. Let $r_0 = a$, $r_1 = b$ and apply the division Algorithm repeatedly to obtain a sequence of remainders defined sucessively,

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 && 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3 && 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_n + r_{n+1} && r_{n+1} = 0 \end{aligned}$$

Then the last non-zero remainder, r_n is the $\gcd(a, b)$.

Theorem. There are infinitely many primes

Theorem (Euclid's Lemma for Primes)**.** Let $a, b \in \mathbb{Z}$ and p be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Theorem (Fundamental Theorem of Arithmetic)**.** Let $1 < n \in \mathbb{N}_1$. Then,

1. (Existence) The number n can be written as a product of primes.

2. (Uniqueness) Suppose that,
$$n = p_1 \dots p_r = q_1 \dots q_s$$
where each p_i and q_j are prime. Assume further that,
$$p_1 \leq p_2 \leq \dots \leq p_r \qquad \text{and} \qquad q_1 \leq q_2 \leq \dots \leq q_s$$
Then $r = s$ and $p_i = q_i$ for all i

Theorem. There are infinitely many primes p with $p \equiv 3 \mod 4$

Theorem (Cancellation law for Congruences)**.** Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}_1$. Let $d = \gcd(c, n)$. Then $ac \mid bc \mod n \iff a \equiv b \mod \frac{n}{d}$. In particular, if n and c are coprime, then $ac \equiv bc \mod n \iff a \equiv b \mod n$.

Theorem (Linear Congruences with exactly one solution)**.** Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose that a and n are coprime. Then the linear congruence,
$$ax \equiv b \mod n$$
has exactly one solution.

Theorem (Solubility of a Linear Congruence)**.** Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Then the linear congruence,
$$ax \equiv b \mod n \tag{1}$$
has one or more solutions if and only if $\gcd(a, b) \mid b$.

Theorem. Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Let $d = \gcd(a, n)$. Suppose $d \mid b$ and write $a = da'$, $b = db'$ and $n = dn'$. Then the linear congruence
$$ax \equiv b \mod n \tag{2}$$
has exactly d solutions modulo n. These are,
$$t, t + n' + t + 2n', \dots, t + (d-1)n' \tag{3}$$
where t is the unique solution $\mod n'$ to,
$$a'x \equiv b' \mod n' \tag{4}$$

Theorem (Special Chinese Remainder Theorem)**.** Let $n, m \in \mathbb{N}$ be coprime and $a, b \in \mathbb{Z}$ be given. Then the pair of linear congruences,
$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$
has a solution $x \in \mathbb{Z}$. Moreover, if x' is another solution $x \equiv x' \mod mn$

Theorem (Chinese Remainder Theorem)**.** Let $n_1, n_2, \dots, n_t \in \mathbb{N}$ with $\gcd(n_i, n_j) = 1$ whenever $i \neq j$ and let $a_1, \dots, a_t \in \mathbb{Z}$ be given. Then the system of congruences
$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ &\vdots \\ x &\equiv a_t \mod n_t \end{aligned}$$
has a solution $x \in \mathbb{Z}$. Moreover if x' is any other solution, then $x' \equiv x \mod N$ where $N := n_1 n_2 \dots n_t$.

Theorem. Let $m, n \in N$ be coprime. Then $\varphi(mn) = \varphi(m)\varphi(n)$

Theorem. Let p be a prime and $r \in \mathbb{N}$. Then

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

Theorem (Euler-Fermat)**.** Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \mod n$.

Theorem (Fermat's Little Theorem)**.** Let p be a prime and let $a \in \mathbb{Z}$. Then $a^p \equiv a \mod p$.

Theorem (Legranges Polynomial Congruence Theorem)**.** Let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$$

and let p be a prime such that $p \not| a_d$. Then $f(x) \equiv 0 \mod p$ has at most d solutions $\mod p$.

Theorem (Hensel's Lemma)**.** Let p be a prime. Let $f(x) \in \mathbb{Z}[x]$ and let $f'(x) \in \mathbb{Z}[x]$ be it's formal derivative. If $a \in \mathbb{Z}$ satisfies,

$$f(x) \equiv 0 \mod p, \qquad f'(a) \not\equiv 0 \mod p$$

then for each $n \in \mathbb{N}$ there exists $a_n \in \mathbb{Z}$ such that

$$f(a_n) \equiv 0 \mod p \qquad \text{and } a_n \equiv a \mod p$$

Moreover, a_n is unique modulo p^n.

Theorem. Let p be a prime and let $d \in \mathbb{N}$ be a divisor of $p-1$. Then there are exactly $\phi(d)$ elements a mod p such that $\text{ord}_p(a) = d$. In particular there are $\phi(p-1)$ primitive roots $\mod p$.

Theorem (Primitive Root Test)**.** Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ where a and n are coprime. Then a is a primitive root $\mod n$ if and only if

$$a^{\frac{\phi(n)}{q}} \not\equiv 1 \mod n$$

for every prime $q \mid \phi(n)$.

Theorem. Let p be a prime. If g is a primitive root mod p, then g is also a primitive root mod p^e for all $e > 1$ if and only if $g^{p-1} \not\equiv 1 \mod p^2$.

Theorem. Let $n \in \mathbb{N}$. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic $\iff$ there exists a primitive root modulo n $\iff$ $n = 1, 2, 4, p^e, 2p^e$ where $e \in \mathbb{N}$ and p is an odd prime.

Theorem (Wilson's Theorem)**.** An integer is prime if and only if $(p-1)! \equiv -1 \mod p$.

Theorem (Eulers Criterion)**.** If p is an odd prime and $a \in \mathbb{Z}$ then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

Theorem (Multiplicity of Legendre's Symbol)**.** Let p be an odd prime and $a, b \in \mathbb{Z}$. Then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Theorem. If p is an odd prime then,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

In other words, $x^2 \equiv -1 \mod p$ is soluble if and only if $p \equiv 1 \mod 4$.

Theorem. There are infinitely many primes p with $p \equiv 1 \mod 4$.

Theorem (Gauss' Lemma)**.** Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then,

$$\left(\frac{a}{p}\right) = (-1)^{\Lambda} \qquad \Lambda = \#\{j \in \mathbb{N} : 1 \leq j \leq \frac{p-1}{2},\, \lambda(aj,p) > \frac{p}{2}\}$$

Theorem. There are infinitely many primes p with $p \equiv -1 \mod 8$

Theorem (LQR)**.** If p and q are distinct odd primes, then,

$$\begin{aligned}\left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ &= \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \mod 4 \text{ or } p \equiv 1 \mod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \mod 4 \end{cases}\end{aligned}$$

Theorem. Let n, m be odd positive integers and $a, b \in \mathbb{Z}$.

1. $\left(\frac{a}{n}\right) = \pm 1$ if a and n are coprime and $\left(\frac{a}{n}\right) = 0$, otherwise,
2. $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ whenever $a \equiv b \mod n$
3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ and $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$,
4. $\left(\frac{a^2}{n}\right) = 1$ whenever a and n are coprime.

Theorem. If n is an odd positive integer then,

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & n \equiv 1 \mod 4 \\ -1 & n \equiv 3 \mod 4 \end{cases}$$

Theorem. If n is an odd positive integer then,

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} +1 & n \equiv \pm 1 \mod 8 \\ -1 & n \equiv \pm 3 \mod 8 \end{cases}$$

Theorem (Reciprocity Law for Jacobi Symbols)**.** Let m and n be coprime odd positive integers. Then,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4} = \begin{cases} +1 & m \equiv 1 \mod 4 \text{ or } n \equiv 1 \mod 4 \\ -1 & m \equiv n \equiv 3 \mod 4. \end{cases}$$

Theorem. Let (x, y, z) be a primitive Pythagorean triple. Then $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.

Theorem. If (x, y, z) is a primitive triple, then one of x and y is even and the other odd. (Equivalently $x + y$ is odd). Also z must be odd.

Theorem. Let (x, y, z) be a primitive Pythagorean triple with x odd. Then there are $r, s \in \mathbb{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd, such that,

$$x = r^2 - s^2 \qquad y = 2rs \qquad z = r^2 + s^2$$

Conversely, if $r, s \in \mathbb{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd, then,

$$(r^2 - s^2, 2rs, r^2 + s^2)$$

is a primitive Pythagorean triple.

Theorem. There do not exist $x, y, z \in \mathbb{N}$ with,

$$x^4 + y^4 = z^4 \tag{5}$$

Theorem. The sets S_2 and S_4 are closed under multiplication. That is,

1. If $m, n \in S_2$, then $mn \in S_2$
2. If $m, n \in S_4$, then $mn \in S_4$.

Theorem. Let p be a prime and $p \equiv 3 \mod 4$ and let $n \in \mathbb{N}$. If $n \in S_2$ then $v_p(n)$ is even.

Theorem. Let p be a prime with $p \equiv 1 \mod 4$. Then $p \in S_2$.

Theorem (Two Square Theorem)**.** Let $n \in \mathbb{N}$. Then $n \in S_2$ if and only if $v_p(n)$ is even whenever p is a prime congruent to $3 \mod 4$.

Theorem. Let p be a prime. If $p = a^2 + b^2 = c^2 + d^2$ with $a, b, c, d \in \mathbb{N}$ then either $a = c$ and $b = d$ or $a = d$ and $b = c$.

Theorem. Let p be a prime. Then $p \in S_4$.

Theorem (Lagrange's four-square theorem)**.** If $n \in \mathbb{N}$ then $n \in S_4$