Number Theory Definitions

Based on lectures by Professor Henri Johnston

Notes taken by James Arthur

Contents

Definition (Well Ordering Principle)**.** Every non-empty subset of $\mathbb{N}_0$ contains a least element

Definition (Divisible)**.** We say that some $a \in \mathbb{Z}$ is divisible by some $b \in \mathbb{Z}$ if and only is,

$$\exists\, n \in \mathbb{Z}, \text{ such that } b = na$$

and denote it, $a \mid b$

Definition (Greatest Common Divisor)**.** Let $a, b \in \mathbb{Z}$. Them d of the previous corollary is just the greatest common divisor of a and b, written $\gcd(a, b)$. Also sometimes seen as $\mathrm{hcf}(a, b)$.

Definition (Prime)**.** A number $p \in \mathbb{N}_1$ with $p > 1$ is prime if and only if it's only divisors are 1 and p, i.e.

$$n \mid p \implies n = 1 \text{ or } n = p$$

Definition (Composite Numbers)**.** A number $n \in \mathbb{N}_1$ with $n > 1$ is composite if and only if it is not prime, i.e.

$$n = ab \qquad 1 < a, b \in \mathbb{N}$$

Definition. Let $n \in \mathbb{N}_1$ and p be a prime. Then,

$$v_p(n) := \max\{k \in \mathbb{N} \cup \{0\} : p^k \mid n\}$$

In other words, k is the unique non-negative integer such that $p^k \mid n$ but $p^{k+1} \mid n$. Equivalently, $v_p(n) = k$ if and only if $n = p^k n'$ where $n' \in \mathbb{N}$ and $p \nmid n'$.

Definition. Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}_1$. We write $a \equiv b \mod n$, and say 'a is congruent to b mod n', if and only if $n \mid (a - b)$. If $n \nmid (a - b)$ we say that a and b are incongruent mod n.

Definition (Residue Class)**.** Consider $n \in \mathbb{N}$, then $a \in \mathbb{Z}$ we write $[a]_n$ for an equivalence class $a \mod n$. Thus,

$$[a]_n = \{x \in \mathbb{Z} : x \equiv a \mod n\} = \{a + qn : q \in \mathbb{Z}\}$$

This is called the residue class of a modulo n

Definition (Complete Residue System)**.** Let $n \in \mathbb{N}_1$. If S is a subset of $\mathbb{Z}$ containing exctly one element of each residue class modulo n we say that S is a complete residue system modulo n.

Definition. Let $n \in \mathbb{N}$. We write $\mathbb{Z}/n\mathbb{Z} = \{[a]_n : 0 \leq a \leq n - 1\}$ (such that $|\mathbb{Z}/n\mathbb{Z}| = n$). We set $[a]_n + [b]_n := [a + b]_n$ and $[a]_n[b]_n := [ab]_n$. (We have showed that both of these are well defined).

Definition. Let $n \in \mathbb{N}$. Let $(\mathbb{Z}/n\mathbb{Z})^\times$ denote the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$. Explicitly, we have

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} : \exists\, [b]_n \in \mathbb{Z}/n\mathbb{Z} \text{ such that } [a]_n[b]_n = 1\}$$

Definition (Multiplicative inverse)**.** Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then the unique solution to $ax \equiv 1\ mod n$ is called the multiplicative inverse of $a \mod n$ and is denoted $[a]_n^{-1}$ or $a^{-1} \mod n$

Definition (Euler Phi Function)**.** For $n \in \mathbb{N}$ we define the φ function as,

$$\varphi(n) = \#\{a \in \mathbb{N} : 1 \leq a \leq n,\ \gcd(a, n) = 1\}$$

Definition (Order)**.** Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ and suppose $\gcd(a, n) = 1$. Then the least $d \in \mathbb{N}$ such that $a^d \equiv 1 \mod n$ is called the order of $a \mod n$ and is written $\mathrm{ord}_n(a)$

Definition (Reduced Residue System)**.** Let $n \in \mathbb{N}$. A subset $R \subseteq \mathbb{Z}$ is said to be a reduced residue system mod n if

- R contains $\varphi(n)$ elements
- no two elements of R are congruent $\mod n$ and,
- $\forall\, r \in R, \gcd(r, n) = 1$

Definition (Primitive Root)**.** Let $n \in \mathbb{N}$, we say $a \in \mathbb{Z}$ is a primitive root $\mod n$ if and only if $\gcd(a,\ n) = 1$ and $\mathrm{ord}_n(a) = \phi(n)$.

Definition (Quadratic Residue)**.** Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then a is a Quadratic Residue mod p if $\exists\, x \in \mathbb{Z}$ such that $x^2 \equiv a \mod p$ and a is a Quadratic Non-Residue if not.

Definition (Legendre Symbol)**.** Let p be an odd prime. For any $a \in \mathbb{Z}$, we define the Legendre Symbol to be,

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & p \nmid a \text{ and } a \text{ is a quadratic residue mod } p \\ -1 & p \nmid a \text{ and } a \text{ is not a quadratic residue mod } p \\ 0 & p \mid a \end{cases}$$

Definition. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. We write $\lambda(a, n)$ for the unique integer such that $a \equiv \lambda(a, n) \mod n$ and $0 \leq \lambda(a, n) < n$, ie. $\lambda(a, n)$ is the remainder of the division algorithm applied to a and n.

Definition (Floor Function)**.** For any $x \in \mathbb{R}$ we set $\lfloor x \rfloor := \max\{n \in \mathbb{Z}\}$

Definition (Jacobi Symbol)**.** Let n be an odd positive integer with prime factorisation $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Then for any $a \in \mathbb{Z}$ we define the Jacobi symbol $\left(\frac{a}{n}\right)$ by,

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i}$$

where the symbols on the right are Legendre symbols. We als define $\left(\frac{a}{1}\right) = 1$.

Definition (Pythagorean Triple)**.** A pythagorean triple (x, y, z) isa triple of positive integers satisfying

$$x^2 + y^2 = z^2$$

If $\gcd(x, y, z) = 1$ then (x, y, z) is called a primitive Pythagorean triple.

Definition (S_k)**.** For $k \in \mathbb{N}$ we let,

$$S_k = \{a_1^2 + a_2^2 + \dots + a_k^2 : a_1, \dots, a_k \in \mathbb{Z}\}$$

be the set of k squares. Note we allow zero.