Definitions, Theorems, etc.

2 Pythagorean Triples

Definition (Primitive Pythagorean Triple)**.** A *primitive Pythagorean triple* (PPT) is a triple of numbers (a, b, c) such that a, b, c have no common factors and satisfy

$$a^2 + b^2 = c^2.$$

Theorem 2.1 (Pythagorean Triple Theorem)**.** *We will get every primitive Pythagorean triple of* (a, b, c) *with* a *odd and* b *even using the formulas*

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

where $s > t \geqslant 1$ *are chosen to be any odd integers with no common factors.*

3 Pythagorean Triples and the Unit Circle

Theorem 3.1. *Every point on the circle*

$$x^2 + y^2 = 1$$

whose coordinates are rational numbers can be obtained from the formula

$$(x, y) = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right)$$

by substituting in rational numbers for m *(except for the point* $(-1, 0)$ *which is the limiting value as* $m \to \infty$*).*

4 Sums of Higher Powers and Fermat's Last Theorem

Theorem (Fermat's Last Theorem)**.** *No three positive integers* a, b, *and* c *satisfy the equation*

$$a^n + b^n = c^n$$

for all $n \geqslant 3$.

5 Divisibility and the Greatest Common Divisor

Definition (Greatest Common Divisor)**.** The *greatest common divisor* of two numbers a and b (not both zero) is the largest number that divides them both. It is denoted by $\gcd(a, b)$.

Definition (Relatively Prime)**.** If $\gcd(a, b) = 1$, then we say that a and b are *relatively prime*.

Definition (Least Common Multiple)**.** A number L is called a *common multiple* of m and n if both m and n divide L. The smallest such L is called the *least common multiple of* m *and* n and is denoted by $\operatorname{lcm}(m, n)$.

Theorem. *Let* $m, n \in \mathbb{Z}$. *Then*

$$\operatorname{lcm}(m, n) = \frac{mn}{\gcd(m, n)}.$$

Theorem 5.1 (Euclidean Algorithm)**.** *To compute the greatest common divisor of two numbers* a *and* b*, let* $r_{-1} = a$*, let* $r_0 = b$*, and compute successive quotients and remainders*

$$r_{i-1} = q_{i+1} \cdot r_i + r_{i+1}$$

for $i = 0, 1, 2, \ldots$ *until some remainder* r_{n+1} *is* 0*. The last nonzero remainder* r_n *is the greast common divisor of* a *and* b*.*

6 Linear Equations and the Greatest Common Divisor

Theorem 6.1 (Linear Equation Theorem)**.** *Let* a *and* b *be nonzero integers, and let* $g = \gcd(a, b)$*. Then the equation*

$$ax + by = g$$

always has a solution (x_1, y_1) *in integers, and this solution can be found by the Euclidean algorithm. Then every solution to the equation can be obtained by substituting integers* k *into the formula*

$$\left(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g}\right).$$

7 Factorization and the Fundamental Theorem of Arithmetic

Definition (Prime)**.** A *prime* integer is an integer $p \geqslant 2$ whose only (positive) divisors are 1 and p.

Definition (Composite). Integers $m \geqslant 2$ that are not primes are called *composite* numbers.

Theorem 7.2 (Prime Divisibility Property). *Let p be a prime number, and suppose that p divides the product $a_1 a_2 \cdots a_r$. Then p divides at least one of the factors $a_1, a_2, \ldots, a_r$.*

Theorem 7.3 (The Fundamental Theorem of Arithmetic). *Every integer $n \geqslant 2$ can be factored in a product of primes*

$$n = p_1 p_2 \cdots p_r$$

in exactly one way (up to rearrangement).

8 Congruences

Definition (Congruence). An integer a is *congruent* to b modulo m, and we write

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

if m divides $a - b$.

Proposition. $\equiv$ is an equivalence relation.

Proposition. Let $a, b, c, d \in \mathbb{Z}$. Assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

(i) $a + c \equiv b + d \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$.

Theorem 8.1 (Linear Congruence Theorem). *Let a, c and m be integers with $m \geqslant 1$, and let $g = \gcd(a, m)$.*

(a) If $g \nmid c$, then the congruence $ax \equiv c \pmod{m}$ has no solutions.

(b) If $g \mid c$, then the congruence $ax \equiv c \pmod{m}$ has exactly g incongruent solutions. To find the solutions, first find a solution (u_0, v_0) to the linear equation

$$au + mv = g$$

Then $x_0 = cu_0/g$ is a solution to $ax \equiv c \pmod{m}$, and a complete set of incongruent solutions is given by

$$x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m} \quad \text{for } k = 0, 1, \ldots, g - 1.$$

Theorem 8.2 (Polynomial Roots modulo p Theorem). *Let p be a prime number and let*

$$f(x) = a_0 d^d + a_1 d^{d-1} + \cdots + a_d$$

be a polynomial of degree $d \geqslant 1$ *with integer coefficients and with* $p \nmid a_0$. *Then the congruence*

$$f(x) \equiv 0 \pmod{p}$$

has at most d *incongruent solutions.*

9 Congruences, Powers, and Fermat's Little Theorem

Theorem 9.1 (Fermat's Little Theorem)**.** *Let* p *be a prime number, and let* a *be any number with* $a \not\equiv 0 \pmod{p}$. *Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

10 Congruences, Powers, and Euler's Formula

Definition (Euler Phi Function)**.** *Euler's phi function* is the is the function $\varphi(m) : \mathbb{N} \to \mathbb{N}$ defined by

$$\varphi(m) = \#\{\, a : 1 \leqslant a \leqslant m \text{ and } \gcd(a, m) = 1 \,\}.$$

Theorem 10.1 (Euler's Formula)**.** *If* $\gcd(a, m) = 1$, *then*

$$a^{\varphi(m)} = 1 \pmod{m}.$$

11 Euler's Phi Function and the Chinese Remainder Theorem

Theorem 11.1 (Phi Function Formulas)**.** *(a) If* p *is prime and* $k \geqslant 1$, *then*

$$\varphi\left(p^k\right) = p^k - p^{k-1}.$$

(b) If $\gcd(m, n) = 1$, *then* $\varphi(mn) = \varphi(m)\varphi(n)$.

Corollary. Let m be a positive integer and suppose $p_1, \dots, p_r$ are the distinct primes that divide m. Then

$$\varphi(m) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Theorem (Generalized Chinese Remainder Theorem)**.** *Let* $m_1, \dots, m_n \in \mathbb{Z}$ *such that* $\gcd(m_i, m_j) = 1$ *for all* $1 \leqslant i, j \leqslant n$ *with* $i \neq j$. *Let* $a_1, \dots, a_n \in \mathbb{Z}$. *Then the* *system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $M = \prod_{i=1}^{n} m_i$*, given by*

$$x \equiv \sum_{i=1}^{n} a_i \left(\frac{M}{m_i}\right) y_i,$$

where $y_i \equiv \left(\frac{M}{m_i}\right)^{-1} \pmod{m_i}$ *for all* $1 \leqslant i \leqslant n$*.*

12 Prime Numbers

Theorem 12.1 (Infinitude of Primes)**.** *There are infinitely many prime numbers.*

Theorem 12.2 (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** *Let* a *and* m *be integers with* $\gcd(a, m) = 1$*. Then there are infinitely primes that are congruent to* a *modulo* m*. That is, there are infinitely many prime numbers* p *satisfying*

$$p \equiv a \pmod{m}.$$

16 Powers Modulo m and Successive Squaring

Algorithm 16.1 (Successive Squaring to Compute a^k modulo m)**.** *The following steps compute the value of* $a^k \pmod{m}$*:*

1. *Write* k *as a sum of powers of 2.*

   $$k = u_0 + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + \cdots + u_r \cdot 2^r,$$

   where each u_i *is either* 0 *or* 1*. (This is called the binary expansion of* k*.)*

2. *Make a table of powers of* a *modulo* m *using successive squaring.*

$$\begin{array}{llll} a^1 & & & \equiv A_0 \pmod{m} \\ a^2 & \equiv (a^1)^2 & \equiv A_0^2 & \equiv A_1 \pmod{m} \\ a^4 & \equiv (a^2)^2 & \equiv A_1^2 & \equiv A_2 \pmod{m} \\ a^8 & \equiv (a^4)^2 & \equiv A_2^2 & \equiv A_3 \pmod{m} \\ & \vdots & & \vdots \\ a^{2r} & \equiv \left(a^{2^{r-1}}\right)^2 & \equiv A_{r-1}^2 & \equiv A_r \pmod{m} \end{array}$$

3. *The product*
$$A_0^{u_0} \cdot A_1^{u_1} \cdot A_2^{u_2} \cdots A_r^{u_R} \pmod{m}$$
will be congruent to $a^k \pmod{m}$. *Note that all the* u_i*'s are either* 0 *or* 1, *so this number is really the product of those* A_i*'s for which* u_i *equals* 1.

17 Computing k^{th} Roots Modulo m

Algorithm 17.1 (How to Compute k^{th} Roots modulo m)**.** *Let* b, k, *and* m *be given integers that satisfy*

$$\gcd(b, m) = 1 \quad \text{and} \quad \gcd(k, \varphi(m)) = 1.$$

The following steps give a solution to the congruence

$$x^k \equiv b \pmod{m}.$$

1. *Compute* $\varphi(m)$.
2. *Find positive integers* u *and* v *that satisfy* $ku - \varphi(m)v = 1$.
3. *Compute* $b^u \pmod{m}$ *by successive squaring. The value obtained gives the solution* x

18 Powers, Roots, and "Unbreakable" Codes

20 Squares Modulo p

Definition (Quadratic Residue modulo p)**.** A nonzero number that is congruent to a square modulo a prime p is called a *quadratic residue modulo* p; otherwise, it is called a *nonresidue modulo* p.

Theorem 20.1. *Let* p *be an odd prime. Then there are exactly* $(p-1)/2$ *quadratic residues modulo* p *and exactly* $(p-1)/2$ *nonresidues modulo* p.

Definition (Legendre Symbol of a modulo p)**.** The *Legendre symbol of* a *modulo* p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a nonresidue modulo } p. \end{cases}$$

Theorem 20.2 (Quadratic Residue Multiplication Rule)**.** *Let* p *be an odd prime. Then*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

21 Is -1 a Square Modulo p

Theorem 21.1 (Euler's Criterion). *Let p be an odd prime. Then*

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

22 Quadratic Reciprocity

Theorem 22.1 (Law of Quadratic Reciprocity). *Let p and q be distinct odd primes.*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}. \end{cases}$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}, \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}. \end{cases}$$

Definition (Jacobi Symbol of a modulo b). Let a and b be odd positive integers. Suppose b has factorization $b = \prod_{i=1}^{r} p_r$, where each p_i is a distinct prime. Then the *Jacobi symbol of* a *modulo* bis

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

Theorem 22.2 (Generalized Law of Quadratic Reciprocity). *Let a and b be odd positive integers.*

$$\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \pmod{4}, \\ -1 & \text{if } b \equiv 3 \pmod{4}. \end{cases}$$

$$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \text{ or } 7 \pmod{8}, \\ -1 & \text{if } b \equiv 3 \text{ or } 5 \pmod{8}. \end{cases}$$

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{a}{b}\right) & \text{if } a \equiv 1 \pmod{4} \text{ or } b \equiv 1 \pmod{4}, \\ -\left(\frac{a}{b}\right) & \text{if } a \equiv b \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}. \end{cases}$$

24 What Primes are Sums of Two Squares?

Theorem 24.1 (Sum of Two Squares Theorem for Primes). *Let p be a prime. Then p is a sum of two squares exactly when*

$$p \equiv 1 \pmod 4 \quad (\text{or } p = 2).$$

Algorithm (Method of Descent). *Let p be prime $\equiv 1 \pmod 4$.*

(i) Given $A^2 + B^2 = Mp$ with $1 < M < p$.

(ii) Choose numbers u and v with

$$u \equiv A \pmod M \quad \text{and} \quad v \equiv B \pmod M,$$

where $-\frac{M}{2} \leqslant u, v \leqslant \frac{M}{2}$.

(iii) Find $1 \leqslant r < M$ such that $r = \frac{u^2+v^2}{M}$.

(iv) If $r = 1$, conclude that

$$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = p;$$

otherwise, write

$$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = rp$$

and repeat.

27 Euler's Phi Function and Sums of Divisors

Definition. The function $F : \mathbb{Z} \to \mathbb{Z}$ is defined by

$$F(n) = \sum_{d|n} \varphi(d).$$

Lemma 27.1. If $\gcd(m, n) = 1$, then $F(mn) = F(m)F(n)$.

Theorem 27.1 (Euler's Phi Function Summation Formula). *Let $n \in \mathbb{Z}$. Then*

$$F(n) = n.$$

28 Powers Modulo P and Primitive Roots

Definition (Order of a modulo p)**.** Let a be an integer not divisible by the prime p. Then *order of* a *modulo* p, denoted $e_p(a)$, is the least positive exponent e such that $a^e \equiv 1 \pmod{p}$.

Theorem 28.1 (Order Divisibility Property)**.** *Let* a *be an integer not divisible by the prime* p*, and suppose that* $a^n \equiv 1 \pmod{p}$*. Then the order* $e_p(a)$ *divides* n*. In particular, the order* $e_p(a)$ *always divides* $p-1$*.*

Definition (Primitve Root modulo p)**.** A number g with maximum order $e_p(g) = p-1$ is called a *primitive root modulo* p.

Theorem 28.2 (Primitve Root Theorem)**.** *Every prime* p *has a primitive root. More precisely, there are exactly* $\varphi(p-1)$ *primitive roots modulo* p*.*

Definition. Define $\psi : \mathbb{N} \to \mathbb{N}$ by

$$\psi(d) = \#\{\, a : 1 \leqslant a \leqslant p \text{ and } e_p(a) = d \,\}.$$

Proposition. If n divides $p-1$, then the congruence

$$X^n - 1 \equiv 0 \pmod{p}$$

has exactly n solutions with $0 \leqslant X < p$.