Part II – Number Theory

Based on lectures by Prof. A. Scholl
Notes taken by Bhavik Mehta

Michaelmas 2017

0 Introduction

Number theory is concerned with the (non-obvious, sometimes mysterious) properties of the integers, $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ and the rationals, $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$. It has been around for thousands of years, and has always been an experimental science where one can conduct experiments with numbers to spot their properties. Experimental data leads to conjectures which can turn out to be very hard to prove, for instance:

1. Congruent number problem: Let $N \geq 1$ be an integer of the form $8n + 5$, $8n + 6$ or $8n + 7$. Does there exist a right-angled triangle with sides of rational length, and area equal to N?

2. Twin prime conjecture: Does there exist infinitely many primes p such that $p + 2$ is also prime? Very recently, we know there are infinitely many primes p such that $\{p + 2, p + 4, \dots, p + 246\}$ contains a prime.

3. $\pi(x)$ refers to the prime counting function, the number of prime numbers $p \leq x$. The prime number theorem says that $\pi(x) \sim \operatorname{li}(x) := \int_2^x \frac{dt}{\log t}$. t is not known whether or not $|\pi(x) - \operatorname{li}(x)| \leq \sqrt{x} \log(x)$, which is equivalent to the Riemann hypothesis - a statement about a certain complex analytic function.

Problem 1 follows from the Birch-Swinnerton-Dyer conjecture, related to algebraic geometry. Often these proofs can require sophisticated theorems, well beyond the statement of the problem.

1 Euclid's algorithm and factoring

Definition (Division algorithm)**.** Given $a, b \in \mathbb{Z}$, with $b > 0$, there are $q, r \in \mathbb{Z}$ with $0 \leq r < b$ and $a = bq + r$, that is, we can divide a by b to give a quotient q and remainder r.

Proof. Let $S = \{\, a - nb \mid n \in \mathbb{Z} \,\}$, which certainly contains some non-negative integers. Let r be the least of them which exists by the well ordering property of the non-negative integers. Claim $r < b$, since if not then $r - b \in S$, and $r - b \geq 0$, contradicting the choice of r. $\square$

Notation. If $r = 0$ (that is, $a = bq$ for some $q \in \mathbb{Z}$), write $b \mid a$ (read as 'b divides a'), otherwise write $b \nmid a$.

Given $a_1, \ldots, a_n \in \mathbb{Z}$ not all zero, let

$$I = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in \mathbb{Z}\}$$

We recognise this from GRM as the ideal generated by $\{a_1, \ldots, a_n\}$. Note if $a, b \in I$, for any choice $l, m \in \mathbb{Z}$ then $la + mb \in I$.

Lemma 1.1. $I = d\mathbb{Z} = \{\lambda d \mid \lambda \in \mathbb{Z}\}$ for some $d \leq 1$, clearly unique.

Proof. As not all of a_i are 0, I contains some positive integer, let d be the least of them. So, $d \in I$, and hence $d\mathbb{Z} \subset I$. On the other hand, for $a \in I$ the ives us $a = qd + r$ with $0 \leq r < d$. But then $r = a - dq \in I$ so by minimality of d we have $r = 0$, and so $a \in d\mathbb{Z}$, giving $I \subset d\mathbb{Z}$ as required. $\square$

Definition (Greatest common divisor)**.** $a_i \in I = d\mathbb{Z}$ so $d \mid a_i$. If in addition, we have that $\forall i$, $e \mid a_i$, then e divides every element of I, so $e \mid d$. Write $d = \gcd(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$, the **greatest common divisor** (alternatively the highest common factor).

The study of **Diophantine equations** involves solving equations with integer solutions, and may have more variables than equations. The simplest case is is linear in two variables, and can be solved easily.

Corollary. Let $a, b, c \in \mathbb{Z}$ with not both a, b equal to 0. Then we can find $x, y \in \mathbb{Z}$ such that $ax + by = c \Leftrightarrow (a, b) \mid c$.

The definition of the greatest common divisor given here is non-constructive, but **Euclid's algorithm** is an efficient way to compute it.

Euclid's algorithm Assume $a > b > 0$. Apply successively the division algorithm:

$$\begin{aligned}
a &= q_1 b + r_1 & 0 &\leq r_1 < b \\
b &= q_2 r_1 + r_2 & 0 &\leq r_2 < b \\
r_1 &= q_3 r_2 + r_3 & 0 &\leq r_3 < b \\
&\vdots \\
r_{k-2} &= q_k r_{k-1} + r_k & 0 &\leq r_k < b \\
r_{k-1} &= q_{k+1} r_k + 0
\end{aligned}$$

for some k, so $r_k \mid r_{k-1}$ We claim $r_k = (a, b)$. Indeed, $(a, b) = (a - q_1 b, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k$.

Remark. By lemma 1.1, $(a, b) = ra + sb$ for some integers r, s. Euclid's algorithm gives such r, s.

Recall that if $n > 1$ then n is **prime** if its only positive divisors are $\{1, \ldots, n\}$, otherwise n is **composite**.

Lemma 1.2. Let p be prime, $a, b \in \mathbb{Z}$. Then $p \mid ab \implies p \mid a$ or $p \mid b$.

Proof. Suppose $p \mid ab$, $p \nmid a$. Then $\gcd(a, b) \neq p$, so it must be 1. So $\exists r, s \in \mathbb{Z}$ such that $ar + ps = 1$. Therefore, $b = (ab)r + p(bs)$, and hence $p \mid b$. □

This lets us prove the fundamental theorem of arithmetic.

Theorem (Fundamental theorem of arithmetic)**.** Every integer $n > 1$ can be written as a product of primes, and this representation is *unique* up to ordering.

Proof. Existence is trivial. Uniqueness: suppose $n = p_1 \ldots p_r = q_1 \ldots q_s$. $p_1 \mid n$, so p_1 divides some q_j. Hence $p_1 = q_j$ and so we can cancel p_1 and q_j from the relation, and repeat the process for $\frac{n}{p_1}$, eventually giving that the $\{p_1, \ldots, p_r\}$ are the same as the $\{q_1, \ldots, q_s\}$, up to ordering. □

If we know $a = \prod_{i=1}^k p_i^{\alpha_i}$, $b = \prod_{i=1}^k p_i^{\beta_i}$ for $\alpha_i, \beta_i \geq 0$ and p_i are distinct primes, then by uniqueness of prime factorisation,

$$(a, b) = \prod_{i=1}^{k} p_i^{\gamma_i}, \quad \gamma_i = \min(\alpha_i, \beta_i)$$

However if a, b are large, this is an inefficient way to compute GCDs.

Definition. An algorithm with input an integer $N > 0$ is **polynomial time** if $\exists b, c > 0$ for which the algorithm completes after less than $c(\log N)^b$ 'elementary operations'. Examples of elementary operations include adding or multiplying digits in some fixed base.

If there are k integer inputs, we require less than $c(\max_k(\log N_i))^b$ operations.

Example.

- Adding, multiplying integers (usual method)
- Computing GCDs by Euclid's algorithm
- Testing if N is prime (recent discovery, 2002)

Factoring What about factoring N? The obvious method is trial division by integers $\leq \sqrt{N}$. If $N = pq$, then $p, q \sim \sqrt{N}$ this will take $\sqrt{N}$ divisions - asymptotically larger than any power of $\log N$. For instance, if N has 100 digits, and we can do 2^9 divisions every second, this will take around $10^{50}/2^9$ seconds, which is about 6×10^{39} years. However, Euclid's algorithm will compute the GCD of two such numbers in a few milliseconds. However, there are better algorithms for factoring which we will see later, but so far no polynomial-time algorithm is known (important for security of encryption algorithms like RSA). These are practical for numbers with fewer than 200 digits (for a large computer - the record is 232 digits using thousands of computers and several months)

We will study the distribution of primes and the counting function later. For now,

Theorem (Euclid)**.** There are infinitely many primes

Proof. It is enough to show that given N, there is a prime $p > N$. Let q be the largest prime $\leq N$, and set $M = (2 \times 3 \times 5 \times \cdots \times q) + 1$. If p is any prime factor of M, then $p \notin \{ 2, 3, \ldots, q \}$ so $p > N$. □

Remark. This is constructive, in that it gives a way to find a prime greater than any N, but is is not efficient. For instance, if $N = 1000$, M has over 400 digits.

Finding large primes For reasonable size numbers (fewer than 1000 digits), it is reasonable to pick numbers at random and test for primality. For very large primes, there are special (faster) tests for primality of numbers of the form $N = 2^q - 1$, called Mersenne numbers. Using these, it has been shown that that $2^q - 1$ is prime when $q = 74207281$.

2 Congruences

Fix $n \geq 1$ (the modulus). Typically we will use $n > 1$.

Definition. $a \equiv b \pmod{n}$ if $n \mid a - b$, and we say 'a is congruent to b mod n'

This defines an equivalence relation on $\mathbb{Z}$. Write $\mathbb{Z}/n\mathbb{Z}$ for the set of equivalence classes $\{ a + n\mathbb{Z} \}$, where $a + n\mathbb{Z} = b + n\mathbb{Z} \iff a \equiv b \pmod{n}$. It is easy to see that the operations of addition and multiplication in $\{ a + n\mathbb{Z} \}$ are well defined. [In other words, $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring.]

Lemma 2.1. Let $a \in \mathbb{Z}$. The following are equivalent:

i. $(a, n) = 1$

ii. $\exists b \in \mathbb{Z}$ with $ab \equiv 1 \pmod{n}$

iii. (The equivalence class of) a is a generator of the group $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proof.

i. $\Rightarrow$ ii. If $(a, n) = 1$, $\exists b, c \in \mathbb{Z}$ with $ab + nc = 1$ so $ab \equiv 1 \pmod{n}$

ii. $\Rightarrow$ i. $ab \equiv 1 \pmod{n} \iff ab + kn = 1$, for some $k \in \mathbb{Z} \implies (a, n) = 1$

ii. $\Leftrightarrow$ iii. $ab \equiv 1 \pmod{n}$ for some $b \iff 1$ belongs to the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by $a \iff$ the subgroup generated by a is $\mathbb{Z}/n\mathbb{Z}$

□

Notation. For $n > 1$, we write $(\mathbb{Z}/n\mathbb{Z})^*$ to denote the set of units (invertible elements) of $\mathbb{Z}/n\mathbb{Z}$. By lemma 2.1, this is the set of classes $a + n\mathbb{Z}$ where $(a, n) = 1$. We can then define $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^* = \# \{ a \in \mathbb{Z} \mid 1 \leq a \leq n, \ (a, n) = 1 \}$, the **Euler ϕ-function**.

Remark. For $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ every non-zero element has an inverse under X $\iff$ n is prime $\iff$ $\phi(n) = n - 1$.

Theorem (Euler-Fermat Theorem)**.** If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Proof. $(n > 1)$ Apply Lagrange's theorem to the group $G = (\mathbb{Z}/n\mathbb{Z})^*$ which has order $\phi(n)$. Then $a \in \mathbb{Z}$ with $(a, n) = 1$ defines an element of G whose order divides $\phi(n)$. So $a^{\phi(n)} \equiv 1 \pmod{n}$. □

This has an important special case, called Fermat's Little Theorem.

Theorem (Fermat's Little Theorem)**.** If p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Proof. Trivial if $p \mid q$. If not, $(a, p) = 1$ so $a^{\phi(p)} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}$ □

Lemma 2.2. Let G be a cyclic group of order $n \geq 1$. Then

$$\begin{aligned} \varphi(n) &= \# \{ g \in G \mid (\text{order of } g) = n \} \\ &= \# \text{ of generators of } G \end{aligned}$$

Proof. We may assume $G = \mathbb{Z}/n\mathbb{Z}$, in which case this is just (2.1) □

2.1 Simultaneous Congruences

Example. We would like to find all $x \in \mathbb{Z}$ such that $x \equiv 7 \pmod{10}$ and $x \equiv 3 \pmod{10}$. One way might be to try $7, 17, 27, \dots$ in turn.

A better way: suppose we have $u, v \in \mathbb{Z}$ such that

$$\begin{aligned} u &\equiv 1 \pmod{10} & \qquad v &\equiv 0 \pmod{10} \\ u &\equiv 0 \pmod{13} & \qquad v &\equiv 1 \pmod{13} \end{aligned}$$

Then $x = 7u + 3v$ is a solution.

To find u, v: $(10, 13) = 1$ so $\exists r, s$ with $10r + 13s = 1$, so setting $u = 13s$ and $v = 10r$ ensures the above congruences are satified. From the Euclidean algorithm, we see $r = 4$ and $s = -3$ work, so $u = -39$ and $v = 40$.

We can confirm $x = 7(-39) + 3(40) \equiv 107 \pmod{130}$ is a solution. In fact, the set of all solutions is $\{\, x \mid x \equiv 107 \pmod{130} \,\}$.

This is a special case of

Theorem (Chinese Remainder Theorem)**.** Let $m_1, \dots, m_k$ be integers ≥ 1 with $(m_i, m_j) = 1$ if $i \neq j$ (they are pairwise coprime). Write $M = m_1 \cdots m_k$ for $k \geq 2$. Let $a_1, \dots, a_k \in \mathbb{Z}$. Then there exists a solution $x \in \mathbb{Z}$ of

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{1}$$

and x is unique mod M.

Remark. If x satisfies equation (1), then so does $x + Mn$ for $n \in \mathbb{Z}$, so the solution is just $x + M\mathbb{Z}$.

Proof.

- Uniqueness: If x, y satisfies equation (1), then $m_i \mid (x - y)$ for every i. As no prime divides two of the m_i, it follows that $M = \prod m_i \mid (x - y)$, so $x \equiv y \pmod{M}$.
- Existence: Write $M_i = M/m_i = \prod_{j \neq i} m_j$. By the hypothesis, $(M_i, m_i) = 1$. So $\exists c_i \in \mathbb{Z}$ with $c_i M_i \equiv 1 \pmod{m_i}$. Obviously $c_i M_i \equiv 0 \pmod{m_j}$ $\forall j \neq i$. Let $x = \sum_{i=1}^{k} a_i c_i M_i$, then x satisfies equation (1), as required.

□

Note we find the c_i by Euclid's algorithm, so this is constructive.

Corollary. If $M = \prod_{i=1}^{k} m_i$, with m_i pairwise coprime, then

$$\varphi(M) = \varphi(m_1) \cdots \varphi(m_k)$$

Proof. $(a, M) = 1 \Leftrightarrow \forall i, (a, m_i) = 1$. So by Chinese Remainder Theorem, we have a bijection

$$\{\, 1 \leq x \leq M \mid (x, M) = 1 \,\} \xleftrightarrow{\sim} \{\, (a_1, \dots, a_k \mid 1 \leq a_i \leq m_i, (a_i, m_i) = 1 \,\}$$

So

$$\#\text{LHS} = \varphi(M)\ ,\ \#\text{RHS} = \prod_i \varphi(m_i)$$

□

Algebraic aside: We can write thus in terms of the rings $R_i = \mathbb{Z}/m_i\mathbb{Z}$.

Definition (Product Ring)**.** The **product ring** is

$$R_1 \times \cdots \times R_k = \{ (r_1, \ldots, r_k) \mid r_i \in R_i \}$$

with +, × defined component-wise. This is a ring with 0 as the zero vector, and 1 as the vector of ones.

Theorem 2.3. Take $M = \prod m_i$, with m_i pairwise coprime. The map

$$\begin{aligned} \Theta : \mathbb{Z}/M\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ a + M\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \ldots, a + m_k\mathbb{Z}) \end{aligned}$$

is an isomorphism of rings.

Proof. $m_i \mid M \Rightarrow a + m_i\mathbb{Z}$ only depends on $a + M\mathbb{Z}$, so Θ is well-defined. It is a homomorphism (by definition of +, × in the product ring), and the Chinese Remainder Theorem implies that it is bijective. □

Definition (Multiplicative function)**.** A **multiplicative function** is a function $f : \mathbb{N} = \{ 1, 2, 3, \ldots \} \to \mathbb{C}$ for which

$$(m, n) = 1 \implies f(mn) = f(m)f(n)$$

(This is the traditional terminology, although it is confusing we don't require $\forall m, n, f(mn) = f(m)f(n)$, which is sometimes called **totally multiplicative**)

Example. Examples of multiplicative functions.

- $\varphi(n)$
- $\tau(n) = \#$ of positive divisors of n
- $\sigma(n) = \sum_{1 \le d \mid n} d$
- More generally $\sigma_k(n) = \sum_{1 \le d \mid n} d^k$, note $\sigma = \sigma_1, \tau = \sigma_0$

Lemma 2.4. Let f be a multiplicative function. Then so is g, defined by

$$g(n) = \sum_{d \mid n} f(d)$$

Proof. Let $(m, n) = 1$. Then $\{ \text{divisors } d \text{ of } mn \} = \{ d = d_1 d_2 \mid d_1 \mid m, d_2 \mid n \}$.

$$g(mn) = \sum_{d \mid mn} f(d) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1 d_2) = \sum_{d_1 \mid m} f(d_1) \sum_{d_2 \mid n} f(d_2) = g(m)g(n)$$

□

Example. $f(n) = n^k$ (obviously multiplicative). Then $g(n) = \sigma_k(n)$. Later we will see how to recover f from g.

Theorem 2.5.

(i) p prime, $k \leq 1 \implies \varphi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$

(ii) $n \geq 1$: $\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$

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

Proof.

(i) $\varphi(p^k) = \#\{\, 1 \leq a \leq p^k \mid p \nmid a \,\} = p^k - p^{k-1}$

(ii) Write

$$n = \prod_i p_i^{k_i}$$

with p_i distinct. Then,

$$\begin{aligned}\varphi(n) &= \prod_i \varphi(p_i^{k_i}) \\ &= \prod_i p_i^{k_i}\left(1 - \frac{1}{p_i}\right) \\ &= n\prod_i\left(1 - \frac{1}{p_i}\right)\end{aligned}$$

(iii) By the previous lemma 2.4, the left hand side is multiplicative. The right hand side is obviously multiplicative, so it is enough to prove for $n = p^k$.

$$\begin{aligned}\sum_{d|n}\varphi(d) &= \varphi(1) + \varphi(p) + \cdots + \varphi(p^k) \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) \\ &= p^k\end{aligned}$$

□

2.2 Polynomial Congruences

We will take $R = \mathbb{Z}, \mathbb{Q}$ or $\mathbb{Z}/n\mathbb{Z}$ (or any commutative ring with 1)

Recall $R[X]$ refers to polynomials in X taking coefficients from R, formally:

$$\{\, a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \mid n \geq 0,\ a_i \in R \,\}$$

Two polynomials are equal if their coefficients are the same. Importantly, a polynomial $f \in R[X]$ determines a function $R \to R$, given by $\alpha \mapsto f(\alpha) = \sum a_i\alpha^i$. It can happen that different polynomials give the same function.

Example. For p a prime and $R = \mathbb{Z}/p\mathbb{Z}$, consider $f(X) = X^p - X$. Then $\forall a \in R$, $f(a) = 0$ in $\mathbb{Z}/p\mathbb{Z}$ by Fermat's Little Theorem. So f and the zero polynomial determine the same function.

Multiplication and addition of polynomials is defined in the obvious way: for $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{n} b_i X_i$, we have

$$f + g = \sum_{i=0}^{n} (a_i + b_i) X^i$$

$$fg = \sum_{i=0}^{2n} \left(\sum_{j+k=i} a_j b_k \right) X^i$$

so $R[X]$ is a ring.

We also have a division algorithm for polynomials, where the measure of size is the degree.

Definition. $\deg(f)$ is the largest i for which the coefficient of X^i is non-zero, and $\deg(f) = \infty$ if f is the zero polynomial.

We also have $\deg(fg) \leq \deg(f) + \deg(g)$.

Definition (Divison algorithm for polynomials)**.** Let $f, g \in R[X]$. Assume that the leading coefficient of g is a unit in R (that is, has an inverse under multiplication) Then $\exists q, r \in R[X]$ with $\deg(r) < \deg(g)$ and $f = gq + r$.

Proof. Induction on $\deg f$. If $\deg f < \deg g$, then $q = 0$ and $r = f$ will do.

Otherwise $f = aX^m + \ldots$, $a \neq 0$, $g = bX^n + \ldots$, with $b = \frac{1}{c}$ invertible by assumption and $m \geq n$.

Then $f_1 = f - acX^{m-n}g \in R[X]$ has degree strictly less than m. So $f_1 = gq_1 + r$ say, $\deg(r) < \deg(g)$ and so $f = (q_1 + acX^{m-n})g + r$, as required. □

Corollary 2.6 (Remainder theorem)**.** Take $f \in R[X]$ and $\alpha \in R$. Then

$$f(X) = (X - \alpha) f_1(X) + f(\alpha)$$

Proof. Apply the division algorithm with $g = X - a$, so $f = (X - \alpha) f_1 + c$. c has degree less than 1, so must be in R. Now, evaluate both sides at $X = \alpha$, so $c = f(\alpha)$. □

In particular, if $f(\alpha) = 0$ then $f(X) = (X - \alpha) f_1(X)$.

However in general a polynomial can have more roots than its degree - consider $f(X) = X^2 - 1$ with $R = \mathbb{Z}/8\mathbb{Z}$

Definition. A nonzero ring R is an integral domain if $ab = 0$ implies $a = 0$ or $b = 0$.

Example. $\mathbb{Q}$ and $\mathbb{Z}$ are integral domains, and $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if N is prime.

Theorem 2.7. If R is an integral domain, and $f \in R[X]$ is a non-zero polynomial of degree $n \geq 0$, then f has $\leq n$ roots in R.

Corollary (Lagrange's Theorem)**.** Take p prime, $f \in \mathbb{Z}[X]$ of degree n, and f not divisible by p. Then the congruence $f(x) \equiv 0 \pmod{p}$ has $\leq n$ solutions mod p.

Proof. The $n = 0$ case is trivial.

Suppose $n > 0$. If f has no roots in R, we have nothing to prove.

Otherwise $\exists \alpha \in R$, $f(\alpha) = 0$ so $f(X) = (X - \alpha)f_1(X)$, $f_1 \in R[X]$ with $\deg(f_1) = n - 1$. By induction, f_1 has $\leq n - 1$ roots in R. If β is a root of f, then $(\beta - \alpha)f_1(\beta) = 0$ so either $\beta = \alpha$ or $f_1(\beta) = 0$, as R is an integral domain. So, the roots of f are exactly α and the roots of f_1, so f has $\leq n$ roots. □

Example. Take p prime, and set

$$f(X) = X^{p-1} - 1 - \prod_{a=1}^{p-1}(X - a) \in \mathbb{Z}/p\mathbb{Z}[X]$$

Then, $\deg f \leq p - 2$. If $a = 1, \dots, p = 1$ then $a^{p-1} \equiv 1 \pmod p$ so $f(a) = 0 \in \mathbb{Z}/p\mathbb{Z}$. So as f has $\geq p - 1$ roots mod p, it must be identically zero mod p. So $f(0)$ is zero mod p, and

$$-1 - \prod_{a=1}^{p-1}(-a) \equiv 0 \pmod p$$

Giving us Wilson's Theorem, $(p - 1)! \equiv -1 \pmod p$.

The additive group $(\mathbb{Z}/n\mathbb{Z}, +)$ is cyclic. What about $((\mathbb{Z}/n\mathbb{Z})^*, \times)$?

Example. Consider $n = 7$, then we can check 3 is a generator of $(\mathbb{Z}/n\mathbb{Z})^*$ and hence the group is cyclic.

Theorem 2.8. If p is prime, then $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$.

Proof. $\#G = p - 1 = \sum_{d|p-1} \phi(d)$ by theorem 2.5 part (iii).

Also, by Lagrange's Theorem in elementary group theory,

$$\#G = \sum_{d|p-1} \#\{\, g \in G \text{ of order d} \,\} = \sum_{d|p-1} N_d$$

Suppose G is not cyclic, so G has no element of order $p - 1$, then $N_{p-1} = 0 < \phi(p - 1)$. As $\sum \phi(d) = \sum N_d$, there exists some d for which $N_d > \phi(d) > 0$. Let $\alpha \in G$ be an element of order d. Then $\langle\alpha\rangle \coloneqq \{\, 1, \alpha, \alpha^2, \dots, \alpha^{d-1} \,\} \subset G$ is a cyclic subgroup of order d so has exactly $\phi(d)$ elements of order d by lemma 2.2. So $\exists \beta \notin \langle\alpha\rangle$ where β has order d. Then $1, \alpha, \alpha^{d-1}, \beta$ are $(d + 1)$ roots of the polynomial $X^d - 1$, contradicting theorem 2.7. So, G must be cyclic. □

Definition (Primitive root)**.** If g is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ then g is said to be a **primitive root mod** p.

By theorem 2.8, primitive roots exist.

Example. Take $p = 19$, and let d be the order of 2 inside $(\mathbb{Z}/19\mathbb{Z})^*$, then $d \mid p-1 = 18$. We have $2^6 \equiv 7 \not\equiv 1 \pmod{19}$, so $d \nmid 6$. Similarly, $2^9 \equiv -1 \pmod{19}$ so $d \nmid 9$. Hence, $d = 18$ and 2 is a primitive root mod 19.

There are many unsolved problems about primitive roots:

1. Artin's Primitive Root conjecture:

   Fix $g \geq 2$. Then there eixst infinitely many p for which g is a primitive root mod p (say g is prime). Even the case $g = 2$ is unknown. From analytic number theory, it is known there are infinitely many p for which one of $2, 3, 5$ is a primitive root.

2. How large is the smallest primitive root mod p?

   We can show that this goes to ∞ as p grows. It is known that is is bounded above by $cp^{1/4+\epsilon}$ for any $\epsilon > 0$, but expected to be smaller (bounded by $c(\log p)^2$).

Now let's consider the more general case of $(\mathbb{Z}/p^n\mathbb{Z})^*$ for $n > 1$, and ask if it is cyclic. $(\mathbb{Z}/8\mathbb{Z})^* = \{\pm 1, \pm 3\}$, which all have order 1 or 2, so the group is not cyclic. If $n \geq 3$, the map $(\mathbb{Z}/2^n\mathbb{Z})^* \to (\mathbb{Z}/8\mathbb{Z})^*$ is surjective:

$$\forall n \geq 1, \quad (x, 8) = 1 \iff x \text{ odd } \iff (x, 2^n) = 1$$

So, $(\mathbb{Z}/2^n\mathbb{Z})^*$ is not cyclic for $n \geq 3$ since a generator would map to a generator of $(\mathbb{Z}/8\mathbb{Z})^*$.

Theorem 2.9. If $p > 2$ and $n \geq 1$ then $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic.

Proof. The proof is deferred until page 12 □

Lemma 2.10. Take p an odd prime, and let $y \in \mathbb{Z}$ and $k \geq 1$. Then,

(i) If $x \equiv 1 + p^k y \pmod{p^{k+1}}$ then $x^p \equiv 1 + p^{k+1} y \pmod{p^{k+2}}$

(ii) $(1 + py)^{p^k} \equiv 1 + p^{k+1} y \pmod{p^{k+2}}$

Proof.

(i) We may as well assume (by replacing y with $y + pz$) that $x = 1 + p^k y$. Then,

$$\begin{aligned} x^p &= \sum_{j=0}^{p} \binom{p}{j} (p^k y)^j \\ &= 1 + p^{k+1} y + \sum_{j=2}^{p-1} \binom{p}{j} p^{kj} y^j + p^{p^k} y^p. \end{aligned}$$

For $2 \leq j \leq p - 1$, we have $\binom{p}{j} \equiv 0 \pmod{p}$ and hence $\binom{p}{j} p^{kj} \equiv 0 \pmod{p^{2k+1}}$ and $2k+1 \geq k+2$. Since $p > 2$, we have $p^k \geq k+2$ so the last term is also $\equiv 0 \pmod{p^{k+2}}$, hence we are done.

(ii) Apply part (i) k times to $1 + py$.

□

Lemma 2.11. If $g \in \mathbb{Z}$, $(g, p) = 1$, g is a primitive root mod p, and $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a generator of $(\mathbb{Z}/p^n\mathbb{Z})^* = G$.

Proof. Let d be the order of g in G. We know $d \mid \#G = p^{n-1}(p-1)$, so if g is not a generator, one of the following two cases must hold:

(i) $d \mid p^{n-2}(p-1)$, so $g^{p^{n-2}(p-1)} \equiv 1 \pmod{p^n}$.

(ii) $d = p^{n-1}e$, with $1 \leq e < p-1$ and $e \mid p-1$, and so $g^{p^{n-1}e} \equiv 1 \pmod{p^n}$.

Deal with these cases in turn:

(i) Let $x = g^{p-1} = 1 + py$ with $y \not\equiv 0 \pmod{p}$, because $g^{p-1} \not\equiv 1 \pmod{p^2}$. Then by lemma 2.10 part (ii), we have $x^{p^{n-2}} \equiv 1 + p^{n-1}y \pmod{p^n}$, so $g^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$.

(ii) $g^{p^{n-1}e} \equiv g^e \pmod{p}$ by Fermat-Euler, and this is not congruent to $1 \pmod{p}$ as g is a primitive root mod p.

So neither (i) nor (ii) can hold, and hence g has order $p^{n-1}(p-1)$. □

We can return and prove theorem 2.9.

Proof of theorem 2.9. Let $g \in \mathbb{Z}$ be a primitive root mod p. If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then by lemma 2.11, g generates $(\mathbb{Z}/p^n\mathbb{Z})^*$. If not, $g^p \equiv g \pmod{p^2}$. Let $g_1 = g(1+p)$. Then, $g_1^p = g^p(1+p)^p$ and $(1+p)^p \equiv 1 \pmod{p^2}$ by lemma 2.10.

So, $g_1^p \equiv g^p \pmod{p^2} \equiv g \pmod{p^2} \not\equiv g_1 \pmod{p^2}$, so by lemma 2.11, g_1 generates $(\mathbb{Z}/p^n\mathbb{Z})^*$. □

Remark.

1. Our proof gives an easy way to find a generator for $(\mathbb{Z}/p^n\mathbb{Z})^*$, independent of $n \geq 2$.

2. What happens when $p = 2$? Lemma 2.10(i) fails to hold for $p = 2$, $k = 1$: $(1+2)^2 \equiv 1 \pmod{8}$. It does hold for $p = 2$ and $k \geq 2$ however. Part (ii) becomes $(1+4)^{k-1} \equiv 1 + 2^{k+1} \pmod{2^{k+2}}$. We can then show (following the argument for p odd), that $(\mathbb{Z}/2^n\mathbb{Z})^*$ for $n \geq 3$ is generated by -1 and 5 which have orders 2 and 2^{n-2} respectively. So, we have that
$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$

3. If $N = \prod_{1 \leq i \leq r} p_i^{k_i}$, then
$$(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/{p_1}^{k_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/{p_r}^{k_r}\mathbb{Z})^*$$
by the Chinese Remainder Theorem.

3 Quadratic residues

Take $p > 2$ an odd prime. If $a \in \mathbb{Z}$, we know $x^2 \equiv a \pmod{p}$ has ≤ 2 solutions mod p.

For $a \equiv 0 \pmod{p}$, then there is one solution, $x \equiv 0 \pmod{p}$.

For $a \not\equiv 0 \pmod{p}$, if x is a solution then so is $-x$, and $-x \equiv x \pmod{p} \Leftrightarrow 2x \equiv 0 \pmod{p}$ but $a \not\equiv 0 \Rightarrow x \not\equiv 0 \pmod{p}$ so we have either 0 or 2 solutions.

Definition. $a \equiv 0 \pmod{p}$ is a **quadratic residue** mod p if $x^2 \equiv a \pmod{p}$ is soluble, and a **quadratic non-residue** if not.

So a is a quadratic residue mod p iff its class in $(\mathbb{Z}/p\mathbb{Z})^*$ is a square.

We can check directly that the quadratic resides mod 7 are $\{1, 2, 4\}$.

Lemma 3.1. Let p be an odd prime. There are exactly $\frac{p-1}{2}$ quadratic residues mod p.

Proof 1. Consider

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})^* &\xrightarrow{\sigma} (\mathbb{Z}/p\mathbb{Z})^* \\ x &\mapsto x^2 \pmod p\end{aligned}$$

$\sigma(x) = \sigma(y) \iff x^2 \equiv y^2 \pmod p \iff (x-y)(x+y) \equiv 0 \pmod p \iff x \equiv \pm y \pmod p$. Since p is odd, if $(x,p) = 1$ then $x \not\equiv -x \pmod p$. So, σ is 2-to-1, hence the image of σ has $\frac{p-1}{2}$ elements. □

Proof 2. Let g be a primitive root mod p. Then $(\mathbb{Z}/p\mathbb{Z})^* = \{1, g, g^2, \dots, g^{p-2}\}$ as $g^{p-1} = 1$. So,

$$\begin{aligned}\{\, x^2 \mid x \in (\mathbb{Z}/p\mathbb{Z})^* \,\} &= \{1, g^2, g^4, \dots, g^{p-3}, g^{p-1}, g^{p+1}, \dots, g^{2p-4}\} \\ &= \{1, g^2, g^4, \dots, g^{p-3}\}\end{aligned}$$

since $g^{p-1} = 1$ and $g^{p+1} = g^2$, and so on, hence there are $\frac{p-1}{2}$ elements. □

Definition. The **Legendre symbol** of $a \pmod p$ (p an odd prime, $a \in \mathbb{Z}$) is

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ +1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \end{cases}$$

Lemma (Euler's Criterion)**.**

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

Remark. $\left(\frac{a}{p}\right) \in \{0, \pm 1\}$ which is a set of 3 *distinct* integers mod p as $p > 2$. So the congruence in the lemma determines $\left(\frac{a}{p}\right)$ completely.

Proof. If $p \mid a$, obvious. Suppose $(a,p) = 1$. Then $a^{p-1} = (a^{\frac{p-1}{2}})^2 \equiv 1 \pmod p$. Hence $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. If $a \equiv x^2 \pmod p$, then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv +1 \pmod p$. By lemma 3.1, this gives $\frac{p-1}{2}$ solutions of $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. So there are no more solutions, ie if $\left(\frac{a}{p}\right) = -1$, then $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. □

Corollary 3.2. Take $a, b \in \mathbb{Z}$ where p is an odd prime. Then

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

Proof.

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

By the previous remark, we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Remark. We have the following equivalent statements

- The map $(\mathbb{Z}/p\mathbb{Z})^* \to \{+1\}$ given by $a \mapsto \left(\frac{a}{p}\right)$ is a homomorphism of groups.

- The product of residues is a residue; the product of a residue and non-residue is a non-residue, and the product of non-residues is a residue.

Another consequence of Euler's Criterion allows equivalent computation of $\left(\frac{a}{p}\right)$ because there is a polynomial time algorithm to compute $a^n \pmod N$.

- write $n = n_0 + 2n_1 + 4n_2 + \cdots + 2^k n_k$ in binary, $n_i \in \{0, 1\}$
- compute a^2, $a^4 = (a^2)^2$, $a^8 = (a^4)^2, \ldots, a^{2^k} \pmod N$.
- $a^n \equiv \prod_{i:n_i=1} a^{2^i} \pmod N$

Corollary 3.3. For p an odd prime,

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

Proof. By Euler's criterion, if $p = 4k + l$, with $l = 1$ or 3,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k+\frac{l-1}{2}} = \begin{cases} +1 & l = 1 \\ -1 & l = 3 \end{cases}$$

□

What about $\left(\frac{2}{p}\right)$? So what is $2^{\frac{p-1}{2}} \pmod p$? Recall the proof of Fermat's Little Theorem, and imitate this using $\left(\frac{p-1}{2}\right)!$ instead. This will prove

Lemma (Gauss's Lemma)**.** Take p an odd prime and $(a, p) = 1$. Then $\left(\frac{a}{p}\right) = (-1)^\mu$ where μ is the number of $j \in \{1, \ldots, \frac{p-1}{2}\}$ such that $aj \equiv k \pmod p$ where $\frac{p+1}{2} \leq k \leq p - 1$.

Proof. $1 \leq j \leq \frac{p-1}{2}$. Write $aj \equiv \epsilon_j c_j \pmod p$ with $1 \leq c_j \leq \frac{p-1}{2}$ and $\epsilon_j \in \{\pm 1\}$ (by reducing a_j mod p into the interval $(-\frac{p}{2}, \frac{p}{2})$).

Now claim that if $j \neq k$ with $1 \leq j, k \leq \frac{p-1}{2}$ then $c_j \neq c_k$. Indeed if $c_j = c_k$ then $\epsilon_j aj \equiv e_k ak \pmod p$, that is, $j \equiv \pm k \pmod p$. As $1 \leq j, k \leq \frac{p-1}{2}$, $j + k \not\equiv 0 \pmod p$ so $j = k$.

So, $\{c_1, \ldots, c_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$ in some order.

Now, $\mu = \#\{\, j \in \{1, \ldots, \frac{p-1}{2}\} \mid aj \equiv k \pmod p, \frac{p+1}{2} \leq k \leq p - 1 \,\} = \#\{\, j \mid \epsilon_j = -1 \,\}$ So,

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! = \prod_{j=1}^{\frac{p-1}{2}} (a_j) \equiv \prod_{j=1}^{\frac{p-1}{2}} \epsilon_j c_j \equiv \left(\prod_{j=1}^{\frac{k-1}{2}} \epsilon_j\right) \left(\prod_{j=1}^{\frac{k-1}{2}} c_j\right) \equiv (-1)^\mu \cdot \frac{p-1}{2}!$$

This gives

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

□