Number Theory

October 23, 2019

1 Euclid's Algorithm

Theorem 1.1 (Division Algorithm)**.** *Given $a, b \in \mathbb{Z}, b > 0$, we can determine $\exists q, r \in \mathbb{Z}$ s.t. $a = qb + r$ with $0 \leq r < b$.*

Proof. Let $S = \{a - nb : n \in \mathbb{Z}\}$. S contains some non-negative integer. Let r be the least such integer, say $a - qb$. Then $a = qb + r$, so STP $r < b$.

Suppose $b \leq r$. Then $0 < r - b = a - (q+1)b \in S$, and $r - b < r$. $\lightning$ (choice of r) □

If $r = 0$, i.e. if $a = qb$ for some $q \in \mathbb{Z}$, then we write $b|a$ and say "b ***divides*** a" or "b is a ***divisor*** of a". If $r \neq 0$, then we instead write $b \nmid a$ and say "b does ***not divide*** a".

Given $a_1, \ldots, a_n \in \mathbb{Z}$ not all 0, let $I = \{\lambda_1 a_1 + \ldots + \lambda_n a_n : \lambda_i \in \mathbb{Z}\}$. Observe if $a, b \in I, \ell, m \in \mathbb{Z}$, then $\ell a + mb \in I$.

Theorem 1.2. *$I = d\mathbb{Z} = \{dm : m \in \mathbb{Z}\}$ for some $d > 0$*

Proof. I contains some positive integer. Let $d > 0$ be the least such. Then clearly $I \supseteq d\mathbb{Z}$.

Conversely, let $a \in I$ and apply **1.1** to obtain $a = qd + r$ for some $q, r \in \mathbb{Z}$, $0 \leq r < d$. Then $r = a - qd \in I \implies r = 0$, so $d\mathbb{Z} \supseteq I$

$\therefore I = d\mathbb{Z}$ □

Note that $a_i \in I \forall i$, so $d|a_i \forall i$. Conversely, if $c|a_i \forall i$ then c divides every element of I, so in particular $c|d$.

We write $d = \gcd(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$, and say d is the ***greatest common divisor*** of the a_i.

Corollary 1.3 (Bézout)**.** *Let $a, b \in \mathbb{Z}$, a, b not both 0. Then $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = c \iff (a,b)|c$.*

The division algorithm gives an efficient method for computing (a, b).

Theorem 1.4 (Euclid's Algorithm)**.** *Suppose* $a > b > 0$*. Then:*

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

and $r_k = (a, b)$

Proof. We have $r_k | r_{k-1} \implies \dots \implies r_k | a, r_k | b \implies r_k | (a, b)$, so $r_k \le (a, b)$. Note also that any m s.t. $m|a$ and $m|b$ also divides r_k. In particular, $(a, b) | r_k$, and thus $(a, b) \le r_k$, hence $r_k = (a, b)$. $\square$

Additionally, by working back up the algorithm, we can obtain a representation $(a, b) = \lambda a + \mu b$ where $\lambda, \mu \in \mathbb{Z}$

An integer $n > 1$ is ***prime*** if its only positive divisors are 1 and n. Otherwise, we say n is ***composite***.

Corollary 1.5. *Let* p *be a prime,* $a, b \in \mathbb{Z}$*. Then* $p|ab \iff p|a$ *or* $p|b$

Proof. It is clear that if $p|a$ or $p|b$, then $p|ab$. Conversely, suppose $p|ab$ but $p \nmid a$. Them $(a, p) \neq p$. By definition, $(a, p)|p \implies (a, p) \in \{1, p\}$, so $(a, p) = 1$. Now by **1.3** we can find $x, y \in \mathbb{Z}$ s.t. $1 = ax + by \implies b = b(ax + py) = x(ab) + (by)p$, so $p|b$. $\square$

Theorem 1.6 (The Fundamental Theorem of Arithmetic)**.** *Every integer* $n > 1$ *can be written as a product of primes uniquely up to reordering*

Proof. We have existence by strong induction.

For uniqueness, n is the least integer with two distinct such representations, say $= n = p_1 \dots p_s = q_1 \dots q_r$ for p_i, q_j primes.
Then $p_1 | q_1 \dots q_r \implies p_1 | q_j$ for some j. WLOG $j = 1$. Since $p_1 > 1$ as 1 is non-primes, $n/p_1 < n$, and $n/p_1 = p_2 \dots p_s = q_2 \dots q_r$ can be written in two distinct ways as a product of primes. $\lightning$ (choice of n) $\square$

If $m = \Pi_{i=1}^k p_i^{\alpha_i}, n = \Pi_{i=1}^k p_i^{\beta_i}$ where p_i are distinct primes, $\alpha_i, \beta_i \ge 0$, then $(m, n) = \Pi_{i=1}^k p_i^{\gamma_i}$ with $\gamma_i = \min\{\alpha_i, \beta_i\}$. However, if m, n are large, it is much more "efficient" to compute the gcd via Euclid's algorithm.

An algorithm with input $N > 0$ is said to run in ***polynomial time*** if it takes at most $c(\log N)^k$ elementary operations to complete, where $c, k > 0$ are constants independent of N. If the algorithm takes inputs $N_1, N_2, \dots, N_s$, the polynomial time means $c(\max \log N_i)^k$.

Examples of polynomial time algorithms:

- Adding and multiplying integers
- The gcd of two numbers via Euclid's algorithm

- Testing of primality

On the other hand, factoring a number into prime factors does not have a polynomial time algorithm, and it is conjectured that one does not exist. For instance, if $N = p \cdot q$ with p, q primes of ~ 50 digits each, to do trial division up to $\sqrt{N}$ at a rate of 2^9 divisions per second, it would take approximately $\sqrt{10^{100}}/2^9$ seconds, or about $6 \times 10^3 9$ years. However, we can compute the gcd in milliseconds using Euclid's algorithm.

Theorem 1.7. *There are infinitely many primes. i.e. $\pi(x) \to \infty$ as $x \to \infty$*

Proof. Fix $N > 1$, let p be the largest prime $\leq N$. Let q be a prime factor of $M = (2 \times 3 \times 5 \times \ldots \times p) + 1$. Then $q > N$ since $q \notin \{2, 3, \ldots, p\}$, but N was arbitrary. □

2 Congruences

Let $n \geq 1$ be an integer. We write $a \equiv b \mod n$ if $n | a - b$. This defines an equivalence relation on $\mathbb{Z}$, and we will write $\mathbb{Z}/n\mathbb{Z}$ for the equivalence classes induced by this relation, which are $a + n\mathbb{Z}$ for $0 \leq a < n$. It is easy to check that $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b + n\mathbb{Z})$ and that $(a + n\mathbb{Z}) \times (b + n\mathbb{Z}) = (ab + n\mathbb{Z})$ are well defined operations, i.e $n\mathbb{Z}$ is an ideal, and $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring.

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

1. $(a, n) = 1$
2. $\exists b \in \mathbb{Z}$ *s.t.* $ab \equiv b \mod n$
3. *The equivalence class of a generates the group $(\mathbb{Z}/n\mathbb{Z}, +)$*

Proof.

- (1) $\implies$ (2): $(a, n) = 1 \implies \exists b, c \in \mathbb{Z}$ s.t. $ab + cn = 1$ by **1.3**, and hence $ab \equiv 1 \mod n$.
- (2) $\implies$ (1): $ab \equiv 1 \mod n \iff ab - 1 = kn$ for some $k \in \mathbb{Z}$, and so by **1.3** $(a, n) = 1$.
- (2) $\iff$ (3): $ab \equiv 1 \mod n \iff 1 \in \langle a \rangle \leq \mathbb{Z}/n\mathbb{Z} \iff \langle a \rangle = \mathbb{Z}/n\mathbb{Z}$

□

We write $(\mathbb{Z}/n\mathbb{Z})^\times$ for the set of ***units*** (the elements with a multiplicative inverse) of $\mathbb{Z}/n\mathbb{Z}$. By **2.1**, $(\mathbb{Z}/n\mathbb{Z})^\times$ contains precisely those classes $a + n\mathbb{Z}$ such that $(a, n) = 1$. Note that if $n > 1$ then $\mathbb{Z}/n\mathbb{Z}$ is a field precisely when n is prime.

Let ***Euler's φ function*** be $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ for $n > 1$, and let $\varphi(1) = 1$. Observe that $\varphi(p) = p - 1$ for p prime. Moreover, φ is a multiplicative function: $(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$.

Corollary 2.2. *Let G be a cyclic group of order $n \geq 1$. Then $\varphi(n) = |\{g \in G : \operatorname{ord}(g) = n\}|$, the number of generators of G.*

Theorem 2.3 (Euler-Fermat)**.** *IF $(a, n) = 1$, $a, n \in \mathbb{Z}$, then $a^{\varphi(n)} \equiv 1 \mod n$*

Proof. By Lagrange's Theorem, the order of a in the group $(\mathbb{Z}/n\mathbb{Z})^\times$ divides the order of $(\mathbb{Z}/n\mathbb{Z})^\times$, which is $\varphi(n)$ □

Theorem 2.4 (Fermat's Little Theorem). *If $a, p \in \mathbb{Z}$ and p is prime, then $a^p \equiv a \mod p$.*

Proof. If $p|a$, then this holds trivially. If $p \nmid a$, $(a,p) = 1$ and so by **2.3** we have $a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \mod p$ $\square$

Multiple Congruences

Can we find all $x \in \mathbb{Z}$ s.t. $x \equiv 4 \mod 7$ and $x \equiv 5 \mod 12$?

Suppose we can find $u, v \in \mathbb{Z}$ s.t. $\begin{cases} u \equiv 1 \mod 7; & u \equiv 0 \mod 12 \\ v \equiv 0 \mod 7; & v \equiv 1 \mod 12 \end{cases}$. Then we can write down that $x = 4u + 5v$. Since $(7, 12) = 1$, by **1.3** there are some $m, n \in \mathbb{Z}$ with $7m + 12n = 1$, and from Euclid's algorithm we can determine these to be $m = -5, n = 3$. Then we can find $u = 12n = 1 - 7m; v = 7m = 1 - 12n$, and substitution gives $u = 36, v = -35$, and so a solution to the original problem is $4 \times 36 - 5 \times 35 = -31$. Now the lowest common multiple of 7 and 12 is 84, and so our solution set is: $\{x \in \mathbb{Z} : x \equiv -31 \mod 84\}$.

We can in fact generalise this process:

Theorem 2.5 (Chinese Remainder Theorem). *Let $m_1, \ldots, m_k$ be pairwise coprime positive integers, and let $M = \Pi_{i=1}^k m_i$. Then given any integers $a_1, \ldots, a_k$ there is a solution x to the the system of congruences:*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

Moreover, this solution is unique modulo M.

Note that if x satisfies this system of equations, then so does $x + tM$ for any $t \in \mathbb{Z}$, and so the complete set of solutions is $x + M\mathbb{Z}$.

Proof.

Uniqueness: If x, y satisfy the system, then $m_i | x - y$ for all $i = 1, \ldots, k$. Since no prime divides any tow the m_i, $M | x - y$ and hence $x \equiv y \mod M$.

Existence: Write $M_i = \frac{M}{m_i} = \Pi_{j \neq i} m_j$ for each $i = 1, 2, \ldots, k$. Since $(m_i, m_j) = 1 \forall i \neq j$, $(m_i, M_i) = 1$ for all $i = 1, 2, \ldots, k$. Therefore, for each $i = 1, 2, \ldots, k$ we can find $b_i \in \mathbb{Z}$ such that $M_i b_i \equiv 1 \mod m_i$ and $M_i b_i \equiv 0 \mod m_j$ for $j \neq i$. Then $x = \sum_{i=1}^k a_i b_i M_i$ solves the system of congruences. $\square$

If $m_1, \ldots, m_k$ are pairwise coprime, and $M = \Pi m_i$, then map $\theta : \mathbb{Z}/M\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$, taking $x \mod M \mapsto (x \mod m_1, \ldots, x \mod m_k)$ is an isomorphism of rings. To see this, note that if $m_i | M$ then $x \mod m_i$ is determined by $x \mod M$ which implies that θ is well-defined. It is a homomorphism by the properties of $+, \times$ in $\mathbb{Z}/n\mathbb{Z}$, and **2.5** implies that θ is a bijection. In particular, if $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ for distinct primes p_i, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$.

Corollary 2.6. *If $m_1, \ldots, m_k$ are pairwise coprime and $M = \Pi_{i=1}^k m_i$ and $a_1, \ldots, a_k \in \mathbb{Z}$ are such that $(a_i, m_i) = 1$ for each $i = 1, 2, \ldots, k$, then there is a solution to the system of congruences in **2.5**, and any such solution is in fact coprime to M.*

Proof. **2.5** gives us a solution, say $x \in \mathbb{Z}$. Suppose $(x, M) > 1$. Then there is a prime p such that $p|x$ and $p|M$ simultaneously. p prime, so WLOG suppose that p divides m_1. Since $x \equiv a_1 \mod m_1$, we must have $p|a_1$, and so $p|(a_1, m_1)$ $\lightning$. $\square$

Corollary 2.7. *If $m_1, \ldots, m_k$ are pairwise coprime with $M = \Pi_{i=1}^k m_i$, then $\varphi(M) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_k)$*

A ***multiplicative function*** is a function $f : \mathbb{N} \to \mathbb{C}$ such that, for all $m, n \in \mathbb{N}$ coprime, $f(mn) = f(m)f(n)$. A function $f : \mathbb{N} \to \mathbb{C}$ is said to be ***totally multiplicative*** if for all $m, n \in \mathbb{N}$, $f(m, n) = f(m)f(n)$.

Some multiplicative functions are:

- $\varphi(m)$
- $\tau(n) =$ the number of positive divisors of n
- $\sigma(n) =$ the sum of the positive divisors of n
- $\sigma_k(n) = \sum_{d|n} d^k$, so that $\sigma_0(n) = \tau(n), \sigma_1(n) = \sigma(n)$.

None of these are totally multiplicative however.

Lemma 2.8. *Let f be a multiplicative function. Then so is g, where $g(n) = \sum_{d|n} f(d)$.*

Proof. Let $m, n \in \mathbb{N}, (m, n) = 1$. Then the divisors of mn are precisely the integers of the form $d_1 d_2$ where $d_1|m, d_2|n$ and $(d_1, d_2) = 1$. This means that we can write down

$$\begin{aligned} g(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= g(m) g(n) \end{aligned}$$

$\square$

Then if we let $f(n) = n^k$ for some $k \in \mathbb{N}$. Then $g(n) = \sum_{d|n} d^k = \sigma_k(n)$. Later on, we shall see that we can recover f from g via Möbius inversion.

Theorem 2.9.

1. *If p is a prime and $m \in \mathbb{N}$ then $\varphi(p^m) = p^{m-1}(p-1) = p^m \left(1 - \frac{1}{p}\right)$*
2. *$\forall n \in \mathbb{N}, \varphi(n) = n \cdot \Pi_{p|n} \left(1 - \frac{1}{p}\right)$*
3. *$\sum_{d|n} \varphi(d) = n$*

Proof.

1.

$$\begin{aligned}\varphi(p^m) &= |\{1 \leq a \leq p^m : (a, p^m) = 1\}| \\ &= p^m - p^{m-1} \\ &= p^m \left(1 - \frac{1}{p}\right)\end{aligned}$$

2. Let $n = \Pi_{i=1}^k p_i^{\alpha_i}$ for p_i distinct primes, $\alpha_1 \geq 1$. Then:

$$\begin{aligned}varphi(n) &= \Pi_{i=1}^k \varphi(p_i^{\alpha_i}) \\ &= \Pi_{i=1}^k p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \\ &= n \cdot \Pi_{p|n} \left(1 - \frac{1}{p}\right)\end{aligned}$$

3. φ is multiplicative and so is $n \mapsto n$, so it suffices to check that both sides agree when n is a prime power. Let p be a prime $m \in \mathbb{N}$. Then:

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

□

Polynomials over $\mathbb{Z}/n\mathbb{Z}$ can have varying numbers of solutions, e.g.:

1. $x^2 + 2 \equiv 0 \mod 5$ has no solutions
2. $x^3 + 1 \equiv 0 \mod 7$ has three solutions
3. $x^2 - 1 \equiv 0 \mod 8$ has four solutions

Let $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}\}$ be a ring. Then we define $R[x]$ to be the ring of polynomials with coefficients in R, with addition and multiplication given in the usual way.

WARNING: Two polynomials are ***equal*** if their coefficients are all equal, however the map from $R[x]$ to the set of all functions $R \to R$ is not necessarily injective. For instance, if $R = \mathbb{Z}/p\mathbb{Z}$ for some prime $\mathbb{Z}$, then under this map $x^p - x$ is the zero function by Fermat's little theorem.

Theorem 2.10 (Division Algorithm for Polynomials)**.** *Let $f, g \in R[x]$, and suppose that the leading coefficient of g is a unit (i.e. has a multiplicative inverse) in R. Then $\exists q, r \in R[x]$ such that $f = q \cdot g + r$ where* $\deg r < \deg g$.

Proof. We prove this by induction on $n = \deg f$. If $\deg f < \deg g$, then just take $q = 0, r = f$. Otherwise, $f(x) = ax^n + \ldots; g(x) = bx^m + \ldots$ for $a, b \neq 0, n \geq m, b = c^{-1}$ for some $c \in R$.

Then define $f'(x) = f(x) - acx^{n-m}g(x)$ has degree $< n$. By the induction hypothesis, there is some $q, r \in R[x]$ such that $f'(x) = q(x)g(x) + r(x)$, with $\deg r < \deg g$.
But now $f(x) = (q(x) + acx^{n-m})g(x) + r(x)$, and we are done. □

Theorem 2.11 (Remainder Theorem)**.** *let $f \in R[x], \alpha \in R$. Then there is some $q \in R[x]$ such that:*

$$f(x) = (x - \alpha)q(x) + f(\alpha)$$

Proof. By **2.10** with $g(x) = x - \alpha$, there is some $q \in R[x]$ and $r \in R$ such that $f(x) = (x-\alpha)q(x) + r$. But now $f(\alpha) = r$, and the required equality holds. $\square$

A (non-zero) ring R is said to be an ***integral domain*** if it doesn't have any zero divisors, i.e. $ab = 0 \iff a = 0$ or $b = 0$. Note that $\mathbb{Z}$ and $\mathbb{Q}$ are integral domains, whilst $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime (if $n = pq$ is a proper factorization, then $pq = 0$ in $\mathbb{Z}/n\mathbb{Z}$).

Theorem 2.12. *Let R be an integral domain, and let $f \in R[x]$ be a non-zero polynomial of degree $n \geq 0$. Then f has at most n roots in R.*

Theorem 2.13 (Lagrange)**.** *Lt p be a prime, and let $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial of degree n such that $p \nmid p$. Then the congruence $f(x) = 0 \mod p$ has at most n distinct solutions.*

Of 2.12. By induction on n. Check $n = 0$ - trivial.

Suppose $n > 0$. If f has no roots the we're done. Otherwise there exists $\alpha \in R$ such that $f(\alpha) = 0$, and so by the remainder theorem, $f(x) = (x - \alpha)q(x)$ with $\deg q < \deg f = n$. So by the induction hypothesis, we know that q has at most $n - 1$ roots. But if $\beta \in R$ is such that $f(\beta) = 0$, then $0 = (\beta - \alpha)q(\beta)$, and since R is an integral domain, we must have $\beta = \alpha$ or $q(\beta) = 0$, and so f has at most n roots. $\square$

Example: Let p be a prime, $G = \mathbb{Z}/p\mathbb{Z}$, and let $f(x) = x^{p-1} - 1 - \Pi_{\alpha \in G}(x - \alpha)$. Observe that $\alpha = 1, 2, \ldots, p-1$, then $f(\alpha) = \alpha^{p-1} - 1 \equiv 0 \mod p$, so f has at least $p - 1$ roots.

But $\deg f < p - 1$ because the coefficient of $x^{p-1} = 0$. This means that f must be the zero polynomial, and hence $0 = f(0) = -1 - (p-1)! \mod p$, and we have Wilson's theorem, that $(p-1)! \equiv -1 \mod p$.

Example: Consider $(\mathbb{Z}/7\mathbb{Z})^\times$.
$3 \in (\mathbb{Z}/7\mathbb{Z})^\times$ since $3 \cdot 5 \equiv 1 \mod 7$, $3^6 \equiv 1 \mod 7$, so 3 generates $(\mathbb{Z}/7\mathbb{Z})^\times$, and $(\mathbb{Z}/7\mathbb{Z})^\times$ is cyclic.

Theorem 2.14. *If p is a prime, then $G = (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic and of order $p - 1$.*

Proof. $|G| = \varphi(p) = p - 1 = \sum_{d|p-1} \varphi(d)$

By Lagrange's Theorem, $|G| = \sum_{a||G|} N_a$ where $N_a = |\{g \in G : \mathrm{ord}(g) = d\}|$. Suppose G is not cyclic, so G does not contain an element of order $p-1$, so $N_{p-1} = 0 < \varphi(p-1)$, and so there must be some d for which $N_d > \varphi(d)$. Let α be an element of order for such a d. Then $\langle \alpha \rangle \leq G$ is cyclic of order d, so it has precisely $\varphi(d)$ elements of order d. Since $N_d > \phi(d), \exists \beta \notin \langle \alpha \rangle$ s.t. $\mathrm{ord}(\beta) = d$. This implies that the polynomial $x^d - 1$ has $d + 1$ roots, namely $1, \alpha, \ldots, \alpha^{d-1}, \beta$ $\lightning$ **2.12**. $\square$

A positive integer is said to be a ***primitives root modulo n*** if $\langle g \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$. Hence **2.14** says that primitive roots exist modulo p for all primes p.

For instance, take $p = 19$, and let $d = \text{ord}(2)$ in $(\mathbb{Z}/19\mathbb{Z})^\times$. Then $d|\varphi(19) = 18$, so $d = 18$ or $d|6$ or $d|9$. $2^6 = 64 \not\equiv 1 \mod 19$, and $2^9 = 512 \not\equiv 1 \mod 19$, so $d = 18$, and 2 is a primitive room modulo 19.

There are many open problems concerning primitive roots:

1. Artin's Primitive Root Conjecture:
   Given $g \geq 1$ does there exist infinitely many primes p such that g is a primitive root modulo p. We do know that there are infinitely many primes for which one of $\{2, 3, 5\}$ is a primitive root.

2. How large is the smallest primitive root modulo p?
   We can prove that it is $\leq cp^{1/4+\epsilon}$ for some constant $c > 0$ and for any $\epsilon > 0$. However, conditional on the Generalised Riemann Hypothesis (GRH), it is $\leq c \log^6 p$ for constant $c > 0$

Now consider $(\mathbb{Z}/8\mathbb{Z})^\times = \{\pm 1, \pm 3\}$. All of these have order 1 or 2, and hence $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic. In fact, let $\theta : (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$ map $x \mod 2^k$ onto $x \mod 8$. Since $(a, 2^k) = 1 \iff (a, 8) = 1$, θ is surjective. Hence, for $k \geq 3$ we have that $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is not cyclic, since a generator would map to a generator.

Theorem 2.15. *If $p > 2$, $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic for $k \geq 1$.*

Lemma 2.16. *Let $p > 2, k \geq 1, y \in \mathbb{Z}$. Then*

1. *If $x \equiv 1 + p^k y \mod p^{k+1}$, then $x^p \equiv 1 + p^{k+1} y \mod p^{k+2}$*
2. $(1 + yp)^{p^k} \equiv 1 + p^{k+1} y \mod p^{k+2}$

Proof.

1. $x^p = (1 + p^k y)^p = \sum_{j=0}^{p} \binom{p}{j} (p^k y)^j = 1 + p^{k+1} y + \ldots + p^{pk} y^p$.

   For $2 \leq j \leq p - 1$, $p | \binom{p}{j}$, so $\binom{p}{j}(p^k y)^j \equiv 0 \mod p^{2k+2}$, and so $\equiv 0 \mod p^{k+2}$.

   Since $p \geq 2, pk \geq k + 2$, so $p^{pk} y^p \equiv 0 \mod p^{k+2}$, and therefore $x^p \equiv 1 + p^{k+1} y \mod p^{k+2}$

2. Let $x = 1 + py$ and apply part 1 k times.

$\square$

Lemma 2.17. *Let $p > 2, k \geq 1$. If g is a primitive root $\mod p$, and $g^{p-1} \not\equiv 1 \mod p^2$, then g generates $(\mathbb{Z}/p^k\mathbb{Z})^\times$ for all $k \geq 1$.*

Proof. Let $d = \text{ord}\, g$ as a member of $(\mathbb{Z}/p^k\mathbb{Z})^\times$. Note that $\varphi(p^k) = p^{k-1}(p-1)$, and so $d | p^{k-1}(p-1)$.

If g is not a generator of $(\mathbb{Z}/p^k\mathbb{Z})^\times$, then one of the following holds:

1. $d | p^{k-2}(p - 1)$
2. $d = p^{k-1} e$ where $e | p - 1, e \neq p - 1$

We tackle each of these cases individually, and will see that they cannot be the case:

1. We thus have $g^{p^{k-2}(p-1}\equiv 1 \mod p^k$. We've already seen that $g^{p-1}\equiv 1 \mod p$ and $g^{p-1}\not\equiv 1 \mod p^2$, and so there exists some $y\not\equiv 0$ such that $x := g^{p-1} = 1+py$.

   Then we have $x^{p^{k-2}} \equiv 1+p^{k-1}y \mod p^k \implies g^{p^{k-2}(p-1)} \equiv 1+p^{k-1}y \mod p^k \not\equiv 1 \mod p^k$ $\lightning$.

2. Here, we have $g^{p^{k-1}e}\equiv 1 \mod p^k$. Fermat tells us that $g^p\equiv g \mod p$, and so $g^{p^{k-1}}\equiv g \mod p \implies g^{p^{k-1}e}\equiv g^e \mod p$. However, $e<p$, and so this is not $1 \mod p$, and hence $g^{p^{k-1}e}\not\equiv 1 \mod p$ $\lightning$.

Hence the only case left is that g is a generator of $(\mathbb{Z}/p^k\mathbb{Z})^\times$. $\square$

Proof of 2.15. Let g be a primitive root modulo p. If $g^{p-1}\not\equiv 1 \mod p^2$, then $(\mathbb{Z}/p^k\mathbb{Z})^\times = \langle g\rangle\ \forall k\geq 1$.

Otherwise, $g^p\equiv g \mod p^2$. Let $h=(1+p)g$, so that $h^p\equiv(1+p)^pg^p\equiv g \mod p^2$. Observe that $g\not\equiv h \mod p^2$, as g is a primitive root modulo p, so that $(g,p)=1$.

So $h^p\not\equiv h \mod p^2$, and so $\langle h\rangle = (\mathbb{Z}/p^k\mathbb{Z})^\times\ \forall k\geq 1$. $\square$

2.16 fails for $p=2$ because of the $k=1$ case in *1.* However, it does hold if $p=2, k\geq 2$. In particular, $(1+4)^{2^{k-1}}\equiv 1+2^{k+1} \mod 2^{k+2}$. So we have $(\mathbb{Z}/2^k\mathbb{Z})^\times = \langle -1,5\rangle \cong \mathbb{Z}/2^{k-2}\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ for $k\geq 3$.

3 Quadratic Residues

Let p be an odd prime, and let $a\in\mathbb{Z}$ such that $a\not\equiv 0 \mod p$. We say that a is a ***quadratic residue modulo p*** if the congruence $x^2\equiv a \mod p$ has a solution. Otherwise, we say that a is a ***quadratic non-residue modulo p***. So a is a quadratic residue mod p if and only if its residue class in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a square.

Conjecture 3.1 (Open)**.** *Let $n(p)$ be the least quadratic non-residue modulo p. We can show that $n(p)\leq cp^\theta$ for any $\theta > \frac{1}{4}\sqrt{e}$ for some constant $c>0$, and, conditional on GRH, $n(p)\leq c\log^2 p$ for some $c>0$*

For instance, let $p=7$. We have

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

.
and so the quadratic residues module 7 are $\{1,2,4\}$, whilst $\{3,5,7\}$ are non-residues.

Lemma 3.2. *Let p be an odd prime. Then there are precisely $\frac{p-1}{2}$ quadratic residues modulo p.*

Proof. Let $\sigma : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times; x\mapsto x^2$.

It suffices to show that σ is $2-to-1$:

$$x^2\equiv y^2 \mod p \iff (x+y)(x-y)\equiv 0 \mod p \qquad \iff x\equiv \pm y \mod p$$

as p is prime and $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. Hence there are precisely $\frac{p-1}{2}$ elements in the image of σ $\square$

Alternative. Let g be a primitive root mod p, i.e. $(\mathbb{Z}/p\mathbb{Z})^\times = \{1,g,g^2,\ldots g^{p-2}\}$, and so $\{x^2 : x\in(\mathbb{Z}/p\mathbb{Z})^\times\} = \{1,g^2,g^4,\ldots,g^{p-3},g^{p-1},g^{p+1},\ldots,g^{2p-4}\}$. But $g^{p-1}\equiv 1 \mod p$, and so the second half of this set is the same as the first half, and hence only half the elements are squares. $\square$

Let p be an odd prime and $a \in \mathbb{Z}$. We define ***Legendre's symbol*** "a on p" to be:

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

Theorem 3.3 (Euler's Criterion)**.** *Let $p > 2, a \in \mathbb{Z}$. Then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$*

Since $p > 2$, the elements $0, 1, -1$ are distinct mod p, so this congruence determines $\left(\frac{a}{p}\right)$ uniquely.

Proof. If $a \equiv 0 \mod p$, then the result is trivial. Suppose therefore that $(a, p) = 1$. Then by Fermat, $a^{p-1} \equiv 1 \mod p$, which means that $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. Observe further that, if $a = x^2 \mod p$, then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p$. By **3.2**, there are precisely $\frac{p-1}{2}$ quadratic residues, so the congruence $a^{\frac{p-1}{2}} \equiv 1 \mod p$ has at least $\frac{p-1}{2}$ solutions. However, this is a polynomial in a of degree $\frac{p-1}{2}$, and so it can only have at most this many solutions, and hence every solution is a quadratic residue. So whenever $\left(\frac{a}{p}\right) = -1$ we must have $a^{\frac{p-1}{2}} \equiv -1 \mod p$. ☐

Corollary 3.4. *Let $p > 2$, $a, b \in \mathbb{Z}$. Then $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$*

Proof.

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} \mod p \\ &\equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \mod p \\ &\equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \mod p \end{aligned}$$

☐

This implies that

1. The map $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$; $a \mapsto \left(\frac{a}{p}\right)$ is a homomorphism.
2. Let R be any residue, N any non-residue. Then $R \times R = R; N \times N = N; R \times N = N$
3. There is a polynomial time algorithm for computing $\left(\frac{a}{p}\right)$ for odd p, because we can efficiently compute $a^n \mod p$ via binary modular exponentiation.

Corollary 3.5. *Let $p > 2$. Then* $\left(\frac{-1}{p}\right) = \begin{cases} +1 & p \equiv 1 \mod 4 \\ -1 & p \equiv -1 \mod 4 \end{cases}$

Proof. $p \equiv \begin{cases} +1 & p \equiv 1 \mod 4 \\ -1 & p \equiv -1 \mod 4 \end{cases} \iff \frac{p-1}{2} \equiv \begin{cases} 0 & \mod 2 \\ 1 & \mod 2 \end{cases}$, and hence $(-1)^{\frac{p-1}{2}} \equiv \begin{cases} +1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$, and so by Euler's criterion, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ ☐

We can think about this in another way, by considering an alternative proof of Fermat's little theorem:
Observe that multiplying by a simply permutes the elements of the multiplicative group mod p as a is a generator, hence:
$(p-1)! = \Pi_{j=1}^{p-1} j \equiv \Pi_{j=1}^{p-1}(aj) = a^{p-1}\Pi_{j=1}^{p-1} j = a^{p-1}(p-1)!$, and hence $a^{p-1} \equiv 1 \mod p$.

Similarly, $\Pi_{j=1}^{\frac{p-1}{2}}(aj) = a^{\frac{p-1}{2}}\Pi_{j=1}^{\frac{p-1}{2}} j = a^{\frac{p-1}{2}}(\frac{p-1}{2})!$ Write $aj \equiv \epsilon_j c_j \mod p$ with $c_j \in \{1, 2, \dots, \frac{p-1}{2}\}$, and $\epsilon_j \in \{\pm 1\}$.

We claim that, if $1 \leq j \lneq k \leq \frac{p-1}{2}$, then $c_j \neq c_k$.

Indeed, if $c_j = c_k$, then $\frac{aj}{\epsilon_j} \equiv \frac{ak}{\epsilon_k} \mod p$, i.e. $j\epsilon_k \equiv k\epsilon_j \mod p iff j \equiv \pm k \mod p$.

Hence, $a^{\frac{p-1}{2}}(\frac{p-1}{2})! = \Pi_{j=1}^{\frac{p-1}{2}}(aj) \equiv \Pi_{j=1}^{\frac{p-1}{2}}(\epsilon_j c_j) \mod p \equiv \left(\Pi_{j=1}^{\frac{p-1}{2}}\epsilon_j\right)(\frac{p-1}{2})! \mod p$, and hence $a^{\frac{p-1}{2}} \equiv \Pi_{j=1}^{\frac{p-1}{2}}\epsilon_j \mod p$. This brings us onto:

Lemma 3.6 (Gauss's Lemma)**.** *Let $p > 2, a \in \mathbb{Z}$. Then:*

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

Where $\mu = \left|\left\{1 \leq j \leq \frac{p-1}{2} | aj \equiv k \mod p \textit{ for some } \frac{p+1}{2} \leq k \leq p-1\right\}\right|$

Proof. By the above and observe that $\mu = |\{n \leq j \leq \frac{p-1}{2} : \epsilon_j = -n\}|$, and hence $(-m)^{\mu} = \Pi_{j=n}^{\frac{p-1}{2}}\epsilon_j$ □