Ma 7 Introduction to Number Theory

by

Dinakar Ramakrishnan
278 Sloan, Caltech

1 Basic Notions

Notation:
$\mathbb{N} = \{1, 2, \dots\}$, $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\} \supset \mathbb{Z}_+ = \{0, 1, 2, \dots\} = \mathbb{N} \cup \{0\}$
$\mathbb{Q} = \{\text{rational numbers}\}$
$\mathbb{R} = \{\text{real numbers }\} \subset \mathbb{C} = \{\text{complex numbers}\}$.

Principle of Mathematical Induction (PMI): A statement P about $\mathbb{Z}_+$ is true if

(i) P holds for $n = 0$;

and

(ii) If P holds for all $m < n$, then P holds for n. (*)

Inputs for Number Theory:
- Logic
- Algebra
- Analysis (Advanced Calculus)
- Geometry

A slightly different principle from induction:

Well ordering axiom (WOA): Every non-empty subset of $\mathbb{Z}_+$ contains a smallest element.

Note: if S is finite then WOA is obvious and can be checked. *Intuitively*, we often apply it to infinte sets; this is accepting the WOA.

Lemma: WOA$\Rightarrow$PMI (for $\mathbb{Z}_+$).

Proof: Suppose (*) (i), (ii) hold for some property P.
To show: P is true for all non-negative integers.
We prove it by contradiction. Suppose P is false. Let S be the subset of $\mathbb{Z}_+$ for which P is false. Since P is assumed to be false S is non-empty. By WOA, $\exists n \geq 0$ such that n is in S, and it is the **smallest** element of S. If $n = 0$, we would get a contradiction by (i). So $n > 0$. Since n is the smallest for which P is false, it is true for all $m < n$. By (ii), P holds for n as well. **Contradiction!** So P holds.
□

Note: First couple of weeks will be very easy, so use them to learn how to write a proof. (People lose more points on easy problems than hard ones.)

Remark: In fact, PMI and WOA are equivalent. Try to show PMI$\Leftrightarrow$ WOA.

Theorem: (*Euclidean Algorithm*) Let a, b be integers ≥ 1. Then we can write $a = bq + r$ with $q, r \in \mathbb{Z},\ 0 \leq r < b$.

Proof: Put $S = \{a - bn | n \in \mathbb{Z}\} \cap \mathbb{Z}_+$. *Claim*: $S \neq \emptyset$. (Easy) *Reason*: we can take n negative. So by WOA, S has a smallest element r. Since $r \in S$, we can write

$$r = a - bq, \text{ for some } q \in \mathbb{Z}$$

Since $S \subset \mathbb{Z}_+,\ r \geq 0$. Only thing to check: $r < b$. Suppose $r \geq b$. Then let

$$r' = a - b(q+1) = r - b \geq 0 \text{ since } r \geq b.$$

Thus $r' \in S$ and $r' < r$, a contradiction.
□

Definition: b divides a, written $b|a$, iff $a = bq$ for some $q \in \mathbb{Z}$. If not, write $b \not| a$.

Definition: An integer $p > 1$ is **prime iff** the only positive integers dividing p are 1 and p.

Examples: 2, 3, 5, 7, 11, 13,... 37,... 691,...

A positive integer which is not a prime is called a **composite** number.

Theorem: Every $n \in \mathbb{N}$ is uniquely written as

$$n = \prod_{i=1}^{r} p_i^{m_i},$$

with each p_i prime and $m_i > 0$.

Proof of unique factorization:

Step 1: Show that any $n \in \mathbb{N}$ is a product of primes.

Proof: If $n = 1$, OK (empty product =1 by convention). So let $n > 1$. If n is a prime, there is nothing to do. So we may assume that n is *composite*. This means that $\exists$ prime p such that $p|n$. So $n = pq$, some $q \geq 1$. Use induction on n. Since $q < n$, by induction q is a product of primes. Hence n is a product of primes.

Step 2: **Uniqueness of factorization**

Suppose this is false. By WOA, $\exists$ smallest n for which it is false. Write $n = p_1 \dots p_r = q_1 \dots q_s$ with p_i, q_j primes, $1 \leq i \leq r,\ 1 \leq j \leq s,\ p_i \neq q_j$

for any (i, j). We may assume $p_1 \leq p_2 \leq \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots \leq q_s$ and $p_1 < q_1$. Now set $n' = p_1 q_2 \ldots q_s < n$. Since p_1 divides n and n', it divides $(n - n')$. We can write, thanks to step 1,

$$n - n' = p_1 \ell_1 \ldots \ell_k \tag{1}$$

for some primes $\ell_1, \ldots, \ell_k$. We can also write

$$q_1 - p_1 = r_1 r_2 \ldots r_t \tag{2}$$

for primes $r_1, \ldots, r_t$. On the other hand, $n - n' = q_1 \ldots q_s - p_1 q_2 \ldots q_s$, i.e., $n - n' = (q_1 - p_1) q_2 \ldots q_s$. Then

$$n - n' = r_1 r_2 \ldots r_t q_2 \ldots q_s \tag{3}$$

Since $n - n' < n$, and since n is the smallest counterexample, the two factorizations of $n - n'$ given by (1) and (3) must coincide. Consequently,

$$p_1 \in \{r_1, r_3 \ldots, r_t, q_2, \ldots, q_s\}$$

But $p_1 \neq q_j$; for any j. Thus

$$p_1 = r_i, \text{ for some } i.$$

Then p_1 divides $(q_1 - p_1) \Rightarrow p_1 | q_1$, contradiction!
□

Analysis enters when we ask questions about the number and distribution of primes.

Theorem. (Euclid) There exist infinitely many primes in $\mathbb{Z}$.

Proof: Suppose not. Then there exist only a finite number of primes; list them as $p_1, p_2, \ldots, p_m$. Put $n = p_1 p_2 \ldots p_m + 1$. If n is prime we get a contradiction since $n > p_m$. So n cannot be prime. Let q be a prime divisor of n. Since $\{p_1, \ldots, p_m\}$ is the set of all primes, q must equal p_j; for some j. Then q divides $n = p_1 \ldots p_m + 1$ and $p_1 \ldots p_m \Rightarrow q | 1$, a contradiction.

Euler's attempted proof. (This can be made rigorous!) Let P be the set of all primes in $\mathbb{Z}$. **Euler's idea**: If P were finite, then $X = \prod_{p \in P} \frac{1}{(1 - \frac{1}{p})} < \infty$.

Lemma.

Let s be any real number > 1. Then

$$\zeta(s) = \prod_{p \in P} \frac{1}{(1 - \frac{1}{p^s})} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

(called the "Riemann" zeta function, though Euler studied it a century earlier).

Proof of Lemma. Recall: If $|x| < 1$, then $\frac{1}{1-x} = 1 + x + x^2 + \dots$ (geometric series). If $s > 1$, $\frac{1}{p^s} < 1$. So $\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots$ Then

$$\prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

by unique factorization.

Euler then argued as follows: let $s \to 1$ from right. X=$\lim_{s \to 1^+} \sum_{n=1}^{\infty} \frac{1}{n^s} \to \sum_{n=1}^{\infty} \frac{1}{n}$, which diverges. But if P is finite, then X is a finite rational number, a contradiction. (To make this rigorous, we need to be careful about limits and uniform convergence.)

The Prime Number Theorem (PNT)

For any $x \geq 2$, put

$$\pi(x) = \#\{p : \text{ prime } \mid p \leq x\}.$$

What does $\pi(x)$ look like for x very large? The **prime number theorem** (PNT) says:

$$\pi(x) \sim \frac{x}{\log x}, \text{ as } x \to \infty$$

In other words, the fraction of integers in $[1, x]$ which are prime is roughly $\frac{1}{\log x}$ for x large. (We can't prove it in this class.)

Twin Primes These are prime pairs (p, q) with $q = p + 2$.

Examples: (3,5), (5,7), (11, 13),...

Conjecture: There exist infinitely many twin primes.

Stronger conjecture: If $\pi_2(x)$ denotes the number of twin primes $\leq x$, then

$$\pi_2(x) \sim \frac{x}{(\log x)^2} \text{ as } x \to \infty.$$

2 Heuristics on Primes

Let $P = \{\text{primes in } \mathbb{Z}\}$. We saw two proofs of the fact that P is infinite.

Prime Number Theorem (PNT). If $\pi(x) = \#\{p \in P | p \leq x\}$ then $\pi(x) \sim \frac{x}{\log x}$ for x large.

Heuristic reason: Let $F(x) =$ the fraction of positive integers $\leq x$ which are prime. Then $F(x) = \frac{\pi(x)}{x}$. We want to take all $n \leq x$ and then throw out composite numbers. First throw out even numbers, i.e., those divisible by 2.

$$\left\{\begin{matrix}\text{fraction of odd numbers} \\ \text{which are } \leq x\end{matrix}\right\} \sim \frac{1}{2} = \left(1 - \frac{1}{2}\right)$$

$$\text{fraction of numbers which are not divisible by } 3 \sim \left(1 - \frac{1}{3}\right)$$

We get

$$F(x) \sim \prod_{p \leq x} \left(1 - \frac{1}{p}\right)$$

In fact, we should use the bound $\sqrt{x}$ for better accuracy. This way we are off by a factor of 2.

Recall Euler's result:

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \sim \sum_{n \leq x} \frac{1}{n} \sim \int_1^x \frac{1}{t} dt = \log x$$

Consequently,

$$F(x) \sim \frac{1}{\log x}, \text{ and so } \pi(x) \sim \frac{x}{\log x}$$

Twin primes

We are looking for numbers n such that n and $n + 2$ are prime.

Put

$$\pi_2(x) = |\{\text{twin primes } \leq x\}|$$

A heuristic argument:

Put

$$F_2(x) = \frac{\pi_2(x)}{x}$$

Again, take all $n \leq x$ and throw out numbers which are not twin primes.

Check:

$$F_2(x) \approx \prod_{p \leq x} \left(1 - \frac{2}{p}\right) \approx \frac{1}{\log^2 x}$$

So one expects:

$$\pi_2(x) \approx \frac{x}{\log^2 x} \quad \leftarrow \text{Not yet proved!}$$

3 More on divisibility and Primes

Proposition 1: Let $a_1, a_2, \ldots, a_n$ be integers. Put

$$M = \{\sum_{i=1}^{n} a_i x_i | x_i \in \mathbb{Z}, \forall i\}.$$

Then $M = d\mathbb{Z}$, for a unique $d \geq 0$. ($d\mathbb{Z}$ is the set of all integers divisible by d.)

Proof. If $M = \{0\}$, take $d = 0$. Otherwise, put $M^+ = \{n \in M | n > 0\}$. Then clearly, M^+ is non-empty since $M \neq \{0\}$, and so by WOA, $\exists$ smallest element, call it d, in M^+. For any n in M, we can write by the Euclidean algorithm: $n = dq + r$, with $q, r \in \mathbb{Z}$, and $0 \leq r < d$.

Note that M is closed under subtraction. So $r = n - dq$ is also in M. If $r = 0$, we are done because then $n = dq$ as desired.

Suppose $r > 0$. Then $r \in M^+$. Since $r < d$, this contradicts the minimality of d. Hence r must be 0, and $n \in d\mathbb{Z}$.
□

Definition: Let $a_1, \ldots, a_n, d$ be as in Prop. 1. Then d is called the gcd (**greatest common divisor**) of $\{a_i\}$. For brevity, write

$$d = (a_1, \ldots, a_n) = gcd(a_1, \ldots, a_n).$$

Check: $(a_1, (a_2, a_3)) = ((a_1, a_2), a_3)$

Definition: $\{a_i\}$ are mutually relatively prime iff $(a_1, \ldots, a_n) = 1$.

Example: (2,3,9) is mutually relatively prime but not *pairwise* relatively prime.

Proposition 2. $a_1, \ldots, a_n$ are mutually relatively prime iff we can solve the equation

$$\sum_{i=1}^{n} a_i x_i = 1 \qquad (*)$$

in integers.

Proof. Suppose $d = (a_1, \ldots, a_n) = 1$. Then by Prop.1, $1 = d \in M = \{\sum_{i=1}^{n} a_i x_i | x_i \in \mathbb{Z}\}$. So (*) can be solved in integers. Conversely, suppose (*) has a solution in integers. Then $1 \in M^+$, and so $d = 1$.
□

Proposition 3. Let $a, b, c \in \mathbb{Z}$, $(a, b) = 1$. Suppose $a|bc$. Then $a|c$.

Proof. Since $(a, b) = 1$, by Prop.2, $\exists\ x, y \in \mathbb{Z}$. Set $ax + by = 1$. Then $c = c(ax + by) = a(cx) + (bc)y$. Since $a|bc$, a divides the right hand side, hence $a|c$.
□

Proof of unique factorization in $\mathbb{Z}$.

Existence

As shown before, every $n \geq 1$ is a product of primes.

Uniqueness (second proof)

Let $n > 1$ be the smallest counterexample. So we can write $n = p_1 \ldots p_r = q_1 \ldots q_s$, with p_i, q_j primes and $p_1 \neq q_j$ for any (i, j). So

$$p_1 | n = q_1 \ldots q_s = q_1(q_2 \ldots q_s).$$

Since $p_1 \neq q_1$, $(p_1, q_1) = 1$, and by Prop. 3, $p_1|(q_2 \ldots q_s)$. Again, since $p_1 \neq q_2$, applying Prop.3 again, $p_1|(q_3 \ldots q_s)$. Finally get $p_1|q_s$. So there is no such counterexample.
□

Third Proof of the Infinitude of Primes in $\mathbb{Z}$ (Polya)

For every $n \geq 1$, put $F_n = 2^{2^n} + 1$, called the nth *Fermat number*.

Lemma. If $n \neq m$, $(F_n, F_m) = 1$.

Proof of Lemma. We may assume $m > n$. Write $m = n + k$, for some $k > 0$. *To show*:

$$(F_n, F_{n+k}) = 1 \quad (\text{for } k > 0.)$$

Suppose $d|F_n$ **and** $d|F_{n+k}$. Put $x = 2^{2^n}$. Then, since

$$F_{n+k} = 2^{2^{n+k}} + 1 = 2^{2^n 2^k} + 1,$$

$$\begin{aligned}\frac{F_{n+k} - 2}{F_n} &= \frac{x^{2^k} - 1}{x + 1} \\ &= x^{2^k - 1} - x^{2^k - 2} + \cdots - 1 \in \mathbb{Z} \\ &\Rightarrow F_n | (F_{n+l} - 2) \Rightarrow d|2.\end{aligned}$$

But F_n, F_{n+k} are odd. So $d = 1$. Hence the lemma. □

Proof of Infinitude of primes

Consider $F_1, F_2, \ldots, F_n \ldots$ By lemma, each F_n is divisible by a prime, call it p_n, not dividing the previous $F_k,\ k < n$. The sequence $\{p_1, p_2, \ldots\}$ is infinite. □

One has: $F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$ (Fermat), $F_5 = (641)(6700417), \ldots$

Primes in "Arithmetic Progressions":

Fix $m > 1$, and $a \in \mathbb{Z}$ such that $(a, m) = 1$.

Theorem (Dirichlet) $\exists$ infinitely many primes p which are $\equiv a \pmod m$.

We cannot possibly prove it in this class. But we can prove the following:

Baby Lemma $\exists$ infinitely many primes p which are $\equiv 3 (\mathrm{mod}\, 4)$.

Proof: Suppose $\exists$ only a finite number of such primes, say 3, p_1, p_2, $\cdots$, p_r.

Consider

$$N = 4p_1\, p_2\, \cdots p_r + 3.$$

By unique factorization in $\mathbb{Z}$ we can write $N = q_1 q_2 \cdots q_s$, with the q_j's being primes.

Claim 1: *Some q_j must be $\equiv 3 (mod\, 4)$.*

Indeed, every q_j is an odd prime as N is odd, and moreover if $q_j \equiv 1 (\mathrm{mod}\, 4)\ \forall j$, then N will also be $\equiv 1 (\mathrm{mod}\, 4)$, contradiction! Hence Claim 1.

Say $q_1 \equiv 3 (\mathrm{mod}\, 4)$.

Claim 2: $q_1 \notin \{3, p_1, \cdots, p_r\}$.

Indeed, if $q_1 = 3$, then $3|N$, and since $N = 4p_1 \cdots p_r + 3$, 3 must divide $4p_1 \cdots p_r, \rightarrow\leftarrow$. So $q_1 \neq 3$. Suppose $q_1 = p_i$ for some $1 \leq i \leq r$. Then $p_i \mid N$, and since $N = 4p_1 \cdots p_r + 3$, $p_i \mid 3, \rightarrow\leftarrow$. So $q_1 \neq p_i$. Hence Claim 2.

So we have produced a new prime $q_1 \equiv 3 (\mathrm{mod}\, 4)$ which is not in the original list, $\rightarrow\leftarrow$. □

Remark: There is no such simple argument to prove Dirichlet's theorem for primes $\equiv 1 (\mathrm{mod}\, 4)$. We can try to start the same way by assuming that we have a finite list of primes $\equiv 1 (\mathrm{mod}\, 4)$, say $p_1, p_2, \cdots, p_r$, and we can consider $N = 4p_1 \cdots p_r + 1$. Factor N as $q_1 \cdots q_s$. Now the analog of Claim 1 will in general fail as the product of an even number of numbers congruent to 3 (mod 4) is 1 (mod 4). However, we will prove the infinitude of such primes later after studying squares mod p.

Earlier we saw a *heuristic reason* for expecting there to be an infinite number of **twin primes**, e.g. {3, 5}, {5, 7}, {11, 13}, $\cdots$
Expectation:

$$\pi_2(x) := \# \begin{pmatrix} \text{twin primes} \\ \leq x \end{pmatrix} \approx \quad C \frac{x}{\log^2 x}, \qquad \text{as } x \to \infty.$$

This twin prime problem is closely related to the **Goldbach problem**, which asks if every even number ≥ 4 is a sum of 2 primes.
Best known result: (Chen)

$$2n = a_1 + a_2, \text{ with } a_i \text{ prime or a product of 2 primes.}$$

A similar heuristic reason makes one expect that there are infinitely many primes p of the form $n^2 + 1$.
Best known result: (Iwaniec)

$$\exists \text{ an infinite of sequence } \{m_1, m_2, \cdots\}$$

such that
(i)

$$m_j = n_j^2 + 1, \qquad \forall j$$

and for every j,
(ii)

$$m_j \text{ is a prime or a product of 2 primes}$$

The proof is quite hard and beyond the scope of our class.

4 Pythagorean Triples

Problem:

Find all $x, y, z \in \mathbb{N}$ such that

$$x^2 + y^2 = z^2 \tag{1}$$

If $d = (x, y, z) > 1$, then $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ is another solution, called the **primitive solution**.

For primitive solutions, we may assume that x is odd and y is even.

The Geometric Method

Solving (1) in integers amounts to solving the following in rational numbers:

$$X^2 + Y^2 = 1 \tag{2}$$

Geometrically, (2) is the equation of the unit circle in $\mathbb{R}^2$ with center at $O = (0, 0)$. Try to parametrize the circle.

One can try as in calculus to set

$$X = \cos\theta,\ Y = \sin\theta.$$

This turns out to be *terrible* for number theory. A better way is to consider the parametrization

$$X = \frac{1 - t^2}{1 + t^2}, \quad Y = \frac{2t}{1 + t^2}$$

This is *ingenious* as this only involves rational functions. If $t \in \mathbb{Q}$, then $X, Y \in \mathbb{Q}$. Of course

$$X^2 + Y^2 = \frac{(1 - t^2)^2 + 4t^2}{(1 + t^2)^2} = 1$$

As $t \to \infty$ (along rationals) then

$$X = \frac{1 - t^2}{1 + t^2} \to -1$$

So we are only missing one solution, $(-1, 0)$, which we will remember.

Check: If $X, Y \in \mathbb{Q}$, then $t \in \mathbb{Q}$. (Show: $t = \frac{Y}{1+X}$.)

So the rational solutions of (2) are obtained by setting

$$X = \frac{1-t^2}{1+t^2}, \quad Y = \frac{2t}{1+t^2},$$

together with the *missing solution* $(-1, 0)$.

Write $t = \frac{u}{v},\ u, v \in \mathbb{Z}$. Then

$$X = \frac{v^2-u^2}{v^2+u^2}, \quad Y = \frac{2vu}{v^2+u^2}$$

It follows that the non-zero solutions in $\mathbb{Z}$ of (1) are given by

$$x = v^2 - u^2,\ y = 2uv,\ z = v^2 + u^2$$

with

$$u \neq \pm v,\ u, v \neq 0$$

To get primitive solutions, it is convenient to put

$$m = v + u,\ n = v - u$$

$$x = (v+u)(v-u) = mn,\ y = \frac{m^2-n^2}{2},\ z = \frac{m^2+n^2}{2}$$

For primitive solutions, take m, n odd $\geq 1,\ m > n$. Check that these are all the primitive solutions.

5 Linear Equations

Basic problem: Fix $a_1, \ldots, a_n \in \mathbb{Z},\ n > 0$. Consider the equation:

$$a_1x_1 + \cdots + a_nx_n = \vec{a} \cdot \vec{x} = m, \tag{*}$$

where $\vec{a} = (a_1, \ldots, a_n)$ and $\vec{x} = (x_1, \ldots, x_n)$. Determine if (*) can be solved **in integers**. If so, determine all the solutions.

These are the simplest Diophantine Equations.

Earlier, we proved that, given $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero, $\exists!$ positive integer d, called the **greatest common divisor**, such that we can solve

$$a_1x_1 + \ldots a_nx_n = m$$

if m is a multiple of d, and that the set

$$M = \{a_1x_1 + \cdots + a_nx_n | x_1, \ldots, x_n \in \mathbb{Z}\}$$

is simply $d\mathbb{Z}$. Moreover, d is the smallest number in $M^+ = \{r \in M | r > 0\}$, which exists by the WOA.

Consequently we have

Lemma 1. (*) can be solved iff m is a multiple of gcd $(\{a_i\})$. □

So the basic problem comes down to determining all solutions of $a \cdot x = dN$, for any $N \geq 1$.

Suppose **n=1**; then it is trivial. We have:

$$a_1 \neq 0,\ d = gcd = |a_1|,$$

and we need to solve

$$a_1x_1 = |a_1|N \qquad (*_N)$$

But there is a **unique** solution, namely:

$$x_1 = sgn(a_1)N$$

n=2:

First look at case **gcd=1**, **N=1**.

$$a_1x_1 + a_2x_2 = 1 \qquad (*_1)$$

By Lemma 1 there exists a solution, call it (u_1, u_2). Suppose (v_1, v_2) is another solution. Then

$$a_1u_1 + a_2u_2 = 1 \qquad (1)$$

$$a_1v_1 + a_2v_2 = 1 \qquad (2)$$

Multiply (1) by v_1; (2) by u_1:

$$\begin{aligned} &a_1u_1v_1 + a_2u_2v_1 = v_1 \\ &\underline{a_1u_1v_1 + a_2u_1v_2 = u_1} \\ &a_2(v_1u_2 - u_1v_2) = v_1 - u_1 = k \end{aligned}$$

Do same with (1) times v_2, (2) times u_2 to get:

$$a_1 \underbrace{(u_1v_2 - u_2v_1)}_{-k} = (v_2 - u_2)$$

So

$$v_1 = u_1 + ka_2, \quad v_2 = u_2 - ka_1.$$

(u_1, u_2) is a **particular solution** which we use to generate all solutions.

Conversely, for **any** integer k,

$$(u_1 + ka_2,\ u_2 - ka_1)$$

is a solution of $\vec{a} \cdot \vec{x} = 1$.

If gcd $(a_1, a_2) = 1$, then we can solve $a_1x_1 + a_2x_2 = 1$ in integers. Moreover, if (u_1, u_2) is a particular solution, then any other solution is of the form $(u_1 + ka_2, u_2 - ka_1),\ k \in \mathbb{Z}$.

n=2, **d >1**, **N=1**:

$$a_1x_1 + a_2x_2 = d \qquad (*_1)$$

Since $d = \gcd(a_1, a_2)$, $d|a_1$ and $d|a_2$. Put $b_i = \frac{a_i}{d}$. Then (*) becomes

$$b_1x_1 + b_2x_2 = 1 \text{ with } (b_1, b_2) = 1.$$

So if (u_1, u_2) is a particular solution, every solution is of the form

$$\left(u_1 + k\frac{a_2}{d},\ u_2 - k\frac{a_1}{d}\right).$$

This finishes the $n = 2$ case. We summarize the results in the following

Proposition *Let a_1, a_2 be non-zero integers, and let d be their gcd. Then the equation*

$$a_1x_1 + a_2x_2 = m$$

is solvable in integers iff m is divisible by d. Moreover, if (u_1, u_2) is any particular solution, then the set of all solutions is parametrized by $\mathbb{Z}$, and for each $r \in \mathbb{Z}$, the corresponding solution is given by

$$x_1 = u_1 + r\frac{a_2}{d}, \quad \text{and} \quad x_2 = u_2 - r\frac{a_1}{d}.$$

n, a, N arbitrary: (general case)

It will be good to understand the example at the end of the section (for $n = 3$). The rest of the section may be difficult and is included here for completeness.

Definition:

$$M_n(\mathbb{Z}) = \{a = (a_{ij}) : \ n \times n - \text{matrices with } a_{ij} \in \mathbb{Z} \ \forall i, j\}.$$

$$I_n = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$

$$GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det(A) = \pm 1\}$$

The equation of interest is

$$(a_1, \ldots, a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = Nd \qquad (*_N)$$

Lemma 1 *Let $a = (a_1, \cdots, a_n) \in \mathbb{Z}^n - \{0\}$ with $d = \gcd(a_1, \cdots, a_n)$. Then $\exists\, C \in GL_n(\mathbb{Z})$ such that $aC = de_n = (0, \cdots, 0, d)$.*

Proof. $n = 1$: $d = |a_1|$, so we can take $C = (sgn(a_1))$. Now let $n > 1$, and assume Lemma by induction for $m < n$. If $a_1 = \cdots = a_{n-1} = 0$ we can take

$$C = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & \text{sgn } (a_n) \end{array} \right).$$

So we may suppose that $a' := (a_1, \cdots, a_{n-1}) \in \mathbb{Z}^{n-1} - \{0\}$.

Let $d' = \gcd(a_1, \cdots, a_{n-1})$. By the inductive hypothesis, $\exists\, C' \in GL_{n-1}(\mathbb{Z})$ such that $a'\, C' = (0, \cdots, d') \in \mathbb{Z}^{n-1}$.

Let

$$A = \left(\begin{array}{c|c} C' & 0 \\ \hline 0 & 1 \end{array} \right) \in GL_n(\mathbb{Z}).$$

Then $aA = (0, \cdots, 0, d', a_n)$. Clearly, $d = \gcd(d', a_n)$, and $\exists\, x, y \in \mathbb{Z}$ such that $d'x + a_n\, y = d$.

Put

$$B = \begin{pmatrix} a_n/d & x \\ -d'/d & y \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Then $(d', a_n)\, B = (0, d)$.

Put

$$C = A \left(\begin{array}{c|c} I_{n-2} & 0 \\ \hline 0 & B \end{array} \right) \in GL_n(\mathbb{Z}).$$

Then

$$aC = (aA) \left(\begin{array}{c|c} I_{n-2} & 0 \\ \hline 0 & B \end{array} \right) = (0, \cdots, 0, d', a_n) \left(\begin{array}{c|c} I_{n-2} & 0 \\ \hline 0 & B \end{array} \right) \tag{3}$$

$$= (0, \cdots, 0, d). \tag{4}$$

□

Theorem 5.1 *Let $a = (a_1, \cdots, a_n) \in \mathbb{Z}^n - \{0\}$ with* gcd *equal to d.*
Let C be the matrix given by Lemma. Pick any $N \in \mathbb{Z}$. Then we have:

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n$$

is a solution of $\sum_{i=1}^{n} a_i x_i = Nd$ if and only if $\exists m_1, \cdots, m_{n-1} \in \mathbb{Z}$ such that

$$x = \sum_{i=1}^{n-1} m_i C^i + NC^n$$

where C^j denotes $(\forall j)$ the j-th column of C.

Proof.
Let $y = x - NC^n$.

Then

$$
\begin{array}{c}
a \cdot x = Nd \Leftrightarrow a \cdot y = 0 \\
\Updownarrow \\
aC(C^{-1}y) = (0, \cdots, 0, d)(C^{-1}y) = 0 \\
\Updownarrow \\
C^{-1}y = m = \begin{pmatrix} m_1 \\ \cdot \\ \cdot \\ m_{n-1} \\ 0 \end{pmatrix}, \text{ for some } m_i \in \mathbb{Z}, 1 \leq i \leq n-1 \\
\Updownarrow \\
y = Cm = \sum_{i=1}^{n-1} m_i \, C^i \\
\Updownarrow \\
x = Cm + NC_n.
\end{array}
$$

Example: Find all the integral solutions of

$$5x + 7y + 11z = 2. \qquad (*)$$

Put $a = (5, 7, 11)$. Then the gcd of the coordinates of a is 1. By Lemma, we can find a 3×3 - integral matrix C of determinant ± 1 such that $aC = (0, 0, 1)$. The proof of Lemma gives a recipe for finding C. First solve $5x + 7y = 1$. Since $1 = \gcd(5, 7)$, this can be solved, and a solution (by inspection) is given by $x = -4$, $y = 3$. Put $C' = \begin{pmatrix} 7 & -4 \\ -5 & 3 \end{pmatrix}$. Next we have to solve $d'u + 11v = 1$, where $d' = \gcd(a_1, a_2) = 1$. A solution is given by $u = 1$, $v = 0$. Let $B = \begin{pmatrix} 11 & 1 \\ -1 & 0 \end{pmatrix}$.

Then the proof of Lemma says that

$$C = \left(\begin{array}{cc|c} & & 0 \\ & C' & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & & \\ 0 & & B \end{array}\right).$$

Matrix multiplication gives

$$C = \begin{pmatrix} 7 & -44 & -4 \\ -5 & 33 & 3 \\ 0 & -1 & 0 \end{pmatrix}.$$

By the Theorem, the complete set of integral solutions of (*) is given by:

$$\begin{bmatrix} x = 7m - 44n - 8 \\ y = -5m + 33n + 6 \\ z = -n \end{bmatrix} \text{ where } m,\, n \in \mathbb{Z}$$

6 Congruences

Fix an integer $m > 1$. We say that two integers a, b are **congruent modulo** m iff $m|(a - b)$.

Remark: If we had done this for $m = 1$, then any pair a, b would be congruent mod 1.

If a, b are congruent mod m, we write

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

Modular arithmetic:

If a is any integer, we can use the Euclidean algorithm to write

$$a = mq + r, \text{ with } 0 \leq r < m$$

Then $m|(a - r)$, so $a \equiv r \pmod{m}$.

Consequently, we can partition $\mathbb{Z}$ into m blocks, one for each integer r, with $0 \leq r < m$. Suppose B_r is the block corresponding to r. Then, for **any** a in B_r, $a \equiv r \pmod{m}$. Note: $B_0 = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$, $B_1 = \{\ldots, -2m + 1, -m + 1, 1, m + 1, 2m + 1, \ldots\}$, etc.

If $\underline{m = 2}$, this partition will yield even and odd integers; the even integers are $\equiv 0 \pmod{2}$ and the odd integers are $\equiv 1 \pmod{2}$.

$\underline{m = 3}$:

These blocks are called **congruence classes modulo** m. There are exactly m classes. We write $\mathbb{Z}/m$ for $\{B_0, B_1, \ldots B_{m-1}\}$.

a	r (mod 3)
0	0
1	1
2	2
3	0
4	1
5	2
6	0

Definition: A **set of representatives** for $\mathbb{Z}/m$ is a subset $S = \{x_0, x_1, \ldots, x_{n-1}\}$ of $\mathbb{Z}$ such that $x_r \in B_r$ for each $r = 0, 1, \ldots, m-1$.
Note: There is a **natural choice** for S, namely $S_0 = \{0, 1, \ldots, m-1\}$, called the **standard** or **usual** set of representatives.

So for $m = 3$, we can use

$$S_0 = \{0, 1, 2\}$$

or

$$S_1 = \{9, 16, -1\}$$

as a set of representatives.
Claim:

One has addition, subtraction, 0, and multiplication in $\mathbb{Z}/m$, just like in $\mathbb{Z}$.

Proof. Consider B_i, B_j. Look at $i + j$. By Euclidean algorithm,

$$i + j = qm + r_{i+j},$$

for some r_{i+j} with $0 \leq r_{i+j} < m$. We put

$$B_i + B_j = B_{r_{i+j}}$$

Similarly, $B_i - B_j = B_{r_{i-j}}$, if $i - j = q'm + r_{i-j}$, with $0 \leq r_{i-j} < m$. B_0 is the "zero" of $\mathbb{Z}/m$, because

$$B_0 + B_i = B_i = B_i + B_0$$

Multiplication

Here is how we determine B_iB_j: Write $ij = bm + r_{ij}$, $0 \leq r_{ij} < m$. Put

$$B_iB_j = B_{r_{ij}}.$$

Note that

$$B_1 B_j = B_j, \text{ for any } j.$$

So B_1 is the (multiplicative) "identity" element.

We also have distributive and associative laws in $\mathbb{Z}/m$ just like in $\mathbb{Z}$.

Definition: If $a \in \mathbb{Z}$, write $a \pmod m$ to denote the block it belongs to. If $a, b \in \mathbb{Z}$, we write $a+b \pmod m$ for any element of $B_i + B_j$, if $a \in B_i,\ b \in B_j$. Similarly, $ab \pmod m$ is defined.

Remark. In $\mathbb{Z}$ the only numbers we can divide by, i.e., which have "multiplicative inverses", are ± 1. The situation is better in $\mathbb{Z}/m$. In fact, when m is a prime p, all the non-zero elements of $\mathbb{Z}/m$ are invertible $\pmod m$.

7 Linear Equations mod m

Given $a, c \in \mathbb{Z}$, we want to solve

$$(A) \qquad ax \equiv c \pmod{m}$$

Note that we can solve the "congruence" (I) iff we can solve

$$(B) \qquad ax + my = c$$

with $x, y \in \mathbb{Z}$.

We have looked at $\star$ before.

Recall:

(i) For $\star$ to have a solution in integers, it is necessary and sufficient to have c be divisible by the gcd, say d, of a, m.

(ii) Let u, v satisfy

$$(C) \qquad \left(\frac{a}{d}\right) u + \left(\frac{m}{d}\right) v = 1$$

This is possible as $(\frac{a}{d}, \frac{m}{d}) = 1$.

All the solutions for (C) are obtained by first finding one solution, say (u_0, v_0) and writing the general solution as

$$(u, v) = \left(u_0 + k\frac{m}{d}, v_0 - k\frac{a}{d}\right)$$

for any $k \in \mathbb{Z}$.

So the general solution of (B) is given by

$$\begin{aligned}(x, y) &= \left(c\left(u_0 + \frac{km}{d}\right),\ c\left(v_0 - \frac{ka}{d}\right)\right) \\ &= \left(cu_0 + k\frac{c}{d}m,\ cv_0 - k\frac{c}{d}a\right)\end{aligned}$$

Thus the general solution to (A) is given by

$$x = cu_0 + k\left(\frac{c}{d}\right)m$$

Suppose x, x' are both solutions of (A) mod m. Then

$$a(x - x') \equiv 0 \bmod m,$$

which means

$$m|a(x-x').$$

Since $d = gcd(a, m)$ we need

$$\frac{m}{d}|(x-x')$$

Example. $m = 6,\ a = 4$

$$4(x-x') \equiv 0 \pmod 6,\ d = 2 \Leftrightarrow 3|(x-x')$$

So

$$(x-x') \equiv 0 \text{ or } 3 \pmod 6$$

In general, if $(a, m) = d$, then

$$a(x-x') \equiv 0 \pmod m \Rightarrow x - x' \text{ is divisible by } \frac{m}{d}$$

There exists exactly d distinct solutions of (*) mod m. So we have

Lemma. $ax \equiv c \pmod m$ has solutions if

$$d = gcd(a, m) \mid c.$$

When $d|c$, there are d distinct solutions mod m.

Corollary: $ax \equiv 1 \pmod m$ can be solved iff $(a, m) = 1$. Moreover, the solution is unique in this case.

Definition: If $(a, m) = 1$, we call the unique $x \pmod m$ such that $ax \equiv 1 \pmod m$ the **inverse** of a mod m.

Often, people write it as $a' \pmod m$.

Example. $m = 7,\ a = 2,\ a' = 4 \pmod 7$.

Recall

$$\mathrm{S}_0 = \{0, 1, \ldots, m-1\}$$

is a set of reps. for $\mathbb{Z}/m$. (It is the standard set of reps.)

Definition:

$$(\mathbb{Z}/m)^* = \{\text{Invertible elements of } \mathbb{Z}/m\}$$

$$\varphi(m) = \#(\mathbb{Z}/m)^*$$

Explicitly,

$$\varphi(m) = |\{a \in \{0, 1, \ldots, m-1\} \ |(a, m) = 1\}|.$$

8 Euler's φ-function

The function φ introduced above is called Euler's totient function.
Note: If m is a prime p, then $\varphi(p) = p - 1$.

Theorem. Fix any $m \geq 1$. Then, for any integer a relatively prime to m, we have

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

Corollary (Fermat's Little Theorem). For any prime p, and for any a not divisible by p,

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

This is *very* useful for computations.

Example: Compute $11^{470} \pmod{37}$.

Idea: Since 37 is a prime, by Fermat's little theorem,

$$a^{36} \equiv 1 \pmod{37}.$$

Hence

$$a^{r+36b} \equiv a^r \pmod{37}.$$

Write, using the Euclidean algorithm,

$$\begin{aligned} 470 &= 36b + r,\ 0 \leq r < 36 \\ &= 36 \cdot 13 + 2 \\ \Rightarrow 11^{470} &\equiv 11^2 \pmod{37} \\ &\equiv 10 \pmod{37}. \end{aligned}$$

Proof of Theorem. Let

$$\mathrm{S} = \{r_0, \ldots, r_{n-1}\}$$

be a set of reps. for $\mathbb{Z}/m$, and let $(a, m) = 1$. Consider

$$\mathrm{S}' = \{ar_0, ar_1, \ldots, ar_{m-1}\}.$$

Claim. S′ is another set of reps for $\mathbb{Z}/m$.

To show the claim, we need to prove

$$ar_i \equiv ar_j \pmod{m} \Rightarrow i = j.$$

Suppose $ar_i \equiv ar_j$, for some $i \neq j$. Then

$$a(r_i - r_j) \equiv 0 \pmod{m},$$

i.e., $m|a(r_i - r_j)$. Since $(a, m) = 1,\ m|(r_i - r_j)$, but this contradicts the fact that S is a set of reps. for $\mathbb{Z}/m$. Hence the claim.

So S and S$'$ are both sets of reps for $\mathbb{Z}/m$. In other words, for each congruence class B_i and m, $\exists!$ number in $B_i \cap$ S and in $B_i \cap$ S$'$. Consequently, the product of all the numbers in S coprime to m will be congruent (mod m) to the product of all the numbers in S$'$ coprime to m.

Moreover, if r_i is coprime to m, so is ar_i. So

$$\prod_{\substack{r_i \in \mathrm{S} \\ (r_i, m)=1}} (ar_i) \equiv \prod_{\substack{r_i \in \mathrm{S} \\ (r_i, m)=1}} r_i \pmod{m}$$

$$\Rightarrow a^{\varphi(m)} \left(\prod_{\substack{r_i \in S \\ (r_i, m)=1}} r_i \right) \equiv \left(\prod_{\substack{r_i \in S \\ (r_i, m)=1}} r_i \right) \pmod{m}$$

If we set

$$b = \prod_{\substack{r_i \in S \\ (r_i, m)=1}} r_i,$$

we then have

$$a^{\varphi(m)} b \equiv b \pmod{m}, \text{ with } (b, m) = 1,$$

which implies that

$$m \mid (a^{\varphi(m)} - 1)b.$$

Since $(b, m) = 1$,

$$m|(a^{\varphi(m)} - 1), \text{ i.e., } a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Done.

Warning: Little Fermat says that $a^{p-1} \equiv 1 \pmod{p}$, for any prime p **and** $1 \leq a < p$. It might happen that $\exists m \geq 1$ which is **not** a prime and a such that

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

For example, consider
$m = 341 = (11)(31)$, and $a = 2$. Then

$$2^{340} \equiv 2^{11-1} \cdot 34 \equiv 1 \pmod{11}$$

by Little Fermat. Also

$$2^{340} \equiv 2^{(31-1)11} \cdot 2^{10} \equiv 2^{10} \pmod{31} \equiv 32^2 \pmod{31} \equiv 1 \pmod{31}.$$

Hence

$$2^{340} \equiv 1 \pmod{31}.$$

In other words, 2^{340} is congruent to 1 modulo both 11 and 31. Since 11 and 31 are relatively prime, this implies

$$2^{341-1} \equiv 1 \pmod{341},$$

though 341 is not a prime. (Some call it a *pseudo-prime*.)

Clearly, if m is a prime p, then $\varphi(m) = p - 1$. It is of great importance to have a formula for computing $\varphi(m)$ even when m is not a prime. To this end we prove the following

Theorem Let $m > 1$. Write $m = \prod_{i=1}^{r} p_i^{a_i}$, where $p_1, \cdots, p_r$ are distinct primes and $a_1, \cdots, a_r$ are positive integers. Then

$$\varphi(m) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1) \tag{a}$$

and

$$m = \sum_{d|m} \varphi(d). \tag{b}$$

Proof: (a) **Step 1:** *Show* $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ *if* n_1, n_2 *are relatively prime.*

Proof of Step 1:

$$\begin{aligned}\varphi(n_1n_2) &= \#\{y \in \{1, 2, \cdots, n_1n_2 - 1\} \mid (y,\, n_1n_2) = 1\} \\ &= \#\{a_in_1 + b_jn_2 \mid a_i \in \mathbb{Z}/n_2, b_j \in \mathbb{Z}/n_1, (a_in_1 + b_jn_2,\, n_1n_2) = 1\}.\end{aligned}$$

But we have

$$(a_in_1 + b_jn_2,\, n_1n_2) = 1 \Longleftrightarrow \begin{pmatrix}(a_in_1 + b_jn_2,\, n_1) = 1 \\ \text{and} \\ (a_in_1 + b_jn_2,\, n_2) = 1\end{pmatrix}$$

Also, $(a_in_1 + b_jn_2, n_1) = 1$ iff $(b_jn_2, n_1) = 1$, that is iff $(b_j, n_1) = 1$, since $(n_1, n_2) = 1$.

Similarly, $(a_in_1 + b_jn_2, n_2) = 1$ iff $(a_i, n_2) = 1$.

Consequently,

$$\begin{aligned}\varphi(n_1n_2) &= \#\{a_in_1 + b_jn_2 \mid (a_i, n_2) = 1, (b_j, n_1) = 1\} \\ &= \varphi(n_1)\,\varphi(n_2).\end{aligned}$$

Hence we have achieved Step 1.

Step 2: *If p is a prime and $a > 0$, then show: $\varphi(p^a) = p^{a-1}(p-1)$.*

Proof of Step 2:

$$\varphi(p^a) = \#\{b \in \{0, \cdots, p^a - 1\} \mid p \nmid b\} = p^a - \#\{b \in \{0, 1, \cdots, p^a\} \mid p \mid b\} = p^a - p^{a-1},$$

which proves the assertion.

Step 3: *Proof of the general case*:

By step 1, we have

$$\text{If} \quad m = \prod_{i=1}^{r} p_i^{a_i}, \text{then} \quad \varphi(m) = \prod_{i=1}^{r} \varphi\left(p_i^{a_i}\right)$$

This is so because $(p_i^{a_i}, p_j^{a_j}) = 1$ if $i \neq j$. Now part (a) of the Theorem follows by Step 2.

(b): $m = \prod_{i=1}^{r} p_i^{a_i}$. So every positive divisor d of m is of the form $m = \prod_{i=1}^{r} p_i^{b_i}$ with $0 \leq b_i \leq a_i$. So

$$\sum_{d|m} \varphi(d) = \sum_{\{(b_1,\ldots,b_r) \mid 0 \leq b_i \leq a_i, \forall i\}} \varphi\left(\prod_{i=1}^{r} p_i^{b_i}\right).$$

By part (a) this equals

$$\sum_{\{(b_1,\ldots,b_r)|0\le b_i\le a_i,\forall i\}} \prod_{i=1}^{r} \varphi(p_i^{b_i}),$$

with $\varphi(p_i^{b_i})$ being $p_i^{b_i} - p_i^{b_i-1}$ (resp. 1) if $b_i > 0$ (resp. $b_i = 0$). Exchanging the sum and the product, and noting that for fixed b_j, $j \neq i$,

$$\sum_{\{(b_1,\ldots,b_r)|0\le b_i\le a_i\}} \varphi(p_i^{b_i}) \;=\; p_i^{a_i},$$

we get

$$\sum_{d|m} \varphi(d) \;=\; \prod_{i=1}^{r} p_i^{a_i} \;=\; m.$$

This finishes our proof of the Theorem.

9 Linear congruences revisited

Theorem. Fix $m > 1$. Let $a, c \in \mathbb{Z}$. Put $d = gcd(a, m)$. Then the congruence

$$ax \equiv c \pmod{m} \qquad (*)$$

has a solution $x \pmod{m}$ iff $d|c$. Moreover, when $d|c$, all d solutions are of the form

$$x \equiv \frac{cu_0 + mk}{d} \pmod{m},$$

with $k \in \mathbb{Z}$, where (u_0, v_0) is a solution of $au + mv = d$.

We already proved (*) has a solution $x \pmod{m}$ iff $d|c$. So let $d|c$. Let (u_0, v_0) be a solution of

$$au + mv = d. \qquad (**)$$

Multiply by c, get

$$acu_0 + mcv_0 = cd,$$

i.e.,

$$a\left(\frac{cu_0}{d}\right) + m\left(\frac{cv_0}{d}\right) = c$$

$$\Rightarrow a\left(\frac{cu_0}{d}\right) \equiv c \pmod{m}$$

$$\Rightarrow x \equiv \frac{cu_0}{d} \pmod{m} \text{ is a solution of (*).}$$

Recall that we get all the solutions of (**) by taking

$$(u, v) = \left(u_0 + \frac{km}{d},\ v_0 - \frac{kc}{d}\right),$$

as k runs over $\mathbb{Z}$. So the general solution of (*) is given by

$$x \equiv \frac{cu_0}{d} + \frac{km}{d} \equiv \frac{cu_0 + km}{d} \pmod{m}$$

QED.

Corollary: $ax \equiv 1 \pmod{m}$ has a solution iff $(a, m) = 1$. In this case there is a unique solution, called the **multiplicative inverse** of a mod m, and denoted $a' \pmod{m}$.

We knew before that a has a multiplicative inverse if $(a, m) = 1$. This corollary replaces the *if* by *iff*.

Definition:

$$(\mathbb{Z}/m)^* = \{a \in \mathbb{Z}/m | (a, m) = 1\}.$$

Note: By corollary, $(\mathbb{Z}/m)^*$ is precisely the subset of $\mathbb{Z}/m$ consisting of elements which have multiplicative inverses mod m.
Recall:

$$\begin{aligned}\varphi(m) &= |(\mathbb{Z}/m)^*|. \\ &= |\{a \in \{0, 1, \ldots, m-1\} | (a, m) = 1\}|.\end{aligned}$$

In the previous section we proved the following:

Theorem: (Euler) For any $a \in \mathbb{Z}$ with $(a, m) = 1$,

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

Corollary. (Fermat's Little Theorem)

$$m = p \text{ (prime)},\ (p, a) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

Remark. Fermat's Little Theorem says that

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

has $p-1$ solutions mod p, namely

$$x \equiv 1, 2, \ldots, p-1 \pmod{p}$$

$$\Rightarrow a^p - a \equiv 0 \pmod{p}, \ \forall a = 1, 2, \ldots, p-1.$$

This is also true for

$$a \equiv 0 \pmod{p}.$$

So,

$$x^p - x \equiv 0 \pmod{p}$$

has p solutions mod p. On the other hand,

$$x^p \equiv 0 \pmod{p}$$

has only one solution, namely $x \equiv 0 \pmod{p}$. In other words, if $a \neq 0 \pmod{p}$, then a^p cannot be $0 \pmod{p}$.

Claim. If $ab \equiv 0 \pmod{p}$, then either a or b must be $\equiv 0 \pmod{p}$.

Proof of Claim. Suppose $a \not\equiv 0 \pmod{p}$. Then a is invertible modulo p, i.e.,

$$a \in (\mathbb{Z}/p)^*.$$

So $\exists a'$ such that $a'a \equiv 1 \pmod{p}$. Multiple both sides of $ab = 0 \pmod{p}$ by a' to get $(aa')b \equiv 0 \pmod{p}$, giving

$$b \equiv 0 \pmod{p}.$$

Conclusion: $\mathbb{Z}/p$ has no "zero divisors." It is a **field** just like $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}$.

Note: If m is any integer > 1 which is **not** a prime, then $\mathbb{Z}/m$ has zero divisors.

Proof. Since m is composite, we can write $m = m_1, m_2$ with $m_1, m_2 > 1$. then

$$m_1 m_2 \equiv 0 \pmod{m},$$

but neither m_1 nor m_2 is $\equiv 0 \pmod{m}$.

Moral: Congruences modulo a prime p are nicer to study. They have much more structure.

10 Number of solutions modulo a prime

Theorem *(Lagrange) Fix a prime p and integer $n \geq 1$. Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial with coefficients $a_i \in \mathbb{Z}$, such that some a_j is prime to p. Then the congruence*

$$f(x) \equiv 0 \, (mod \, p) \tag{1}$$

has at most n solutions mod p.

Proof: Suppose $n = 1$. Then the congruence is $a_1 x \equiv -a_0 \, (\mathrm{mod}\, p)$. By hypothesis, either a_1 or a_0 is not divisible by p. The former case must happen as otherwise we would have $0 \equiv -a_0 \pmod{p}$, implying a_0 and a_1 are both $\equiv 0 \pmod{p}$, leading to a contradiction. Thus a_1 is invertible $\mathrm{mod}\, p$; let a_1' be such that $a_1' \, a_1 \equiv 1 (\mathrm{mod}\, p)$. Multiplying $a_1 x \equiv -a_0 \, (\mathrm{mod}\, p)$ by a_1', get

$$(a_1' a_1) x \equiv x \equiv -a_1' a_0 (\mathrm{mod}\, p)$$

Thus we get a unique solution, and the Theorem is O.K. for $n = 1$.

Now let $n > 1$, and assume by induction that the Theorem holds for all $k < n$. Suppose (1) has no solutions $\mathrm{mod}\, p$. Then there is nothing to prove. So we may assume that there is at least one solution, say $x \equiv x_1 \, (\mathrm{mod}\, p)$. Then we get

$$f(x_1) \equiv 0 \, (\mathrm{mod}\, p). \tag{2}$$

Subtracting (2) from (1), we get

$$f(x) - f(x_1) \equiv a_n (x^n - x_1^n) + a_{n-1} (x^{n-1} - x_1^{n-1}) + \cdots a_1 (x - x_1) \equiv 0 \, (\mathrm{mod}\, p).$$

But for any $k \geq 1$, $(x - x_1) \mid (x^k - x_1^k)$, so $f(x) - f(x_1) = (x - x_1) g(x)$, where $g(x)$ is a polynomial in x of degree $k - 1$. Thus, $f(x) - f(x_1) \equiv 0 \, (\mathrm{mod}\, p)$ holds iff

$$(x - x_1) g(x) \equiv 0 \, (\mathrm{mod}\, p). \tag{3}$$

Then **either** $x - x_1 \equiv 0$ **or**

$$g(x) \equiv 0 \, (\mathrm{mod}\, p) \tag{4}$$

The coefficients of g cannot all be $\equiv 0 \pmod{p}$, for otherwise $f(x)$ would be congruent to 0 (mod p). Since the degree of g is $< n$, we then have by the inductive hypothesis, that the number of solutions of (4) mod p is bounded above by $n - 1$. Then the number of solutions mod p of (1) is $\leq 1 + n - 1 = n$.

QED.

11 Fermat's Last Theorem and Gauss

Recall the Fermat equation $x^n+y^n = z^n$. For $n = 2$, this leads to Pythagorean triples and we classified all the solutions in this case.

Theorem (A. Wiles) ('97): For $n \geq 3$, $x^n + y^n = z^n$ has no positive integral solutions.

There is no way we can prove this magnificent result in this class.

Note: To prove this, it suffices to prove in the cases where $n = 4$ and when $n = p$, where p is any odd prime.

Reason: If $m|n$, then any solution of $u^n + v^n = w^n$ will give a solution for m, namely $(u^{n/m})^m + (v^{n/m})^m = (w^{n/m})^m$.

Moreover, for any $n \geq 3$, n will be divisible by 4 or by an odd prime p.

We also proved in the first week that $x^4+y^4 = z^4$ has no integral solutions for. (In fact, we showed Fermat's result that $x^4 + y^4 = w^2$ has no integral solutions.) Consequently, the key fact needed to be proven is that $x^p+y^p = z^p$ has no solution for any odd prime.

This gets split into two cases:

$$\begin{aligned} \text{Case I:} &\quad p \nmid xy\,z. \\ \text{Case II:} &\quad p \mid xy\,z. \end{aligned}$$

Gauss showed almost no interest in the Fermat equation. We say *almost* because there is just one place where he discusses a congruence which is of some relevance for the first case of FLT.

Proposition (Gauss). Suppose the congruence

$$(*) \qquad x^p + y^p \equiv (x + y)^p \pmod{p^2}$$

has no *non-trivial* solutions, i.e. with none of x, y, $x + y \equiv 0 \pmod{p}$. Then Case I of FLT holds for p, i.e.

$$\nexists\, x, y, z \in \mathbb{Z}_{>0}, \quad p \nmid x\,y\,z, \text{ such that } x^p + y^p = z^p.$$

Note:

$$(x + y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j}, \quad \binom{p}{j} = \frac{p!}{(p-j)!j!}$$

If $j \neq 0$ or p, then $\binom{p}{j}$ is divisible by p. Since $(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j}$, we get

$$(x+y)^p \equiv x^p + y^p \,(\mathrm{mod}\, p).$$

Proof of Prop.

Suppose we have positive integers x, y, z, with $p \nmid xyz$, such that $x^p + y^p = z^p$. We have just seen that $x^p + y^p \equiv (x+y)^p \,(\mathrm{mod}\, p)$, so $z^p \equiv (x+y)^p \,(\mathrm{mod}\, p)$.

Moreover, we have the Little Fermat Theorem, which says that $x^p \equiv x \,(\mathrm{mod}\, p)$, $z^p \equiv z \,(\mathrm{mod}\, p)$, $y^p \equiv y \,(\mathrm{mod}\, p)$, and $(x+y)^p \equiv x + y \,(\mathrm{mod}\, p)$. Consequently, $z \equiv x + y \,(\mathrm{mod}\, p)$, i.e. $z = x + y + mp$, for some $m \in \mathbb{Z}$.

Since $x^p + y^p = z^p$, we get

$$\begin{aligned} x^p + y^p = (x+y+mp)^p &= \sum_{i=0}^{p} \binom{p}{i} (x+y)^i (mp)^{p-i} \\ &= (mp)^p + p(x+y)(mp)^{p-1} + \cdots + p(x+y)^{p-1}(mp) + (x+y)^p. \end{aligned}$$

Therefore $x^p + y^p \equiv (x+y)^p \,(\mathrm{mod}\, p^2)$

QED.

Difficulty:

If $p \equiv 1 \,(\mathrm{mod}\, 3)$, one can always solve the congruence $x^p + y^p \equiv (x+y)^p \,(\mathrm{mod}\, p^2)$. So Gauss's Proposition doesn't help us. On the other hand, when $p \equiv 2 (\mathrm{mod}\, 3)$, $x^p + y^p \equiv (x+y)^p \,(\mathrm{mod}\, p^2)$ has no solution for many small p.

Still, there are primes $p \equiv 2 \,(\mathrm{mod}\, 3)$ for which $\exists$ solutions to this congruence. This happens for 13 primes less than 1000, as you will verify in a HW exercise in Assignment 2. For example, when $p = 59$, $1^{59} + 3^{59} \equiv 4^{59} \,(\mathrm{mod}\, 59^2)$.

12 Mersenne Primes, Perfect Numbers and the Lucas-Lehmer primality test

Basic idea: try to construct primes of the form $a^n - 1$; $a, n \geq 1$. e.g.,
$2^2 - 1 = 3$ but $2^4 - 1 = 3 \cdot 5$
$2^3 - 1 = 7$
$2^5 - 1 = 31$
$2^6 - 1 = 63 = 3^2 \cdot 7$
$2^7 - 1 = 127$
$2^{11} - 1 = 2047 = (23)(89)$
$2^{13} - 1 = 8191$

Lemma: $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$

Corollary: $(x-1)|(x^n - 1)$

So for $a^n - 1$ to be prime, we need $a = 2$.
Moreover, if $n = md$, we can apply the lemma with $x = a^d$. Then

$$(a^d - 1)|(a^n - 1)$$

So we get the following

Lemma If $a^n - 1$ is a prime, then $a = 2$ and n is prime.

Of course this is a necessary, but not sufficient condition as seen by the case $2^{11} - 1$.

Definition: A *Mersenne prime* is a prime of the form

$$q = 2^p - 1, \ p \text{ prime.}$$

Question: *Are they infinitely many Mersenne primes?*

A conjecture of Lenstra, Pomerance and Wagstaff predicts that there are infinitely many Mersenne primes.

Best result (as of May 2013):
The largest known Mersenne prime $q = 2^p - 1$ is associated to $p = 57,885,161$, and this was checked in Febuary 2013. This q is in fact the largest known prime.
Definition: *A positive integer n is perfect iff it equals the sum of all its (positive) divisors $< n$.*

Definition: $\sigma(n) = \sum_{d|n} d$ *(divisor function)*

So n is perfect if $n = \sigma(n) - n$, i.e. if $\sigma(n) = 2n$.
Well known example: $n = 6 = 1 + 2 + 3$
Properties of σ:

1. $\sigma(1) = 1$
2. n is a prime *iff* $\sigma(n) = n + 1$
3. If p is a prime, $\sigma(p^j) = 1 + p + \cdots + p^j = \frac{p^{j+1}-1}{p-1}$
4. (Exercise) If $(n_1, n_2) = 1$ then $\sigma(n_1)\sigma(n_2) = \sigma(n_1 n_2)$ "multiplicativity".

Consequently, if

$$n = \prod_{j=1}^{r} p_i^{e_j},$$

with positive integers e_j and pairwise distinct primes p_j, we have

$$\sigma(n) = \prod_{j=1}^{r} \sigma(p_j^{e_j}) = \prod_{j=1}^{r} \left(\frac{p^{e_j+1} - 1}{p - 1} \right)$$

Examples of perfect numbers: $\begin{cases} 6=1+2+3 \\ 28=1+2+4+7+14 \\ 496 \\ 8128 \end{cases}$

Questions:

1. Are there infinitely many perfect numbers?
2. Is there any odd perfect number?

Note:

$$6 = (2)(3),\ 28 = (4)(7),\ 496 = (16)(31),\ 8128 = (64)(127)$$

They all look like

$$2^{n-1}(2^n - 1),$$

with $2^n - 1$ prime (i.e., of Mersenne type).

Theorem (Euler) *Let n be a positive, even integer. Then*

$$n \text{ is perfect} \Leftrightarrow n = 2^{p-1}(2^p - 1), \text{ for a prime } p, \text{ with } 2^p - 1 \text{ a prime.}$$

Corollary. *There exists a bijection between even perfect numbers and Mersenne primes.*

Proof of Theorem. ($\Leftarrow$) Start with $n = 2^{p-1}q$, with $q = 2^p - 1$ a Mersenne prime. To show: n is perfect, i.e., $\sigma(n) = 2n$. Since $2^{p-1}q$, and since $(2^{p-1}, q) = 1$, we have

$$\sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)(q + 1) = q2^p = 2n.$$

($\Rightarrow$): Let n be a even, perfect number. Since n is even, we can write

$$n = 2^j m, \text{ with } j \geq 1, \ m \text{ odd } \neq n$$

.

$$\Rightarrow \sigma(n) = \sigma(2^j)\sigma(m) = (2^{j+1} - 1)\sigma(m)$$

Since n is perfect,

$$\sigma(n) = 2n = 2^{j+1}m$$

Get

$$2^{j+1}m = (2^{j+1} - 1)\sigma(m)$$

Since $2^{j+1} - 1$ is odd,

$$2^{j+1} | \sigma(m),$$

implying that

$$r2^{j+1} = \sigma(m) \tag{1}$$

for some $r \geq 1$.

Also,

$$2^{j+1}m = (2^{j+1} - 1)r2^{j+1},$$

so

$$m = (2^{j+1} - 1)r. \tag{2}$$

Suppose $r > 1$. Then

$$m = (2^{j+1} - 1)r$$

will have $1, r$ and m as 3 distinct divisors.
(*Explanation*: By hypothesis, $1 \neq r$. Also, $r = m$ iff $j = 0$ iff $n = m$, which will then be odd!)

Hence

$$\begin{aligned}\sigma(m) \geq & 1 + r + m \\ = & 1 + r + (2^{j+1} - 1)r \\ = & 1 + 2^{j+1}r \\ = & 1 + \sigma(m)\end{aligned}$$

Contradiction!

So $r = 1$, and so (1) and (2) become

$$\sigma(m) = 2^{j+1} \tag{1'}$$

$$m = 2^{j+1} - 1 \tag{2'}$$

Since $n = 2^j m$, we will be done if we prove that m is a prime. It suffices to show that $\sigma(m) = m + 1$. But this is clear from (1') and (2').
QED.

For any integer $n \geq 1$, let us call $M_n = 2^n - 1$ a Mersenne number. Define numbers S_n recursively by setting

$$S_n = S_{n-1}^2 - 2, \text{ with } S_1 = 4.$$

Then we have

$$S_2 = 14,\ S_3 = 194,\ S_4 = 37634,\ S_5 = 1416317954,$$

$$S_6 = 2005956546822746114, \ldots$$

Some books have a shift and start with the sequence a_n with $a_0 = 4$ and $a_n = a_{n-1}^2 - 2$. This is not a serious difference, but one has to be careful when checking various tables available online.

Theorem: (Lucas-Lehmer Primality Test) *Suppose for some $n \geq 2$ that M_n divides S_{n-1}. Then M_n is prime.*

Look at $n = 5$. Since $S_4 = 37634$ is divisible by $31 = 2^5 - 1$, the criterion checks in this simple case. In fact, 37304 has the prime factorization $2(31)(607)$, but the fact that 607 is a prime, etc. is not important to check the primality of 31. We don't care about factoring S_{n-1}, which can be forbidding, only that it is divisible (or not) by M_n.

Note also that it is not too time-consuming to check in an integer m is divisible by $2^n - 1$, since we can first write $m = q \cdot 2^n + r$ (by writing m in binary, for example), and then adding, to r, $q \bmod 2^n - 1$.

Proof of Theorem. (*Very clever*) Put $\alpha = 2 + \sqrt{3}$, $\beta = 2 - \sqrt{3}$. Note that $\alpha + \beta = 4$, $\alpha\beta = 1$. So $S_1 = \alpha + \beta$.

Lemma. For any $n \geq 1$, $S_n = \alpha^{2^{n-1}} + \beta^{2^{n-1}}$.

Proof of Lemma: $n = 1 :\ S_1 = \alpha + \beta = 4$. So let $n > 1$, and assume that the lemma holds for $n - 1$. Since

$$S_n = S_{n-1}^2 - 2$$

we get (by induction)

$$S_n = (\alpha^{2^{n-1}} + \beta^{2^{n-1}})^2 - 2$$

Note:

$$\begin{aligned}(\alpha^k + \beta^k)^2 &= \alpha^{2k} + 2\alpha^k\beta^k + \beta^{2k} \\ &= \alpha^{2k} + \beta^{2k} + 2, \text{ as } \alpha\beta = 1.\end{aligned}$$

So we get (setting $k = 2^{n-2}$)

$$S_n = \alpha^{2^{n-1}} + \beta^{2^{n-1}} + 2 - 2.$$

Hence the lemma.

Proof of Theorem (continued): Suppose $M_n | S_{n-1}$. Then we may write $rM_n = S_{n-1}$, some positive integer. By the lemma, we get

$$rM_n = \alpha^{2^{n-2}} + \beta^{2^{n-2}} \tag{3}$$

Multiply (3) by $\alpha^{2^{n-2}}$ and subtract 1 to get:

$$\alpha^{2^{n-1}} = rM_n\alpha^{2^{n-2}} - 1 \tag{4}$$

Squaring (4) we get

$$\alpha^{2^n} = (rM_n\alpha^{2^{n-2}} - 1)^2 \tag{5}$$

Suppose M_n is not a prime. Then $\exists$ a prime ℓ dividing M_n, $\ell \leq \sqrt{M_n}$. Let us work in the number system

$$R = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$$

Check: R is closed under addition, subtraction, and multiplication (it is what one calls a ring). Equations (4) and (5) happen in R. Define $R/\ell = \{a, b\sqrt{3} | a, b \in \mathbb{Z}/\ell\}$.

Note: $|R/\ell| = \ell^2$

We can view α, β as elements of R/ℓ. Since $\ell | M_n$, (4) becomes the following congruence in R/ℓ:

$$\alpha^{2^{n-1}} \equiv -1 \ (mod\ \ell) \tag{6}$$

Similarly, (5) says

$$a^{2^n} \equiv 1 \ (mod\ \ell)$$

Put

$$X = \{\alpha^j \bmod \ell | 1 \leq j \leq 2^n\}.$$

Claim $|X| = 2^n$.

Proof of claim. Suppose not. Then $\exists j, k$ between 1 and 2^n, with $j \neq k$, such that $\alpha^j \equiv \alpha^k \pmod{\ell}$.

If r denotes $|j - k|$, then $0 < r < 2^n$ and $\alpha^r \equiv 1 \pmod{\ell}$. Let d denote the gcd of r and 2^n, so that $ar + b2^n = d$ for some $a, b \in \mathbb{Z}$. Then we have

$$\alpha^d = \alpha^{ar+b2^n} = (\alpha^r)^a \cdot (\alpha^{2^n})^b \equiv 1 \pmod{\ell}.$$

But since $d | 2^n$, d is of the form 2^m for some $m < n$, and $\alpha^d \equiv 1 \pmod{\ell}$ contradicts $\alpha^{2^{n-1}} \equiv -1 \pmod{\ell}$. Hence the claim.

So $|X| \leq \ell^2 - 1$, i.e., we need $2^n \leq \ell^2 - 1$.

Since

$$\ell \leq \sqrt{M_n},\ \ell^2 - 1 < M_n = 2^n - 1.$$

$\Rightarrow 2^n < 2^n - 1$, a contradiction!

So M_n is prime.

QED

13 RSA Encryption

The mathematics behind the very successful RSA encryption method is very simple and uses mainly Euler's congruence for any $N \geq 1$:

$$b^{\varphi(N)} \equiv 1 \pmod{N}$$

if $(b, N) = 1$. (When N is a prime, this is Fermat's little theorem.)

Imagine that a person X wants to send a carefully encrypted message to another person Y, say. X will look in a directory which publishes the *public key* of various people including Y. The public key of Y will be a pair (e, N) of positive integers, where N will be a large number which is a product of 2 distinct primes p and q. The point is that the directory will contain no information on the factorization of N. For large enough N it will become impossible (virtually) to factor N. The number e will be chosen mod N and it will be prime to $\varphi(N)$.

The person X will first represent his/her *plain text* message by a numeral a (which can be done in many ways). For simplicity, suppose that a is prime to N. X will then raise a to the power e mod N and send the message as b. So

$$b \equiv a^e \pmod{N}.$$

If someone intercepts the message, he or she will be unable to recover a from b without knowing the factorization of N. So it is secure. On the other hand, the recipient of the message, namely Y, will be able to decode (decrypt) the message as follows. He/she will pick a number d (*decryption constant*) such that

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Y can do this because he/she knows the prime factors p, q and because e is prime to $\varphi(N)$; observe that since p and q are distinct primes and $N = pq$, one has

$$\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

So by applying Euler's congruence mod N, we get

$$b^d \equiv a^{ed} \equiv a^{1+c(p-1)(q-1)} \equiv a \pmod{N}.$$

Thus Y recovers a.

Note that if someone does not have the factorization of N, he/she will find it hard to decrypt the message.

The major fault line in this method is that there is no proof – at all, that the only reasonably fast way to decrypt the RSA-encrypted message is to know the factorization of N. In a sense this is scary because so much of the internet traffic is dependent on RSA for secure transmission of possibly sensitive information.

14 Primitive roots mod p and Indices

Fix an odd prime p, and $x \in \mathbb{Z}$. By little Fermat:

$$x^{p-1} \equiv 1 \ (mod\ p) \text{ if } x \not\equiv 0 \ (mod\ p)$$

Example: $\mathbf{p = 5}$

x	x^2	x^3	x^4
1	1	1	1
2	-1	3	1
3	-1	2	1
4	1	-1	1

2 and 3 are called **primitive roots mod 5**, since no smaller power than $4 = 5 - 1$ is $\equiv 1 \pmod 5$.

Definition: Let $x \in \mathbb{Z}$, $p \not| x$. Then the *exponent* of x (relative to p) is the smallest integer r among $\{1, 2, \ldots, p-1\}$ such that $x^r \equiv 1 \pmod p$. One writes $r = e_p(x)$.

When $p = 5,\ e_5(1) = 1,\ e_5(2) = 4 = e_5(3),\ e_5(4) = 2$.

Definition: x is a *primitive root mod p* iff $e_p(x) = p - 1$.

Again, when $p = 5$, 2 and 3 are primitive roots.

Claim: For any x prime to p,

$$e_p(x) | (p-1).$$

Proof: Since $1 \leq e_p(x) \leq p - 1$, by definition, it suffices to show that

$$d = \gcd(e_p(x), p-1) \geq e_p(x).$$

Suppose $d < e_p(x)$. Since d is the gcd of $e_p(x)$ and $p-1$, we can find $a, b \in \mathbb{Z}$ such that $ae_p(x) + b(p-1) = d$. Then

$$x^d = x^{ae_p(x)+b(p-1)} = (x^{e_p(x)})^a (x^{p-1})^b$$

But

$$x^{p-1} \equiv 1 \pmod{p} \text{ by Little Fermat,}$$

and

$$x^{e_p(x)} \equiv 1 \pmod{p} \text{ by definition of } e_p(x).$$

Thus

$$x^d \equiv 1 \pmod{p}$$

Since we are assuming that $d < e_p(x)$, we get a contradiction as $e_p(x)$ is the smallest such number in $\{1, 2, \ldots, p-1\}$.

$\Rightarrow d \geq e_p(x)$.

Since $d = \gcd(e_p(x), p-1),\ d|e_p(x) \Rightarrow d = e_p(x)$. Hence the Claim.

Two natural questions

1. Are there primitive roots mod p?
2. If so, how many are there?

For $p = 5$, the answers are *yes* for (1), and *two* for (2).

Theorem: Fix an odd prime p. Then

(i) $\exists$ primitive roots mod p

(ii) $\#\{\text{primitive roots mod } p\} = \varphi(p-1)$.

Of course, (i) implies (ii) as $\varphi(m) \geq 1$ for any positive integer m.

Proof: For every (positive) divisor d of $p-1$, put

$$\psi(d) = \#\{x \in \{1, \ldots, p-1\} | e_p(x) = d\}$$

Both (i) and (ii) will be proved if we show

$$\psi(p-1) = \varphi(p-1). \qquad (*)$$

We will in fact show that

$$\psi(d) = \varphi(d) \quad \forall d|(p-1)$$

Every x in $\{1, \ldots, p-1\}$ has an exponent, and by the Claim above, this exponent is a divisor d of $p-1$. Consequently,

$$(p-1) = \sum_{d|(p-1)} \psi(d) \tag{1}$$

Recall, on the other hand, that we proved in Chapter 8 that

$$p-1 = \sum_{d|(p-1)} \varphi(d) \tag{2}$$

Consequently,

$$\sum_{d|(p-1)} \psi(d) = \sum_{d|(p-1)} \varphi(d) \tag{3}$$

Since $\psi(d)$ and $\varphi(d)$ are both non-negative, it suffices to show that

$$(A) \qquad \psi(d) \leq \varphi(d), \quad \forall d|(p-1)$$

Proof of (A): Pick any $d|(p-1)$. If $\psi(d) = 0$, we have nothing to prove. So assume that $\psi(d) \neq 0$. Then

$$\exists a \in \{1, \ldots, p-1\} \text{ such that } e_p(a) = d.$$

Consider

$$Y = \{1, a, \ldots, a^{d-1}\}$$

Then Y supplies d distinct solutions to the congruence

$$x^d \equiv 1 \pmod{p}.$$

(If they are not distinct, then a^{i-j} will be 1 mod p for some $i \neq j$, $i, j \in [1, d-1]$, which will contradict $d = e_p(a)$ being the smallest integer $m > 0$ such that $a^m \equiv 1 \pmod{p}$.) In Chapter 10 we proved Lagrange's theorem which says that given any polynomial $f(x)$ with integral coefficients f degree n, with not all of whose coefficients are zero mod p, there are at most n solutions mod p of $f(x) \equiv 0 \pmod{p}$. So $x^d - 1 \equiv 0 \pmod{p}$ has at most d solutions mod p. Consequently, Y is exactly the set of solutions to this congruence and $\#Y = d$.

Claim:

$$\psi(d) = \#\{a^j \in Y | e_p(a^j) = d \,|\, (j, d) = 1\}.$$

Indeed, let $r = \gcd(j, d)$. Then by the proof of the earlier Claim,

$$e_p(a^j) = \frac{d}{r}.$$

So $r = 1$ iff $e_p(a^j) = d$. Hence the Claim.

So we have:

$$\psi(d) = \#\left\{ a^j \in Y \middle| \begin{array}{c} j \in \{0, 1, \ldots, d-1\} \\ (j, d) = 1 \end{array} \right\} \leq \varphi(d) \text{ for all } d|(p-1).$$

In fact we see that $\psi(d) = 0$ or $\varphi(d)$, which certainly proves (A), and hence the Theorem. QED

2 is a primitive root modulo the following primes < 100:

$$3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83$$

Artin's Conjecture:

There are infinitely many primes with 2 as a primitive root.

More generally, for any non-square a, one can ask if there are infinitely many primes with a a primitive root mod p.

This blind generalization cannot be true if a is a perfect square. Indeed if $a = b^2$, since $b^{(p-1)} \equiv 1 \pmod{p}$, if $p \not| b$, we have

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

So, for any odd $p \not| a$, $e_p(a)|(\frac{p-1}{2})$. Similarly, $a = -1$ is another bad case, because

$$(-1)^2 = 1 \text{ and } e_p(-1) = 2 \text{ or } 1, \ \forall p \text{ odd}.$$

So one is led to the following

Generalized Artin Conjecture. Let a be an integer which is not -1 and not a perfect square. Then $\exists$ infinitely many primes such that $e_p(a) = p - 1$.

Here is a positive result in this direction:

Theorem: (Gupta, Murty, and Heath-Brown) There are at most three pairwise relatively prime a's for which there are possibly just a finite number of primes such that $e_p(a) = p - 1$.

Problem: *No one seems to have any clue as to the nature and size of these three possible exceptions, or whether they even exist. Is* 2 *an exception?*

Indices

Fix an odd prime p and a primitive root a mod p. We can consider

$$Y = \{a^j | 0 \leq j < p-1\}.$$

Then each element of Y is in $(\mathbb{Z}/p)^*$ and we get $p-1$ distinct elements. But $\#(\mathbb{Z}/p)^* = p-1$. So Y gives a set of reps. for $(\mathbb{Z}/p)^*$.

Consequently, given any integer b prime to p, we can find a *unique* $j \in \{0, 1, \ldots, p-2\}$ such that $b \equiv a^j \pmod{p}$.

This (unique) j is called the **index** of b mod p relative to a, written $I_p(b)$ or $I(b)$. One has the following

Properties:

$$I(ab) \equiv I(a) + I(b) \,(\mod p)$$

$$I(ka) \equiv kI(a) \,(\mod p)$$

15 Squares mod p

Recalll that a real number x is a square if and only if the sign of x sis positive. One can ask a similar question if we replace the field $\mathbb{R}$ by the finite field $\mathbb{Z}/p$, for a fixed prime p.

Basic question: Given $a$in $\mathbb{Z}$, how can we determine if $\exists b \in \mathbb{Z}$ such that $a \equiv b^2 \pmod{p}$?

Trivial case: If $p|a$, one can take $b \equiv 0$. Also, every integer is a square mod 2. So from now on we may (and we will) assume that $(a, p) = 1$ with p odd.

Let's make a table for very small odd primes: (with $x \not\equiv 0 \bmod p$)

p = 3

x	x^2
1	1
2	1

p = 5

x	x^2
1	1
2	-1
3	-1
-1=4	1

p = 7

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

1 : square mod 3	$1, 4$: squares mod 5	$1, 2, 4$: squares mod 7
2 : non-square mod 3	$2, 3$: non-squares mod 5	$3, 5, 6$: non-squares mod 7

Guess:

$$\#\text{ of squares in } (\mathbb{Z}/p)^\times = \#\text{ of non-squares in } (\mathbb{Z}/p)^\times$$

for any odd prime p.

Definition: *The Legendre symbol of a mod p is given by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \equiv \text{ square mod } p \\ -1, & \text{if } a \not\equiv \text{ square mod } p \end{cases}$$

We say a is a *quadratic residue* mod p if it is a $\square$, otherwise a quadratic *non-residue*. (Some would allow a to be divisible by p and set $(\frac{a}{p}) = 0$ if $p|a$.)

Lemma: *The Guess is on the money.*

Proof: Let $S = \{1, 2, \ldots, p-1\}$. We know that S is a set of representatives for $(\mathbb{Z}/p)^\times$. Put

$$T = \left\{1, 2, \ldots, \frac{p-1}{2}\right\},$$

which we will call a **half-set of representatives**,and

$$T^2 = \{b^2 | b \in T\}.$$

Claim A: *$\#(T^2 \ mod\ p) = \frac{p-1}{2}$, i.e., if $b, c \in T$, $b \neq c$, then $b^2 \not\equiv c^2$ (mod p).*

Proof of Claim A: Indeed, if $b^2 \equiv c^2 \pmod{p}$ then $b \equiv \pm c \pmod{p}$. This cannot happen as, $\forall b \in T$, $\exists$ unique b' in $S - T$ such that $b' \equiv -b \pmod{p}$, unless $b = c$. □

Claim B: *$T^2 \equiv S^2$ (mod p)*

Proof: Let $a \in S - T$. Then $\exists! a' \in T$ such that $a' \equiv -a \pmod{p}$. Then $a^2 \equiv (a')^2 \pmod{p}$. Hence $a^2 \in T^2 \bmod p \Rightarrow$ the square of any element of S is in $T^2 \bmod p$. Hence the claim. □

End of Proof of Lemma 1:

Note that $\#\{\text{quad res. mod } p\} = \#S^2 \pmod{p}$. On the other hand, by the Claims A and B, there is $\frac{p-1}{2} \Rightarrow \#\{\text{quad. non-res. mod } p\} = p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$.

□

Corollary of Lemma 1: *Let p be an odd prime. then*

$$\sum_{a \in (\frac{\mathbb{Z}}{p})^\times} \left(\frac{a}{p}\right) = 0.$$

Proof of Corollary: Since $\left(\frac{a}{p}\right)$ is 1 for quadratic residues a and -1 for quadratic non-residues, we obtain

$$\sum_{a \in (\frac{\mathbb{Z}}{p})^\times} \left(\frac{a}{p}\right) = \#\{\text{quadratic residues}\} - \#\{\text{quadratic non-residues}\}$$

$$= \frac{p-1}{2} - \frac{p-1}{2} = 0.$$

Done. □

Remark: *Let a, b be integers prime to p. Then with what we have established so far, we can deduce that if at least one of $\{a, b\}$ is a quadratic residue, then*

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

Indeed, is a, b are both quadratic residues mod p, i.e. $a \equiv a_1^2$, $b \equiv b_1^2 \pmod{p}$ for some a_1, b_1, then $ab \equiv (a_1 b_1)^2 \pmod{p}$, and $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}) = 1 \cdot 1$. Now suppose a is a quadratic residue mod p, but not b. $(\frac{a}{p}) = 1$, $(\frac{b}{p}) = -1$. If $(\frac{ab}{p}) = 1$, then $\exists c$ such that $ab \equiv c^2$. Since $(\frac{a}{p}) = 1$, $\exists a_1$ such that $a_1^2 \equiv a \pmod{p}$, implying $a_1^2 b \equiv c^2 \pmod{p}$.

Since $p \not| a_1$, a_1 is invertible mod p, i.e., $\exists a_1'$ such that $a_1 a_1' \equiv 1$. Then $b \equiv (a_1' c)^2 \pmod{p}$, contradicting the assumption that $\left(\frac{b}{p}\right) = -1$.

This multiplicative property still remains valid when $(\frac{a}{p}) = (\frac{b}{p}) - 1$, but the best way to prove it is to appeal to a *criterion of Euler* – see Proposition below and Corollary 1.

Lemma 3 (**Wilson's Theorem**) *For any prime p, $(p-1)! \equiv -1$ (mod p).*

Proof: If $p = 2$, both sides $\equiv 1 \pmod{2}$, done. So assume p odd. Look at $S = \{1, \ldots, p-1\}$, set of resp. $foralla \in S$, let a' be the unique element of S such that $aa' = 1 \pmod{p}$.

$a = a'$ iff $a^2 = 1 \pmod{p}$, i.e., iff $a = 1$ or $a = p - 1$. So,

$$\forall a \in \{2, \ldots, p-2\},\ a' \neq a \text{ and } a' \in \{2, \ldots, p-1\}.$$

$$\Rightarrow (2)(3) \cdot (p-2) \equiv 1 \pmod{p}.$$

$$\Rightarrow (p-1)! \equiv 1(p-1) \pmod{p}$$

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

□

Proposition (*Euler's criterion*) Let p be an odd prime, and let $a \in \mathbb{Z}$ with $(a, p) = 1$. Then

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

Recall that the Little Fermat theorem says that

$$a^{p-1} \equiv +1 \pmod{p} \text{ since } p \not| a;$$

so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

Corollary of Proposition (Strict multiplicativity)

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \quad \forall a, b \in \mathbb{Z} \text{ with } p \not| ab.$$

Proposition ⇒ Corollary 1: By Euler,

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

Corollary 2 of Proposition: If p = odd prime, -1 is a square mod p iff $p \equiv 1 \pmod 4$.

Proposition ⇒ Corollary 2: By Euler, $(\frac{-1}{p}) = 1$ iff $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Since p is odd, $p \equiv 1 \pmod 4$ are -1 (mod 4).

$p \equiv 1 \pmod 4$:
$p = 4m + 1$, some $m \in \mathbb{Z}$:

$$\Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{2m} = 1$$

$p \equiv -1 \pmod 4$:
$p = 4m - 1$:

$$(-1)^{\frac{p-1}{2}} = (-1)^{2m-1} \equiv -1 \pmod p.$$

Proof of proposition: By Fermat, $a^{p-1} \equiv 1 \pmod p$. Since p is odd, $\frac{p-1}{2} \in \mathbb{Z}$ and we can factor:

$$\underbrace{a^{p-1} - 1}_{\equiv 0 \text{ by Fermat}} = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$$

$$\Rightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \bmod p$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

Now suppose a is a square mod p. Then $\exists b$ such that $a \equiv b^2 \pmod p$. So

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

So:

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

On the other hand, the congruence $X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ has at most $\frac{p-1}{2}$ solutions mod p by Lagrange. We have just proved that, given any quadratic residue a mod p,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

i.e., a is a solution of

$$X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}.$$

By lemma 1, there exists exactly $\frac{p-1}{2}$ quadratic residues mod p. Consequently,

$$X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

has exactly $\frac{p-1}{2}$ solutions, and each of them is a quadratic residue mod p. In other words, if a is a quad. non-residue mod p, then a is not a solution of $X^{\frac{p-1}{2}} \equiv 0 \pmod{p}$.

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

if $a \not\equiv \text{square}(modp)$.

□

To summarize, we have the following properties of $(\frac{\cdot}{p})$:

(i) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ (*Product formula*)

(ii) $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$, i.e., -1 is a square (mod p) iff $p \equiv 1 \pmod{4}$.

Remark:

Thanks to (i) and the unique factorization in $\mathbb{Z}$, in order to find $(\frac{a}{p})$ for any $a \in \mathbb{Z}$ with $(a, p) = 1$, we need only know

$$\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \text{ and } \left(\frac{q}{p}\right), \ q \neq p \text{ an odd prime.}$$

We have already found a formula for $(\frac{-1}{p})$.

As an application of (ii) we will prove the following, special case of Dirichlet's theorem:

Proposition: There are infinitely many primes p which are congruent to 1 modulo 4.

Earlier we proved that there exists infinitely many primes $\equiv 3 \pmod 4$ in the following way: Suppose there exists a finite number of such primes. List them as $3, p_1, \ldots, p_r$. Consider

$$N = 4p_1 \ldots p_r + 3.$$

Factor N as $q_1, \ldots q_s$, q_j prime for all j. Since N is odd, each q_j is an odd prime. Moreover, since $N \equiv 3 \pmod 4$, some q_j must be $\equiv 3 \pmod 4$. But this q_j cannot be among $\{3, p_1, \ldots, p_r\}$. Done.

Suppose we tried this for primes $\equiv 1 \pmod 4$. Assume there exists only finitely many such primes $p_1, \ldots, p_m$. Put $N = 4p_1 \ldots p_m + 1$. Factor N as $q_1 \ldots q_s$. Since N is odd, each q_j is an odd prime. But, if s is even, we cannot hope to say that some q_j must be $\equiv 1 \pmod 4$. The method breaks down.

Proof of Proposition: Now we try again using (ii). As before start by assuming there exists only a finite number of primes $\equiv 1 \pmod 4$, say $p_1, \ldots, p_m$. Let $N = 4(p_1 p_2 \ldots p_m)^2 + 1$. Factor N as $q_1 \ldots q_k$, q_j prime for all j. Evidently, each q_j is an odd prime because N is odd.

Claim: *Every q_j is $\equiv 1$ (mod 4).*

Proof of Claim: Pick any odd prime q_j dividing N. Then, since $N = (2p_1 \ldots p_m)^2 + 1$, we get $-1 \equiv b^2 \pmod{q_j}$, where $b = 2p_1 \ldots p_m$. By the criterion (ii), -1 is a square mod q_j iff $q_j \equiv 1 \pmod 4$. Hence the claim.

Back to the proof of Prop. So q_j is a prime which is $\equiv 1 \pmod 4$, and it cannot be among $\{p_1, \ldots, p_m\}$ because if $p_i = q_j$ for some i, we will get $1 \equiv 0 \pmod{q_j}$, a contradiction, proving the proposition.

□

Remark: This proof tells us a way to generate new primes which are $\equiv 1 \pmod 4$ from known ones. Here are some simple examples:

1. Start with 5, and consider $N = 4(5)^2 + 1 = 101$; this is a prime.
2. Start with 13, and consider $N = 4(13)^2 + 1$. Then $N = 677$, also prime.
3. Start with 17. $N = 4(17)^2 + 1 = 1157 = (13)(89)$. Note: 13 and 89 are both $\equiv 1 \pmod 4$.

Next Question: *When is 2 a square mod p?*

To answer this question, Gauss established the following:

Proposition A (**Gauss' Lemma**) Fix a, prime to p. Let T be a subset of $\mathbb{N}$ such that $T \cup (-T)$ is a set of reps. for $(\mathbb{Z}/p)^\times$. Given any $t \in T$, we can then write $at \equiv e_t(a)t_a \pmod{p}$, where $t_a \in T$ and $e_t(a) \in \{\pm 1\}$. Then

$$\left(\frac{a}{p}\right) = \prod_{t \in T} e_t(a).$$

Proof: Let t, t' be distinct numbers in T. Then $at \not\equiv \pm at' \pmod{p}$, i.e., $t_a \not\equiv t'_a$. Hence the map $T \to T$ given by $t \to t_a$ has to be a bijection, i.e., 1-1 and onto. (This is also called a *permutation*, meaning a rearrangement, of T.) We get

$$\begin{aligned} a^{(p-1)/2} \prod_{t \in T} t \equiv \prod_{t \in T} (at) &\equiv \prod_{t \in T} e_t(a) t_a \pmod{p} \\ &\equiv \left(\prod_{t \in T} e_t(a)\right)\left(\prod_{t \in T} t_a\right) \pmod{p} \\ &\equiv \left(\prod_{t \in T} e_t(a)\right)\left(\prod_{t \in T} t\right) \pmod{p} \end{aligned}$$

So

$$a^{\frac{p-1}{2}} \left(\prod_{t \in T} t\right) \equiv \left(\prod_{t \in T} e_t(a)\right)\left(\prod_{t \in T} t\right) \pmod{p}.$$

Cancelling $(\prod_{t \in T} t)$, which is invertible mod p, from each side, we get

$$a^{\frac{p-1}{2}} \equiv \prod_{t \in T} e_t(a)$$

Done because

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

□

Remark: Very often one chooses T to be the "canonical" half set of reps for $(\mathbb{Z}/p)^\times$, namely $T = \{1, 2, \ldots, \frac{p-1}{2}\}$.

Formulation (II) of Gauss' Lemma: *Let* $T = \{1, 2, \ldots, \frac{p-1}{2}\}$, *and* a *an integer prime to* p. *For each* $j \in T$, *find the smallest positive residue* $\bar{a}_j$ *of* aj *mod* p, *which is well defined with* $\bar{a}_j \in \{1, 2, \ldots, p-1\}$. *Let*

$$k = \#\{j \in T | \bar{a}_j \notin T\}.$$

Then

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

Corollary of Gauss' lemma:

$$\left(\frac{2}{p}\right) = (-1)^{n(p)},$$

$n(p)$ *is the number of integers* s *such that*

$$\frac{p-1}{4} < s \leq \frac{p-1}{2}.$$

Explicitly,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p = \pm 1 \ (mod\ 8) \\ -1, & if\ p = \pm 5 \ (mod\ 8) \end{cases}$$

Proof of Corollary. Apply Gauss' lemma to $T = \{1, 2, \ldots, \frac{p-1}{2}\}$ with $a = 2$. Then

$$e_t(2) = \begin{cases} 1, & \text{if } 2s \leq \frac{p-1}{2} \\ -1, & \text{otherwise} \end{cases}$$

Since $\left(\frac{2}{p}\right) = \prod_{s \in T} e_t(2) \pmod{p}$, $(\frac{2}{p}) = (-1)^{n(p)}$. The rest follows.

□

Definition: If $x \in \mathbb{R}$, its integral part $[x]$ is the largest integer $\leq x$.

Proposition (**Formulation III of Gauss' Lemma**) *Let* p *odd prime, and* a *be an odd integer with* $p \not| a$. *Then*

$$\left(\frac{a}{p}\right) = (-1)^t, \ \textit{where } t = \sum_{j=1}^{(p-1)/2} [\frac{ja}{p}].$$

This follows easily from the Formulation II of Gauss's lemma with a little book-keeping. We will indicate how this is done.

Proof: For every $j \in \{1, 2, \ldots, \frac{p-1}{2}\}$, it is easy to see that

$$aj = q_j p + \bar{a}_j, \text{ with } 0 < \bar{a}_j < p.$$

Easy exercise:

$$q_j = \left[\frac{aj}{p}\right].$$

So $\bar{a}_j = aj - [\frac{aj}{p}]$.

Summing over all the j's from 1 to $\frac{p-1}{2}$, we get

$$\sum_{j=1}^{\frac{p-1}{2}} aj = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{aj}{p}\right] p + \sum_{i=1}^{k} r_i + \sum_{i=1}^{k'} \ell_i, \tag{15}$$

where $k' = \frac{p-1}{2} - k$, $\{r_i\}$ = residues $\bar{a}_j$ *not* in T, $\{\ell_i\}$ = residues in T.

Also

$$\sum_{j=1}^{\frac{(p-1)}{2}} j = \sum_{i=1}^{k} (p - r_i) - \sum_{i=1}^{k} \ell_i. \tag{16}$$

Subtracting equation (2) from equation (1), we get

$$(a-1) \sum_{j=1}^{\frac{(p-1)}{2}} j \;=\; p \left(\sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right] - k \right) + 2 \sum_{i=1}^{k} r_i.$$

And we have

$$\sum_{j=1}^{\frac{(p-1)}{2}} j \;=\; \frac{1}{2} \left(\frac{p-1}{2}\right) \left(\frac{p+1}{2}\right) = \frac{p^2-1}{8}$$

Thus

$$\underbrace{(a-1)}_{\text{even since } a \text{ is odd}} \left(\frac{p^2-1}{8}\right) = \sum_{j=1}^{\frac{(p-1}{2}} \left[\frac{ja}{p}\right] - k \qquad (\text{mod } 2)$$

Consequently, k has the same parity as

$$\sum_{j=1}^{\frac{(p-1)}{2}} \left[\frac{ja}{p}\right].$$

□

Review: Let p be a prime, $a \in \mathbb{Z}$, $p \not| a$. Put

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \equiv \text{square} \mod p \\ -1, & a \not\equiv \text{square} \mod p \end{cases}$$

(Some also define $\left(\frac{a}{p}\right)$ for all $\mathbb{Z}$ by setting $(\frac{a}{p}) = 0$ if $p|a$.)

$p = 2$: Everything is a square mod p. So assume p odd from now on. One has the multiplicativity property

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

This follows from Euler's result that

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

Note: Since p is odd, if $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod{p}$, for some a, b prime to p, then $(\frac{a}{b}) = (\frac{b}{p})$. So $(*)$ reduces the problem to finding $(\frac{a}{p})$ in the following three cases

(i) $a = -1$
(ii) $a = 2$
(iii) $a = q$, an odd prime $\neq p$

We have already proved

(i)
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv -1 \pmod 4 \end{cases}$$

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

(iii) q: odd prime $\neq p$.
$$\left(\frac{q}{p}\right) = ?$$

To solve (iii) Gauss introduced his **law of quadratic reciprocity**, which we will study in the next chapter.

16 The Quadratic Reciprocity Law

Fix an odd prime p. If q is another odd prime, a fundamental question, as we saw in the previous section, is to know the sign of $\left(\frac{q}{p}\right)$, i.e., whether or not q is a square mod p. This is a very hard thing to know in general. But Gauss noticed something remarkable, namely that knowing $\left(\frac{q}{p}\right)$ is equivalent to knowing $\left(\frac{p}{q}\right)$; they need not be equal however. He found the precise law which governs this relationship, called the *Quadratic Reciprocity Law*. Gauss was very proud of this result and gave several proofs. We will give one of his proofs, which incidentally introduces a very basic, ubiquitous sum in Mathematics called the **Gauss sum**. We will also give an alternate proof, which is in some sense more clever than the first, due to Eisenstein.

Theorem (Gauss) (Quadratic reciprocity) *Let p, q be distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)(p-1)}{4}} \left(\frac{p}{q}\right).$$

Explicitly,

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

This theorem is very useful in computations.

Example:

$$\left(\frac{37}{691}\right) = 1$$

It is not easy to establish this by computing $(37)^{\frac{691-1}{2}} \pmod{691}$. But one can do it fast by appealing to quadratic reciprocity:

$$\begin{aligned} \left(\frac{37}{691}\right) &= \underbrace{(-1)^{\left(\frac{37-1}{2}\right)\left(\frac{691-1}{2}\right)}}_{1} \left(\frac{691}{37}\right) \\ &= \left(\frac{691}{37}\right); \ \frac{691}{37} = 18\ \frac{25}{37} \\ &= \left(\frac{25}{37}\right) = \left(\frac{5}{37}\right)^2 = 1 \end{aligned}$$

Proof I of Theorem: p, q odd primes, $p \neq q$. Put

$$\xi = e^{\frac{2\pi i}{q}} \in \mathbb{C}$$

Then

$$\xi^q = 1, \text{ but } \xi^m \neq 1 \text{ if } m < q.$$

ξ is called a primitive qth root of unity in $\mathbb{C}$. All powers of ξ will be on the unit circle. In fact, we get a regular q-gon by connecting the q points

$$1, \xi, \ldots, \xi^{q-1}.$$

If the q points are connected to the center of the circle, one divides the circle into wedges – **cyclotomy**, a Greek word meaning *circle cutting*, or more appropriately, **circle division**.

Put

$$R = \{\alpha = a_0 + a_1\xi + \cdots + a_{q-1}\xi^{q-1} | a_0, a_1, \ldots, a_{q-1} \in \mathbb{Z}\}.$$

Clearly, $R \supset \mathbb{Z}$, hence R has 0 and 1. Let

$$\alpha = \sum_{i=0}^{q-1} a_i\xi^i, \ \beta = \sum_{i=0}^{q-1} b_i\xi^i$$

be in R. Then

$$\alpha \pm \beta = \sum_{i=0}^{q-1} (a_i \pm b_i)\xi^i \in R.$$

Since $\xi^q = 1$, given any $n \in \mathbb{Z}$ we can write $n = \ell q + r$, $0 \leq r \leq q-1$ by Euclidean algorithm in $\mathbb{Z}$, and conclude that

$$\xi^n = \xi^r.$$

So R contains all the integral powers of ξ. Then it also contains finite integral linear combinations of such powers. Consequently,

$$\alpha\beta \in R \text{ if } \alpha, \beta \in R.$$

So R is very much like $\mathbb{Z}$. It is a q-dimensional analog of $\mathbb{Z}$. This allows us to define the divisibility in R. To be precise, if $\alpha, \beta \in R$, we say that β divides α, $\beta|\alpha$ iff $\exists\gamma \in R$ such that $\alpha = \beta\gamma$.

In particular, since $p \in R$, it makes sense to ask if p divides some number in R.

Definition: Let $\alpha, \beta \in R$. We say that

$$\alpha \equiv \beta \pmod{p} \text{ iff } p|(\alpha - \beta) \text{ in } R.$$

This allows us to do "congruence arithmetic" mod p in R.

To study $(\frac{q}{p})$, Gauss introduced the following **Gauss Sum**:

$$S_q = \sum_{a \bmod q} \left(\frac{a}{q}\right) \xi^a.$$

Clearly, $S_q \in R$.

We will follow the **convention** that

$$q \mid a \Rightarrow \left(\frac{a}{q}\right) = 0.$$

Aside: (Not necessary for the proof of Quadratic Reciprocity, but interesting)

$$S_q = \sum_{a=1}^{\frac{q-1}{2}} \left(\left(\frac{a}{q}\right) \xi^a + \underbrace{\left(\frac{-a}{q}\right) \xi^{-a}}_{\left(\frac{-1}{q}\right)\left(\frac{a}{q}\right)\bar{\xi^a}} \right)$$

So

$$\left(\frac{-1}{q}\right) = 1 \Rightarrow \quad S_q = \sum_{a=1}^{\frac{q-1}{2}} \left(\frac{a}{q}\right) (\xi^a + \bar{\xi^a}) \in \mathbb{R}$$

and

$$\left(\frac{-1}{q}\right) = -1 \Rightarrow \quad S_q \in i\mathbb{R}$$

In other words, S_q is real in the first case and purely imaginary in the second.

Lemma 1:

$$S_q^2 = (-1)^{\frac{q-1}{2}} q$$

Proof of Lemma 1:

$$\begin{aligned} S_q^2 &= \left(\sum_{a \bmod q} \left(\frac{a}{q}\right) \xi^a \right) \left(\sum_{b \bmod q} \left(\frac{b}{q}\right) \xi^b \right) \\ &= \sum_{a \bmod q} \sum_{b \bmod q} \left(\frac{a}{q}\right) \left(\frac{b}{q}\right) \xi^a \xi^b \\ &= \sum_{a \bmod q} \sum_{b \bmod q} \left(\frac{ab}{q}\right) \xi^{a+b} \\ &= \sum_{c \bmod q} \xi^c \left(\sum_{a \bmod q} \left(\frac{a(c-a)}{q}\right) \right) \end{aligned}$$

So

$$\begin{aligned} S_q^2 &= \sum_{c \bmod q} \xi^c \sum_{a \bmod q} \left(\frac{ac - a^2}{q}\right) \\ &= \sum_{c \bmod q} \xi^c \sum_{a \bmod q} \left(\frac{-a^2(1 - a'c)}{q}\right), \end{aligned}$$

where the second sum runs over a prime to q, with $a'a \equiv 1 \pmod{q}$.

But

$$\left(\frac{-a^2(1-a'c)}{q}\right) = \underbrace{\left(\frac{-1}{q}\right)}_{(-1)^{\frac{q-1}{2}}} \underbrace{\left(\frac{a^2}{q}\right)}_{=1} \left(\frac{1-a'c}{q}\right)$$

$$\Rightarrow S_q^2 = (-1)^{\frac{q-1}{2}} \sum_{c \bmod q} \xi^c f(c),$$

where

$$f(c) = \sum_{a \bmod q} \left(\frac{1-a'c}{q}\right) \quad a \not\equiv 0 \bmod q$$

We now need to evaluate $f(c)$, and there are two cases.

$\mathbf{c \equiv 0 \pmod{q}}$:

$$f(0) = \sum_{\substack{a \bmod q \\ a \not\equiv 0 \pmod{q}}} \left(\frac{1}{q}\right)$$

$$\Rightarrow f(0) = q - 1$$

$c \not\equiv 0 \pmod{q}$: Note that, in this case, the set

$$\{1 - a'c | a \bmod q,\ a \not\equiv 0 \bmod q\}$$

runs over elements of $\mathbb{Z}/q - \{1\}$ exactly once. Indeed, given any $b \in \mathbb{Z}/q$, $b \not\equiv 1 \pmod{q}$, we can solve $a' + b \equiv 1 \pmod{q}$, and the solution is unique.

Therefore,

$$f(c) = \sum_{\substack{b \bmod q \\ b \not\equiv 1 \pmod{q}}} \left(\frac{b}{q}\right).$$

We proved earlier that

$$\sum_{b \bmod q} \left(\frac{b}{q}\right) = 0$$

so

$$f(c) = -\left(\frac{1}{q}\right) = -1,$$

when $c \not\equiv 0 \pmod{q}$.

Consequently

$$S_q^2 = (-1)^{\frac{q-1}{2}} \left[(q-1) + (-1) \sum_{\substack{c \bmod q \\ c \not\equiv 0 \bmod q}} \xi^c \right]$$

Claim: $\sum_{c \bmod q} \xi^c = 0$.

Proof of claim:

$$\sum_{c \bmod q} \xi^c = \sum_{(c-1) \bmod q} \xi^c = \sum_{c \bmod q} \xi^{c+1} = \xi \sum_{c \bmod q} \xi^c$$

$$\Rightarrow \underbrace{(1-\xi)}_{\neq 0} \sum_{c \bmod q} \xi^c = 0 \Rightarrow \sum_{c \bmod q} \xi^c = 0 \text{ as claimed.}$$

Proof 2 of claim:

$$\sum_{c \bmod q} \xi^c = 1 + \xi + \cdots + \xi^{q-1} = \frac{1 - \xi^q}{1 - \xi}$$

$$= 0 \text{ since } \xi^q = 1.$$

By claim,

$$S_q^2 = (-1)^{\frac{q-1}{2}} \left((q-1) + \underbrace{(-1)(0-1)}_{+1} \right)$$
$$= (-1)^{\frac{q-1}{2}} q.$$

This proves Lemma 1.

□

Lemma 2: $S_q^{p-1} \equiv (\frac{p}{q}) \pmod{p}$
(This happens in R mod p)

Proof of Lemma 2:

$$S_q^p = \left(\sum_{a \bmod q} \left(\frac{a}{q}\right) \xi^a \right)^p$$
$$= \sum_{a \bmod q} \left(\frac{a}{q}\right)^p \xi^{ap} + pw, w \in R.$$

Note that $(\frac{a}{q})^p = (\frac{a}{q})$ because $(\frac{a}{q}) = \pm 1$ and p is odd.
In other words,

$$S_q^p \equiv \sum_{a \bmod q} \left(\frac{a}{q}\right) \xi^{ap} \pmod{p}.$$

Since $p \neq q$, p is invertible mod q, and the map $a \mapsto ap$ is a permutation of $\mathbb{Z}/q$, also $ap \equiv 0 \pmod{q}$ iff $a \equiv 0 \pmod{q}$. so the sum over a mod q can be replaced with the same over ap mod q. Write b for ap mod q. Then

$$a \equiv bp' \pmod{q}, \text{ where } pp' \equiv 1(\bmod q).$$

$$\Rightarrow S_q^p \equiv \sum_{b \bmod q} \left(\frac{bp'}{q}\right) \xi^b \pmod{p} \qquad (*)$$

But

$$\left(\frac{bp'}{q}\right) = \left(\frac{b}{q}\right)\left(\frac{p'}{q}\right).$$

Since $p'p \equiv 1 \pmod{q}$,

$$\left(\frac{p'}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1 \Rightarrow \left(\frac{p'}{q}\right) = \left(\frac{p}{q}\right)$$

So

$$\left(\frac{bp'}{q}\right) = \left(\frac{b}{q}\right)\left(\frac{p}{q}\right).$$

So $(*)$ gives

$$S_q^p \equiv \left(\frac{p}{q}\right) \underbrace{\sum_{b \bmod q} \left(\frac{b}{q}\right) \xi^b}_{S_q} \pmod{p}$$

$$\Rightarrow S_q^{p-1} \equiv \left(\frac{p}{q}\right) \pmod{p}$$

This is justified because

$$S_q \not\equiv 0 \pmod{p},$$

which follows from Lemma 1.

□

Proof of Theorem: We will compute S_q^{p-1} in 2 different ways. On the one hand, by using Lemma 1,

$$S_q^{p-1} = (S_q^2)^{\frac{p-1}{2}} = \left((-1)^{\frac{q-1}{2}} q\right)^{\frac{p-1}{2}}$$

$$\overset{\equiv}{\text{Euler}} \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) \pmod{p}$$

$$\Rightarrow S^{p-1} \equiv \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p,}$$

i.e.,

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

On the other hand, by Lemma 2,

$$S^{p-1} \equiv \left(\frac{p}{q}\right) \pmod{p}.$$

Putting them together we get

$$\left(\frac{p}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \left(\frac{q}{p}\right).$$

□

Example:

Is 29 a square mod 43 ?: As 29 and 43 are distinct odd primes, we have by definition 29 is a square mod 43 iff $\left(\frac{29}{43}\right) = 1$. By the Quadratic Reciprocity Law (QRL),

$$\begin{aligned}
\left(\frac{29}{43}\right) &= (-1)^{\frac{28(42)}{4}} \left(\frac{43}{29}\right) = \left(\frac{43}{29}\right) \\
&= \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) \\
\left(\frac{2}{29}\right) &= -1 \text{ as } 29 \equiv 5 \pmod 8 \\
\left(\frac{29}{43}\right) &= -\left(\frac{7}{29}\right) \underbrace{=}_{\text{QRL}} -(-1)^{\frac{6(28)}{4}} \left(\frac{29}{7}\right) \\
&= -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1
\end{aligned}$$

So 29 is *not* a square mod 43.

Remarks:

1. Though QRL gives an effective way to know whether q is a square mod p or not, when q *is* a square, it gives no procedure to find the square root, which can be a problem.

2. One can use QRL to check whether a number q is a prime, similar to the way one uses Fermat's little theorem. For example, one can show that $m = 1729$ is not a prime by looking at

   $$y := 11^{864} \pmod{1729}$$

   Note: $864 = \frac{1729-1}{2}$. So, if m is a prime, $y \equiv (\frac{11}{1729}) \pmod m$.

   Since $1729 \equiv 1 \pmod 4$, by QRL,

   $$\left(\frac{11}{1729}\right) = \left(\frac{1729}{11}\right) = \left(\frac{2}{11}\right) = -1$$

as $11 \equiv 3 \pmod 8$. on the other hand, one can check using PARI, or by successively squaring mod $m = 1729$, that

$$11^{864} \equiv 1 \pmod m.$$

(This is part of a homework problem.) Get a contradiction! So the only possibility is that 1729 is not a prime (which is easy to verify directly as $1729 = 13 \cdot 133 = 13 \cdot 7 \cdot 17$). But this method is helpful, when it works, for larger numbers.

A historical remark: G.H. Hardy went to see S. Ramanujan, when the latter was dying of TB in England. Then Ramanujan asked Hardy if the number of the taxicab Hardy came in was an interesting number. Hardy said "No, not so interesting, just 1729". Ramanujan replied immediately, saying, "On the contrary, that number *is* very interesting because it is the first number which can be written as a sum of 2 cubes in two different ways". Indeed we have

$$1729 = 10^3 + 9^3 = 12^3 + 1^3,$$

and no smaller whole number can be written this way in two different ways. (Can you verify it?)

Here is an intriguing second proof of quadratic reciprocity due to Eisenstein. First we need his **trignometric lemma** below:

Lemma: Let n be a positive, odd integer. Then

$$\frac{\sin nx}{\sin x} = (-4)^{\frac{n-1}{2}} \prod_{j=1}^{\frac{(n-1)}{2}} \left(\sin^2 x - \sin^2 \frac{2\pi j}{n} \right)$$

Note that both sides are polynomials in $\sin^2 x$, so it suffices to check that they have the same roots and the same constant term.

Example: ($\mathbf{n = 3}$)

Write LHS (resp. RHS) for the expression on the left (resp. right) hand

side of the identity claimed in the Lemma. Then

$$\begin{aligned}
\text{LHS} &= \frac{\sin 3x}{\sin x} = \frac{\sin(2x+x)}{\sin x} \\
&= \frac{\sin 2x \cos x + \cos 2x \sin x}{\sin x} \\
&= \frac{2\sin x \cos^2 x + (1-2\sin^2 x)\sin x}{\sin x} \\
&= 2(1-\sin^2 x) + (1-2\sin^2 x) = 3 - 4\sin^2 x \\
\text{RHS} &= -4(\sin^2 x - (\sin\frac{2\pi}{3})^2) = -4\left(\sin^2 x - \frac{3}{4}\right) \\
&= 3 - 4\sin^2 x.
\end{aligned}$$

Sketch of proof of lemma: Use induction on n to show that

$$\frac{\sin nx}{\sin x} = f_n(\sin^2 x),$$

where f_n is a polynomial in $\sin^2 x$ of degree $\frac{n-1}{2}$.

$$(f_0(t) = 1,\ f_3(t) = 3 - 4t, \dots)$$

On the other hand, the RHS of lemma is also of the form $g_n(\sin^2 x)$, where g_n is the explicitly given polynomial in $\sin^2 x$ of degree $\frac{n-1}{2}$.

So it suffices to show that f_n and g_n have the same roots and that the leading coefficient of f_n is $(-4)^{\frac{n-1}{2}}$. So when we use induction on n, check that the leading coefficient is $(-4)^{\frac{(n-1)}{2}}$ and that its roots are

$$\left\{ \sin^2 \frac{2\pi j}{n} \middle| 1 \le j \le \frac{n-1}{2} \right\}.$$

Alternatively, check the constant coefficient by checking at $x \to 0$.

Now recall **Gauss's lemma**:

$$\left(\frac{q}{p}\right) = \prod_{s \in S} e_s(q)$$

where $S = \{1, 2, \dots, \frac{p-1}{2}\}$ and $e_s(q) \in \{\pm 1\}$ defined by

$$qs = e_s(q)s' \,(\mathrm{mod} p), \text{ with } s' \in S.$$

Applying the function $\sin(\frac{2\pi x}{p})$ to both sides, we get

$$\begin{aligned}\sin\left(\frac{2\pi qs}{p}\right) &= \sin\left(\frac{2\pi e_s(q)s'}{p}\right)\\ &= e_s(q)\sin\left(\frac{2\pi s'}{p}\right)\end{aligned}$$

since sin is an odd function. So

$$e_s(q) = \frac{\sin\left(\frac{2\pi qs}{p}\right)}{\sin\left(\frac{2\pi s'}{p}\right)}$$

By Gauss's lemma,

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{s\in S}\frac{\sin\left(\frac{2\pi qs}{p}\right)}{\sin\left(\frac{2\pi s'}{p}\right)}\\ &= \frac{\prod_{s\in S}\sin\left(\frac{2\pi qs}{p}\right)}{\prod_{s\in S}\sin\left(\frac{2\pi s'}{p}\right)}.\end{aligned}$$

Note the map $s \mapsto s'$ is a permutation of S. So,

$$\prod_{s\in S}\sin\left(\frac{2\pi s'}{p}\right) = \prod_{s\in S}\sin\left(\frac{2\pi s}{p}\right)$$

$$\Rightarrow \left(\frac{q}{p}\right) = \prod_{i=1}^{\frac{(p-1)}{2}}\frac{\left(\sin\frac{2\pi iq}{p}\right)}{\sin\frac{2\pi i}{p}} \tag{1}$$

Applying Eisenstein's trigonometric lemma with $n = q$ and substituting in (1), we get

$$(2)\qquad \left(\frac{q}{p}\right) = (-4)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\prod_{j=1}^{\frac{(p-1)}{2}}\prod_{i=1}^{\frac{(q-1)}{2}}\left(\sin^2\left(\frac{2\pi i}{p}\right) - \sin^2\left(\frac{2\pi j}{p}\right)\right)$$

We can get everything we need from this without computing the sines:

Reversing the roles of p and q, we get

$$\left(\frac{p}{q}\right) = (-4)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \prod_{j=1}^{\frac{p-1}{2}} \prod_{i=1}^{\frac{q-1}{2}} \left(\sin^2\left(\frac{2\pi j}{p}\right) - \sin^2\left(\frac{2\pi i}{p}\right)\right) \tag{3}$$

Comparing (2) and (3), we see that

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}} \left(\frac{p}{q}\right),$$

which is the quadratic reciprocity law. □