

# Part II - Number Theory

Lectured by Prof. T. A. Fisher

Artur Avameri

Lent 2022

## Contents

<b>0</b>	<b>Introduction</b>	<b>2</b>
<b>1</b>	<b>Euclid's algorithm and factoring</b>	<b>3</b>
<b>2</b>	<b>Congruences</b>	<b>5</b>
2.1	Polynomial congruences . . . . .	9

## 0 Introduction

06 Oct 2022,  
Lecture 1

Books:

- A. Baker, *A concise introduction to the theory of numbers*, CUP 1984
- N. Koblitz, *A course in number theory & cryptography*, Springer 1994
- H. Davenport, *The higher arithmetic*, CUP 2008

Number theory studies the hidden and mysterious properties of the integers and the rational numbers.

It has always been an experimental science. Examining numerical data leads to **conjectures**, many of which are very old and still unproven today.

**Example 0.1.** (i) Let  $N \geq 1$  be an integer of the form  $8n + 5, 8n + 6$  or  $8n + 7$ . Does there exist a right-angled triangle of area  $N$ , all of whose sides have rational length? We don't know.

(ii) Let  $\pi(x)$  be the number of primes less than or equal to  $x$  and define  $\text{li}(x) = \int_2^x \frac{dt}{\log t}$ . Then for all  $x \geq 3$ ,  $|\pi(x) - \text{li}(x)| \leq \sqrt{x} \log x$ . This is in fact equivalent to the Riemann hypothesis.

(iii) There are infinitely many twin primes. We now know there is an integer  $N \leq 246$  such that there are infinitely many pairs of primes the form  $p, p + N$ .

## 1 Euclid's algorithm and factoring

**Definition 1.1** (Division algorithm). Given  $a, b \in \mathbb{Z}$ , with  $b > 0$ , there exist  $q, r \in \mathbb{Z}$  such that  $a = qb + r$ , and  $0 \leq r < b$ .

**Notation.** If  $r = 0$ , then we write  $b|a$ , else  $b \nmid a$ .

*Proof.* Let  $S = \{a - nb \mid n \in \mathbb{Z}\}$ . This certainly contains integers  $\geq 0$ , so take the smallest one  $r$ . We claim  $r < b$ . Indeed, if not, then  $r - b \geq 0$ , contradicting minimality.  $\square$

Given  $a_1, \dots, a_n \in \mathbb{Z}$  not all zero, let  $I = \{\lambda_1 a_1 + \dots + \lambda_n a_n \mid \lambda_i \in \mathbb{Z}\}$ .

**Lemma 1.1.**  $I = d\mathbb{Z}$  for some  $d > 0$ .

*Proof.*  $I$  certainly contains integers  $\geq 0$ . Let  $d$  be the least positive element of  $I$ . We claim it works. Take  $a \in I$ , then  $a = qd + r$  with  $0 \leq r < d$ . But  $r = a - qd \in I \implies r = 0$ .  $\square$

**Remark.** We get from this that  $d$  divides each  $a_i$ , and any common divisor of the  $a_i$  must divide  $d$ . Why?

We write  $d = \gcd(a_1, \dots, a_n)$  for the **greatest common divisor** (or **highest common factor**), or just use the shorthand  $d = (a_1, \dots, a_n)$ .

**Corollary 1.2.** Let  $a, b, c \in \mathbb{Z}$ . Then there exist  $x, y \in \mathbb{Z}$  such that  $ax + by = c$  if and only if  $(a, b) | c$ .

The division algorithm gives a very efficient way to compute  $(a, b)$ . Assume  $a > b > 0$ . Apply the division algorithm recursively to get

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

**Claim.**  $r_k = (a, b)$ . Indeed,  $(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{k-1}, r_k) = r_k$ . This is called **Euclid's algorithm**.

**Remark.** If  $d = (a, b)$ , then by Lemma 1.2, there exist  $r, s \in \mathbb{Z}$  such that  $ra + sb = d$ . Euclid's algorithm gives us a way to find  $r$  and  $s$ .

In the following table,  $x$  and  $y$  stand for 34 and 25, and we then compute remainders as linear combinations of them.

We can use a trick here to speed this up: find each row as  $q \cdot$  the row before it + the second row before it, then figure out signs at the end. (In fact, the minus signs zigzag down).

$$\begin{array}{r|rr}
 & x & y \\
 a = 34 & 1 & 0 \\
 b = 25 & 0 & 1 \\
 34 = 1 \cdot 25 + 9 & 1 & -1 \\
 25 = 2 \cdot 9 + 7 & -2 & 3 \\
 9 = 1 \cdot 7 + 2 & 3 & -4 \\
 7 = 3 \cdot 2 + 1 & -11 & 15
 \end{array}$$

We hence get  $-11 \cdot 34 + 15 \cdot 25 = 1$ .

**Definition 1.2.** An integer  $n > 1$  is **prime** if its only positive divisors are 1 and  $n$ . Otherwise  $n$  is **composite**.

**Lemma 1.3.** Let  $p$  be a prime, and  $a, b \in \mathbb{Z}$ . If  $p|ab$ , then  $p|a$  or  $p|b$ .

*Proof.* Assume  $p \nmid a$ . Then  $(a, p) = 1$ . By Lemma 1.2,  $\exists r, s \in \mathbb{Z}$  such that  $ra + sp = 1 \implies rab + spb = b$ . Since  $p|ab$ ,  $p|b$  follows.  $\square$

**Theorem 1.4 (Fundamental Theorem of Arithmetic).** Every integer  $n > 1$  can be written as a product of primes. This representation is unique up to reordering.

*Proof.* Existence is obvious. For uniqueness, suppose  $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$  for  $p_i, q_i$  primes. We have  $p_1 | q_1 q_2 \dots q_r$ , so by Lemma 1.5,  $p_1 | q_j$  for some  $j$ , so  $p_1 = q_j$ . Now cancel these out and induct.  $\square$

**Remark.** If  $m = \prod_{i=1}^k p_i^{\alpha_i}$  and  $n = \prod_{i=1}^k p_i^{\beta_i}$  for  $p_i$  distinct primes and  $\alpha_i, \beta_i \geq 0$ , then

$$(m, n) = \prod_{i=1}^k p_i^{\min(\alpha_i, \beta_i)}.$$

However, if  $m$  and  $n$  are large, it is more efficient to compute  $(m, n)$  using Euclid's algorithm.

Suppose we have some large positive integer  $N$ . An obvious algorithm for factoring  $N$  is to trial divide by 2 and the odd integers up to  $\sqrt{N}$ .

**Definition 1.3.** An algorithm with input a positive integer  $N$  is **polynomial** or a **polynomial time** algorithm if it takes  $\leq c(\log N)^b$  **elementary operations** for some constants  $b$  and  $c$ .

**Remark.** An elementary operation is just adding/multiplying two numbers in  $\{0, 1, \dots, 9\}$ .

08 Oct 2022,  
Lecture 2

**Remark.** "Polynomial" makes sense here as it takes  $\log N$  digits to write  $N$ .

Polynomial algorithms are known for:

- Adding and multiplying integers (the usual way);
- Computing gcd's (via Euclid's algorithm);
- Detecting  $n^{\text{th}}$  powers (compute  $\sqrt[n]{\phantom{x}}$  numerically and round)
- More remarkably, primality testing (Agrawal, Kayal, Saxena in 2002)

But trial division up to  $\sqrt{N}$  is not polynomial.

**Fundamental question:** Is there a polynomial time algorithm for factoring? This is unknown.

Later in this course we study the distribution of the prime numbers, in particular the function  $\pi(x)$ , the number of primes  $\leq x$ .

**Theorem 1.5.** There are infinitely many prime numbers, i.e.  $\lim_{x \rightarrow \infty} \pi(x) \rightarrow \infty$ .

*Proof.* Suppose there are only finitely many, say  $p_1, \dots, p_k$ . Consider  $N = \prod_{i=1}^k p_i + 1$ . Then  $N$  must be divisible by some prime other than the  $p_i$ , so we're done.  $\square$

All the largest known primes are of the form  $2^n - 1$  for  $n$  a prime. These are called **Mersenne primes**. 51 of them are known, the largest being  $2^{82589933} - 1$ .

## 2 Congruences

Fix a positive integer  $n$  (the modulus).

**Definition 2.1.** We say  $a \equiv b \pmod{n}$ , or that  $a$  is congruent to  $b \pmod{n}$  if  $n$  divides  $a - b$ .

This defines an equivalence relation on  $\mathbb{Z}$ , and we write  $\mathbb{Z}/n\mathbb{Z}$  for the set of equivalence classes. We can denote these by  $a + n\mathbb{Z}$ , or (more commonly) by  $a \pmod{n}$ . We can check that addition and multiplication are well-defined.

**Remark.**  $n\mathbb{Z}$  is a subgroup/ideal of  $\mathbb{Z}$  and  $\mathbb{Z}/n\mathbb{Z}$  is the quotient group/ring.

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

- (i)  $(a, n) = 1$
- (ii)  $\exists b \in \mathbb{Z}$  such that  $ab \equiv 1 \pmod{n}$
- (iii)  $a$  is a generator for  $\mathbb{Z}/n\mathbb{Z}$ .

*Proof.* (i)  $\implies$  (ii):  $(a, n) = 1 \implies \exists r, s \in \mathbb{Z}$  such that  $ra + sn = 1$ , so  $ra \equiv 1 \pmod{n}$ .

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

(ii)  $\iff$  (iii):  $\exists b \in \mathbb{Z}$  s.t.  $ab \equiv 1 \pmod{n} \iff 1$  belongs to the subgroup of  $\mathbb{Z}/n\mathbb{Z}$  generated by  $a$ .  $\square$

**Notation.**  $(\mathbb{Z}/n\mathbb{Z})^\times$  is the group of **units** in  $\mathbb{Z}/n\mathbb{Z}$ , i.e. the elements with an inverse under multiplication.

**Definition 2.2.**  $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$  is called the **Euler totient function**. We also have  $\phi(n) = |\{1 \leq a \leq n \mid (a, n) = 1\}|$ .

**Remark.**  $\mathbb{Z}/n\mathbb{Z}$  is a field  $\iff \phi(n) = n - 1 \iff n$  is prime.

**Theorem 2.2** (Euler-Fermat theorem). If  $(a, n) = 1$ , then  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

*Proof.* Apply Lagrange's theorem to the group  $G = (\mathbb{Z}/n\mathbb{Z})^\times$ . Then for  $a \in G$ , its order divides  $|G| = \phi(n)$ .  $\square$

As a corollary:

**Theorem 2.3** (Fermat's little theorem). If  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

**Lemma 2.4.** Let  $G$  be a cyclic group of order  $n$ . We have

$$|\{g \in G \mid \text{order}(g) = d\}| = \begin{cases} \phi(d) & \text{if } d \mid n \\ 0 & \text{otherwise} \end{cases}$$

In particular,  $\sum_{d \mid n} \phi(d) = n$ .

*Proof.* WLOG let  $G = (\mathbb{Z}/n\mathbb{Z}, +)$ . We have  $|\{g \in G \mid \text{order}(g) = n\}| \stackrel{(*)}{=} \phi(n)$  by Lemma 2.2. If  $d \mid n$ , say  $n = dk$ , then the elements of order dividing  $d$  are the classes  $0, k, 2k, \dots, (d-1)k \pmod{n}$ . These form a cyclic subgroup of order  $d$ . Applying  $(*)$  to this cyclic subgroup shows that there are  $\phi(d)$  elements of order  $d$ .  $\square$

**Example 2.1.** Consider the simultaneous linear congruences  $x \equiv 7 \pmod{10}$  and  $x \equiv 3 \pmod{13}$ . Suppose we can find  $u, v \in \mathbb{Z}$  such that

$$\begin{cases} u \equiv 1 \pmod{10} \\ u \equiv 0 \pmod{13} \end{cases}, \begin{cases} v \equiv 0 \pmod{10} \\ v \equiv 1 \pmod{13} \end{cases}.$$

Then  $x = 7u + 3v$  is a solution. But  $(10, 13) = 1 \implies \exists r, s \in \mathbb{Z}$  such that  $10r + 13s = 1$ , and we can just take  $u = 13s, v = 10r$ . To find  $r, s$ , we can use Euclid's algorithm to get  $r = 4, s = -3$ , so  $u = -39, v = 40$ , and so  $x \equiv 7 \cdot (-39) + 3 \cdot 40 \equiv 107 \pmod{130}$ .

**Theorem 2.5** (Chinese Remainder Theorem). Let  $m_1, \dots, m_k$  be pairwise coprime integers greater than 1. Let  $a_1, \dots, a_k \in \mathbb{Z}$ . Let  $M = m_1 m_2 \dots m_k$ . Then  $\exists x \in \mathbb{Z}$  satisfying

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

Moreover, the solution is unique mod  $M$ .

*Proof.* Uniqueness: Suppose  $x \equiv x' \pmod{m_i} \forall i$ . Then by considering the prime factorization of  $x - x'$  and using the fact that the  $m_i$  are pairwise coprime, we get  $x \equiv x' \pmod{M}$ .

Existence: Put  $M_i = \frac{M}{m_i}$ , so  $(M_i, m_i) = 1 \forall i$ . Hence we can find  $u_i \in \mathbb{Z}$  such that  $u_i M_i \equiv 1 \pmod{m_i} \forall i$ . Let  $x = \sum_{j=1}^k a_j u_j M_j$ . Then  $x \equiv a_i u_i M_i \equiv a_i \pmod{m_i}$ .  $\square$

We can write this theorem in one line using ring theory.

**Definition 2.3.** Let  $R_i = \mathbb{Z}/m_i\mathbb{Z}$ , and define  $R_1 \times \dots \times R_k = \{(r_1, \dots, r_k) \mid r_i \in R_i\}$  with addition and multiplication defined componentwise. This is a ring.

**Theorem 2.6** (CRT, ring-theoretic version). Let  $m_1, \dots, m_k$  be pairwise coprime integers greater than 1 and put  $M = m_1 \dots m_k$ . Then the map

$$\begin{aligned} \theta : \mathbb{Z}/M\mathbb{Z} &\rightarrow \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \\ a + M\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \dots, a + m_k\mathbb{Z}) \end{aligned}$$

is an isomorphism of rings.

*Proof.*  $\theta$  is a well defined ring homomorphism since  $m_i \mid M \forall i$ . Injectivity of  $\theta$  follows from uniqueness in CRT, and surjectivity of  $\theta$  follows from existence in CRT.  $\square$

**Corollary 2.7.**  $\theta$  induces an isomorphism of groups under multiplication

$$\begin{aligned} (\mathbb{Z}/M\mathbb{Z})^\times &\cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/m_k\mathbb{Z})^\times \\ a + M\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \dots, a + m_k\mathbb{Z}). \end{aligned}$$

**Remark.** If  $a \in \mathbb{Z}$ , then  $(a, M) = 1 \iff (a, m_i) = 1 \forall i$ .

In particular, by looking at orders of the LHS and the RHS above, we get  $\phi(M) = \phi(m_1) \dots \phi(m_k)$ , i.e. the Euler phi function is multiplicative.

**Definition 2.4.** A function  $f : \mathbb{Z}^+ \rightarrow \mathbb{C}$  is **multiplicative** if  $f(mn) = f(m)f(n)$  whenever  $(m, n) = 1$ .

**Examples:**

- $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ ;
- $\tau(n) = \sum_{d|n} 1$ , the number of divisors of  $n$ ;
- $\sigma(n) = \sum_{d|n} d$ , the sum of divisors of  $n$ ;
- more generally,  $\sigma_k(n) = \sum_{d|n} d^k$ , so  $\sigma_0 = \tau$  and  $\sigma_1 = \sigma$ .

To prove this:

**Lemma 2.8.** If  $f : \mathbb{Z}^+ \rightarrow \mathbb{C}$  is multiplicative, then so is  $g : \mathbb{Z}^+ \rightarrow \mathbb{C}$ , defined by  $g(n) = \sum_{d|n} f(d)$ .

*Proof.* Let  $m, n$  be coprime. Note that every divisor  $d$  of  $mn$  can be written as  $d = d_1 d_2$ , where  $d_1 | m$ ,  $d_2 | n$  and  $(d_1, d_2) = 1$ . Thus

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

□

**Lemma 2.9.** (i) For  $p$  a prime,  $\phi(p^k) = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$ .

(ii)  $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$ .

*Proof.* (i):  $\phi(p^k)$  counts the number of integers  $a$  between 1 and  $p^k$  such that  $(p^k, a) = (p, a) = 1$ . So we have  $p^a$  numbers, and we don't count the multiples of  $p$ , so  $\phi(p^k) = p^k - p^{k-1}$ .

(ii): Follows from the fact that  $\phi$  is multiplicative.

□

**Alternative proof** that  $\sum_{d|n} \phi(d) = n$  (cf Lemma 2.6).

*Proof.* Obviously the RHS is multiplicative. Since  $\phi(n)$  is multiplicative, the LHS is multiplicative by Lemma 2.13, so it suffices to check for  $n$  a prime power, say  $n = p^k$ . To this end, compute

$$\sum_{d|p^k} \phi(d) = \phi(1) + \phi(p) + \dots + \phi(p^k) = 1 + (p-1) + (p^2-p) + \dots + (p^k - p^{k-1}) = p^k.$$

□



## 2.1 Polynomial congruences

Let  $R = \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}$  (or more generally any commutative ring). Set  $R[X] = \{\text{polynomials with coefficients in } R\}$ , i.e.  $a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  for  $a_i \in R$ .

By definition, two polynomials are equal if and only if they have the same coefficients. We can check that  $R[X]$  is a ring (with usual  $+$  and  $\times$ ).

**Warning.** The map  $R[X] \rightarrow \{\text{functions } R \rightarrow R\}$  by  $f \mapsto (\alpha \mapsto f(\alpha))$  is not always injective. For example, if  $R = \mathbb{Z}/p\mathbb{Z}$  for  $p$  a prime, and  $f(X) = X^p - X$ , then  $f(\alpha) = 0 \forall \alpha \in R$ , but  $f$  is not the zero function.

**Question.** Can we show that if  $f \in R[X]$  has degree  $n$ , then  $f$  has at most  $n$  roots in  $R$ ?

**Answer.** No. For example, take  $R = \mathbb{Z}/8\mathbb{Z}$ , then  $f(X) = X^2 - 1$  has 4 solutions in  $\mathbb{Z}/8\mathbb{Z}$ .

Let  $R = \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}$  (or any commutative ring).

We have a **division algorithm** on  $R[X]$ :

Let  $f, g \in R[X]$  and suppose the leading coefficient of  $g$  is a unit. Then  $\exists q, r \in R[X]$  such that  $f(X) = Q(X)g(X) + r(X)$  and  $\deg(r) < \deg(g)$ .

*Proof.* By induction on  $\deg(f)$ . If  $\deg(f) < \deg(g)$ , take  $q = 0, r = f$ . Otherwise, let  $f(X) = aX^m + \dots$  and  $g(X) = bX^n + \dots$  with  $m \geq n$  and  $b$  a unit.

Let  $f_1(X) = f(X) - ab^{-1}X^{m-n}g(X)$ . Then  $\deg(f_1) < \deg(f)$ , so by the induction hypothesis,  $f_1(x) = q_1(x)g(x) + r_1(x)$  for some  $q_1, r_1 \in R[X]$  and  $\deg(r_1) < \deg(g)$ . Now take  $q(X) = ab^{-1}X^{m-n} + q_1(X)$  and  $r = r_1$ , so we're done.  $\square$

**Corollary 2.10.** If  $f \in R[X]$  and  $\alpha \in R$  is such that  $f(\alpha) = 0$ , then  $f(X) = (X - \alpha)f_1(X)$  for some  $f_1 \in R[X]$ .

*Proof.* By the division algorithm,  $f(X) = (X - \alpha)f_1(X) + r$  for some  $r \in R$  (as  $\deg(r) < \deg(X - \alpha)$ ). Plug in  $X = \alpha$  to get  $r = 0$ .  $\square$

**Definition 2.5.**  $R$  is an **integral domain** if  $R$  has no zero divisors, i.e.  $\alpha, \beta \in R, \alpha\beta = 0 \implies \alpha = 0$  or  $\beta = 0$ .

**Note.** Let  $n > 1$ . Then  $\mathbb{Z}/n\mathbb{Z}$  is an integral domain  $\iff n$  is prime.

**Theorem 2.11.** If  $R$  is an integral domain, then any polynomial  $f \in R[X]$  of degree  $n$  has at most  $n$  roots.

*Proof.* By induction on  $n$ , the degree of  $f$ . If  $n = 0$ , then our polynomial is a nonzero constant and we're done. Now suppose  $\exists \alpha \in R$  such that  $f(\alpha) = 0$  (otherwise we're done). By Corollary 2.10,  $f(X) = (X - \alpha)f_1(X)$ . Since  $R$  is an integral domain, every root of  $f$ , except possibly  $\alpha$  is a root of  $f_1$ . By induction,  $f_1$  has at most  $n - 1$  roots, hence  $f$  has at most  $n$  roots and we're done.  $\square$

13 Oct 2022,  
Lecture 4

**Corollary 2.12** (Lagrange's Theorem). Let  $p$  be a prime and  $a_0, \dots, a_n \in \mathbb{Z}$  with  $p \nmid a_n$ . Then the congruence

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$$

has at most  $n$  solutions mod  $p$ .

*Proof.* Take  $R = \mathbb{Z}/p\mathbb{Z}$  in Theorem 2.17. □

**Remark.** In this course, we will refer to the above theorem as Lagrange's Theorem.

**Example 2.2.** Let  $p$  be a prime. We will factor  $X^{p-1} - 1 \pmod{p}$ . Let  $f(X) = X^{p-1} - 1 - \prod_{a=1}^{p-1} (X - a)$  in  $\mathbb{Z}/p\mathbb{Z}[X]$ . By Fermat's Little Theorem,  $f$  has at least  $p - 1$  roots mod  $p$ . But  $\deg(f) < p - 1$ , since the  $X^{p-1}$  terms cancel out, so by Lagrange's Theorem,  $f = 0$ , i.e.  $X^{p-1} - 1 = \prod_{a=1}^{p-1} (X - a)$  in  $\mathbb{Z}/p\mathbb{Z}[X]$ . Plugging in  $X = 0$  gives  $(p - 1)! \equiv -1 \pmod{p}$ , i.e. Wilson's Theorem.

**Example 2.3.** Working mod 7, the powers of 3 (starting from 0) are 1, 3, 2, 6, 4, 5. So  $(\mathbb{Z}/7\mathbb{Z})^\times$  is cyclic, generated by 3.

**Theorem 2.13.** Let  $p$  be a prime. Then  $(\mathbb{Z}/p\mathbb{Z})^\times$  is cyclic.

*Proof.* Let  $S_d = \{a \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \text{ord}(a) = d\}$ . Suppose  $S_d \neq \emptyset$ , say  $a \in S_d$ . Then  $1, a, a^2, \dots, a^{d-1}$  are distinct elements in  $\mathbb{Z}/p\mathbb{Z}$  and they are solutions of  $x^d \equiv 1 \pmod{p}$ . By Lagrange's theorem, this has at most  $d$  solutions, and we found  $d$  solutions, so those are all of them, i.e.  $S_d \subseteq \{1, a, a^2, \dots, a^{d-1}\}$ . Note that the LHS is a cyclic group of order  $d$ , so this has  $\phi(d)$  elements of order  $d$ .

We conclude that for every  $d$ ,  $|S_d| = 0$  or  $|S_d| = \phi(d)$ . In particular,  $|S_d| \leq \phi(d)$ . Hence

$$p - 1 \stackrel{(\star)}{=} \sum_{d \mid (p-1)} |S_d| \leq \sum_{d \mid (p-1)} \phi(d) = p - 1,$$

where  $(\star)$  follows since we just count all the elements in  $(\mathbb{Z}/p\mathbb{Z})^\times$ . Hence  $|S_d| = \phi(d) \forall d \mid (p - 1)$ . In particular,  $S_{p-1} \neq \emptyset$ , i.e.  $(\mathbb{Z}/p\mathbb{Z})^\times$  contains elements of order  $p - 1$ , i.e.  $(\mathbb{Z}/p\mathbb{Z})^\times$  is cyclic. □

**Remark.** The same argument shows that any finite subgroup of the multiplicative group of a field is cyclic.

**Definition 2.6.** An integer  $a$  such that  $a \pmod{n}$  generates  $(\mathbb{Z}/n\mathbb{Z})^\times$  is called a **primitive root** mod  $n$ .

Theorem 2.21 showed that primitive roots exist mod  $p$ .

**Example 2.4.** Let  $p = 19$ . Let  $d$  be the order of 2 in  $(\mathbb{Z}/19\mathbb{Z})^\times$ . We know  $d \mid 18$ , so we work out

$$\begin{aligned} 2^3 &\equiv 8 \pmod{19} \\ 2^6 &\equiv 7 \not\equiv 1 \pmod{19} \implies d \nmid 6 \\ 2^9 &\equiv -1 \not\equiv 1 \pmod{19} \implies d \nmid 9, \end{aligned}$$

so  $d = 18$  and hence 2 is a primitive root mod 19.

In general,  $g \in \mathbb{Z}$  (coprime to  $p$ ) is a primitive root mod  $p$  if and only if  $g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \quad \forall \text{ primes } q \mid (p-1)$ .

**Remark.** The number of primitive roots mod  $p$  is  $\phi(p-1) = \phi(\phi(p))$ .

Here are some (open) problems concerning primitive roots:

- (i) Artin's conjecture (1927) – Let  $a > 1$  be an integer which is not a square. Then  $a$  is a primitive root mod  $p$  for infinitely many primes  $p$ . This is unknown for  $a = 2$ . Hooley (1967) proved this assuming GRH. Heath-Brown (1986) proved that Artin's conjecture holds for at least one of 2, 3 or 5. In fact, he proved something stronger: he proved the conjecture fails for at most 2 prime values of  $a$ .
- (ii) How large is the smallest primitive root mod  $p$ ? Burgess (1962) showed it is  $\leq cp^{1/4+\epsilon} \quad \forall \epsilon > 0$  and some constant  $c = c(\epsilon)$ . Shoup (1992) showed it is  $\leq c(\log p)^6$  assuming GRH.

We now consider  $\mathbb{Z}/p^n\mathbb{Z}$  for  $n > 1$ . For  $n \geq 3$ , there is a surjective group homomorphism from  $(\mathbb{Z}/2^n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/8\mathbb{Z})^\times = \{\pm 1, \pm 3\} \cong C_2 \times C_2$ , so  $(\mathbb{Z}/2^n\mathbb{Z})^\times$  is not cyclic (since generators map to generators).

**Theorem 2.14.** Let  $p$  be an odd prime. Then  $(\mathbb{Z}/p^n\mathbb{Z})^\times$  is cyclic  $\forall n \geq 1$ .

We divide the proof into 3 lemmas.

**Lemma 2.15.** Let  $n \geq 2$ . Then  $g$  is a primitive root mod  $p^n$  if and only if the following two conditions hold:

$$\begin{cases} g \text{ is a primitive root mod } p \\ g^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n} \end{cases}.$$

*Proof.* ( $\implies$ ) is clear, as  $\phi(p^n) = p^{n-1}(p-1)$ .

( $\impliedby$ ): Let  $d$  be the order of  $g$  in  $(\mathbb{Z}/p^n\mathbb{Z})^\times$ . Then  $d \mid \phi(p^n) = p^{n-1}(p-1)$ . Since  $g^d \equiv 1 \pmod{p^n}$ , we have  $g^d \equiv 1 \pmod{p}$ . Hence by assumption 1, we have  $(p-1) \mid d$ . Say  $d = p^j(p-1)$  for some  $0 \leq j \leq n-1$ . If  $j \leq n-2$ , then this contradicts assumption 2. Hence  $j = n-1$ , so  $d = \phi(p^n)$  is a primitive root mod  $p^n$ .  $\square$

Next we show  $\exists g \in \mathbb{Z}$  satisfying conditions 1 and 2 in the case  $n = 2$ .

**Lemma 2.16.**  $\exists g \in \mathbb{Z}$  a primitive root mod  $p$  such that  $g^{p-1} \not\equiv 1 \pmod{p^2}$ .

*Proof.* Let  $g$  be a primitive root mod  $p$ . If  $g^{p-1} \equiv 1 \pmod{p^2}$ , then consider  $g + p$ , which is still a primitive root mod  $p$ , but

$$(g + p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \dots \equiv 1 + (p-1)g^{p-2}p \pmod{p^2},$$

where the second term is not divisible by  $p^2$ , so  $(g + p)^{p-1} \not\equiv 1 \pmod{p^2}$ .  $\square$

Next we show that if  $g$  is a primitive root mod  $p^2$ , then it is a primitive root mod  $p^n \forall n \geq 2$ .

**Lemma 2.17.** If  $g^{p-1} \not\equiv 1 \pmod{p^2}$ , then  $g^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n} \forall n \geq 2$ .

*Proof.* By induction on  $n$ , the case  $n = 2$  being given. Suppose the result is true for  $n$ . By Euler-Fermat,  $g^{p^{n-2}(p-1)} \equiv 1 \pmod{p^{n-1}}$ , so  $g^{p^{n-2}(p-1)} = 1 + bp^{n-1}$  for some  $b \in \mathbb{Z}$ , where  $p \nmid b$  by the induction hypothesis. Taking  $p^{\text{th}}$  powers gives

$$\begin{aligned} g^{p^{n-1}(p-1)} &= (1 + bp^{n-1})^p = 1 + bp^n + \binom{p}{2}b^2p^{2(n-1)} + \dots \equiv \\ &1 + bp^n + \binom{p}{2}b^2p^{2(n-1)} \star 1 + bp^n \pmod{p^{n+1}}, \end{aligned}$$

where  $\star$  follows since  $p$  is odd, so  $p \mid \binom{p}{2}$  (and also we use  $3(n-1) \geq n+1$  and  $2(n-1)+1 \geq n+1$ ). Thus  $g^{p^{n-1}(p-1)} \equiv 1 + bp^n \not\equiv 1 \pmod{p^{n+1}}$ , so the result follows for  $n+1$ .  $\square$

This completes the proof of Theorem 2.24.

**Example 2.5.** We saw 3 is a primitive root mod 7. We calculate  $3^3 = -1 + 4 \cdot 7$ , so  $3^6 \equiv 1 - 8 \cdot 7 \not\equiv 1 \pmod{7^2}$ . Hence 3 is a primitive root mod  $7^n \forall n$ .

For the case  $p = 2$ , let  $G = \{a \in (\mathbb{Z}/2^n\mathbb{Z})^\times \mid a \equiv 1 \pmod{4}\}$ . Then  $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \{\pm 1\} \times G$  by  $a + 2^n\mathbb{Z} \mapsto \begin{cases} (1, a + 2^n\mathbb{Z}) & \text{if } a \equiv 1 \pmod{4} \\ (-1, -a + 2^n\mathbb{Z}) & \text{if } a \equiv 3 \pmod{4}. \end{cases}$

**Exercise.** Show that  $G$  is cyclic (and generated by 5).

**Exercise.** For which  $n$  is  $(\mathbb{Z}/n\mathbb{Z})^\times$  cyclic?