

# Number Theory

Vinesh Ramgi

April 5, 2018

### **Abstract**

What did the number theorist say as he drowned?

Log, log, log, log....

For an up to date version of this pdf, check my GitHub :)

<https://github.com/vrvinny/number-theory>

# Contents

<b>1</b>	<b>Introduction/Review</b>	<b>4</b>
1.1	Introduction . . . . .	4
1.2	Review . . . . .	4
1.2.1	Congruences . . . . .	4
1.2.2	Solving Linear Congruences . . . . .	5
1.3	Chinese Remainder Theorem . . . . .	6
1.4	Prime numbers . . . . .	8
1.5	Fermat's Little Theorem . . . . .	8
1.5.1	General method to solve $x^a \equiv b \pmod{p}$ . . . . .	9
1.6	Fundamental Theorem of Arithmetic . . . . .	9
1.6.1	Euclid's Lemma . . . . .	9
1.6.2	Checking whether a number is prime . . . . .	10
<b>2</b>	<b>Elementary Number Theory</b>	<b>11</b>
2.1	Euler Totient Function . . . . .	11
2.2	Euler's Theorem . . . . .	13
2.2.1	Solving equations of the form $x^a \equiv b \pmod{n}$ . . . . .	14
2.3	Primitive roots . . . . .	15
2.4	Roots of unity and Cyclotomic Polynomials . . . . .	16
2.4.1	How to calculate $\Phi_n(x)$ . . . . .	17
2.4.2	Gauss' Theorem . . . . .	18
2.5	Quadratic reciprocity (Quadratic equations modulo prime numbers) . . . . .	19
2.5.1	Quadratic Reciprocity Law . . . . .	20
2.5.2	First Nebensatz . . . . .	20
2.5.3	Second Nebensatz . . . . .	21
2.6	Uniqueness Lemma . . . . .	23
2.6.1	General Uniqueness Lemma . . . . .	23

# 1 Introduction/Review

## 1.1 Introduction

Number Theory is the theory of the ring  $\mathbb{Z}$  and other related rings. A ring (in this course) is a set  $R$  with two binary operations  $+$  and  $*$  such that:

- $(R, +)$  is an abelian group
- $*$  is associative, commutative and has an identity element 1
- $x(y + z) = xy + xz \quad \forall x, y, z \in R$

Examples of rings:

- $\mathbb{Z}$  is a ring
- Every field is a ring, (e.g.  $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ )
- $\mathbb{Z}/n$   $\mathbb{Z}$  modulo  $n = \{0, \dots, n-1\}$
- $\mathbb{F}[X] = \{ \text{polynomials } f(x) \text{ with coefficients in } \mathbb{F} \}$

## 1.2 Review

### 1.2.1 Congruences

Let  $n$  be a positive integer. Given  $x, y \in \mathbb{Z}$ , we say  $x$  is congruent to  $y$  modulo  $n$  if  $x - y$  is a multiple of  $n$ .

$$x \equiv y(n) \quad \text{or} \quad x \equiv y \pmod{n}$$

**E.g** 
$$\begin{aligned} 2 &\equiv 12 \pmod{10} \\ &\equiv -8 \pmod{10} \end{aligned}$$

We write  $\mathbb{Z}/n$  for the ring of congruency classes modulo  $n$ , i.e. the elements are integer, with two of them regarded as the same if they are congruent modulo  $n$ .

Since every integer is congruent to a unique integer in the set  $\{0, \dots, n-1\}$ , we have  $\mathbb{Z}/n = \{0, \dots, n-1\}$ .

An element  $x$  of  $\mathbb{Z}/n$  is called "invertible" or a "unit" if  $\exists y \in \mathbb{Z}/n$  such that  $xy \equiv 1(n)$ .

**Theorem 1.1.**  $x$  is invertible modulo  $n$  iff  $x$  and  $n$  are coprime

**Recall** Two numbers are coprime if their highest common factor is 1.

Here's how we find the inverse of  $x$  in  $\mathbb{Z}/n$ . Since  $X$  and  $n$  are coprime we can find  $h, k \in \mathbb{Z}$  such that  $hx + kn = 1 \implies hx \equiv 1 \pmod{n}$ . So  $h$  is the inverse of  $x$  modulo  $n$ .

**E.g** We'll find the inberse of 7 modulo 25 using Euclid's algorithm

$$25 = 3 \times 7 + 4$$

$$7 = 1 \times 4 + 3$$

$$4 = 1 \times 3 + 1$$

$$1 = 4 - 1(3)$$

$$1 = 4 - 1(7 - 1(4)) = 2(4) - 1(7)$$

$$1 = 2(25 - 3(7)) - 1(7) = 2(25) - 7(7)$$

$$2(25) - 7(7) = 1$$

$$- 7(7) = 1 \pmod{25}$$

$$(7^{-1}) = -7 = 18 \pmod{25}$$

$$7 \times 18 = 126 = 1 \pmod{25}$$

We'll write  $(\mathbb{Z}/n)^\times$  for the invertible elements in  $\mathbb{Z}/n$

**E.g**

$$(\mathbb{Z}/3)^\times = \{ \emptyset, 1, 2 \}$$

$$(\mathbb{Z}/6)^\times = \{ \emptyset, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5 \}$$

**Theorem 1.2.**  $(\mathbb{Z}/n)^\times$  is a group with the operation of multiplicity.

### 1.2.2 Solving Linear Congruences

Suppose we want to solve  $ax \equiv b \pmod{n}$  (given  $a, b$  and  $n$ ).

**Case 1:** If  $a$  is coprime to  $n$  then we can find  $a^{-1}$  modulo  $n$  by Euclid's algorithm,  
 $x \equiv a^{-1}b \pmod{n}$

**Case 2:** If  $a$  is a factor of  $n$ , then there are two possibilities:

**2a)** if  $a$  is also a factor of  $b$  then  $ax \equiv b \pmod{n}$  is equivalent to  $x = \frac{b}{a} \pmod{\frac{n}{a}}$

**2b)** if  $a$  is not a factor of  $b$  then there are no solutions

**E.g.** Solve  $5x = 11 \pmod{13}$

This is case 1 because 5 and 13 are coprime

$$13 = 2 \times 5 + 3$$

$$5 = 1 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$1 = (3) - 1(2)$$

$$1 = (3) - 1(5 - 1(3)) = 2(3) - (5)$$

$$1 = 2(13 - 2(5)) - (5) = 2(13) - 5(5)$$

$$1 \equiv -5(5) \pmod{13}$$

$$5^{-1} \equiv -5 \equiv 8 \pmod{13}$$

$$5x \equiv 11 \pmod{13}$$

$$x \equiv 8 \times 11 \equiv 88 \pmod{13}$$

$$x \equiv 10 \pmod{13}$$

**E.g.** Solve  $7x \equiv 84 \pmod{490}$

7 is a factor of 490 so case 2)

7 is a factor of 84 so case 2a)

$$7x \equiv 84 \pmod{490}$$

$$x \equiv 12 \pmod{70}$$

**E.g.** Solve  $7x \equiv 85 \pmod{490}$

This is case 2b (7 is a factor of 490 but not of 85)  $\therefore$  No solutions

$$7x \equiv 85 \pmod{490}$$

$$\implies 7x = 85 + 490y \text{ for some } y \in \mathbb{Z}$$

$$\implies 0 \equiv 1 \pmod{7}$$

**E.g.** Solve  $6x \equiv 3 \pmod{21}$

This is neither case 1 nor case 2 but we can rewrite as:

$$3(2x) \equiv 3 \pmod{21}$$

$$\text{By case 2 we can solve for } 2x \equiv 1 \pmod{7}$$

but now 2 is invertible modulo 7 so now solve by case 1

$$\therefore x \equiv 4 \pmod{7}$$

### 1.3 Chinese Remainder Theorem

Suppose we know the congruency class of  $x$  modulo 10. Then we can work out its congruency class mod 2 and mod 5.

**E.g.** if  $x \equiv 7 \pmod{10}$ , then  $x \equiv 1 \pmod{2}$  and  $x \equiv 2 \pmod{5}$

Then the Chinese Remainder Theorem allows us to do the opposite, i.e. if we know  $x$  modulo 2 and modulo 5, then we can work out the value of  $x$  modulo 10.

Suppose  $n$  &  $m$  are coprime positive integers, let  $a \in (\mathbb{Z}/n)$  and  $b \in (\mathbb{Z}/m)$  then there is a unique

$$x \in (\mathbb{Z}/nm) \text{ such that } \begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

**Proof of existence part:**

Since  $n$  &  $m$  are coprime, we can find  $h, k \in \mathbb{Z}$  such that  $hn + km = 1$ .

Let  $x = hnb + kma$

Check that this a solution to both congruences:

$$\begin{aligned} x &\equiv kma \pmod{n} \\ x &\equiv (1 - hn)a \pmod{n} \\ x &\equiv (1)a \pmod{n} \\ x &\equiv a \pmod{n} \end{aligned}$$

Similarly, this holds for  $x \equiv b \pmod{m}$ .

**E.g.** Solve the simultaneous congruence:

$$\begin{aligned} x &\equiv 3 \pmod{8} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

By the Chinese Remainder Theorem, there is unique solution modulo 40. To find the solution we let  $x = hnb + kma$ .

First find  $h, k$  by Euclid's algorithm.

$$\begin{aligned} 8 &= 1 \times 5 + 3 & 1 &= (3) - 1(2) \\ 5 &= 1 \times 3 + 2 & 1 &= (3) - 1(5 - 1(3)) = 2(3) - (5) \\ 3 &= 1 \times 2 + 1 & 1 &= 2(8 - 2(5)) - (5) = 2(8) - 5(5) \end{aligned}$$

$$\begin{aligned} \therefore x &= (2 * 8 * 4) - (3 * 5 * 3) \\ x &= 64 - 45 \end{aligned}$$

$$\implies x \equiv 19 \pmod{40}$$

Remark: We can use the Chinese Remainder Theorem to solve a congruence modulo  $nm$ , by first solving mod  $n$  and then mod  $m$  and then combining the results.

**E.g.** Solve  $x^2 \equiv 2 \pmod{119}$ . Note  $119 = 7 * 17$ .

By CRT this is equivalent to:

$$\begin{aligned} x^2 &\equiv 2 \pmod{7} & \implies x &\equiv \pm 3 \pmod{7} \\ x^2 &\equiv 2 \pmod{17} & \implies x &\equiv \pm 6 \pmod{17} \end{aligned}$$

Now we combine the solutions:

$$\begin{aligned} 17 &= 2 * 7 + 3 & 1 &= (7) - 2(3) \\ 7 &= 2 * 3 + 1 & 1 &= (7) - 2(17 - 2(7)) \\ & & 1 &= 5(7) - 2(17) \end{aligned}$$

Since

$$\begin{array}{ll} x \equiv \pm 3 \pmod{7} & \text{We get } x \equiv 5 * 7 * (\pm 6) - 2 * 17 * (\pm 3) \\ x \equiv \pm 6 \pmod{17} & x \equiv \pm 11 \text{ or } \pm 45 \pmod{119} \end{array}$$

## 1.4 Prime numbers

**Defintion 1.3.** An integer  $p \geq 2$  is a prime number if the only factors of  $p$  are  $\pm 1, \pm p$

We'll write  $\mathbb{F}_p$  for  $\mathbb{Z}/p$ . This is because:

**Theorem 1.4.** If  $p$  is prime, then  $\mathbb{F}_p$  is a field

*Proof.* Need to check that the non-zero elements of  $\mathbb{F}_p$  all have inverses.

Let  $x \in \mathbb{F}_p$  with  $x \not\equiv 0 \pmod{p}$  i.e.  $x$  is not a multiple of  $p$

$$\therefore \text{hcf}(x, p) = 1$$

$\therefore x$  &  $p$  coprime

□

## 1.5 Fermat's Little Theorem

**Theorem 1.5.** Let  $p$  be a prime number. If  $x$  is not a multiple of  $p$  then  $x^{p-1} \equiv 1 \pmod{p}$

*Proof.*  $x \in \mathbb{F}_p^\times = \{1, 2, \dots, p-1\}$  a group with  $p-1$  elements.

Let  $n$  be the order of  $x$  in this group.

(order of  $x$  is smallest  $n > 0$  such that  $x^n \equiv 1 \pmod{p}$ )

By corollary to Lagrange's Theorem,  $p-1$  is a multiple of  $n$

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

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

□

**Theorem 1.6.** Lagrange's Theorem: If  $H$  is a subgroup of a finite group  $G$ , then  $|H|$  is a factor of  $|G|$ .

**Corollary 1.7.** Order of an element is a factor of  $|G|$

We can use Fermat's Little Theorem to do calculations.

**E.g.** Calculate  $10^{100}$  modulo 19

By Fermat's Little Theorem:  $10^{18} \equiv 1 \pmod{19}$

$$\begin{aligned} 10^{100} &\equiv (10^{18})^5 * 10^{10} \pmod{19} \\ &\equiv 100^5 \pmod{19} \\ &\equiv 5^5 \pmod{19} \\ &\equiv 25 * 125 \equiv 6 * 11 \equiv 9 \pmod{19} \end{aligned}$$

Also using Fermat's Little Theorem we can solve congruence of the form  $x^a \equiv b \pmod{p}$  as long as  $p$  prime and  $a$  invertible modulo  $p-1$



### 1.5.1 General method to solve $x^a \equiv b \pmod{p}$

Let

$$\begin{aligned}c &= a^{-1} \pmod{p-1} \\ac &= 1 + (p-1)r\end{aligned}$$

Raise both sides of the congruence to power  $c$ :

$$\begin{aligned}\therefore x^{ac} &\equiv b^c \pmod{p} \\x^{1+(p-1)r} &\equiv b^c \pmod{p} \\x &\equiv b^c\end{aligned}$$

So the solution is  $x \equiv b^c \pmod{p}$

**E.g.** Solve  $x^5 \equiv 2 \pmod{19}$

19 is prime and 5 is coprime to 18.

Find  $c = 5^{-1} \pmod{18}$

$$\begin{array}{ll}18 = 3 * 5 + 3 & 1 = 2 * 3 - 5 \\5 = 2 * 3 - 1 & 1 = 2(18 - 3 * 5) - 5 \\ & 1 = 2 * 18 - 7 * 5\end{array}$$

$$\begin{aligned}\therefore 5^{-1} &\equiv -7 \pmod{18} \\ &\equiv 11 \pmod{18}\end{aligned}$$

$$\begin{aligned}\therefore x &\equiv 2^{11} \pmod{19} \\ &\equiv 2048 \pmod{19} \\ &\equiv 15 \pmod{19}\end{aligned}$$

## 1.6 Fundamental Theorem of Arithmetic

If  $n$  is a positive integer then there is a unique factorisation,  $n = p_1 p_2 \dots p_r$  with  $p_i$  prime. "Unique" means up to reordering the primes  $p_1, \dots, p_r$ . Showing that a factorisation exists is easy. For the uniqueness part we use:

### 1.6.1 Euclid's Lemma

**Lemma 1.8.** Suppose  $p$  prime, and  $p|ab$ . Then  $p|a$  or  $p|b$ .

To prove Euclid's lemma we use Bezout's lemma.

*Proof.* Assume  $p|ab$  but  $p \nmid a$ . Then  $\text{hcf}(a, p) = 1$

By Bezout's lemma,  $\exists h, k$  such that:

$$1 = ha + kp$$

$$b = hab + kpb$$

Both  $hab$  and  $kpb$  are multiples of  $p$ .

$\therefore p|b$

□

### 1.6.2 Checking whether a number is prime

If  $n$  is composite then the smallest factor of  $n$  is (apart from 1) is a prime number  $p \leq \sqrt{n}$ , i.e. to show that  $n$  is prime, we just need to show that none of the primes up to  $\sqrt{n}$  are factors of  $n$ .

E.g. Is 199 prime?

$$\sqrt{199} < 15 \text{ since } 15^2 = 225$$

The primes up to 15 are ~~2~~,~~3~~,~~5~~,~~7~~,~~11~~,~~13~~

$199 \equiv 3 \quad (7)$   
 $199 \equiv 4 \quad (13)$   
 $\therefore 199$  is prime

**Theorem 1.9.** *There are infinitely many primes*

*Proof.* Suppose  $p_1, \dots, p_n$  are all the primes.

Let  $N = p_1 \dots p_n + 1$

$\therefore N$  has no prime factors  $\nmid$

5

Similarly there are infinitely many primes  $p \equiv 2 \pmod{3}$  (3)

*Proof.* Assume there are only finitely many primes, call them  $p_1, p_2, \dots, p_r$ . All other primes are either 3 or are congruent to 1 mod 3.

Let  $N = 3p \dots p_{r-1}$ . Since  $3 \nmid N$  and  $p_i \nmid N$  then all the prime factor of  $N$  are congruent to 1 mod 3.

$$\therefore N \equiv 1 \pmod{3} \implies \text{because clearly } N \equiv 2 \pmod{3}$$
☐

## 2 Elementary Number Theory

### 2.1 Euler Totient Function

Recall  $(\mathbb{Z}/n)^\times$  is the group of invertible elements in  $\mathbb{Z}/n$ .

**E.g.**  $(\mathbb{Z}/6)^\times = \{1, 5\}$

$(\mathbb{Z}/8)^\times = \{1, 3, 5, 7\}$

These are groups with the multiplication operation,  $*$ . The multiplication table for  $(\mathbb{Z}/8)^\times$  is given below.

$*$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

**Definition 2.1.** The Euler Totient function is  $\phi(n) = |(\mathbb{Z}/n)^\times|$

**E.g.**  $\phi(6) = 2$

$\phi(8) = 4$

If  $p$  prime then  $(\mathbb{Z}/p)^\times = \{1, \dots, p-1\}$  so  $\phi(p) = p-1$

**Theorem 2.2.** Euler's Theorem- Let  $x \in (\mathbb{Z}/n)^\times$  then  $x^{\phi(n)} \equiv 1 \pmod{n}$

In the case  $n = p$  is prime, this is just Fermat's Little Theorem.

*Proof.* Let  $d$  be the order of  $x$ , i.e.  $x^d \equiv 1 \pmod{n}$ . By a corollary to Lagrange's Theorem,  $d$  is a factor of  $\phi(n) \implies x^{\phi(n)} \equiv 1 \pmod{n}$   $\square$

We can use Euler's theorem to solve congruences and calculate powers mod  $n$ . To use the theorem, we need a quick way of calculating  $\phi(n)$ .

**Lemma 2.3.** Let  $n = p^a$  where  $p$  is prime  $a > 0$ . Then  $\phi(n) = (p-1)p^{a-1}$

**E.g.**  $\phi(8) = \phi(2^3) = (2-1)2^{3-1} = 4$

*Proof.* An integer is coprime to  $p^a$  as long as it's not a multiple of  $p$ .

$\therefore$  The elements of  $\mathbb{Z}/p^a$  which are not invertible are the multiples of  $p$ .  $0, p, 2p, \dots, p^a - p$ .

There are  $p^a - 1$  of these:

$$\therefore |(\mathbb{Z}/p^a)^\times| = p^a - p^{a-1} = (p-1)p^{a-1} \quad \square$$

**Theorem 2.4.** Let  $n$  and  $m$  be coprime. Then there is an isomorphism:

$$(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times * (\mathbb{Z}/m)^\times$$

We'll use the theorem before we prove it.

**Remark:** If  $G$  and  $H$  are groups,  $G \times H = \{(x, y) : x \in G, y \in H\}$ , then  $G \times H$  is a group with the operation  $(x, y)(x', y') = (xx', yy')$  and  $G \times H$  is the "direct product" of  $G$  and  $H$

**Corollary 2.5.** *If  $n$  and  $m$  are coprime then  $\phi(nm) = \phi(n)\phi(m)$*

*Proof.*

$$\begin{aligned}\phi(nm) &= |(\mathbb{Z}/nm)^\times| = |(\mathbb{Z}/n)^\times * (\mathbb{Z}/m)^\times| \\ &= |(\mathbb{Z}/n)^\times| * |(\mathbb{Z}/m)^\times| \\ &= \phi(n)\phi(m)\end{aligned}$$

□

**Corollary 2.6.** *(Corollary of the corollary): Suppose  $n = p_1^{a_1} \dots p_r^{a_r}$  with  $p_1, \dots, p_r$  distinct primes and  $a_i > 0$ . Then*

$$\phi(n) = (p_1 - 1)p_1^{a_1-1} * \dots * (p_r - 1)p_r^{a_r-1}$$

*Proof.* Since  $p_1^{a_1}, \dots, p_r^{a_r}$  are coprime,

$$\begin{aligned}\phi(n) &= \phi(p_1^{a_1}) \dots \phi(p_r^{a_r}) && \text{by the corollary} \\ &= (p_1 - 1)p_1^{a_1-1} \dots (p_r - 1)p_r^{a_r-1} && \text{by the lemma}\end{aligned}$$

□

**E.g.** Calculate  $\phi(200)$

$$\begin{aligned}\phi(200) &= \phi(2^3 * 5^2) \\ &= (2 - 1)2^{3-1} * (5 - 1)5^{2-1} \\ &= 4 * 4 * 5 \\ &= 80\end{aligned}$$

**Theorem 2.7.** *Suppose  $n$  and  $m$  are coprime, then  $(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times * (\mathbb{Z}/m)^\times$ . The isomorphism is the map  $x \mapsto (x \bmod n, x \bmod m)$*

**E.g.**  $n = 4, m = 5$

$$\begin{aligned}(\mathbb{Z}/4)^\times &= \{1, 3\} \\ (\mathbb{Z}/5)^\times &= \{1, 2, 3, 4\} \\ \therefore (\mathbb{Z}/4)^\times * (\mathbb{Z}/5)^\times &= \{(1, 1), (1, 2), (1, 3), (1, 4), \\ &\quad (3, 1), (3, 2), (3, 3), (3, 4)\} \\ (\mathbb{Z}/20)^\times &= \{1, 3, 7, 9, 11, 13, 17, 19\}\end{aligned}$$

The isomorphism is:

$$\begin{array}{ll} 1 \mapsto (1, 1) & 11 \mapsto (3, 1) \\ 3 \mapsto (3, 3) & 13 \mapsto (1, 3) \\ 7 \mapsto (3, 2) & 17 \mapsto (1, 2) \\ 9 \mapsto (1, 4) & 19 \mapsto (3, 4) \end{array}$$

*Proof.* Let  $\Phi : \mathbb{Z}/nm \mapsto \mathbb{Z}/n * \mathbb{Z}/m$

$$\Phi(x) = (x \bmod n, x \bmod m)$$

This is a bijection by the Chinese Remainder Theorem.

We'll next show that  $x$  is invertible mod  $nm \iff x$  is invertible mod  $n$  and mod  $m$

( $\implies$ ) Suppose  $x$  is invertible mod  $nm$

$$\text{Let } xy \equiv 1 \pmod{nm}$$

$$\therefore xy \equiv 1 \pmod{n}$$

$$xy \equiv 1 \pmod{m}$$

$$\therefore x \text{ invertible mod } n \text{ and } m$$

( $\impliedby$ ) Suppose  $x$  invertible mod  $n$  and  $m$

$$xa \equiv 1 \pmod{n}$$

$$xb \equiv 1 \pmod{m}$$

By the Chinese Remainder Theorem,  $\exists y$  such that  $y \equiv a \pmod{n}$

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

$$\left. \begin{array}{l} \therefore xy \equiv xa \equiv 1 \pmod{n} \\ \equiv xb \equiv 1 \pmod{m} \end{array} \right\} \implies xy \equiv 1 \pmod{nm} \text{ by the Chinese Remainder Theorem}$$

We've shown that  $\Phi$  gives a bijection between  $(\mathbb{Z}/nm)^\times$  and  $(\mathbb{Z}/n)^\times * (\mathbb{Z}/m)^\times$ . We'll next check that  $\Phi(xy) = \Phi(x)\Phi(y)$ .

$$\begin{aligned} \Phi(xy) &= (xy \bmod n, xy \bmod m) \\ &= (x \bmod n, x \bmod m) * (y \bmod n, y \bmod m) \\ &= \Phi(x)\Phi(y) \end{aligned}$$

□

## 2.2 Euler's Theorem

If  $x \in (\mathbb{Z}/n)^\times$  then  $x^{\phi(n)} \equiv 1 \pmod{n}$  and  $\phi(p_1^{a_1} \dots p_r^{a_r}) = (p_1 - 1)p_1^{a_1-1} \dots (p_r - 1)p_r^{a_r-1}$

**E.g.** Calculate  $7^{135246872002} \bmod 10000$

$$7 \text{ coprime to } 10000 \text{ so } 7^{\phi(10000)} \equiv 1 \pmod{10000}$$

$$10000 = 2^4 * 5^4$$

$$\therefore \phi(10000) = (2-1)2^3 * (5-1) * 5^3 = 8 * 500$$

$$7^{4000} \equiv 1 \pmod{10000} \implies 7^n \text{ depends only on } n \bmod 4000$$

$$135246872002 \equiv 2 \pmod{4000}$$

$$\therefore 7^{135246872002} \equiv 7^2 \equiv 49 \pmod{10000}$$

We can also use Euler's THEorem to solve congruence with powers

### 2.2.1 Solving equations of the form $x^a \equiv b \pmod{n}$

Suppose we want to solve  $x^a \equiv b \pmod{n}$  where  $b$  is coprime to  $n$  and  $a$  is coprime to  $\phi(n)$ .

Clearly any solution  $x$  must be coprime to  $n$  by Euler's Theorem  $x^{\phi(n)} \equiv 1 \pmod{n}$ .

$\therefore$  The congruency class of  $x^y \pmod{n}$  depends only  $y \pmod{\phi(n)}$

Let

$$c = a^{-1} \pmod{\phi(n)}$$

Raise both sides of the congruence to power  $c$ :

$$x^{ac} \equiv x^1 \equiv b^c \pmod{n}$$

$\therefore$  The solution is  $x \equiv b^c \pmod{n}$

**E.g.**  $x^7 \equiv 3 \pmod{50}$

3 is coprime to 50,

$$\begin{aligned} 50 &= 2 * 5^2 \\ \implies \phi(50) &= 1 * 4 * 5 = 20 \end{aligned}$$

7 is coprime to  $\phi(50)$ . To solve, we need to find

$$\begin{aligned} c &\equiv 7^{-1} \pmod{\phi(50)} \\ &\equiv 3 \pmod{20} \end{aligned}$$

$$x \equiv 3^3 \equiv 27 \pmod{50}$$

**E.g.**  $x^{27} \equiv 5 \pmod{123}$

5 is coprime to 123,

$$\begin{aligned} 123 &= 3 * 41 \\ \implies \phi(123) &= 2 * 40 = 80 \end{aligned}$$

27 is coprime to 80

To solve, we find  $27^{-1} \pmod{80}$

$$\begin{aligned} 80 &= 3 * 27 - 1 \\ \implies 1 &= 3 * 27 - 80 \end{aligned}$$

$$27^{-1} = 3$$

$$\begin{aligned} x &= 5^3 \\ x &= 125 \equiv 2 \pmod{123} \end{aligned}$$

### 2.3 Primitive roots

Recall, let  $G$  be a finite group.  $G$  is called a cyclic group if  $\exists x \in G$  such that, every element in  $G$  has the form  $x^n$  for some  $n \in \mathbb{Z}$ , i.e.  $G = \{1, x, x^2, \dots, x^{n-1}\}$  where  $n$  is the order of  $x$ , equivalentl the order of  $x$  is  $|G|$ . The element  $x$  is called a generator of  $G$ .

**Theorem 2.8.** (Gauss' Theorem), For ever prime number  $p$ , the group  $\mathbb{F}_p^\times$  is cyclic

**Defintion 2.9.** A generator of  $\mathbb{F}_p^\times$  is called a primitive root. Equivalently, this is an element of order  $p - 1$

**E.g.**  $p = 7, x = 3$  We'll see that 3 is a primitive root modulo 7

$$\begin{array}{llll} \text{Powers of 3 in } F_7^\times : & 3^0 = 1 & 3^3 \equiv 6 \pmod{7} & 3^6 \equiv 1 \pmod{7} \\ & 3^1 = 3 & 3^4 \equiv 4 \pmod{7} & \\ & 3^2 \equiv 2 \pmod{7} & 3^5 \equiv 1 \pmod{7} & \end{array}$$

so 3 is a primitive root modulo 7. There is a quicker way to check whether  $x$  is a primitive root.

**Proposition 2.10.** Let  $x \in \mathbb{F}_p^\times$ , then  $x$  is a primitive root modulo  $p$  if and only if for every prime factor  $q$  of  $p - 1$ :

$$x^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

*Proof.* Assume the second statement is false, so  $\exists$  prime factor  $q$  of  $p - 1$  such that:

$$\begin{array}{ll} x^{\frac{p-1}{q}} \equiv 1 \pmod{p} & \therefore \text{order of } x \leq \frac{p-1}{q} < p-1 \\ & \therefore x \text{ is not a primitive root} \end{array}$$

Conversely, assume  $x$  is not a primitive root, so  $x$  doe not have order  $p - 1$ . But the order of  $x$  is a factor of  $p - 1$ .

Suppose the order of  $x$  is  $\frac{p-1}{d}$ ,  $d > 1$ .

Let  $q$  be a prime factor of  $d \implies q|p-1$

$$\frac{p-1}{q} \text{ is a multiple of } \frac{p-1}{d} \text{ but } x^{\frac{p-1}{q}} \equiv 1 \pmod{p} \implies x^{\frac{p-1}{d}} \equiv 1 \pmod{p}$$

□

**E.g.**  $p = 29$

By the proposition  $x$  is a primitive root mod 29  $\iff x^{28/2} \not\equiv 1 \pmod{29}$  and  $x^{28/7} \not\equiv 1 \pmod{29}$

$$\iff x^{14} \not\equiv 1 \pmod{29} \text{ and } x^4 \not\equiv 1 \pmod{29}$$

Try  $x = 2$ :

$$2^4 \equiv 16 \not\equiv 1 \pmod{29}$$

$$2^{14} \equiv 128^2 \equiv 12^2 \equiv 144 \equiv -1 \pmod{29}$$

$\therefore 2$  is a primitive root mod 29

Another trick to speed up the calculation:

$\mathbb{F}_p$  is a field  $\therefore$  every polynomial of  $d$  has no more than  $d$  in  $\mathbb{F}$  (proved in 2201).

$\therefore$  if  $x^2 \equiv 1 \pmod{p}$  then  $x \equiv \pm 1 \pmod{p}$

This means that checking whether  $x^{14} \equiv 1 \pmod{29}$  is equivalent to checking whether  $x^7 \equiv \pm 1 \pmod{29}$ .

**E.g** 3 is also a primitive root modulo 29

$$3^2 \equiv 9 \not\equiv \pm 1 \pmod{29}$$

$$3^4 \equiv 1 \pmod{29}$$

$$3^7 \equiv 27^2 * 3 \pmod{29}$$

$$\equiv (-2)^2 * 3 \equiv 12 \pmod{29}$$

$$\equiv \pm 1 \pmod{29}$$

$$\therefore 3^{14} \not\equiv 1 \pmod{29}$$

## 2.4 Roots of unity and Cyclotomic Polynomials

A complex number  $\zeta$  is called an  $n^{th}$  root of unity if  $\zeta^n = 1$ . The  $n^{th}$  roots of unity are  $e^{2\pi i \frac{a}{n}}$  for  $a = \{0, 1, \dots, n-1\}$

We call  $\zeta$  a primitive  $n^{th}$  root of unity if  $n$  smaller power than  $\zeta^n$  is equal to 1, i.e.  $\zeta$  has order  $n$  in  $\mathbb{C}^\times$  if  $\zeta$  is not a primitive  $n^{th}$  root of unity  $\zeta = e^{2\pi i \frac{b}{d}}$  where  $b = \{0, \dots, d-1\}$  for  $d < n$

$$\therefore \frac{a}{n} = \frac{b}{d}$$

The cancellation happens when  $a$  is not coprime to  $n$ . This shows that the primitive  $n^{th}$  of unity are  $e^{2\pi i \frac{a}{n}}$ ,  $a \in (\mathbb{Z}/n)^\times$ .

**Corollary 2.11.** *There are exactly  $\phi(n)$  primitive  $n^{th}$  roots of unity*

We'll actually prove a more precise version of Gauss' Theorem.

**Theorem 2.12.** *For every factor  $d$  of  $p-1$  there are  $\phi(d)$  elements in  $\mathbb{F}_p^\times$  of order  $d$ .*

**Defintion 2.13.** *The  $n^{th}$  cyclotomic polynomial is:*

$$\Phi_n(x) = \prod_{\substack{\text{primitive} \\ n^{th} \text{ roots} \\ \text{of unity } \zeta}} (X - \zeta)$$

i.e  $\zeta^n = 1$  and no smaller power of  $\zeta$  is 1,  $\zeta = e^{2\pi i \frac{a}{n}}$ ,  $a \in (\mathbb{Z}/n)^\times$

This has degree  $\phi(n)$ .



**E.g.**  $n=4$

Primitive  $4^{th}$  roots of unity are  $i, -i$ :

$$\begin{aligned}\Phi_4(x) &= (x - i)(x - (-i)) \\ &= x^2 + 1\end{aligned}$$

**Lemma 2.14.** For every  $n > 0$ :

$$x^n - 1 = \prod_{\substack{d \text{ factors} \\ d \text{ of } n}} \Phi_d(x)$$

**E.g.** Calculate  $\Phi_6(x)$

$$\begin{aligned}\text{By the lemma} \quad x^6 - 1 &= \Phi_1 \Phi_2 \Phi_3 \Phi_6 & x^6 - 1 &= (x^3 - 1) \Phi_2 \Phi_6 \\ x^3 - 1 &= \Phi_1 \Phi_3\end{aligned}$$

$$\therefore \Phi_6 = \frac{x^6 - 1}{(x^3 - 1)(x + 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

Let  $p$  be a prime number. A primitive root mod  $p$  is an  $x \in \mathbb{F}_p^\times$ , such that  $x$  generates  $\mathbb{F}_p^\times$ .  
Equivalently order =  $p - 1$

#### 2.4.1 How to calculate $\Phi_n(x)$

**Lemma 2.15.**  $x^n - 1 = \prod_{d|n} \Phi_d(x)$

**E.g.**  $n = 4$

$$\begin{aligned}x^4 - 1 &= \Phi_1 \Phi_2 \Phi_4 & \Phi_1 &= x - 1 \\ & & \Phi_2 &= (x - (-1)) = x + 1 \\ & & \Phi_4 &= (x - i)(x - (-i)) = x^2 + 1 \\ &= (x - 1)(x + 1)(x^2 + 1)\end{aligned}$$

*Proof.*

$$x^n - 1 = \prod_{\substack{\zeta \text{ is an} \\ n^{th} \text{ root of} \\ \text{unity}}} (x - \zeta)$$

but every  $n^{th}$  root of unity is a primitive  $d^{th}$  root of unity for some  $d|n$ .

$$x^n = \prod_{d|n} (\prod_{\substack{\text{primitive} \\ d^{th} \text{ roots} \\ \text{of unity}}} (x - \zeta)) = \prod_{d|n} \Phi_d(x)$$

□

**E.g.** Calculate  $\Phi_5(x)$

$$\begin{aligned} x^5 - 1 &= \Phi_1(x)\Phi_5(x) \\ &= (x - 1)\Phi_5(x) \end{aligned}$$

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = 1 + x + x^2 + x^3 + x^4$$

More generally if  $p$  prime then  $x^p - 1 = (x - 1)\Phi_p(x) \implies \Phi_p(x) = 1 + x + \dots + x^{p-1}$

**E.g.** Calculate  $\Phi_8(x)$

$$x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)$$

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x) \implies \Phi_8(x) = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1$$

**Corollary 2.16.**  $\Phi_n(x)$  has coefficients in  $\mathbb{Z}$

$$\text{Proof. } \Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}$$

We'll prove the corollary by induction on  $n$ , clearly true when  $n = 1$ . Assume  $\Phi_d$  has integer coefficients  $\forall d < n$ .

It is proved in Algebra 3 (MATH2201) that, if  $f, g \in \mathbb{Z}[X]$  and  $g$  monic then  $f = qg + r$  where  $\deg(r) < \deg(g)$  and  $g, r \in \mathbb{Z}[x]$ .

Using this, we get that the denominator  $\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$  is a monic polynomial with coefficients in  $\mathbb{Z} \implies \Phi_n \in \mathbb{Z}[X]$ . □

## 2.4.2 Gauss' Theorem

**Theorem 2.17.** Let  $n$  be a factor of  $p - 1$ , where  $p$  is prime. Then there are exactly  $\phi(n)$  elements of order  $n$  in  $\mathbb{F}_p^\times$ . These are the roots of  $\Phi$  in  $\mathbb{F}_p^\times$ . In particular there are  $\phi(p - 1)$  primitive roots.

*Proof.* Let  $f(x) = x^{p-1} - 1$

By Fermat's Little theorem,  $f(x) = 0 \pmod{p}$  for  $x = 1, \dots, p - 1$  for  $(x \neq 0)$

$$\begin{aligned} \therefore f(x) &= (x - 1)(x - 2) \dots (x - (p - 1)) \\ &= \prod_{n|p-1} \Phi_n(x) \end{aligned}$$

This implies that:

- Each  $\Phi_n$  (for  $n|p - 1$ ) factorises completely into linear factors with no repeated roots  $\therefore \Phi_n$  has  $\phi(n)$  roots in  $\mathbb{F}_p$
- Every element of  $\mathbb{F}_p^\times$  is a root of exactly one of the polynomials  $\Phi_n$  with  $n|p - 1$

It remains to show that the roots of  $\Phi_n(x)$  in  $\mathbb{F}_p$  has order of exactly  $n$ .  
 Suppose  $\Phi_n(x) \equiv 0 \pmod{p}$

By the lemma  $\Phi_n(x)$  is a factor  $x^n - 1$   
 $\therefore x^n - 1 \equiv 0 \pmod{p}$   
 $\therefore x^n \equiv 1 \pmod{p}$

Suppose  $x^m \equiv 1 \pmod{p}$  for some  $m|n, m < n$   
 $\implies x^m - 1 \equiv 0 \pmod{p}$

By the lemma  $\Pi_{d|m} \Phi_d(x) \equiv 0 \pmod{p}$   
 $\implies \Phi_d(x) \equiv 0 \pmod{p}$  for some  $d \nmid n$

We already know that  $x$  is only a root of 1 of the cyclotomic polynomials, therefore  $x$  has order  $n$ .  $\square$

## 2.5 Quadratic reciprocity (Quadratic equations modulo prime numbers)

Recall we can solve  $x^a \equiv b \pmod{p}$  as long as  $a$  is coprime to  $p - 1$ . This won't work if  $a = 2$  because  $a$  will not be invertible mod  $p - 1$ . An easier question to ask is, which quadratic equations have solutions modulo  $p$ ?

**E.g.** Does  $x^2 \equiv 37 \pmod{149}$  have solutions?

Notation: We always let  $p$  be an odd prime (i.e.  $p \neq 2$ )

An element  $a \in \mathbb{F}_p^\times$  is a quadratic residue if  $x^2 \equiv a \pmod{p}$  has solutions.

An element  $a \in \mathbb{F}_p^\times$  is a quadratic non-residue if there are no solutions.

The quadratic residue symbol is defined for  $a \in \mathbb{F}_p^\times$  by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{a quadratic residue} \\ -1 & \text{a quadratic non-residue} \end{cases}$$

**Lemma 2.18.** *Let  $g$  be a primitive root modulo  $p$  ( $p$  odd prime). Then  $g^r$  is a quadratic residue iff  $r$  even.*

*Proof.*

( $\Leftarrow$ ) Assume  $r$  even

Clearly  $g^r$  is a square in  $\mathbb{F}_p^\times$

So  $g^r$  is a quadratic residue

( $\Rightarrow$ ) Assume  $g^r \equiv x^2 \pmod{p}$

$x \equiv g^s \pmod{p}$  ( $s \in \mathbb{Z}$ ) since  $g$  primitive roots

$\therefore g^r \equiv g^{2s} \pmod{p}$

$g^{r-2s} \equiv 1 \pmod{p}$

$g$  has order  $p - 1$ , so  $r - 2s$  is a multiple of  $p - 1$

$p$  odd  $\implies p - 1$  is even  $\implies r$  is even

$\square$

**E.g.**  $p = 7$

$x$	$x^2 \pmod{7}$		$a$	$\left(\frac{a}{7}\right)$
$\pm 1$	1	$\implies$	1	1
$\pm 2$	4		2	1
$\pm 3$	2		3	-1
			4	1
			5	-1
			6	-1

So 1,2,4 are quadratic residues; 3,4,6 are quadratic non-residues

**Corollary 2.19.** *There are exactly  $\frac{p-1}{2}$  quadratic residues and  $\frac{p-1}{2}$  quadratic non-residues mod  $p$*

**Defintion 2.20.** *Euler's criterion: Let  $p$  be an odd prime and  $a \in \mathbb{F}_p^\times \implies \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$*   
*Also  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*

*Proof.*  $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$  by Fermat's Little theorem.

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

Let  $a = g^r$  where  $g$  is a primitive root  $\implies a^{\frac{p-1}{2}} \equiv g^{(p-1)\frac{r}{2}}$

$$\begin{aligned} a \text{ is a quadratic residue} &\iff r \text{ is even} \\ &\iff (p-1)\frac{r}{2} \text{ is a multiple of } p-1 \\ &\iff g^{(p-1)\frac{r}{2}} \equiv 1 \pmod{p} \\ &\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \end{aligned}$$

□

To calculate  $\left(\frac{a}{p}\right)$ , we'll use three theorems:

### 2.5.1 Quadratic Reciprocity Law

Let  $p, q$  be distinct odd prime numbers. Then  $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

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

### 2.5.2 First Nebensatz

If  $p$  is an odd prime, then  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

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

### 2.5.3 Second Nebensatz

Let  $p$  be an odd prime, then  $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

$$\text{i.e. } (\frac{2}{p}) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$$

We'll prove the theorems later.

**E.g.** Does the congruence  $x^2 \equiv 37 \pmod{199}$  have solutions?

$$\begin{aligned} 199 \text{ is an odd prime } (\frac{37}{199}) &= +(\frac{199}{37}) && \text{by quadratic reciprocity} \\ &\equiv (\frac{14}{37}) && \text{because } 199 \equiv 14 \pmod{37} \\ &\equiv (\frac{2}{37})(\frac{7}{37}) && \text{by the corollary} \\ &\equiv (-1)(\frac{7}{37}) && \text{by the 2}^{nd} \text{ Nebensatz} \\ &\equiv (-1)(+1)(\frac{37}{7}) && \text{by the quadratic reciprocity law} \\ &\equiv -(\frac{2}{7}) && \text{because } 37 \equiv 2 \pmod{7} \\ &\equiv -(+1) && \text{by the 2}^{nd} \text{ Nebensatz} \\ &\equiv -1 && \therefore x^2 \equiv 37 \pmod{199} \text{ has no solutions} \end{aligned}$$

**E.g.**  $x^2 \equiv 47 \pmod{53}$  have solutions?

$$(\frac{47}{53}) = +(\frac{53}{47}) = (\frac{6}{47}) = (\frac{2}{47})(\frac{3}{47}) = (+1)(-1)(\frac{47}{3}) = -(-\frac{1}{3}) = -(-1) = +1$$

This shows that 47 is a quadratic residue mod 53, so  $x^2 \equiv 47 \pmod{53}$  does have solutions. ( $x = 10$ )

We can speed up the test for primitive roots using quadratic reciprocity,

$$x \text{ is a primitive root mod } p \iff \forall q|p-1, q \text{ prime } x^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

This means we need to calculate  $x^{\frac{p-1}{q}} \pmod{p}$  for primes  $q|p-1$ , the biggest power of  $x$  to calculate is  $x^{\frac{p-1}{2}}$ . But we can calculate this, because it is  $(\frac{x}{p})$  by Euler's criterion.

**E.g.** Is 35 a primitive root modulo 83?

The primes  $q$  dividing 82 are 2, 41, need to check  $35^2, 35^{41}$   
 $35^2 \not\equiv 1 \pmod{83}$  because  $35 \not\equiv \pm 1 \pmod{83}$ , a quadratic equation cannot have more than 2 roots.  
 $35^{41} \equiv (\frac{35}{83}) \pmod{83} = (\frac{5}{83})(\frac{7}{83}) = (\frac{83}{5})(-1)(\frac{83}{7}) = (\frac{3}{5})(-1)(\frac{-1}{7}) = (\frac{5}{3})(-1)(-1) = (\frac{2}{3})$   
 $= -1 \not\equiv 1 \pmod{83}$

So 35 is a primitive root modulo 83.

*Proof. First Nebensatz:*

By Euler's criterion,  $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ .

Both sides are  $\pm 1$ , and  $+1 \not\equiv -1 \pmod{p}$  because  $p \geq 3 \implies$  they are equal.  $\square$

**E.g.** Find the first primitive root modulo 41

$$40 = 2^3 * 5$$

$$x \in \mathbb{F}_{41}^\times \text{ is a primitive root} \iff \begin{cases} x^{\frac{40}{2}} \not\equiv 1 \pmod{41} \\ x^{\frac{40}{5}} \not\equiv 1 \pmod{41} \end{cases}$$

$$\text{We can then simplify the conditions to: } \begin{cases} \frac{x}{41} = -1 \\ x^4 \not\equiv \pm 1 \pmod{41} \end{cases}$$

$$\text{Try } x = 2 : \left(\frac{2}{41}\right) = 1 \implies \text{not a primitive root}$$

$$\text{Try } x = 3 : \left(\frac{3}{41}\right) = \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = -1 \quad \text{and } 3^4 = 81 \equiv -1 \pmod{41} \implies \text{not a primitive root}$$

$$\text{Try } x = 4 : \implies \text{not a primitive root}$$

$$\text{Try } x = 5 : \left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1 \implies \text{not a primitive root}$$

$$\begin{aligned} \text{Try } x = 6 : \left(\frac{6}{41}\right) &= \left(\frac{2}{41}\right)\left(\frac{3}{41}\right) = 1 * -1 = -1 \\ 2^4 * 3^4 &= -2^4 \equiv 16 \pmod{41} \not\equiv \pm 1 \implies \text{so 6 is a primitive root} \end{aligned}$$

**E.g.** For which primes  $p$  does the congruence  $x^2 \equiv -3 \pmod{p}$  have solutions?

Notice  $x = 1$  is a solution mod 2,

$x = 2$  is a solution mod 3.

For primes  $p \neq 2, 3$  it depends on  $\left(\frac{-3}{p}\right)$

$$\begin{aligned} \text{We'll calculate } \left(\frac{-3}{p}\right) & \quad \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) \\ &= (-1)^{\frac{(3-1)(p-1)}{4}} \left(\frac{p}{3}\right) \\ &= \left(\frac{p}{3}\right) \end{aligned}$$

List the squares mod 3,  $1^2 = 1 \pmod{3}, 2^2 = 1 \pmod{3}$

$$\therefore \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{3} \\ -1 & \text{if } p \equiv 2 \pmod{3} \end{cases}$$

We've shown that  $x^2 \equiv -3 \pmod{p}$  has solutions iff  $p \neq 2$  or  $p \equiv 1 \pmod{3}$ .

**Corollary 2.21.** *There are infinitely many primes  $p \equiv 1 \pmod{3}$*

*Proof.* Assume there are only finitely many, and call them  $p_1, p_2, \dots, p_r$   
Let  $N = n^2 + 3$  where  $n = 2p_1 \dots p_r$   
Take a prime factor  $q$  of  $N$

$$N \equiv 0 \pmod{q}$$

$$n^2 + 3 \equiv 0 \pmod{q}$$

$$n^2 \equiv -3 \pmod{q}$$

We've just shown that this implies  $q = 2$  or  $3$  or  $q \equiv 1 \pmod{3}$  but  $q \neq 2, 3, q \not\equiv 1 \pmod{3}$  □

Before we prove the  $2^{nd}$  Nebensatz, we need to know about a new ring.

Let  $\zeta = e^{\frac{2\pi i}{8}}$ , a primitive  $8^{th}$  root of unity.

We'll use the ring  $\mathbb{Z}[\zeta] = \{f(\zeta) : f \in \mathbb{Z}\} = \{a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_n\zeta^n : a_i \in \mathbb{Z}\}$

This is clearly a ring (closed under  $+, *$ ).

## 2.6 Uniqueness Lemma

Every  $A \in \mathbb{Z}[\zeta]$  can be written uniquely as  $A = W + x\zeta + y\zeta^2 + z\zeta^3$  with  $w, x, y, z \in \mathbb{Z}$ .

We'll use congruence modulo  $p$  in the ring  $\mathbb{Z}[\zeta]$  to prove the  $2^{nd}$  Nebensatz.

**Defintion 2.22.** Let  $A, B \in \mathbb{Z}[\zeta]$

We'll say  $A \equiv B \pmod{p\mathbb{Z}[\zeta]}$  if  $A - B = pC$  for some  $C \in \mathbb{Z}[\zeta]$

$$\text{Suppose } A = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$$

$$B = b_0 + b_1\zeta + b_2\zeta^2 + b_3\zeta^3$$

$$C = c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3$$

The equation  $A - B = pC$  is equivalent (by uniqueness lemma) to:

$$a_0 - b_0 = pC_0,$$

$$a_1 - b_1 = pC_1,$$

$$a_2 - b_2 = pC_2,$$

$$a_3 - b_3 = pC_3,$$

This implies that the congruence  $A \equiv B \pmod{p\mathbb{Z}[\zeta]}$  is equivalent to  $a_i \equiv b_i \pmod{p}$  for  $i = 0, 1, 2, 3$

**Corollary 2.23.**  $1 \not\equiv -1 \pmod{p\mathbb{Z}[\zeta]}$  if  $p$  is an odd prime.

This means that to calculate  $\left(\frac{2}{p}\right)$  it is enough to calculate its congruency class mod  $(p\mathbb{Z}[\zeta])$

The uniqueness lemma is implied by a more general result:

### 2.6.1 General Uniqueness Lemma

Let  $m \in \mathbb{Z}[X]$  be monic and irreducible over  $\mathbb{Q}$  of degree  $d$ . If  $\alpha \in \mathbb{C}$  is a root of  $m$ , then every element of  $\mathbb{Z}[\alpha]$  can be written uniquely as  $a_0 + a_1\alpha + \dots + a_{d-1}\alpha^{d-1}$  with  $a_i \in \mathbb{Z}$ .

The uniqueness lemma for  $\mathbb{Z}[\zeta]$  follows because  $\zeta$  is a root of  $m(x) = \Phi_8(x) = x^4 + 1$ . It is proved in (7202 Groups & Rings) that  $x^4 + 1$  is irreducible over  $\mathbb{Q}$ .

*Proof.* (General Uniqueness Lemma)

Let  $A \in \mathbb{Z}[\alpha]$  and  $m(\alpha) = 0$

Existence:  $A = f(\alpha)$  for some  $f \in \mathbb{Z}[X]$

divide  $f$  by  $m$  with remainder,  $f = q * m + r$   $\deg(r) < \deg(m) < d$

$$\therefore f(\alpha) = q(\alpha)m(\alpha) + r(\alpha)$$

$$\therefore A = r(\alpha)$$

Uniqueness: Suppose  $A = f(\alpha) = g(\alpha)$  ( $f \neq g$ ) where  $f$  &  $g$  both have degree  $< d$

$$\therefore h(\alpha) = 0 \text{ where } h = f - g \text{ } (\neq 0)$$

$m$  is irreducible over  $\mathbb{Q}$  and has a bigger degree than  $h$

$$\therefore m \nmid h \text{ in } \mathbb{Q}[x], \text{ so } m \text{ and } h \text{ are coprime in } \mathbb{Q}[x]$$

$\exists a, b \in \mathbb{Q}[x]$  such that :

$$1 = am + bh = a(\alpha)m(\alpha) + b(\alpha)h(\alpha) = 0$$

$$m(\alpha) = 0 \quad h(\alpha) = 0$$

$$\implies 1 = 0$$

$$\implies f = g$$

□

**Lemma 2.24.** *In any ring  $R$  with any prime  $p$*

$$(x + y)^p \equiv x^p + y^p \text{ } (pR) \text{ for any } x, y \in R$$

*Proof.* Sufficient to show that each binomial coefficient:

$$c = \frac{p!}{i!(p-i)!}$$

$i = 1, 2, \dots, p-1$  is a multiple of  $p$

$$i!(p-i)! \not\equiv 0 \text{ } (p) \implies \in \mathbb{F}_p^\times$$

□



*Proof.* 2<sup>nd</sup> Nebensatz

Let  $p$  be an odd prime and let  $G = \zeta + \zeta^{-1} = \sqrt{2}$ . We'll calculate  $G^p \bmod (p\mathbb{Z}[\zeta])$  in two ways.

**First Calculation:**

$$\begin{aligned} G^p &= (\zeta + \zeta^{-1})^p \\ &= \zeta^p + \zeta^{-p} \bmod (p\mathbb{Z}[\zeta]) \text{ by the lemma} \end{aligned}$$

Since  $\zeta^8 = 1$  this only depends  $p$  modulo 8 if  $p \equiv \pm 1(8)$  then,

$$G^p = \zeta + \zeta^{-1} \equiv G \bmod (p\mathbb{Z}[\zeta])$$

If  $p \equiv \pm 3(8)$  then,

$$G^p \equiv \zeta^3 + \zeta^{-3} \equiv -G \bmod (p\mathbb{Z}[\zeta])$$

So in summary,

$$G^p \equiv (-1)^{\frac{p^2-1}{8}} G \bmod (p\mathbb{Z}[\zeta])$$

**Second calculation:**

Since  $G^2 = 2$ ,

$$\begin{aligned} G^p &= G * 2^{\frac{p^2-1}{2}} \\ &= G * \left(\frac{2}{p}\right) \bmod (p\mathbb{Z}[\zeta]) \text{ by Euler's criterion} \end{aligned}$$

Comparing the results of these two calculations we get:

$$\left(\frac{2}{p}\right)G = (-1)^{\frac{p^2-1}{8}} G \bmod (p\mathbb{Z}[\zeta])$$

Note  $G^2 * \frac{p+1}{2} \equiv 1 \bmod (p\mathbb{Z}[\zeta])$ , i.e.  $G$  is invertible modulo  $p\mathbb{Z}[\zeta]$  with inverse  $G * \frac{p+1}{2}$

$$\implies \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \bmod (p\mathbb{Z}[\zeta])$$

Since  $1 \equiv -1 \bmod (p\mathbb{Z}[\zeta])$ ,

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

□

The proof of the 2<sup>nd</sup> Nebensatz worked because  $\sqrt{2} \in \mathbb{Z}[\zeta]$