

# MATH7701 Number Theory

Vinesh Ramgi

Spring 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>5</b>
1.1	Introduction . . . . .	5
1.2	Review . . . . .	5
1.2.1	Congruences . . . . .	5
1.2.2	Solving Linear Congruences . . . . .	6
1.3	Chinese Remainder Theorem . . . . .	7
1.4	Prime numbers . . . . .	9
1.5	Fermat's Little Theorem . . . . .	9
1.5.1	General method to solve $x^a \equiv b \pmod{p}$ . . . . .	10
1.6	Fundamental Theorem of Arithmetic . . . . .	10
1.6.1	Euclid's Lemma . . . . .	10
1.6.2	Checking whether a number is prime . . . . .	11
<b>2</b>	<b>Elementary Number Theory</b>	<b>12</b>
2.1	Euler Totient Function . . . . .	12
2.2	Euler's Theorem . . . . .	14
2.2.1	Solving equations of the form $x^a \equiv b \pmod{n}$ . . . . .	15
2.3	Primitive roots . . . . .	16
2.4	Roots of unity and Cyclotomic Polynomials . . . . .	17
2.4.1	How to calculate $\Phi_n(x)$ . . . . .	18
2.4.2	Gauss' Theorem . . . . .	19
2.5	Quadratic reciprocity (Quadratic equations modulo prime numbers) . . . . .	20
2.5.1	Quadratic Reciprocity Law . . . . .	21
2.5.2	First Nebensatz . . . . .	21
2.5.3	Second Nebensatz . . . . .	22
2.6	Uniqueness Lemma . . . . .	24
2.6.1	General Uniqueness Lemma . . . . .	24
2.6.2	Uniqueness Lemma for $\mathbb{Z}[\zeta_p]$ . . . . .	28
<b>3</b>	<b>P-adic Number theory</b>	<b>30</b>
3.1	Hensel's Lemma . . . . .	31
3.2	Quadratic Congruences . . . . .	34
3.3	P-adic congruence . . . . .	36
3.4	Power Series Trick . . . . .	38
3.4.1	P-adic log & exp . . . . .	41
3.5	Teichmüller Lifts . . . . .	44
3.6	Fractional Powers . . . . .	49
3.7	P-adic integers . . . . .	50
<b>4</b>	<b>Quadratic rings</b>	<b>53</b>
4.0.1	Properties of conjugates . . . . .	54
4.0.2	Formula for norms . . . . .	55
4.0.3	Properties of norms . . . . .	56
4.1	Norm-Euclidean quadratic rings . . . . .	57

4.2	The Decomposition Theorem . . . . .	60
4.3	Solving $ N(A) = n $ . . . . .	62
4.4	Continued Fractions . . . . .	65
4.5	Pell's equation and units in real quadratic rings . . . . .	69
4.5.1	Convergence of continued fractions . . . . .	74

# 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**  $2 \equiv 12 \pmod{10}$   
 $\equiv -8 \pmod{10}$

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  $hx + kn = 1 \implies hx = 1 \pmod{n}$ . 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:

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

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

**Definition 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  $n$

$$\begin{aligned} x^n &\equiv 1 \pmod{p} \\ x^{p-1} &\equiv 1 \pmod{p} \end{aligned} \quad \square$$

**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~~

$$199 \equiv 3 \pmod{7} \quad (7)$$

$$199 \equiv 4 \pmod{13} \quad (13)$$

$\therefore 199$  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

**Definition 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

$$\begin{array}{llll} \text{Powers of 3 in } \mathbb{F}_7^\times : & 3^0 = 1 & 3^3 \equiv 6 \pmod{7} & 3^6 \equiv 1 \pmod{7} \\ & 3^1 = 3 & 3^4 \equiv 4 \pmod{7} & \\ & 3^2 \equiv 2 \pmod{7} & 3^5 \equiv 1 \pmod{7} & \end{array}$$

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:

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

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  $x^{28/7} \not\equiv 1 \pmod{29}$

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

$$\begin{aligned} \text{Try } x = 2 : & & 2^4 &\equiv 16 \not\equiv 1 \pmod{29} \\ & & 2^{14} &\equiv 128^2 \equiv 12^2 \equiv 144 \equiv -1 \pmod{29} \end{aligned}$$

$\therefore 2$  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  $d$ .*

**Definition 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  $p$*

**Definition 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  $\left(\frac{-3}{p}\right)$

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

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.

**Definition 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  $\sqrt{2} \in \mathbb{Z}[\zeta]$   
To prove the quadratic reciprocity law, we'll show that  $\sqrt{\pm p}$  is in another cyclotomic ring

Let  $\zeta_p = e^{\frac{2\pi i}{p}}$ , a primitive  $p^{\text{th}}$  root of unity. We'll work in the ring modulo  $q\mathbb{Z}[\zeta]$ .

**Definition 2.25.** The  $p^{\text{th}}$  Gauss sum (where  $p$  is an odd prime):

$$G(p) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a \in \mathbb{Z}[\zeta_p]$$

**Lemma 2.26.**  $G(p)^2 = (-1)^{\frac{p-1}{2}}$

*Proof.*

$$\begin{aligned} G(p)^2 &= \left( \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a \right) \left( \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \zeta_p^b \right) \\ &= \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \zeta_p^a \zeta_p^b \\ &= \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta_p^{a+b} \end{aligned}$$

Let  $c \equiv a^{-1}b \pmod{p}$ , as  $b$  runs through  $\mathbb{F}_p^\times$ , so does  $c$

$$\begin{aligned} &= \sum_{a,c \in \mathbb{F}_p^\times} \left(\frac{a^2}{p}\right) \zeta_p^{a+ac} \\ &= \sum_{c \in \mathbb{F}_p^\times} \left(\frac{c}{p}\right) \left( \sum_{a=1}^{p-1} (\zeta_p^{1+c})^a \right) \end{aligned}$$

Note the second summation is a geometric progression. Recall that,

$$\sum_{i=1}^{p-1} r^i = \begin{cases} \frac{r^p - 1}{r - 1} & r \neq 1 \\ p - 1 & r = 1 \end{cases}$$

Summing the geometric progression:

$$\begin{aligned} \sum_{a=1}^{p-1} (\zeta_p^{1+c})^a &= \begin{cases} \frac{(\zeta_p^{1+c})^p - \zeta_p^{1+c}}{\zeta_p^{1+c} - 1} & \text{if } c \not\equiv 1 \pmod{p} \\ p - 1 & \text{if } c \equiv 1 \pmod{p} \end{cases} \\ &= \begin{cases} -1 & c \not\equiv -1 \pmod{p} \\ p - 1 & c \equiv -1 \pmod{p} \end{cases} \end{aligned}$$

$$\therefore G(p)^2 = \sum_{c \in \mathbb{F}_p^\times} \left(\frac{c}{p}\right)(-1) + p\left(\frac{-1}{p}\right)$$

$\sum_{c \in \mathbb{F}_p^\times} \left(\frac{c}{p}\right)(-1) = 0$  since there are  $\frac{p-1}{2}$  quadratic residues and quadratic non-residues.

$$\begin{aligned} &= p\left(\frac{-1}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} p \end{aligned} \quad \text{by the 1}^{st} \text{ Nebensatz}$$

□

### 2.6.2 Uniqueness Lemma for $\mathbb{Z}[\zeta_p]$

Every element  $A \in \mathbb{Z}[\zeta_p]$  can be written uniquely as:

$$A = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \quad \text{with } a_i \in \mathbb{Z}$$

This is because  $\zeta_p$  is a root of  $m(x) = \Phi_p(x) = 1 + x + \cdots + x^{p-1}$ . It's proved in 7202 that  $\Phi_p$  is irreducible over  $\mathbb{Q}$ .

*Proof.* Quadratic Reciprocity law

We'll calculate  $G(p)^q$  ( $q\mathbb{Z}[\zeta_p]$ ) in two ways.

**First Calculation:**

$$\begin{aligned} G(p)^q &= \left( \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a \right)^q \\ &= \sum_{a=1}^{p-1} \left( \left(\frac{a}{p}\right) \zeta_p^a \right)^q \quad (p\mathbb{Z}[\zeta]) \end{aligned}$$

Since  $q$  is odd,  $\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right)$

$$G(p)^q \equiv \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta_p^{aq}$$

Let  $b \equiv aq \pmod{p}$ , and as  $a$  runs through  $\mathbb{F}_p^\times$  so does  $b$

$$\begin{aligned} G(p)^q &\equiv \sum_{b \in \mathbb{F}_p^\times} \left(\frac{bq^{-1}}{p}\right) \zeta_p^b \\ &= \left(\frac{q^{-1}}{p}\right) \sum_{b \in \mathbb{F}_p^\times} \left(\frac{b}{p}\right) \zeta_p^b \end{aligned}$$

Note that  $G(p) = \sum_{b \in \mathbb{F}_p^\times} \left(\frac{b}{p}\right) \zeta_p^b$  which implies,

$$\begin{aligned} G(p)^q &\equiv \left(\frac{q^{-1}}{p}\right) G(p) \pmod{q\mathbb{Z}[\zeta_p]} \\ &\equiv \left(\frac{q}{p}\right) G(p) \pmod{q\mathbb{Z}[\zeta_p]} \end{aligned}$$

**Second Calculation:**

Since  $G(p)^2 = (-1)^{\frac{p-1}{2}} p$ ,

$$\begin{aligned} G(p)^q &= G(p) \left( (-1)^{\frac{p-1}{2}} p \right)^{\frac{q-1}{2}} \\ &= G(p) (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}} \\ \therefore G(p)^q &\equiv G(p) (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) \pmod{q\mathbb{Z}[\zeta_p]} \quad \text{by Euler's criterion} \end{aligned}$$

Comparing the two results we get:

$$\left(\frac{q}{p}\right) G(p) \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) G(p) \pmod{q\mathbb{Z}[\zeta_p]}$$

We need to check that  $G(p)$  is invertible modulo  $q\mathbb{Z}[\zeta_p]$ ,

$G(p)^2 = \pm p$ , which is invertible modulo  $q$

$G(p)$  has inverse  $G(p) * (\pm p)^{-1} \pmod{q\mathbb{Z}[\zeta_p]}$

$$\therefore \left(\frac{p}{q}\right) \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) \pmod{q\mathbb{Z}[\zeta_p]}$$

Since  $1 \equiv -1 \pmod{q\mathbb{Z}[\zeta_p]}$ , it follows that  $\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)$  □

### 3 P-adic Number theory

This means methods for congruences modulo  $p^n$ ,  $p$  prime and  $n$  large.

If we want to solve  $f(x) = 0$ ,  $x \in \mathbb{R}$  we can use the Newton-Raphson method:

- Begin with an "approximate solution"  $a_0$
- Define a sequence recursively  $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$

Very often  $a_n$  converge to a limit  $a$  and  $f(a) = 0$ .

We can use the same method in number theory for solving congruences. Suppose  $f(x)$  is a polynomial with coefficients in  $\mathbb{Z}$  and we want to solve  $f(x) \equiv 0 \pmod{p^n}$  ( $p$  prime,  $n$  large)

We can try this:

- Find a solution  $a_0$  to  $f(a_0) \equiv 0 \pmod{p^r}$  where  $r$  is small
- Define a recursive sequence  $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$

If  $n$  is large enough, then often  $f(a_n) \equiv 0 \pmod{p^N}$

**E.g.** Let  $f(x) = x^2 + 2$ ,  $p = 3$

Suppose we want to solve  $x^2 + 2 \equiv 0 \pmod{3^N}$

Let  $a_0 = 1$  :  $f(a_0) = 1^2 + 2 = 3 \equiv 0 \pmod{3}$

Define the sequence  $a_n$  by  $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} = a_n - \frac{a_n^2 + 2}{2a_n} = \frac{a_n}{2} - \frac{1}{a_n}$

$$\begin{aligned} a_0 &= 1 \\ a_1 &= \frac{1}{2} - 1 = \frac{-1}{2} \\ a_2 &= \frac{-1}{4} + 2 = \frac{7}{4} \end{aligned}$$

It turns out that  $\frac{-1}{2}$  is a solution mod 9  $\implies -1 * 2^{-1} \pmod{9}$   
 $\frac{7}{4}$  is a solution mod 81  $\implies 7 * 4^{-1} \pmod{81}$

$$2^{-1} \equiv 5 \pmod{9} \implies a_1 \equiv 4 \pmod{9}$$

$$4^{-1} \equiv -20 \pmod{81} \implies a_2 = \frac{7}{4} \equiv -140 \equiv 22 \pmod{81}$$

$a_3$  would be a solution mod  $3^8$ .

In this example, we're reducing rational numbers mod  $p^n$  not just integers. If  $\frac{a}{b}$  is a rational number then we can reduce this modulo  $p^n$  as long as  $b$  is invertible mod  $p^n$ , i.e. when  $b$  is not a multiple of  $p$ . We'll write:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}$$

$\mathbb{Z}_{(p)}$  is closed under  $+$ ,  $*$ , so  $\mathbb{Z}_{(p)}$  is a ring contained in  $\mathbb{Q}$  containing  $\mathbb{Z}$ . This is called the "local ring of  $p$ " and is the set of rational number which can be reduced modulo  $p^n$  ( $\forall n$ )

**Definition 3.1.** If  $p$  is a prime number and  $n \in \mathbb{Z}$ , then the valuation of  $n$ , at  $p$  is:

$$V_p(n) = \begin{cases} \max\{a : p^a | n\} & n \neq 0 \\ \infty & n = 0 \end{cases}$$

A simple statement that can be made is,  $V_p(nm) = V_p(n) + V_p(m)$ . We can also extend  $V_p$  to a function on  $\mathbb{Q}$ ,  $V_p(\frac{n}{m}) = V_p(n) - V_p(m)$ .

With this notation:

$$Z_{(p)} = \{x \in \mathbb{Q} : V_p(x) \geq 0\}$$

$$x \equiv y \pmod{p^a} \iff V_p(x - y) \geq a$$

**E.g**

$$V_2(\frac{7}{12}) = -2 \quad V_2(\frac{7}{12}) = -1 \quad V_5(\frac{7}{12}) = 0 \quad V_7(\frac{-7}{12}) = +1$$

### 3.1 Hensel's Lemma

Let  $p$  be a prime number. Let  $f \in \mathbb{Z}_{(p)}[x]$  and  $a_0 \in \mathbb{Z}_{(p)}$  such that  $f(a_0) \equiv 0 \pmod{p^{2c+1}}$  where  $c = V_p(f'(a_0))$ .

Then if we define  $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$  then  $a_n \in \mathbb{Z}_{(p)}$  and  $f(a_n) \equiv 0 \pmod{p^{2c+2^n}}$

*Proof.* We'll prove the following by induction on  $n$

1.  $a_n \in \mathbb{Z}_{(p)}$  and  $a_n \equiv a_0 \pmod{p^{c+1}}$
2.  $V_p(f'(a_n)) = c$
3.  $f(a_n) \equiv 0 \pmod{p^{2c+2^n}}$

If  $n = 0$  then the statements 1,2,3 are all true for  $a$  by assumption. Now assume 1,2,3 for  $a_n$ , we'll prove them for  $a_{n+1}$

Let  $a_{n+1} = a_n - \delta$  where  $\delta = \frac{f(a_n)}{f'(a_n)}$

**1:**

$$\begin{aligned} V_p(\delta) &= V_p(f(a_n)) - V_p(f'(a_n)) \\ &= c && \text{by 2:} \\ &\geq 2c + 2^n && \text{by 3:} \\ V_p(\delta) &\geq 2c + 2^n - c \\ V_p(\delta) &\geq c + 2^n && (*) \end{aligned}$$

By (\*)

$$V_p(\delta) \geq 0 \implies \delta \in \mathbb{Z}_{(p)}$$

$$\therefore a_{n+1} = a_n - \delta \in \mathbb{Z}_{(p)}$$

By (\*)

$$V_p \geq c + 1 \implies \delta \equiv 0 \pmod{p^{c+1}}$$

$$a_{n+1} \equiv a_n \pmod{p^{c+1}}$$

$$\equiv a_0 \pmod{p^{c+1}}$$

by 1

2: We've shown that  $a_{n+1} \equiv a_0 \pmod{p^{c+1}}$

$$\therefore f'(a_{n+1}) \equiv f'(a_0) \pmod{p^{c+1}}$$

$$\not\equiv 0$$

$$\text{because } V_p(f'(a_0)) = c$$

$$\text{also } f'(a_{n+1}) \equiv f'(a_0) \pmod{p^c}$$

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

$$\text{because } V_p(f'(a_0)) = c \pmod{p^c}$$

$$\therefore V_p(f'(a_{n+1})) = c$$

3: Must show that  $f(a_{n+1}) \equiv 0 \pmod{p^{2c+2^{n+1}}}$

$$a_{n+1} = a_n - \delta$$

$$a_{n+1}^r = (a_n - \delta)^r$$

$$= a_n^r - r a_n^{r-1} \delta + \text{multiples of } \delta^2$$

By (\*):

$$V_p(\delta) \geq c + 2^n$$

$$\therefore V_p(\delta^2) \geq 2c + 2^{n+1}$$

$$\therefore \delta^2 \equiv 0 \pmod{p^{2c+2^{n+1}}}$$

This implies  $a_{n+1}^r \equiv a_n^r - r a_n^{r-1} \delta \pmod{p^{2c+2^{n+1}}}$

Suppose  $f(x) = \sum c_r * x$ . Substituting  $a_{n+1}$ , we get:

$$\begin{aligned} f(a_{n+1}) &= \sum c_r (a_n^r - r a_n^{r-1} \delta) \pmod{p^{2c+2^{n+1}}} \\ &= \sum c_r a_n^r - \left( \sum r c_r a_n^{r-1} \right) \delta \pmod{p^{2c+2^{n+1}}} \\ &= f(a_n) - f'(a_n) * \frac{f(a_n)}{f'(a_n)} \equiv 0 \pmod{p^{2c+2^{n+1}}} \end{aligned}$$

□



**E.g.**  $f(x) = x^3 + x + 1$ ,  $p = 3$

Find a root of  $f \bmod 81$

Note that  $f'(x) = 3x^2 + 1$  and  $f(1) = 3 \equiv 0$

Try  $a_0 = 1$

$$\begin{aligned}c &= V_3(f'(a_0)) \\&= V_3(4) \\&= 0\end{aligned}$$

$3^{2c+1} = 3$  and  $a_0$  is a root of  $f$  modulo 3

$\therefore a_0 = 1$  satisfies the conditions of Hensel's lemma.

$$\begin{aligned}a_1 &= 1 - \frac{a_0}{f'(a_0)} \\&= 1 - \frac{3}{4}\end{aligned}$$

It is sufficient to work out  $a_1 \bmod 9$

$$4^{-1} \equiv 1 \pmod{3} \qquad \frac{3}{4} \equiv 3 * 1 \pmod{9} \qquad a_1 \equiv -2 \pmod{9}$$

Check

$$\begin{aligned}f(a_1) &\equiv (-2)^3 + (-2) + 1 \\f(2) &= -9 \equiv 0 \pmod{9}\end{aligned}$$

$$\begin{aligned}a_2 &= -2 - \frac{f(-2)}{f'(-2)} \\&= -2 - \frac{-9}{13}\end{aligned}$$

This should be a root of  $f$  modulo 81.

$$13^{-1} \equiv -2 \pmod{9}$$

$$\implies \frac{9}{13} \equiv -18$$

$$a_2 \equiv -2 - 18 \equiv -20$$

$$\begin{aligned}\text{Check } f(a_2) &= (-20)^3 - 20 + 1 \equiv -8000 - 19 \\&= -8019 \\&= -81 * 99 \\&= 0 \pmod{81}\end{aligned}$$

### 3.2 Quadratic Congruences

We'll see how to find out whether  $x^2 \equiv b \pmod{n}$  has solutions.

Suppose  $n = p_1^{a_1} \dots p_r^{a_r}$  ( $p_i$  distinct primes). There are solutions modulo  $n \iff \forall i$ , there are solutions modulo  $p_i^{a_i}$  by the Chinese Remainder Theorem.

**Proposition 3.2.** *Suppose  $p$  is an odd prime not dividing  $b$ . If  $x^2 \equiv b \pmod{p}$  has solutions then  $x^2 \equiv b \pmod{p^r}$  has solutions for all  $r$*

*Proof.* Suppose there is a solution  $a_0$  modulo  $p$ , i.e.  $a_0^2 \equiv b \pmod{p}$

Let  $f(x) = x^2 - b$ . We'll check that  $a_0$  satisfies the conditions of Hensel's lemma.

$$\begin{aligned} c &= V_p(f'(a_0)) \\ &= V_p(2a_0) \quad \text{and since } p \neq 2 \\ \implies c &= V_p(a_0) \end{aligned}$$

Also since  $p \nmid b$ , we know  $p \nmid a_0$ :

$$\begin{aligned} \therefore c &= 0 \\ \therefore f(a_0) &\equiv 0 \pmod{p^{2c+1}} \implies a_0 \text{ satisfies the conditions of Hensel's lemma} \\ \therefore &\text{ We have roots of } f \text{ modulo all powers of } p \end{aligned}$$

□

#### Remark

Suppose we want a root of  $f$  modulo  $p^{13}$

Choose  $n$  so that  $2c + 2^n \geq 13$

$$f(a_n) \equiv 0 \pmod{p^{2c+2^n}} \implies f(a_n) \equiv 0 \pmod{p^{13}}$$

The proposition would be false if we allowed  $p = 2$

**E.g.** Let  $b = 3$

$x$	$x^2 \pmod{4}$
0	0
1	1
2	0
3	1

$$x^2 \equiv 3 \pmod{2} \text{ has a solution}$$

$$x^2 \equiv 3 \pmod{4} \text{ has no solutions}$$

if  $b = 5$

$x$	$x^2 \pmod{8}$
0	0
$\pm 1$	1
$\pm 2$	4
$\pm 3$	1
$\pm 4$	0

$$x^2 \equiv 5 \pmod{2} \text{ has a solution}$$

$$x^2 \equiv 5 \pmod{4} \text{ has solutions}$$

$$x^2 \equiv 5 \pmod{8} \text{ has no solutions}$$

**Proposition 3.3.** Suppose  $b$  is odd. If  $x^2 \equiv b \pmod{8}$  has solutions then  $x^2 \equiv b \pmod{2^r}$  has solutions for all  $r$

*Proof.* Suppose  $a_0 \equiv b \pmod{8}$ , this implies  $a_0$  is odd.

Let  $f(x) = x^2 - b$

$\therefore c = V_2(f'(a_0)) = V_2(2a_0) = 1$  because  $a_0$  is odd

$\therefore 2^{2c+1} = 8$

$\therefore a_0$  is a root of  $f$  modulo  $p^{2c+1}$

By Hensel's lemma, there are solutions modulo all powers of 2.

□

**E.g.** For which  $n$  does the congruence  $x^2 \equiv 5 \pmod{5}$  have solutions?

First consider the case  $n \equiv p^r$  ( $p$  prime)

If  $p \neq 2, 5$  then by the first proposition, there are solutions  $p^n \iff \left(\frac{5}{p}\right) = 1$

$\left(\frac{5}{p}\right) = +\left(\frac{p}{5}\right)$  depends on  $p \pmod{5}$

$x$	$s$	
1	1	(different $x$ )
2	-1	The congruence $x^2 \equiv 5 \pmod{p}$ has solutions
3	-1	$\iff p \equiv 1, 4 \pmod{5}$ (in the cases $p \neq 2, 5$ )
4	1	

For  $p = 2$ ,  $x^2 \equiv 5 \pmod{2}$  has a solution,  $x = 1$

$x^2 \equiv 5 \pmod{4}$  has a solution,  $x = 1$

But the only odd square mod 8 is 1. So  $x^2 \equiv 5 \pmod{8}$  has no solutions.

$\therefore$  no solutions mod  $2^n$  if  $n \geq 3$

For  $p = 5$   $x^2 \equiv 5 \pmod{5}$  has solutions, here's how we check. Assume:

$$x^2 \equiv 5 \pmod{25}$$

$$\therefore x^2 \equiv 0 \pmod{5}$$

$$\text{So } 5|x^2$$

$$\text{So } 5|x$$

$$\therefore x^2 \equiv 0 \pmod{25} \quad \nexists$$

So there are solution modulo  $n$  if  $n = 2^a * 5^b * \prod p_i^{c_i}$  where  $a \leq 2, b \leq 1, p_i \equiv 1 \pmod{5}, c_i \in \mathbb{N}$

**E.g.** For which  $n$  does  $x^2 \equiv -7 \pmod{n}$  have solutions?

Assume  $p$  is a prime  $\neq 2, 7$

$$\begin{aligned}
\left(\frac{-7}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) \\
&= (-1)^{\frac{p-1}{2}} (-1)^{\frac{(7-1)(p-1)}{4}} \left(\frac{p}{7}\right) \\
&= (-1)^{\frac{p-1}{2} + \frac{3(p-1)}{2}} \left(\frac{p}{7}\right) \\
&= (+1)\left(\frac{p}{7}\right) \text{ depends on } p \bmod 7
\end{aligned}$$

x	$\left(\frac{x}{7}\right)$
1	1
2	1
3	-1
4	1
5	-1
6	-1

$$\begin{aligned}
3^2 &\equiv 9 \equiv 2 \pmod{7} \\
x^2 &\equiv -7 \pmod{p^r} \text{ has solutions} \\
&\implies p \equiv 1, 2, 4 \pmod{7}
\end{aligned}$$

For  $p = 2$ :  $-7 \equiv 1 \pmod{8}$  so  $-7$  is a square modulo 8 by the proposition.  
 $x^2 \equiv -7 \pmod{2^r}$  has solutions for all  $r$ .

For  $p = 7$ :  $x^2 \equiv -7 \pmod{7}$  has a solution  $x = 0$  but  $x^2 \equiv -7 \pmod{7^2}$  has no solutions. Suppose

$$\begin{aligned}
x^2 &\equiv -7 \pmod{7^2} \\
\therefore x^2 &\equiv 0 \pmod{7} \\
\therefore 7|x^2 \\
\implies 7|x \\
\implies x^2 &\equiv 0 \pmod{49} \quad \nexists
\end{aligned}$$

So  $x^2 \equiv -7 \pmod{n}$  has solutions  $\iff n = 7^a * \prod p_i^{b_i}$  where  $a \leq 1$ ,  $p_i \equiv 1, 2, 4 \pmod{7}$ ,  $b_i \in \mathbb{N}$

### 3.3 P-adic congruence

Suppose we have a series  $\sum_{n=1}^{\infty} x_n$  for  $x_n \in \mathbb{Z}_{(p)}$ . We'll say that the series converges **p-adically** if for every  $a$ , there are only finitely many terms  $x_n$  with  $x_n \not\equiv 0 \pmod{p^a}$ . We can add up the series in  $\mathbb{Z}/p^a$  because only finitely many terms are non zero.

**Lemma 3.4.**  $\sum x_n$  converges *p-adically*  $\iff V_p(x_n) \rightarrow \infty$

*Proof.* If  $V_p(x_n) \rightarrow \infty$  then for  $n$  significantly large,  $V_p(x_n) \geq a$ , i.e.,  $x_n \equiv 0 \pmod{p^a}$

□

**E.g.**  $p=3$

$$(1 + 3x)^{\frac{1}{2}} = 1 + \frac{1}{2}(3x) + \frac{\left(\frac{1}{2}\right)\left(\frac{-1}{2}\right)(3x)^2}{2!} + \frac{\left(\frac{1}{2}\right)\left(\frac{-1}{2}\right)\left(\frac{-3}{2}\right)(3x)^3}{3!}$$

if  $x \in \mathbb{Z}_{(3)}$  then this series converge 3-adically.

$$\begin{aligned}
(1 + 3x)^{\frac{1}{2}} &\equiv 1 \quad (3) \\
&\equiv 1 + \frac{3x}{2} \quad (9) \\
&\equiv 1 + \frac{3x}{2} + \frac{9}{8}x^2 \quad (27) \\
&\equiv 1 + \frac{3x}{2} + \frac{9}{8}x^2 + \frac{27}{16}x^3 \quad (27)
\end{aligned}$$

We can write these polynomials with integer coefficients.

$$\begin{aligned}
(1 + 3x)^{\frac{1}{2}} &\equiv 1 + 15x + 9x^2 \quad (27) \\
&\equiv 1 + 42x + 9x^2 + 27x^3 \quad (81)
\end{aligned}$$

Important point; these polynomials play the same role in number theory  $(1 + 3x)^{\frac{1}{2}}$  does in analysis  $\sqrt{1 + 3x}$

**E.g.**

$$\begin{aligned}
(1 + 15x + 9x^2)^2 &= 1 + (30)x + (18 + 15^2)x^2 + (2 * 9 * 15)x^3 + (81)x^4 \\
&\equiv 1 + 3x \quad (27)
\end{aligned}$$

**E.g.** Find a square root of 7 in  $\mathbb{Z}/81$

$$\begin{aligned}
7^{\frac{1}{2}} &= (1 + 3 * 2)^{\frac{1}{2}} \\
&\equiv 1 + 42 * 2 + 9 * 2^2 + 27 * 2^3 \quad (81) \\
&\equiv 1 + 84 + 36 - 27 \quad (81) \\
&\equiv 13 \quad (81)
\end{aligned}$$

Check  $13^2 = 169 \equiv 7 \quad (81)$

This works because of a result called the power series trick.

**Notation** We'll write  $\mathbb{Z}_{(p)}[[x]]$  for the set of power series in  $x$  with coefficient in  $\mathbb{Z}_{(p)}$ .

$\mathbb{Z}_{(p)}[[x]]$  is a ring with addition and multiplication of power series as operations. We can often compose two power series  $f, g \in \mathbb{Z}_{(p)}[[x]]$  to get a new power series  $f \circ g$ .

$(f \circ g)(x) = f(g(x))$ .

We can define  $f \circ g$  as long as either  $f$  is a polynomial or  $g$  has zero constant term. Suppose

$$\begin{aligned}
f(x) &= \sum_{n=0}^{\infty} a_n x^n \\
g(x) &= \sum_{n=0}^{\infty} b_n x^n
\end{aligned}$$

We'll see that  $f \circ g$  is a power series

$$\begin{aligned} f(g(x)) &= \sum_{n=0}^{\infty} a_n \left( \sum_{m=1}^{\infty} b_m x^m \right)^n \\ &= \sum_{n=0}^{\infty} a_n \sum_{m_1=0}^{\infty} \sum_{m_2=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} b_{m_1} \cdots b_{m_n} x^{m_1 + \cdots + m_n} \end{aligned}$$

so  $f(g(x)) = \sum c_d x^d$  where

$$c_d = \underbrace{\sum_{m_1, \dots, m_n=1}^{\infty} a_n b_{m_1} \cdots b_{m_n}}_{\text{finite sum in } \mathbb{Z}_{(p)}}$$

Note  $f \circ g$  is not defined otherwise.

**E.g**

$$\begin{aligned} f(x) &= 1 + x + x^2 + \dots \\ g(x) &= 1 + x \end{aligned}$$

$$\implies f(g(x)) = 1 + (1 + x) + (1 + x)^2$$

This has constant term  $1 + 1 + 1 + 1 + \dots$ , so  $f \circ g$  is not defined.

### 3.4 Power Series Trick

Suppose  $f, g, h$  are power series with coefficients in  $\mathbb{Z}_{(p)}$ . Assume either  $f$  is a polynomial or  $g$  has no constant term. Also assume:

- For small real numbers  $x$ ,  $f(x), g(x), h(x)$  converge and  $f(g(x)) = h(x)$
- For all  $x \in \mathbb{Z}_{(p)}$ ,  $f(x), g(x)$  and  $h(x)$  converge p-adically

Then for all  $x \in \mathbb{Z}_{(p)}$ ,  $f(g(x)) \equiv h(x) \pmod{p^n}$

In the example  $f(x) = x^2, g(x) = (1 + 3x)^{\frac{1}{2}}, h(x) = 1 + 3x$ .

For small real  $x$ ,  $f(g(x)) = h(x)$ , so as long as we know that  $g(x)$  converges 3-adically ( $\forall x \in \mathbb{Z}_{(3)}$ ) the power series trick implies  $g(x)^2 \equiv 1 + 3x \pmod{3^n}$

How do we check for p-adic convergence?

**Lemma 3.5.**  $\sum x_n$  converge p-adically if and only if  $V_p(x_n) \rightarrow \infty$

We need a way of calculating valuations of  $n^t$  term of a square.

**Proposition 3.6.**  $V_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots \leq \frac{n}{p-1}$

We'll prove this later, first use the properties to show that  $(1 + 3x)^{\frac{1}{2}}$  converge 3-adically for all  $x \in \mathbb{Z}_{(3)}$

$$(1 + 3x)^{\frac{1}{2}} = 1 + \frac{1}{2}(3x) + \frac{(\frac{1}{2})(\frac{-1}{2})(3x)}{2!} + \dots$$

$$n^{th} \text{ term} = \frac{(\frac{1}{2})(\frac{1}{2} - 1)(\frac{1}{2} - 2) \dots (\frac{1}{2} - n + 1)}{n!} (3x)^n$$

$$\begin{aligned} V_3(n^{th} \text{ term}) &= V_3\left(\frac{(\frac{1}{2})(\frac{1}{2} - 1) \dots (\frac{1}{2} - n + 1)}{n!}\right) - V_3(n!) + V_3((3x)^n) \\ &\geq 0 - \frac{n}{3-1} + n \\ &\geq \frac{n}{2} \rightarrow \infty \text{ as } n \rightarrow \infty \\ &\implies \text{series converges 3-adically} \end{aligned}$$

**E.g.** Assume  $p$  is an odd prime

Let  $\exp(px) = 1 + px + \frac{(px)^2}{2!} + \frac{(px)^3}{3!} + \dots$

We'll see that this converges for all  $x \in \mathbb{Z}_{(p)}$

$$n^{th} \text{ term} = \frac{(px)^n}{n!}$$

$$\begin{aligned} V_p(n^{th} \text{ term}) &= V_p((px)^n) - V_p(n!) \\ &= (n * V_p(p)) + (n * V_p(x)) - V_p(n!) \\ &\quad 1 \qquad \qquad \geq 0 \qquad \leq \frac{n}{p-1} \\ &\geq n - \frac{n}{p-1} \\ &\geq \left(\frac{p-2}{p-1}\right)n \rightarrow \infty \text{ for } p \neq 2 \end{aligned}$$

**E.g.**  $\log(1 + px)$  converges p-adically for all  $x \in \mathbb{Z}_{(p)}$

$$\begin{aligned} V_p\left(\pm \frac{(px)^n}{n}\right) &= V_p((px)^n) - V_p(n) \\ &\quad nV_p(px) < V_p(n!) \\ &\geq n - \frac{n}{p-1} \\ &\geq \left(\frac{p-2}{p-1}\right)n \rightarrow \infty \text{ if } p \neq 2 \end{aligned}$$

**Remark** A quick way to remember the series for  $\log(1 + px)$

$$\frac{1}{1-x} = 1 + x + x^2 + \dots \quad \text{geometric series}$$

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \dots$$

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

$$\log(1+px) = x - \frac{(px)^2}{2} + \frac{(px)^3}{3} - \frac{(px)^4}{4} + \dots$$

*Proof.* Calculating  $V_p(n!)$

$$n! = 1 * 2 * \dots * n$$

$$V_p(n) = \sum_{i=1}^n V_p(i) \quad (*)$$

The number of  $i$  between 1 &  $n$  which are multiples of  $p$  is  $\lfloor \frac{n}{p} \rfloor$ .

There are  $\frac{n}{p^2}$  values of  $i$  which are multiples of  $p^2$ , etc.

$\lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor$  values of  $i$  are multiples of  $p$ , but not of  $p^2$ , i.e.  $V_p(i) = 1$

So  $\lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor$  terms in the sum  $(*)$  are equal to 1.

Similarly  $\lfloor \frac{n}{p^2} \rfloor - \lfloor \frac{n}{p^3} \rfloor$  terms in the sum  $(*)$  are equal to 2.

In general there are exactly  $\lfloor \frac{n}{p^a} \rfloor - \lfloor \frac{n}{p^{a+1}} \rfloor$  terms in  $(*)$  which are equal to  $a$

$$\therefore V_p(n!) = 1 * \text{no of terms equal to 1} + 2 * \text{number of terms equal to 2} + \dots$$

$$\begin{aligned} V_p(n!) &= 1 * (\lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor) \\ &\quad + 2 * (\lfloor \frac{n}{p^2} \rfloor - \lfloor \frac{n}{p^3} \rfloor) \\ &\quad + 3 * (\lfloor \frac{n}{p^3} \rfloor - \lfloor \frac{n}{p^4} \rfloor) \\ &\quad + \dots \\ &= \lfloor \frac{n}{p} \rfloor + (2-1)\lfloor \frac{n}{p^2} \rfloor + (3-2)\lfloor \frac{n}{p^3} \rfloor + \dots \\ &= \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \dots \end{aligned}$$



Using this we can prove the upper bound.

$$\begin{aligned}
V_p(n!) &\leq \frac{n}{p} + \frac{n}{p^2} + \dots \\
&\leq \frac{n}{p} \underbrace{\left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right)}_{\text{geometric series } \frac{1}{1-\frac{1}{p}}} \\
&\leq \frac{n}{p-1}
\end{aligned}$$

□

### 3.4.1 P-adic log & exp

Let  $p$  be an odd prime. Use the notation

$$p\mathbb{Z}/p^n = \{px : x \in p\mathbb{Z}/p^n\}$$

**E.g.**

$$3\mathbb{Z}/27 = \{0, 3, 6, 9, 12, 15, 18, 21, 24\}$$

$p\mathbb{Z}/p^n$  is closed under  $+$ , so it is a subgroup of  $(\mathbb{Z}/p^n)^\times$

$$1 + p\mathbb{Z}/p^n = \{1 + px : x \in p\mathbb{Z}/p^n\}$$

**E.g.**

$$1 + 3\mathbb{Z}/27 = \{1, 4, 7, 10, 13, 16, 19, 22, 25\}$$

$1 + p\mathbb{Z}/p^n$  is closed under  $*$ , so  $1 + p\mathbb{Z}/p^n$  is a subgroup  $(\mathbb{Z}/p^n)^\times$ . Both subgroups have  $p^{n-1}$  elements, but one is additive and the other is multiplicative. But actually there are isomorphic. This isomorphism is exp & log.

**Theorem 3.7.** *Let  $p$  be an odd prime. Then there is an isomorphism:*

$$p\mathbb{Z}/p^n \xleftrightarrow[\exp]{\log} 1 + p\mathbb{Z}/p^n$$

$$px \longmapsto \exp(px)$$

$$1 + px \longmapsto \log(1 + px)$$

**E.g.**  $\mathbb{Z}/27$  ( $p = 3$ ) We'll find the isomorphisms in this case.

$$\exp(3x) \equiv 1 + 3x + \frac{3^2 x^2}{2!} + \frac{3^3 x^3}{3!} \quad (27)$$

$$\equiv 1 + 3x + 18x^2 + 18x^3 \quad (27)$$

$$\log(1 + 3x) \equiv 3x - \frac{(3x)^2}{2} + \frac{(3x)^3}{3} \quad (27)$$

$$\equiv 3x + 9x^2 + 9x^3 \quad (27)$$

Check:

$$\begin{aligned}
 \log(\exp(3x)) &\equiv \log(1 + 3(x + 6x^2 + 6x^3)) \\
 &\equiv 3(x + 6x^2 + 6x^3) + 9(x + 6x^2 + 6x^3)^2 + 9(x + 6x^2 + 6x^3) \\
 &\equiv 3x + 18x^2 + 18x^3 + 9x^2 + 9x^3 \\
 &\equiv 3x
 \end{aligned}$$

Similarly  $\exp(\log(1 + 3x)) \equiv 1 + 3x$  (27)

We can use the theorem to solve congruences.

**E.g.** Solve  $7^x \equiv 13$  (27)

7 and 13 are in  $1 + 3\mathbb{Z}/27$ , so we can take their logarithms.

$$x \log(7) \equiv \log(13)$$

Using the formula for  $\log(1 + 3x)$ , we get:

$$\begin{aligned}
 \log(7) &= \log(1 + 6) \\
 &\equiv 6 - \frac{6^2}{2} + \frac{6^3}{3} - \frac{6^4}{4} \\
 &\equiv 6 - 18 + 72 \\
 &\equiv 6 \quad (27)
 \end{aligned}$$

$$\begin{aligned}
 \log(13) &\equiv \log(1 + 12) \\
 &\equiv 12 - \frac{12^2}{2} + \frac{12^3}{3} \quad (27) \\
 &\equiv 12 - 72 + 3^2 * 4^3 \quad (27) \\
 &\equiv 12 - 72 + 9 \quad (27) \\
 &\equiv 3 \quad (27)
 \end{aligned}$$

So  $7^x \equiv 13$  (27) reduces to:

$$\begin{aligned}
 7^x &\equiv 13 \quad (27) \\
 \implies 6x &\equiv 3 \quad (27) \\
 \implies 2x &\equiv 1 \quad (9) \\
 \implies x &\equiv 5 \quad (9)
 \end{aligned}$$

*Proof.*

We'll use the power series trick. We've shown that  $\log(1 + px), \exp(px)$  converge p-adically for  $x \in \mathbb{Z}_{(p)}$  and they converge for small real numbers and for small real  $x$

$$\begin{aligned}\log(\exp(px)) &= px \\ \exp(\log(1 + px)) &= 1 + px\end{aligned}$$

By the power series trick:

$$\begin{aligned}\exp(\log(1 + px)) &\equiv 1 + px \pmod{p^n} \\ \log(\exp(px)) &\equiv px \pmod{p^n}\end{aligned}$$

$\therefore \log$  and  $\exp$  are inverse functions, so they are bijective.

Remains to show that  $\exp(px + py) \equiv \exp(px) * \exp(py) \pmod{p^n}$

For any  $a \in \mathbb{N}$ :  $\exp(pax) = \exp(px)^a$  for small real  $x$

By the power series trick with:

$$\begin{aligned}f(x) &= x^a \\ g(x) &= \exp(px) \\ h(x) &= \exp(pax) \\ \exp(pax) &\equiv (\exp(px))^a \pmod{p^a}\end{aligned}$$

Take  $x = 1$

$$\begin{aligned}\exp(pa) &\equiv \exp(p)^a \pmod{p^a} \\ \therefore \exp(pa + pb) &\equiv \exp(p)^{a+b} \pmod{p^a} \\ &\equiv \exp(p)^a * \exp(p)^b \\ &\equiv \exp(pa) * \exp(pb) \pmod{p^n}\end{aligned}$$

We've proved this when  $a$  &  $b$  are positive integers, but every element of  $\mathbb{Z}/p^n$  can be written as a positive integer. □

### 3.5 Teichmüller Lifts

Let  $p$  be an odd prime. We saw that  $(\mathbb{Z}/p^n)^\times$  has a big subgroup  $1 + p\mathbb{Z}/p^n$  and we can easily do calculations in the subgroup. Teichmüller lifts is another subgroup.

$$(\mathbb{Z}/p^n)^\times = \text{Teichmüller lifts} * (1 + p\mathbb{Z}/p^n)$$

Let  $x \in \mathbb{Z}_{(p)}$  and assume  $x \not\equiv 0 \pmod{p}$  :

$$x, x^p, x^{p^2}, x^{p^3}, \dots$$

All these terms are constant mod  $p$ :

$$\begin{aligned} x^{p-1} &\equiv 1 \pmod{p} \\ x^p &\equiv x \pmod{p} \end{aligned}$$

The sequence is constant mod  $p^2$ , but all terms after the  $2^{nd}$  are constant mod  $p^2$ .

**E.g.**  $p = 3, x = 2$

We'll look at the sequence mod 9:

$$\begin{aligned} 2^3 &\equiv 8 \pmod{9} \\ 2^9 &\equiv 8^3 \equiv 8 \pmod{9} \\ 2^{27} &\equiv 8 \pmod{9} \quad \text{etc} \end{aligned}$$

The sequence is eventually constant modulo  $p^n$

**Definition 3.8.** *The Teichmüller lift of  $x$  modulo  $p^n$  is:*

$$T(x) \equiv x^{p^{n-1}} \pmod{p^n}$$

To calculate Teichmüller lifts, we use:

**Lemma 3.9.** *Suppose  $x \equiv y \pmod{p^n}$  then  $x^p \equiv y^p \pmod{p^{n+1}}$*

*Proof.* Let  $x \equiv y + p^n \implies$

$$x^p \equiv (y + p^n)^p$$

$$x^p \equiv y^p + py^{p-1}p^n + \text{multiples of } p^{2n}$$

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

□

**E.g.** Calculate  $T(12) \pmod{125}$

Definition is  $12^{25} \pmod{125}$ . Using the lemma:

$$12 \equiv 2 \pmod{5}$$

$$\begin{aligned} 12^5 &\equiv 2^5 \pmod{5^2} \\ &\equiv 32 \equiv 7 \pmod{25} \end{aligned}$$

$$12^5 \equiv 7 \pmod{25}$$

$$12^{25} \equiv 7^5 \pmod{5^3}$$

$$\begin{aligned} T(12) &\equiv (2 + 5)^5 \pmod{125} \\ &\equiv 2^5 + 5(2^4) * 5 + 10 * 2^3 * 5^2 + \text{multiples of } 125 \\ &\equiv 2^5 + 5^2 * 2^4 \pmod{125} \\ &\equiv 2^5 + 25 * 16 \pmod{125} && \text{note } 16 \equiv 1 \pmod{5} \\ &\equiv 2^5 + 25 * 1 \pmod{125} \\ &\equiv 32 + 25 \pmod{125} \\ &\equiv 57 \pmod{125} \end{aligned}$$

$x$	$T(x) \pmod{125}$
1	1
2	57
3	$T(-1) * T(2) = -1 * 57 \equiv 68 \pmod{125}$
4	$(-1)^{25} \equiv -1$

**Theorem 3.10.**

1. If  $r > n - 1$  then  $x^{p^r} \equiv T(x) \pmod{p^n}$
2.  $T(x)^{p-1} \equiv 1 \pmod{p^n}$
3.  $T(x)$  depends only on  $x \pmod{p}$  and  $T(x) \equiv x \pmod{p}$
4.  $T: \mathbb{F}_p^\times \mapsto (\mathbb{Z}/p^n)^\times$  is an injective homomorphism

*Proof.*

By Euler's theorem,  $\phi(p^n) = (p-1)p^{n-1}$

$$\begin{aligned} &\implies \underbrace{x^{(p-1)p^{n-1}}}_{T(x)^{p-1}} \equiv 1 \pmod{p^n} \\ &\implies T(x)^{p-1} \equiv 1 \pmod{p^n} \end{aligned}$$

This proves **2**.

$$\therefore T(x)^p \equiv T(x) \pmod{p^n}$$

Doing this several times we get  $T(x) \equiv T(x)^p \equiv T(x)^{p^2} \equiv \dots \pmod{p^n}$

This proves **1**.

Suppose:

$$\begin{aligned} x &\equiv y \pmod{p} \\ x^p &\equiv y^p \pmod{p^2} && \text{by the lemma} \\ x^{p^2} &\equiv y^{p^2} \pmod{p^3} && \text{by the lemma} \\ &\vdots \\ T(x) &\equiv T(y) \pmod{p^n} && \text{by Fermat's Little Theorem} \\ x &\equiv x^p \equiv x^{p^2} \equiv \dots \equiv T(x) \pmod{p} \end{aligned}$$

This proves **3**.

$$\begin{aligned} T(xy) &\equiv (xy)^{p^{n-1}} \equiv x^{p^{n-1}} y^{p^{n-1}} \\ &\equiv T(x)T(y) \pmod{p} \end{aligned}$$

So  $T$  is a homomorphism, suppose:

$$\begin{aligned} T(x) &\equiv T(y) \pmod{p^n} \\ \therefore T(x) &\equiv T(y) \pmod{p} \\ x &\equiv y \pmod{p} && \text{by 3.} \end{aligned}$$

$$\therefore T: \mathbb{F}_p^\times \mapsto (\mathbb{Z}/p^n)^\times \text{ is injective}$$

□

**Corollary 3.11.** *Let  $p$  be an odd prime, every element in  $(\mathbb{Z}/p^n)^\times$  can be written uniquely in the form:*

$$\begin{aligned} &T(x) * \exp(py) \text{ with } x \in \mathbb{F}_p^\times \\ &py \in p\mathbb{Z}/p^n \end{aligned}$$

**E.g**  $22 \in (\mathbb{Z}/125)^\times$

$$22 = T(x) \exp(5y) \pmod{125}$$

$$\equiv 2 \pmod{5}$$

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

$$\implies x \equiv 2 \pmod{5}$$

$$22 = T(2) \exp(5y) \pmod{125}$$

$$22 * T(2^{-1}) \equiv \exp(5y) \pmod{125}$$

from the table  $T(3) = 68$

$$\exp(5y) \equiv 22 * 68 \pmod{125}$$

$$\equiv 121 \pmod{125}$$

$$\equiv -4 \pmod{125}$$

$$\therefore 5y \equiv \log(-4) \pmod{125}$$

$$\equiv \log(1 - 5) \pmod{125}$$

$$\equiv -5 - \frac{25}{2} - \frac{125}{3} + \dots$$

$$\equiv -5 - 75$$

$$\equiv 45 \pmod{125}$$

$$\therefore 22 = T(2) \exp(45) \pmod{125}$$

**E.g** Calculate  $22^{37} \pmod{125}$

$$22^{37} \equiv (T(2) \exp(45))^{37}$$

$$\equiv T(2^{37}) * \underbrace{\exp(45 * 37)}_{\equiv 40} \pmod{125}$$

$$\equiv 2 \pmod{5}$$

$$\therefore 22^{37} \equiv \underbrace{T(2)}_{\equiv 57} * \underbrace{\exp(40)}_{\equiv 841}$$

$$\equiv 57 * 91 \pmod{125}$$

$$\equiv 62 \pmod{125}$$

**E.g.** Calculate  $T(23) \pmod{7^3}$

$$\begin{aligned} 23 &\equiv 2 \pmod{7} \\ 23^7 &\equiv 2^7 \equiv 128 \equiv 30 \pmod{7^2} \\ 23^{7^2} &\equiv 30^7 \pmod{7^3} \end{aligned}$$

Using the binomial theorem:

$$\begin{aligned} 23^{7^2} &\equiv (2 + 4 \cdot 7)^7 \pmod{7^3} \\ &\equiv 2^7 + 7 \cdot 2^6 \cdot 4 + \text{multiples of } 7^3 \pmod{7^3} \end{aligned}$$

Since  $2^6 \cdot 4 \equiv 4 \pmod{7}$ , it follows that  $(7^2 \cdot 2^6 \cdot 4) \equiv (49 \cdot 4) \equiv 196 \pmod{7^3}$ . This shows that  $T(23) \equiv 128 + 196 \equiv 324 \pmod{7^3}$

The following corollary was stated but not proved:

**Corollary 3.12.** *Let  $p$  be an odd prime number. Every element of  $(\mathbb{Z}/p^n)^\times$  can be written uniquely in the form  $T(x) \cdot \exp(py)$  where  $x \in \mathbb{F}_p^\times$  and  $py \in p\mathbb{Z}/p^n$ . This is an isomorphism of groups:*

$$(\mathbb{Z}/p^n)^\times \cong \mathbb{F}_p^\times * p\mathbb{Z}/p^n$$

*Proof.* Take any  $a \in (\mathbb{Z}/p^n)^\times$  and let  $x \equiv a \pmod{p}$ . We have  $a \equiv x \equiv T(x) \pmod{p}$ . Therefore  $aT(x)^{-1} \equiv 1 \pmod{p}$ . This implies that  $\log(\frac{a}{T(x)})$  converges  $p$ -adically. Let  $py = \log(aT(x)^{-1})$ . Then obviously  $a = T(x) \exp(py)$ .

For uniqueness, suppose  $T(x) \cdot \exp(py) \equiv T(x') \cdot \exp(py') \pmod{p^n}$ . Since the image of  $\exp$  is congruent to 1  $\pmod{p}$ , we have  $T(x) \equiv T(x') \pmod{p}$ .

This implies  $x \equiv x' \pmod{p}$ . Therefore  $T(x) \equiv T(x') \pmod{p^n}$ . From this we get  $\exp(py) \equiv \exp(py') \pmod{p^n}$ . Taking logs we get  $py \equiv py' \pmod{p^n}$

□

This corollary can be used to solve the following types of equations:

**E.g**  $x^{21} \equiv 71 \pmod{81}$

Note 21 is not coprime to  $\phi(81) = 54$ , so previous methods cannot be used to solve this equation. Also  $(1 + 70)^{\frac{1}{21}}$  does not converge 3-adically. Start with  $71 \equiv 2 \pmod{3}$ :

$$\implies 71 \equiv T(2) \exp(3y) \pmod{81}$$

$$T(2) \equiv -1 \pmod{81},$$

$$\implies \exp(3y) \equiv -71$$

$$\implies 3y \equiv \log(1 + 9) = 9 - \frac{81}{2} + \dots \equiv 9 \pmod{81}$$

$$\implies 71 = T(2) \exp(9) \pmod{81}$$



Suppose we also decompose  $x = T(u) \exp(3v)$ . Then

$$x^{21} = T(u^{21}) \exp(3 * 21v) = T(2) \exp(9)$$

Since such a representation is unique, this gives us two simultaneous equations:

$$u^{21} \equiv 2 \pmod{3} \implies u \equiv -1 \equiv 2 \pmod{3}$$

$$\begin{aligned} 63v &\equiv 9 \pmod{81} \implies 7v \equiv 1 \pmod{9} \\ v &\equiv 4 \pmod{9} \\ 3v &\equiv 12 \pmod{27} \end{aligned}$$

$$x \equiv T(2) \exp(12) \pmod{27}$$

$$\begin{aligned} \exp(12) &\equiv 1 + 12 + \frac{12^2}{2} + \frac{12^3}{6} + \frac{12^4}{4!} + \dots \\ &\equiv 1 + 12 + 72 + 288 \\ &\equiv 1 + 12 + 18 + 18 \\ &\equiv 22 \pmod{27} \end{aligned}$$

$$T(2) \equiv -1 \pmod{27}$$

So  $x \equiv 5 \pmod{27} \implies x \equiv 5, 32, 59 \pmod{81}$

### 3.6 Fractional Powers

If  $p$  is an odd prime  $n$  and  $a \equiv 1 \pmod{p}$  and  $b \in \mathbb{Z}_{(p)}$  then  $a^b$  modulo  $p^n$  is:

$$a^b \equiv \exp(b \log(a)) \pmod{p^n}$$

The usual rules hold for powers:

- $(ab)^c \equiv a^c b^c \pmod{p^n}$
- $a^{b+c} \equiv a^b a^c \pmod{p^n}$
- $a^{bc} \equiv (a^b)^c \pmod{p^n}$

**E.g**  $4^{\frac{1}{2}} \pmod{27}$  First find  $\log(4) \pmod{27}$

$$\begin{aligned}\log(4) &\equiv (1 + 3) \pmod{27} \\ &\equiv 3 - \frac{9}{2} + \frac{27}{3} \pmod{27} \\ &\equiv 3 + 9 + 9 \pmod{27} \\ &\equiv 6 \pmod{27}\end{aligned}$$

So

$$\begin{aligned}4^b &\equiv \exp(-6b) \pmod{27} \\ 1 - 6b + \frac{36b^2}{2} - \frac{6^3b^3}{6} &\pmod{27} \\ 1 - 6b + 18b^2 - 36b^3 &\pmod{27} \\ 1 - 6b - 9b^2 - 9b^3 &\pmod{27}\end{aligned}$$

$$\begin{aligned}4^{\frac{1}{2}} &\equiv 1 - 3 - 9\left(\frac{1}{4} + \frac{1}{8}\right) \\ &\equiv 1 - 3\frac{27}{8} \\ &\equiv 1 - 3 \\ &\equiv -2 \pmod{27}\end{aligned}$$

### 3.7 P-adic integers

This section is slightly more highbrow way of looking at the results of the previous lectures. We've defined several congruency classes such as  $\exp(px) \pmod{p^n}$ ,  $T(a) \pmod{p^n}$ ,  $\log(1 + px) \pmod{p^n}$ . It's a little bit more convenient to be able to write down just  $\exp(px)$ ,  $T(a)$ , etc ... without needing to write modulo  $p^n$  everywhere. The problem is that there is no integer (or even an element of the local ring) which is congruent  $T(a) \pmod{p^n}$  for all  $n$ . Instead, we work in a bigger ring, the ring  $\mathbb{Z}_p$  of p-adic integers. In this ring, the expression  $T(a)$ ,  $\exp(px)$  etc all make sense.

Let  $p$  be any prime number. By a p-adic integer, we shall mean a p-adically convergent series

$$\sum_{i=1}^{\infty} a_i \qquad a_i \in \mathbb{Z}_{(p)}, V_p(a_i) \longrightarrow \infty$$

Recall that any series represents an element of  $\mathbb{Z}/p^n$  for every  $n$ . We call two p-adic integers equal if they are congruent modulo  $p^n$  for every  $n$ . The set of all p-adic integers is denoted  $\mathbb{Z}_p$  (without the brackets around the  $p$ ). Note that we can add, subtract and multiply p-adically convergent series, so in fact  $\mathbb{Z}_p$  is a ring.

The advantage of this kind of notation is that we can write (for example)  $\log(1 + px)$  to mean a p-adic integer, without having to reduce modulo  $p^n$ . This allows us to state many of the recent theorems more simply. If  $a \in \mathbb{Z}$  or  $\in \mathbb{Z}_{(p)}$ , then we can regard  $a$  as the series  $a = a + 0 + 0 + 0 + \dots$  and so  $a$  is a p-adic integer as well. Therefore  $\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Z}$ .

However, it turns out that there are many more p-adic integers than there are elements in the local ring  $\mathbb{Z}_{(p)}$ . For example consider the following 5-adic integer:

$$\begin{aligned} a &= (1 + 5)^{\frac{1}{2}} \\ &= 1 + \frac{1}{2} * 5 + \frac{\frac{1}{2} * \frac{-1}{2}}{2} + 5^2 + \dots \end{aligned}$$

In fact  $a$  is a square root of 6. We've shown earlier that  $a^2 \equiv 6 \pmod{5^n}$  for all  $n$  and therefore  $a^2 \equiv 6 \in \mathbb{Z}_5$ . However, the local ring  $\mathbb{Z}_{(5)}$  has no square roots of 6 since its elements are rational numbers. This shows that  $a$  is in  $\mathbb{Z}_5$  but not  $\mathbb{Z}_{(5)}$ .

**Proposition 3.13.** *Every p-adic integer can be written uniquely in the form:*

$$\sum_{i=0}^{\infty} a_i p^i$$

with coefficients  $a_i \in \{0, 1, \dots, p-1\}$

*Proof.*

Let  $x$  be a p-adic integer, so  $x$  is defined modulo  $p^n$  for all  $n$ . There is a unique choice of  $a_0$  such that  $a_0 \equiv x \pmod{p}$ .

This means that  $x - a_0$  is a multiple of  $p$ . There is a unique choice of  $a_1$  such that  $a_1 \equiv \frac{x - a_0}{p} \pmod{p}$ .

This implies  $pa_1 \equiv x - a_0 \pmod{p^2}$ , so  $x \equiv a_0 + a_1 p \pmod{p^2}$ . This implies  $x - a_0 - a_1 p$  is a multiple of  $p^2$  and there is a unique  $a_2$  such that  $p^2 a_2 \equiv x - a_0 - a_1 p \pmod{p^3}$ , etc.  $\square$

We've already seen what it means for a series to converge p-adically. We'll now make a corresponding definition for sequences.

**Definition 3.14.** *Let  $a_n$  be a sequence for elements of  $\mathbb{Z}_{(p)}$ . We'll say that this sequence converges p-adically if the corresponding series:*

$$a_0 + (a_1 - a_0) + (a_2 - a_1) + \dots$$

If this is the case, then we define the limit of the sequence to be this series, regarded as an element of  $\mathbb{Z}_p$ . Note that the partial sums of the series above are exactly the terms of the sequence  $a_n$ . In fact, we have already seen many examples of p-adic limits.

Suppose  $a_0 \in \mathbb{Z}_{(p)}$  satisfies the conditions of Hensel's lemma for a polynomial  $f(x)$ , i.e.  $f(a_0) \equiv 0 \pmod{p^{2c+1}}$ , where  $c = V_p(f'(a_0))$ . Consider the series:

$$a = a_0 + (a_1 - a_0) + (a_2 - a_1) + (a_3 - a_2) + \dots$$

We'll show that this series converges p-adically. Recall that  $a_{n+1} - a_n = \frac{f(a_n)}{f'(a_n)}$

When proving Hensel's lemma, we showed that  $f(a_n) \equiv 0 \pmod{p^{2c+2^n}}$ ,  $V_p(f'(a_n)) = c$

Therefore  $V_p(a_{n+1} - a_n) \geq 2c + 2^n - c = c + 2^n \rightarrow \infty$

Hence  $a$  is a  $p$ -adic integer, and is congruent to  $a_n \pmod{p^{c+2^n}}$ . We can re-interpret Hensel's lemma as saying the following:

**Proposition 3.15.** *Let  $a_0$  and  $f$  satisfy the conditions of Hensel's lemma and let  $a \in \mathbb{Z}_p$  be the  $p$ -adic integer defined above. Then  $f(a) = 0$*

*Proof.*

We just need to prove that  $f(a) \equiv 0 \pmod{\text{any power of } p}$ . But we have  $f(a) \equiv f(a_n) \equiv 0 \pmod{p^{c+2^n}}$  □

Next consider Teichmüller lifts. For an odd prime  $p$  and an element  $a \in \mathbb{Z}_{(p)}$  such that  $p \nmid a$  let:

$$T(a) = a + (a^p - a) + (a^{p^2} - a^p) + (a^{p^3} - a^{p^2}) + (a^{p^4} - a^{p^3}) + \dots$$

We've shown that  $a^{p^n} - a^{p^{n-1}} \equiv 0 \pmod{p^n}$ , and therefore the valuation of the  $n$ -th term is at least  $n$ . This shows that the series converges  $p$ -adically, so  $T(a) \in \mathbb{Z}_p$ . Now the properties of Teichmüller lifts can be restated as follows:

**Proposition 3.16.** *The  $p$ -adic integer  $T(a)$  depends only on the congruence class of  $a$  modulo  $p$ , and the map  $T: \mathbb{F}_p^\times \mapsto \mathbb{Z}_p^\times$  is an injective group homomorphism.*

*Proof.*

Since  $T(x) \equiv x \pmod{p}$ , it follows that  $T$  is injective. For every  $n$ , we have  $T(xy) \equiv T(x)T(y) \pmod{p^n}$ . Therefore  $T(xy) = T(x)T(y) \in \mathbb{Z}_p$  □

## 4 Quadratic rings

An integer  $d$  is called square-free if  $d$  is not a multiple of a square (apart from  $1^2$ ). Let  $d$  be a square-free integer with  $d \neq 1$ . Define a complex number  $\alpha$  by:

$$\alpha = \begin{cases} \sqrt{d} & \text{when } d \not\equiv 1 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{when } d \equiv 1 \pmod{4} \end{cases}$$

Consider the set  $\{x + y\alpha : x, y \in \mathbb{Z}\}$ . This is called a "Quadratic Ring".

**Lemma 4.1.** *Every quadratic ring is a ring, i.e. closed under  $+$ ,  $\times$ .*

*Proof.* Clearly closed under  $+$

$$(x + y\alpha)(r + s\alpha) = xr + (xs + yr)\alpha + ys\alpha^2$$

Sufficient to show that  $\alpha^2$  is in the quadratic ring.

**Case 1:**

$$\alpha = \sqrt{d} \implies \alpha^2 = d \text{ which is in the quadratic ring}$$

**Case 2:**

$$\alpha = \frac{1 + \sqrt{d}}{2} \qquad d \equiv 1 \pmod{4}$$

$$\left(\alpha - \frac{1}{2}\right)^2 = \frac{d}{4}$$

$$\alpha^2 - \alpha + \frac{1}{4} = \frac{d}{4}$$

$$\alpha \equiv \alpha + \frac{d-1}{4} \qquad d-1 \equiv 0 \pmod{4} \implies \frac{d-1}{4} \in \mathbb{Z}$$

$\therefore \alpha^2$  is in the quadratic ring. □

We call  $\mathbb{Z}[\alpha] = \{x + y\alpha : x, y \in \mathbb{Z}\}$ :

- A real quadratic ring if  $d > 0$
- A complex quadratic ring if  $d < 0$

**E.g**  $d = -1$

$$-1 \equiv 1 \pmod{4}$$

$$\therefore \alpha = \sqrt{-1} = i$$

$\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}$  is the ring of Gaussian integers.

**E.g**  $d = -3$

$$-3 \equiv 1 \pmod{4} \text{ so } \alpha = \frac{1+\sqrt{3}}{2}$$

This is the ring of Eisenstein integers. It is the same as  $\mathbb{Z}[\zeta_3] = \mathbb{Z}[e^{\frac{2\pi i}{3}}]$ .

**Definition 4.2.** Let  $\mathbb{Z}[\alpha]$  be a quadratic ring. The elements all have the form  $A = x + y\sqrt{d}$  where  $x, y$  are rational. The conjugate of such an element  $\bar{A} = x - y\sqrt{d}$

#### 4.0.1 Properties of conjugates

1  $\bar{\alpha} =$

$$1. \bar{\alpha} = \begin{cases} -\alpha & d \not\equiv 1 \pmod{4} \\ 1 - \alpha & d \equiv 1 \pmod{4} \end{cases}$$

$$2. \overline{A+B} = \bar{A} + \bar{B} \\ \overline{AB} = \bar{A} \bar{B}$$

$$3. \bar{A} \in \mathbb{Z}[\alpha] \text{ if } A \in \mathbb{Z}[\alpha]$$

$$4. \bar{\bar{A}} = A$$

*Proof.*

$$1. \text{ If } d \not\equiv 1 \pmod{4} \text{ then } \alpha = \sqrt{d} \\ \implies \bar{\alpha} = -\sqrt{d} = -\alpha$$

$$\text{If } d \equiv 1 \pmod{4} \text{ then } \alpha = \frac{1+\sqrt{d}}{2} \\ \implies \bar{\alpha} = \frac{1-\sqrt{d}}{2} = 1 - \alpha$$

2. Suppose:

$$A = x + y\sqrt{d}$$

$$B = r + s\sqrt{d}$$

Clearly  $\overline{A+B} = \bar{A} + \bar{B}$

$$\begin{aligned} \overline{A+B} &= \overline{(x + y\sqrt{d})(r + s\sqrt{d})} \\ &= \overline{(xr + dys) + (xs + yr)\sqrt{d}} \\ &= \overline{(xr + dys) - (xs + yr)\sqrt{d}} \end{aligned}$$

$$\begin{aligned} \bar{A} \cdot \bar{B} &= (x - y\sqrt{d})(r - s\sqrt{d}) \\ &= (xr + dys) + (-xs - yr)\sqrt{d} \end{aligned}$$

**3.** Let  $A = x + y\alpha$        $x, y \in \mathbb{Z}$

by **2.**  $\bar{A} = x + y\alpha$

by **1.**  $\bar{\alpha} \in \mathbb{Z}[\alpha]$

$\therefore \bar{A} \in \mathbb{Z}[\alpha]$

**4.** Trivial □

**Definition 4.3.** For an element  $A \in \mathbb{Z}$  we define  $N(A) = A\bar{A}$  - The norm of  $A$

Remark: If  $\mathbb{Z}[\alpha]$  is a complex quadratic ring then  $\bar{A}$  is the complex conjugate of  $A$ . This means  $N(A) = |A|^2$

**E.g.**  $d = -1 \implies \mathbb{Z}[\alpha] = \mathbb{Z}[i]$

The elements have the form  $x + iy$ ,  $x, y \in \mathbb{Z}$

$$\begin{aligned} N(x + iy) &= (x + iy)(x - iy) \\ &= x^2 + y^2 \end{aligned}$$

**E.g.**  $d = -3 \implies -3 \equiv 1 \pmod{4}$ , so  $\alpha = \frac{1+\sqrt{-3}}{2}$

$$\begin{aligned} N(x + y\alpha) &= (x + y\alpha)(x + y\bar{\alpha}) & \bar{\alpha} &= 1 - \alpha \\ &= x^2 + xy \underbrace{(\alpha + 1 - \alpha)}_{=1} + y^2 \underbrace{(\alpha(1 - \alpha))}_{=1} \end{aligned}$$

Note that:

$$\begin{aligned} \alpha &= \frac{1 + \sqrt{d}}{2} \\ \implies \left(\alpha - \frac{1}{2}\right)^2 &= \frac{d}{4} \\ \implies \alpha^2 - \alpha + \frac{1}{4} &= \frac{d}{4} \\ \implies \alpha(1 - \alpha) &= \frac{1 - d}{4} \end{aligned}$$

In this case:

$$N(x + y\alpha) = x^2 + xy + y^2$$

#### 4.0.2 Formula for norms

The general formula for norms is given by:

$$N(x + y\alpha) = \begin{cases} x^2 - dy^2 & \text{if } d \not\equiv 1 \pmod{4} \\ x^2 + xy + \frac{1-d}{4}y^2 & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

**Case 1:**  $d \neq 1$  (4)

$$\implies \bar{\alpha} \equiv -\alpha$$

$$N(x + y\alpha) = (x + y\alpha)(x - y\alpha) = x^2 - dy^2 \quad \alpha^2 = d$$

**Case 2:**  $\bar{\alpha} = 1 - \alpha$

$$\implies \alpha = \frac{1+\sqrt{d}}{2}$$

$$\begin{aligned} N(x + y\alpha) &= (x + y\alpha)(x + y(1 - \alpha)) \\ &= x^2 + xy + y^2(\underbrace{\alpha - \alpha^2}_{\frac{1-d}{4}}) \end{aligned}$$

#### 4.0.3 Properties of norms

1.  $N(A) \in \mathbb{Z}$
2.  $N(AB) = N(A)N(B)$
3. If  $N(A) = 0$  then  $A = 0$

*Proof.*

1. Follows from formulas for norms
2.  $N(AB) = AB\overline{AB} = AB\bar{A}\bar{B}$
3. If  $N(A) = 0$  then  $A\bar{A} = 0$   
 $\therefore$  either  $A = 0$  or  $\bar{A} = 0$   
 $\therefore \bar{A} = 0$  then  $A = \bar{A} = \bar{0} = 0$

□

Recall - A unit in a ring  $R$  is an element with an inverse in  $R$ .

**E.g.**  $1 + \sqrt{2}$  is a unit in  $\mathbb{Z}[\sqrt{2}] \implies (1 + \sqrt{2})(\sqrt{2} - 1) = 1$

**Corollary 4.4.** An element  $A \in \mathbb{Z}[\alpha]$  is a unit if and only if  $N(A) = \pm 1$

*Proof.* If  $N(A) = \pm 1$  then  $A\bar{A} = \pm 1$

$$\implies A^{-1} = \pm A \in \mathbb{Z}[\alpha]. \text{ So } A \text{ is a unit.}$$

□

If  $A$  is a unit with inverse  $B$ ,  $AB = 1 \implies N(A)N(B) = N(AB) = N(1) = 1$

Using this proposition, it's easy to find all the units in any complex quadratic ring.

**E.g** The units in  $\mathbb{Z}[i]$  are  $\pm 1, \pm i$

*Proof.* Since  $N(x + iy) = x^2 + y^2$ , the units correspond to the solutions to  $x^2 + y^2 = 1$ .

These solutions are  $x = \pm 1, y = 0$  and  $x = 0, y = \pm 1$

□



**E.g.** The units in the Eisenstein integers  $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$  are  $\pm 1, \pm \alpha, \pm(\alpha - 1)$ . Equivalently these are  $\pm 1, \pm \zeta_3, \pm \zeta_3^2$

*Proof.* Find all solutions to  $x^2 + xy + y^2 = 1$ . We can complete the square to get:

$$(x + \frac{1}{2}y)^2 + \frac{3}{4}y^2 = 1$$

$y^2 < \frac{4}{3}$  and since  $y$  is an integer  $|y| < 1$   
Similarly  $|x| < 1$ .

If  $y = 0$  then  $x = \pm 1$

If  $y = \pm 1$  then  $x^2 + xy + 1 = 1 \implies x = 0, -y$  are solutions.

So the 6 solutions are  $(1, 0), (-1, 0), (0, 1), (-1, 1), (0, -1), (1, -1)$

□

**Corollary 4.5.** If  $d < 0$  and  $d \neq -1, -3$  then the units in  $\mathbb{Z}[\alpha]$  are  $\{1, -1\}$

*Proof.* Assume first that  $d \not\equiv 1 \pmod{4}$

$$\implies N(x + y\alpha) = x^2 - dy^2 \quad x, y \in \mathbb{Z} \text{ and } -d > 1 \text{ so } y = 0 \implies x = \pm 1$$

So  $(1, 0), (-1, 0)$  give us the two units  $1, -1$

Assume now  $d \equiv 1 \pmod{4} \implies -d \geq -7$  and need to find solutions to the equation:

$$x^2 + xy + \frac{1-d}{4}y^2 = 1$$

$$\implies (x + \frac{1}{2}y)^2 - \frac{d}{4}y^2 = 1$$

Since  $\frac{d}{4} > 1, y^2 < 1 \implies y = 0 \implies x = \pm 1$

□

## 4.1 Norm-Euclidean quadratic rings

**Definition 4.6.** A quadratic ring  $\mathbb{Z}[\alpha]$  is norm-Euclidean if  $\forall A, B \in \mathbb{Z}[\alpha]$  with  $B \neq 0$   $\exists Q, R \in \mathbb{Z}[\alpha]$  such that:

- $A = QB + R$
- $|N(R)| < N(B)$

Finitely many of the quadratic rings are norm-Euclidean.

**Theorem 4.7.** If  $\mathbb{Z}[\alpha]$  is norm-Euclidean then every non-zero element of  $\mathbb{Z}[\alpha]$  can be factorised as  $UQ_1 \dots Q_r$

$Q_i$  are irreducible elements of  $\mathbb{Z}[\alpha]$ ,  $U$  is a unit.

This factorisation is unique in the sense that if  $U_1Q_1 \dots Q_r = U_2R_1 \dots R_s$  then  $r = s$  and (after reordering  $Q_r, R_i$  is a unit for each  $U$

**E.g** Let  $d = -7$  so  $\alpha = \frac{1+\sqrt{-7}}{2}$ . This is norm-Euclidean.

Suppose  $z = x + y\sqrt{-7}$   $x, y \in \mathbb{Q}$ . We'll show that there is an element  $Q \in \mathbb{Z}[\alpha]$  such that  $|N(Z - Q)| < 1$ .

Choose  $b \in \mathbb{Z}$  such that  $|y - \frac{b}{2}| < \frac{1}{4}$

Note that  $z - b\alpha = (x - \frac{b}{2}) + (y - \frac{b}{2})\sqrt{-7}$

Then choose  $a \in \mathbb{Z}$  so that  $|x - \frac{b}{2} - a| \leq \frac{1}{2}$ . Also note that the maximum distance to the closest integer is  $\frac{1}{2}$ .

We let  $Q = a + b\alpha$  and we have:

$$Z - Q = (x - \frac{b}{2} - a) + (y - \frac{b}{2})\sqrt{-7}$$

$$N(Z - Q) \leq (\frac{1}{2})^2 + 7(\frac{1}{4})^2 = \frac{11}{16} < 1$$

Now to show the ring is norm-Euclidean. Choose  $A, B \in \mathbb{Z}[\alpha]$  with  $B \neq 0$ . By what we've shown there is an element  $Q \in \mathbb{Z}[\alpha]$  such that  $|N(\frac{A}{B} - Q)| \leq 1$

Let  $R = A - QB$  then  $A = QB + R$

$$\begin{aligned} |N(R)| &= |N(A - QB)| \\ &= |N(\frac{A}{B} - Q)N(B)| \\ &< |N(B)| \end{aligned}$$

**E.g** Let  $d = 3$ . In this case  $\alpha = \sqrt{3}$ . We'll show that the quadratic ring  $\mathbb{Z}[\sqrt{3}]$  is norm-Euclidean.

Let  $z = x + y\sqrt{3}$  with  $x, y \in \mathbb{Q}$ . Need to show there is an element  $Q = r + s\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$  such that  $|N(Z - Q)| < 1$ . Choose  $r, s \in \mathbb{Z}$  such that:

$$|x - r| \leq \frac{1}{2} \qquad |y - s| \leq \frac{1}{2}$$

$$\begin{aligned} \implies N(Z - A) &= (x - r)^2 - 3(y - s)^2 \\ \implies -\frac{3}{4} &\leq N(Z - Q) \leq \frac{1}{4} \\ \implies |N(Z - Q)| &< 1 \end{aligned}$$

Now to show that  $\mathbb{Z}[\sqrt{3}]$  is norm-Euclidean. Suppose  $A, B \in \mathbb{Z}[\sqrt{3}]$  with  $B \neq 0$ , there is already a  $Q \in \mathbb{Z}[\sqrt{3}]$  such that  $|N(\frac{A}{B} - Q)| < 1$ .

Let  $R = A - QB$ . This implies  $A = QB + R$

$$\begin{aligned} \implies |N(R)| &= |N(A - QB)| \\ &= |N(\frac{A}{B} - Q)N(B)| \\ &< |N(B)| \end{aligned}$$

Hence  $\mathbb{Z}[\sqrt{3}]$  is norm-Euclidean.

**Theorem 4.8.** *The disappointing theorem - The quadratic rings with  $d = -1, -2, -3, -7, 1, 2, 3, 5, 13$  are norm-Euclidean.*

**Definition 4.9.** Suppose  $A, B \in \mathbb{Z}[\alpha]$ . A highest common factor of  $A$  and  $B$  is an element  $C \in \mathbb{Z}[\alpha]$  with the following properties:

- $C$  is a factor of both  $A$  and  $B$  i.e.  $\frac{A}{C}$  and  $\frac{B}{C}$  are both in  $\mathbb{Z}[\alpha]$
- If  $D$  is a factor of both  $A$  and  $B$  then  $D$  is a factor of  $C$  (and hence  $|N(D)| \leq |N(C)|$ )

If  $C$  is a highest common factor of  $A$  and  $B$ , then so is  $UC$  for every unit  $U$ , but these are all the highest common factors. Hence highest common factors, if they exist are unique up to multiplication by a unit.

**Lemma 4.10.** *Bezout's Lemma - Let  $\mathbb{Z}[\alpha]$  be norm-Euclidean ring and let  $A, B \in \mathbb{Z}[\alpha]$  not both 0. Then there is a highest common factor  $C$  of  $A, B$  and there exist  $H, K \in \mathbb{Z}[\alpha]$ , such that  $HA + KB = C$*

*Proof.* The proof goes similarly to in the ring  $\mathbb{Z}$ . We prove by induction on  $\min(|N(A)|, |N(B)|)$ . The induction step consists of writing  $A = QB + R$  with  $|N(R)| < |N(B)|$  and using the lemma. To prove the start of the induction, we assume  $B = 0$ . But then it's easy to check that  $A$  is a highest common factor.  $\square$

**Definition 4.11.** An element  $P \in \mathbb{Z}[\alpha]$  is called irreducible if:

- $P$  is not a unit
- If  $P = AB$  with  $A, B \in \mathbb{Z}[\alpha]$  then either  $A$  or  $B$  is a unit

**Definition 4.12.** We'll say that a quadratic ring  $\mathbb{Z}[\alpha]$  has unique factorisation if the following is true:

- For every non-zero element  $A \in \mathbb{Z}[\alpha]$  there is a factorisation  $A = UP_1 \dots P_r$  with  $U$  a unit and each  $P_i$  irreducible
- If we have another factorisation  $A = U'Q_1 \dots Q_s$ , then  $r = s$  and we can reorder  $Q_1, \dots, Q_s$  so that each  $P_i/Q_i$  is a unit.

**Lemma 4.13.** *Let  $\mathbb{Z}[\alpha]$  be norm-Euclidean. Let  $p$  be irreducible and suppose  $P|AB$  in  $\mathbb{Z}[\alpha]$ . Then  $P|A$  or  $P|B$*

*Proof.* Suppose  $P$  does not divide  $A$ . Then the highest common factor of  $P$  and  $A$  is not  $P$ , so it must be 1. Therefore we can find  $H, K \in \mathbb{Z}[\alpha]$  such that  $HP + KA = 1$ . This implies  $B = HPB + KPB$  which is a multiple of  $P$ .  $\square$

**Theorem 4.14.** *If  $\mathbb{Z}[\alpha]$  is norm-Euclidean, then  $\mathbb{Z}[\alpha]$  has unique factorisation.*

*Proof.*

The proof is exactly as for  $\mathbb{Z}$  (using the previous lemma for the uniqueness part), except that we prove by induction on  $N(A)$ .  $\square$

In fact, there are many examples when  $\mathbb{Z}[\alpha]$  has unique factorisation, even though it is not norm-Euclidean. It's known that a complex quadratic ring has unique factorisation for exactly the following values of  $d$  and no more:

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

In contrast, it is much more common for a real quadratic ring to have unique factorisation. In fact, the following is believed (but not proved):

**Conjecture:** There are infinitely many positive square-free integers  $d$  such that  $\mathbb{Z}[\alpha]$  has unique factorisation. On the other hand, there are many quadratic rings which do not have unique factorisation.

**E.g** In the ring  $\mathbb{Z}[\sqrt{-5}]$  we have non-unique factorisation. For example  $6 = 2 * 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ .

The elements  $2, 3, 1 \pm \sqrt{-5}$  are all irreducible. To see this, note that they have norms 2, 9, 6&6. Hence any proper factors would have norm 2 and 3. However the ring  $\mathbb{Z}[\sqrt{-5}]$  has no elements of norm 2 and 3 since  $x^2 + 5y^2$  is never equal to 2 or 3 for integers  $x, y$ .

## 4.2 The Decomposition Theorem

Assume that  $\mathbb{Z}[\alpha]$  is a quadratic ring with unique factorisation into irreducible elements, e.g.  $\mathbb{Z}[\alpha]$  could be norm-Euclidean.

**Lemma 4.15.** *If  $Q$  is an irreducible element in  $\mathbb{Z}[\alpha]$  then there exists a unique prime number  $p$  such that  $Q|p$*

*Proof.*

$$Q|N(Q) = \pm p_1 p_2 \dots p_r \quad (p_i \text{ prime})$$

By uniqueness of factorisation  $Q|p_i$  for some  $i$  if  $Q|p$  and  $Q|q$  where  $p, q$  are distinct primes,  $hcf(p, q) = 1 = hp + kq \quad (h, k \in \mathbb{Z}) \implies Q|1 \nmid$   $\square$

The lemma means that to find all the irreducible elements, we just need to factorise all the primes in  $\mathbb{Z}[\alpha]$ . Suppose  $Q|p$ , where  $Q$  is irreducible in  $\mathbb{Z}[\alpha]$ ,  $p$  prime:

$$\begin{aligned} \implies N(Q)|N(p) &= p^2 \\ \implies N(Q) &= \pm p \text{ or } \pm p^2 \end{aligned}$$

If  $N(Q) = \pm p^2$  then  $Q = \text{unit} * p$  so  $p$  is irreducible.

- If  $P = Q_1 Q_2$  where  $\frac{Q_1}{Q_2}$  is not a unit, then we say  $P$  is **split** in  $\mathbb{Z}[\alpha]$
- If  $P = U Q^2$  ( $U$  a unit,  $Q$  irreducible) then we say  $P$  is **ramified** in  $\mathbb{Z}[\alpha]$
- If  $P$  is irreducible in  $\mathbb{Z}[\alpha]$  then we say that  $P$  is **inert** in  $\mathbb{Z}[\alpha]$

**E.g**  $d = -1$   $\alpha = \sqrt{-1} = i$   $N(x + iy) = x^2 + y^2$

A prime number  $p$  factorises in  $\mathbb{Z}[i] \implies$  there is an element with norm  $\pm p$

- $2 = 1^2 + 1^2 = N(1 + i) = (1 + i)(1 - i) = -i(1 + i)^2 \implies 2$  is ramified
- $3$  is inert
- $5 = 2^2 + 1^2 = (2 + i)(2 - i)$   $5$  is split
- $7$  is inert
- $11$  is inert
- $13 = 3^2 + 2^2 = (3 + 2i)(3 - 2i)$   $13$  is split

Check if a number is ramified by dividing one by the other and checking if the result is in the ring.

**E.g**  $d = -3$   $\alpha = \frac{1+\sqrt{3}}{2}$   $N(x + y\alpha) = x^2 + xy + y^2$

- $2$  inert
- $3 = -\sqrt{-3}^2 = -(1 - 2\alpha)^2$   $3$  ramified
- $5$  inert
- $7 = N(2 + \alpha) = (2 + \alpha)(3 - \alpha)$
- $11$  inert

Assume  $\mathbb{Z}[\alpha]$  is a quadratic ring with unique factorisation. Let  $p$  be an odd prime number.

$$\begin{array}{ll} p \text{ is ramified} & \iff p|d \\ p \text{ is split} & \iff \left(\frac{d}{p}\right) = 1 \\ p \text{ is inert} & \iff \left(\frac{d}{p}\right) = -1 \end{array} \qquad \begin{array}{ll} 2 \text{ splits} & \iff d \equiv 1 \pmod{8} \\ 2 \text{ inert} & \iff d \equiv 5 \pmod{8} \\ \text{in other cases } 2 & \text{ is ramified} \end{array}$$

Idea of proof:

Assume  $d \not\equiv 1 \pmod{4}$ ,  $N(x + y\alpha) = x^2 - dy^2$

If  $p$  factorises then  $\exists x, y \in \mathbb{Z}, x^2 - dy^2 = \pm p$

$$\begin{aligned} &\implies x^2 \equiv dy^2 \pmod{p} \\ &\implies \left(\frac{x}{y}\right)^2 \equiv d \pmod{p} \end{aligned}$$

If  $d$  is a quadratic residue then  $x^2 \equiv d \pmod{p}$   $p \mid (x + \sqrt{d})(x - \sqrt{d})$ .

If  $p$  were inert then  $p \mid x + \sqrt{d}$  or  $x - \sqrt{d} \nmid$  (number not in ring)  
 $\implies$  factorises

### 4.3 Solving $|N(A)| = n$

Assume that  $\mathbb{Z}[\alpha]$  has unique factorisation, does the equation  $|N(A)| = n$  have solutions?

**E.g**  $d = -1$   $\mathbb{Z}[\alpha] = \mathbb{Z}[i]$   $N(x + iy) = x^2 + y^2$

$2 = 1^2 + 1^2$	$8 = 2^2 + 2^2$
$3 \times$	$9 = 3^2 + 0^2$
$4 = 2^2 + 0^2$	$10 = 3^2 + 1^2$
$5 = 2^2 + 1^2$	$11 \times$
$6 \times$	$12 \times$
$7 \times$	$13 = 3^2 + 2^2$

The answer is a corollary to the Decomposition Theorem.

**Corollary 4.16.** Assume  $\mathbb{Z}[\alpha]$  has unique factorisation and let  $n$  be a positive integer. Then the following are equivalent:

1.  $\exists A \in \mathbb{Z}[\alpha] : |N(A)| = n$
2.  $\forall$  inert primes  $p \mid n$ ,  $V_p(n)$  is even

*Proof.*

**1  $\implies$  2** Assume  $|N(A)| = n$

$$A = Q_1^{a_1} \dots Q_r^{a_r} \text{ for } Q_i \text{ irreducible in } \mathbb{Z}[\alpha]$$

$$Q_i \mid P_i \quad (p_i \text{ prime})$$

$$|N(Q_i)| = \begin{cases} P_i & \text{if } P_i \text{ splits or is ramified} \\ P_i^2 & P_i \text{ inert} \end{cases}$$

$$n = |N(A)| = \left( \prod_{\substack{P_i \text{ split} \\ \text{or ramified}}} P_i^{a_i} \right) * \left( \prod_{P_i \text{ inert}} P_i^{2a_i} \right)$$

So powers of inert primes are even.

**2**  $\implies$  **1** Let

$$n = \left( \prod_{\substack{P_i \text{ split} \\ \text{or ramified}}} P_i^{a_i} \right) * \left( \prod_{P_i \text{ inert}} P_i^{2a_i} \right)$$

Choose an element  $Q_i$  with norm  $\pm P_i$  if  $P_i$  is split or ramified:

$$n = N \left( \prod_{\substack{P_i \text{ ramified} \\ \text{or split}}} Q_i^{a_i} \times \prod_{P_i \text{ inert}} P_i \right)$$

□

**E.g** Solve  $x^2 + y^2 = 585$  i.e.  $N(x + iy) = 585$

Note  $585 = 3^2 * 5 * 13$

- 3 is inert because  $\left(\frac{-1}{3}\right) = -1$
- 5 is split because  $\left(\frac{-1}{5}\right) = +1$
- 13 is split because  $\left(\frac{-1}{13}\right) = +1$

The only inert prime factor of 585 is 3 and its power is even so  $x^2 + y^2 = 585$  will have solutions.

$$\begin{aligned} 5 &= 2^2 + 1^2 = N(2 + i) = (2 + i)(2 - i) \\ 13 &= 3^2 + 2^2 = N(3 + 2i) = (3 + 2i)(3 - 2i) \end{aligned}$$

$$\begin{aligned} 585 &= 3^2 * 5 * 13 \\ &= N(3 * (2 + i)(3 + 2i)) \\ &= N(3(6 + 7i - 2)) \\ &= N(12 + 21i) \\ &= 12^2 + 21^2 \end{aligned}$$

The other elements of norm 585 are unit multiples of it:

- $3(2+i)(3-2i) = 24 - 3i$
- $3(2-i)(3+2i) = 24 + 3i$
- $3(2-i)(3-2i) = 12 - 21i$

**E.g.**  $x^2 + xy + y^2 = 84$

Note that  $84 = 2^2 * 3 * 7$

- 2 is inert in  $\mathbb{Z}[\alpha]$
  - $3 = -(\sqrt{3})^2 = -(1 - 2\alpha)^2 \implies$  ramified
  - $7 \left( \frac{-3}{7} \right) = \left( \frac{4}{7} \right) = 1 \implies 7$  splits
- $$7 = N(2 + 2\alpha) = (2 + \alpha)(3 - \alpha)$$

So the elements with norm 84 are:

- $2(1 - 2\alpha)(2 + \alpha) * \text{unit}$
- $2(1 - 2\alpha)(3 - \alpha) * \text{unit}$

There are 6 units in this ring, therefore there are 12 solutions to  $x^2 + xy + y^2 = 84$

One possible solution is:

$$\begin{aligned} 2(1 - 2\alpha)(2 + \alpha) &= 2(2 - 3\alpha = 3\alpha^2) \\ &= 2(2 - 3\alpha - 2\alpha + 2) \\ &= 8 - 10\alpha \end{aligned}$$

so  $N(8 - 10\alpha) = 84$

**Super cool trick**

Using  $\alpha = \frac{1+\sqrt{d}}{2}$

$$\begin{aligned} \left( \alpha - \frac{1}{2} \right)^2 &= \frac{d}{4} \\ \alpha^2 - \alpha + \frac{1}{4} &= \frac{d}{4} \\ \alpha^2 &= \frac{d-1}{4} + \alpha \end{aligned}$$



#### 4.4 Continued Fractions

A finite continued fraction is  $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots \frac{1}{a_n}}}}$  where  $a_0 \in \mathbb{Z}$

and  $a_1, \dots, a_n \in \mathbb{Z} > 0$ .

We'll use the notation  $[a_0, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots \frac{1}{a_n}}}}$

$$\mathbf{E.g.} \quad [1, 2, 3, 2] = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2}}} = 1 + \frac{1}{2 + \frac{1}{7/2}} = 1 + \frac{1}{2 + \frac{2}{7}} = 1 + \frac{7}{16} = \frac{23}{16}$$

More generally if  $\alpha \in \mathbb{R}$ ,  $\alpha > 0$

$$[a_0, \dots, a_n, \alpha] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots \frac{1}{a_n + \frac{1}{\alpha}}}}}$$

and as a consequence  $[a_0, \dots, a_n] = [a_0, \dots, a_r, [a_{r+1}, \dots, a_n]]$

$$\mathbf{E.g} \quad [1, 2, 3, 2] = [1, 2, [3, 2]] = [1, 2, \frac{7}{2}] = [1, 2 + \frac{2}{7}] = [1, \frac{16}{7}] = 1 + \frac{7}{16} = \frac{23}{16}$$

Clearly every finite continued fraction is in  $\mathbb{Q}$ . Conversely if  $\frac{n}{m} \in \mathbb{Q}$ , then we can write  $\frac{n}{m}$  as a finite continued fraction.

**E.g.** By Euclid's algorithm:

$$\begin{array}{ll}
89 = 2 * 39 + 11 & 89/39 = 2 + \frac{11}{39} \\
39 = 3 * 11 + 6 & 39/11 = 3 + \frac{6}{11} \\
11 = 1 * 6 + 5 & 11/6 = 1 + \frac{5}{6} \\
6 = 1 * 5 + 1 & 6/5 = 1 + \frac{1}{5} \\
5 = 1 * 5 + 0 & 5/1 = 5
\end{array}$$

Therefore  $\frac{89}{39} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{5}}}} = [2, 3, 1, 1, 5]$

Now suppose we have a sequence  $a_n \in \mathbb{Z}$  for all  $n, a_1, a_2, \dots > 0$ . For any  $n$  we have a finite continued fraction  $[a_0, \dots, a_n] = \frac{h_n}{k_n} \in \mathbb{Q}$

We define  $[a_0, a_1, \dots] = \lim_{n \rightarrow \infty} [a_0, \dots, a_n] = \lim_{n \rightarrow \infty} \frac{h_n}{k_n}$

**Definition 4.17.**  $[a_0, a_1, \dots]$  is called an infinite continued fraction

**Theorem 4.18.** For any sequence of integers  $a_n > 0$  for  $n > 0$ , the limit  $[a_0, \dots]$  exists. If  $\alpha = [a_0, a_1, \dots]$  then  $\left| \alpha - \frac{h_n}{k_n} \right| < \frac{1}{k_n^2}$  (will be proved later)

Sometimes we can calculate infinite continued fractions.

**E.g.**  $\alpha = [1, 2, 1, 2, 1, 2, 1, 2, \dots]$  Which real number is  $\alpha$ ?

$$\begin{aligned}
\alpha &= [1, 2, \alpha] \\
&= \left[ 1, 2 + \frac{1}{\alpha} \right] \\
&= \left[ 1, \frac{2\alpha + 1}{\alpha} \right] \\
&= 1 + \frac{\alpha}{2\alpha + 1} \\
&= \frac{3\alpha + 1}{2\alpha + 1}
\end{aligned}$$

$$\begin{aligned} 2\alpha^2 + \alpha &= 3\alpha + 1 \\ 2\alpha^2 - 2\alpha - 1 &= 0 \end{aligned}$$

$$\alpha = \frac{1 \pm \sqrt{3}}{2}$$

Since  $\alpha = 1 + \frac{2}{1 + \dots} > 1$ ,  $\alpha = \frac{1 + \sqrt{3}}{2}$ .

Every infinite continued fraction converges to a real number. Conversely if  $\alpha$  is an irrational real number, then we can write  $\alpha$  as an infinite continued fraction.

**Method:** We define a sequence  $\alpha_n \in \mathbb{R}$ ,  $a_n \in \mathbb{Z}$  such that  $\alpha_0 = \alpha$  and  $a_n = \lfloor \alpha_n \rfloor$

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} > 1 \qquad a_n > 0$$

From this definition:

$$\begin{aligned} \alpha &= \alpha_0 \\ &= a_0 + \frac{a_0}{\alpha_1} \\ &= a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}} \\ &= [a_0, a_1, a_2, \alpha_3] \text{ etc} \end{aligned}$$

Using this we can show that  $\alpha = [a_0, a_1, \dots]$

**E.g.** Write  $\sqrt{2}$  as an infinite continued fraction

$$\begin{aligned} \alpha_0 &= \sqrt{2} & a_0 &= \lfloor \sqrt{2} \rfloor = 1 \\ \alpha_1 &= \frac{1}{\alpha_0 - a_0} & a_1 &= \lfloor \sqrt{2} + 1 \rfloor = 2 \\ &= \frac{1}{\sqrt{2} - 1} \\ &= \frac{\sqrt{2} + 1}{(\sqrt{2} - 1)(\sqrt{2} + 1)} \\ &= \frac{\sqrt{2} + 1}{2 - 1} \\ &= \sqrt{2} + 1 \end{aligned}$$

$$\begin{aligned}
\alpha_2 &= \frac{1}{\alpha_1 - a_1} \\
&= \frac{1}{(\sqrt{2} + 1) - 2} \\
&= \frac{1}{\sqrt{2} - 1} \\
&= \alpha_1
\end{aligned}$$

$$a_2 = \lfloor \alpha_2 \rfloor = \lfloor \alpha_1 \rfloor = 2$$

$$\begin{aligned}
\alpha_3 &= \frac{1}{\alpha_2 - a_2} \\
&= \frac{1}{\alpha_1 - a_1} \\
&= \alpha_2
\end{aligned}$$

$$a_3 = \lfloor a_1 \rfloor = 2$$

So  $\alpha_2 = \alpha_3 = \alpha_4 = \dots = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1$  and  $a_3, a_4, a_5 = 2$

Therefore  $\sqrt{2} = [a_0, a_1, a_2, \dots] = [1, 2, 2, 2, \dots]$ .

Using this method we can write  $\sqrt{d}$  for any +ve  $d$  as an infinite continued fraction.

Recall that an element in  $\mathbb{Z}[\sqrt{2}]$  is a unit if its norm is  $\pm 1$ , i.e. elements  $x + y\sqrt{2}$  where  $x^2 - 2y^2 = \pm 1$  i.e.  $\left| \left( \frac{x}{y} \right)^2 - 2 \right| = 1$  so  $\frac{x}{y}$  is close to  $\sqrt{2}$ .

Let  $\frac{h_n}{k_n} = \underbrace{[1, 2, 2, \dots, 2]}_{n \text{ terms}}$

This is close to  $\sqrt{2}$

$[1] = 1/1 = 1$	$1^2 - 2 * 1^2 = -1$
$[1, 2] = 1 + 1/2 = 3/2$	$3^2 - 2 * 2^2 = +1$
$[1, 2, 2] = 7/5$	$7^2 - 2 * 5^2 = -1$
$[1, 2, 2, 2] = 17/12$	$17^2 - 2 * 12^2 = +1$

In this case when  $\frac{h}{k} = [1, 2, \dots, 2]$ , we always have  $h^2 - 2 * k^2 = \pm 1$ , so  $h + k\sqrt{2}$  is a unit in  $\mathbb{Z}[\sqrt{2}]$

## 4.5 Pell's equation and units in real quadratic rings

Let  $d > 1$  be a square free integer. Pell's equation is  $x^2 - dy^2 = 1$ . We'll see how to find the solutions  $(x, y)$  in integers.

Let  $A = x + y\sqrt{d}$ . Pell's equation  $\leftrightarrow N(A) = 1$ . Therefore  $A$  is a unit in  $\mathbb{Z}[\sqrt{d}]$  with norm 1.

There are obvious solutions  $x = \pm 1, y = 0$ . We'll call these the trivial solutions, these correspond to the units  $A = \pm 1$

**Theorem 4.19.** *For any  $d$ , there are non-trivial solutions*

**Definition 4.20.** *The smallest solution  $(x, y)$  with  $x, y > 0$  is called the fundamental solution*

**E.g.**  $d = 2$

$x^2 - 2y^2 = 1$  and so  $(x, y) = (3, 2)$  is the fundamental solution

$A^n$  is also a unit with norm 1. This gives an infinite sequence of solutions to Pell's equations.

$$A^2 = (3 + 2\sqrt{2})^2 = 9 + 12\sqrt{2} + 8 = 17 + 12\sqrt{2}$$

$$A^3 = (3 + 2\sqrt{2})(17 + 12\sqrt{2}) = 99 + 70\sqrt{2}$$

So  $(17, 12)$  and  $(99, 70)$  are also the solutions to  $x^2 - 2y^2 = 1$

**Proposition 4.21.** *If  $(x, y)$  is the fundamental solution, then any other solution in positive integers will be  $(x_n, y_n)$  where  $(x_n + y_n\sqrt{d}) = (x + y\sqrt{d})^n$*

*Proof.* Let  $A = x + y\sqrt{d}$

$A$  is the smallest unit with norm 1 such that  $A > 1$

Let  $B$  be any unit in  $\mathbb{Z}[\sqrt{d}]$  which is bigger than 1, and has norm 1.

Want to show  $B = A^n$  for some  $n$

$$1 < A < A^2 < A^3 < \dots \rightarrow \infty$$

There exists  $n$  such that  $A^n \leq B < A^{n+1} \implies 1 \leq A^{-n}B < A$

$A^{-n}B$  is a unit with norm 1. By choice of  $A$ ,  $A^{-n}B = 1$  and  $B = A^n$  □

Once we have the fundamental solution, we've solved the equation. Sometimes the fundamental solution is big so it's difficult to find, for example:

$$d = 151 \implies x^2 - 151y^2 = 1$$

Fundamental solution  $x = 1728148040, y = 140634693$

So we need a fast way of finding the fundamental solution.

If  $\alpha \in \mathbb{R}$  and  $\alpha$  is irrational then it has an infinite continued fraction expansion.

$$\alpha = [a_0, a_1, \dots] = \lim_{n \rightarrow \infty} a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots \frac{1}{\ddots a_n}}}$$

The limit above converges to  $\sqrt{d}$  and  $[a_0, \dots, a_n]$ .

Let  $\frac{h_n}{k_n} = [a_0, \dots, a_n]$ .

**Definition 4.22.** The rational numbers  $\frac{h_n}{k_n}$  are called **convergents** of  $\alpha$

**Theorem 4.23.** If  $\frac{h}{k} \in \mathbb{Q}$  with  $\left| \alpha - \frac{h}{k} \right| < \frac{1}{2k^2}$  then  $\frac{h}{k}$  must be one of the convergents of  $\alpha$

**Corollary 4.24.** If  $(x, y)$  is a solution to Pell's equation  $x^2 - dy^2 = 1$  for  $x > y > 0$ , then  $\frac{x}{y}$  is a convergent in the continued fraction of  $\sqrt{d}$

*Proof.* (Corollary)

$$\begin{aligned} x^2 - dy^2 &= 1 \\ (x + y\sqrt{d})(x - y\sqrt{d}) &= 1 \end{aligned}$$

$$\begin{aligned} |x - y\sqrt{d}| &= \frac{1}{x + y\sqrt{d}} < \frac{1}{2y} \\ \left| \frac{x}{y} - \sqrt{d} \right| &< \frac{1}{2y^2} \end{aligned}$$

$\frac{x}{y}$  is a convergent. □

**E.g.**  $d = 7 \implies x^2 - 7y^2 = 1$

To find the fundamental solution we find  $\sqrt{7}$  as a continued fraction.

$$\begin{aligned}
\alpha_0 &= \sqrt{7} & a_n &= \lfloor \alpha_n \rfloor \\
\alpha_{n+1} &= \frac{1}{\alpha_n - a_n} \\
\alpha_1 &= \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{(\sqrt{7} - 2)(\sqrt{7} + 2)} = \frac{\sqrt{7} + 2}{3} & a_1 &= 1 \\
\alpha_2 &= \frac{1}{\frac{\sqrt{7} + 2}{3} - 1} = \frac{3}{\sqrt{7} - 1} = \frac{3(\sqrt{7} + 1)}{(\sqrt{7} - 1)(\sqrt{7} + 1)} = \frac{\sqrt{7} + 1}{2} & a_2 &= 1 \\
\alpha_3 &= \frac{1}{\frac{\sqrt{7} + 1}{2} - 1} = \frac{2}{\sqrt{7} - 1} = \frac{2(\sqrt{7} + 1)}{6} = \frac{\sqrt{7} + 1}{3} & a_3 &= 1 \\
\alpha_4 &= \frac{1}{\frac{\sqrt{7} + 1}{3} - 1} = \frac{3}{\sqrt{7} - 2} = \frac{3(\sqrt{7} + 2)}{3} = \sqrt{7} + 2 & a_4 &= 4 \\
\alpha_5 &= \frac{1}{\sqrt{7} + 2 - 4} = \frac{1}{\sqrt{7} - 2} = \alpha_1 & a_5 &= 1
\end{aligned}$$

So  $\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \dots]$

$$\begin{aligned}
[2] &= 2/1 & 2^2 - 7 * 1^2 &= -3 \\
[2, 1] &= 3/1 & 3^2 - 7 * 1^2 &= 2 \\
[2, 1, 1] &= 5/2 & 5^2 - 7 * 2^2 &= -3 \\
[2, 1, 1, 1] &= 8/3 & 8^2 - 7 * 3^2 &= 1
\end{aligned}$$

Therefore  $(8, 3)$  is fundamental solution.

**Proposition 4.25.** *If  $(x, y)$  is any solution in integers to  $x^2 - dy^2 = 1$ , with  $x > y > 0$  then  $\frac{x}{y}$  is a convergent.*

**E.g.** If  $d = 13$ , find the fundamental solution to  $x^2 - 13y^2 = 1$

We define sequences  $\alpha_n, a_n$  by  $\alpha_0 = \sqrt{d}$ ,  $a_n = \lfloor \alpha_n \rfloor$ ,  $\alpha_{n+1} = \frac{1}{\alpha_n - a_n} = \frac{1}{\alpha_n - \lfloor \alpha_n \rfloor}$

$$\alpha_0 = \sqrt{13}$$

$$a_0 = 3$$

$$\alpha_1 = \frac{1}{\sqrt{13} - 3}$$

$$a_1 = 4$$

$$= \frac{\sqrt{13} + 3}{(\sqrt{13} + 3)(\sqrt{13} - 3)}$$

$$= \frac{\sqrt{13} + 3}{4}$$

$$\alpha_2 = \frac{1}{\frac{\sqrt{13} + 3}{4} - 1}$$

$$a_2 = 1$$

$$= \frac{4}{\sqrt{13} - 1}$$

$$= \frac{4(\sqrt{13} + 1)}{(\sqrt{13} - 1)(\sqrt{13} + 1)}$$

$$= \frac{4(\sqrt{13} + 1)}{12}$$

$$= \frac{\sqrt{13} + 1}{3}$$

$$\alpha_3 = \frac{1}{\frac{\sqrt{13} + 1}{3} - 1}$$

$$a_3 = 1$$

$$= \frac{3}{\sqrt{13} - 2}$$

$$= \frac{3(\sqrt{13} + 2)}{9}$$

$$= \frac{\sqrt{13} + 2}{3}$$



$$\alpha_4 = \frac{1}{\frac{\sqrt{13}+2}{3}-1} \qquad a_4 = 1$$

$$= \frac{3}{\sqrt{13}-1}$$

$$= \frac{3(\sqrt{13}+1)}{12}$$

$$= \frac{\sqrt{13}+1}{4}$$

$$\alpha_5 = \frac{1}{\frac{\sqrt{13}+1}{4}-1} \qquad a_5 = 6$$

$$= \frac{4}{\sqrt{13}-3}$$

$$= \frac{4(\sqrt{13}+3)}{4}$$

$$= \sqrt{13}+3$$

$$\alpha_6 = \frac{1}{\sqrt{13}-3} = \alpha_1$$

$$\alpha_7 = \alpha_2 \text{ etc}$$

$$\text{So } \sqrt{13} = [3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \dots] = [3, \overline{1, 1, 1, 1, 6}]$$

$$[3] = 3/1$$

$$[3, 1] = 4/1$$

$$[3, 1, 1] = 7/2$$

$$[3, 1, 1, 1] = 11/3$$

$$[3, 1, 1, 1, 1] = 18/5$$

$$3^2 - 13 * 1^2 = -4$$

$$4^2 - 13 * 1^2 = +3$$

$$7^2 - 13 * 2^2 = -3$$

$$11^2 - 13 * 3^2 = +4$$

$$18^2 - 13 * 5^2 = -1$$

$$\begin{aligned} N(18 + 5\sqrt{13}) &= -1 \\ \implies N((18 + 5\sqrt{13})^2) &= 1 \end{aligned}$$

$$\begin{aligned} (18 + 5\sqrt{13})^2 &= 324 + 180\sqrt{13} + 325 \\ &= 649 + 180\sqrt{13} \end{aligned}$$

This means that  $649^2 - 13 * 180^2 = 1$ . If we find a unit of norm  $-1$ , before any unit of norm  $+1$ , then its square will be the fundamental solution.

In general if  $\sqrt{d} = [a_0, \overline{a_1, \dots, a_n, 2a_0}]$  and if  $[a_0, \dots, a_n] = \frac{h_n}{k_n}$  then  $h_n^2 - dk_n^2 = (-1)^{n+1}$

#### 4.5.1 Convergence of continued fractions

Let  $[a_0, a_1, \dots]$  be a continuous fraction. Then  $x_n = [a_0, \dots, a_n]$  is the  $n^{th}$  convergent. Want a formula for numerator and denominator of  $x_n$

$$x_0 = \frac{a_0}{1} \qquad x_1 = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1}$$

Define sequences of integers  $h_n, k_n$  by:

$$\begin{aligned} h_0 &= a_0 & k_0 &= 1 \\ h_1 &= a_1 a_0 + 1 & k_1 &= a_1 \\ h_n &= a_n h_{n-1} + h_{n-2} & k_n &= a_n k_{n-1} + k_{n-2} \end{aligned}$$

**Lemma 4.26.**  $x_n = \frac{h_n}{k_n}$

*Proof.* By induction on  $n$ . True for  $n = 0, 1$ .

$$\begin{aligned} x_n &= [a_0, \dots, a_n] \\ &= \left[ a_0, \dots, a_{n-1} + \frac{1}{a_n} \right] \\ &= \frac{h_{n-1}}{k_{n-1}} \end{aligned}$$

By the inductive hypothesis:

$$\begin{aligned} h'_{n-1} &= (a_{n-1} + \frac{1}{a_n})h_{n-2} + h_{n-3} \\ k'_{n-1} &= (a_{n-1} + \frac{1}{a_n})k_{n-2} + k_{n-3} \end{aligned}$$

This means that:

$$\begin{aligned}
x_n &= \frac{(a_{n-1} + \frac{1}{a_n})h_{n-2} + h_{n-3}}{(a_{n-1} + \frac{1}{a_n})k_{n-2} + k_{n-3}} \\
&= \frac{a_n a_{n-1} h_{n-2} + h_{n-2} + a_n h_{n-3}}{a_n a_{n-1} k_{n-2} + k_{n-2} + a_n k_{n-3}} \\
&= \frac{a_n \overbrace{(a_{n-1} h_{n-2} + h_{n-3})}^{h_{n-1}} + h_{n-2}}{a_n \underbrace{(a_{n-1} k_{n-2} + k_{n-3})}_{k_{n-1}} + k_{n-2}} \\
x_n &= \frac{\overbrace{a_n h_{n-1} + h_{n-2}}^{h_n}}{\underbrace{a_n k_{n-1} + k_{n-2}}_{k_n}}
\end{aligned}$$

Therefore  $x_n = \frac{h_n}{k_n}$

Since  $k_0 = 1 > 0$ ,  $k_1 = a_1 > 0$ ,  $k_n = a_n k_{n-1} + k_{n-2} > k_{n-1}$ , the denominators are an increasing sequence of positive integers.

□

**Lemma 4.27.**  $h_n$  and  $k_n$  are coprime and  $h_{n+1}k_n - h_n k_{n+1} = (-1)^n$

*Proof.* By induction on  $n$ . Check in cases  $n = 0, 1$ . Assume true for  $n - 1 > 1$  and prove for  $n$ .

$$\begin{aligned}
h_{n+1}k_n - h_n k_{n+1} &= (\overbrace{a_{n+1}h_n + h_{n-1}}^{h_{n+1}})k_n - h_n(\underbrace{a_{n+1}k_n + k_{n-1}}_{k_{n+1}}) \\
&= -(h_n k_{n-1} - h_{n-1} k_n) \\
&= -(-1)^{n-1} \\
&= (-1)^n
\end{aligned}$$

□

**Theorem 4.28.** The continued fraction  $[a_0, \dots]$  converges to a real number  $\alpha$  and

$$\left| \alpha - \frac{h_n}{k_n} \right| < \frac{1}{k_n^2}$$

**Alternating Series Test** Suppose  $y_n$  is decreasing and  $y_n \rightarrow 0$ . Then  $\sum_{n=1}^{\infty} (-1)^n y_n$  converges if  $S = \sum_{n=1}^{\infty} (-1)^n y_n$  then  $S$  is between  $\sum_{n=1}^N (-1)^n y_n$  and  $\sum_{n=1}^{N+1} (-1)^n y_n$

*Proof.* Let  $x_n = \frac{h_n}{k_n}$

$$x_{n+1} - x_n = \frac{h_{n+1}}{k_{n+1}} - \frac{h_n}{k_n} = \frac{h_{n+1}k_n - h_nk_{n+1}}{k_nk_{n+1}} = \frac{(-1)^n}{k_nk_{n+1}}$$

$$\begin{aligned} x_n &= x_0 + (x_1 - x_0) + (x_2 - x_1) + \cdots + (x_n - x_{n-1}) \\ &= x_0 + \frac{1}{k_0k_1} - \frac{1}{k_1k_2} + \frac{1}{k_2k_3} - \cdots + \frac{-1}{k_{n-1}k_n} \end{aligned}$$

Therefore  $x_n$  converges to some  $\alpha \in \mathbb{R}$  by the alternating series test. Also  $\alpha$  is between  $x_n$  and  $x_{n+1}$

$$|x_n - \alpha| < |x_n - x_{n+1}| \implies \frac{1}{k_nk_{n+1}} < \frac{1}{k_n^2}$$

□

Using the theorem we'll prove:

**Theorem 4.29.** *For any square-free  $d > 1$ , Pell's equation has non trivial solutions in integers. Equivalently, every real quadratic ring has non trivial units.*

*Proof.*  $\sqrt{d}$  has a continued fraction expansion. For any convergent  $\frac{h}{k}$  we have

$$\begin{aligned} \left| \frac{h}{k} - \sqrt{d} \right| &< \frac{1}{k^2} \\ |h - k\sqrt{d}| &< \frac{1}{k} \\ |h^2 - k^2d| &= |h + k\sqrt{d}| * |h - k\sqrt{d}| \\ &< \left| \frac{h}{k} + \sqrt{d} \right| < 2\sqrt{d} + 1 \end{aligned}$$

This shows that for the convergents  $\frac{h}{k}$  to  $\sqrt{d}$ ,  $h^2 - dk^2$  takes only finitely many values.

There exists  $n$  which can be written as  $h^2 - dk^2$  in infinitely many ways. The values of  $h$  and  $k \bmod n$  have only finitely many possibilities but we have infinitely many pairs  $(h, k)$  such that  $h^2 - dk^2 = n$

Choose two solutions  $(h, k), (h', k')$  where  $h \equiv h' \pmod{n}$  and  $k \equiv k' \pmod{n}$ .

Let  $A = \frac{h + k\sqrt{d}}{h' + k'\sqrt{d}}$ . Claim  $A$  is a unit in  $\mathbb{Z}[\sqrt{d}]$ .

Clearly  $N(A) = \frac{N(h + k\sqrt{d})}{N(h' + k'\sqrt{d})} = \frac{n}{n} = 1$ . Remains to show that  $A \in \mathbb{Z}[\sqrt{d}]$ .

$$A = \frac{h + k\sqrt{d}}{h' + k'\sqrt{d}} = \frac{(h + k\sqrt{d})(h' - k'\sqrt{d})}{h'^2 - dk'^2} = \frac{(hh' - dk k') + (kh' - hk')\sqrt{d}}{n}$$

Recall  $h = h' \pmod{n}$  and  $k = k' \pmod{n}$ .

Therefore

$$\begin{aligned} hh' - dk k' &= h^2 - dk^2 = n \equiv 0 \pmod{n} \\ kh' - hk' &\equiv kh - hk \equiv 0 \pmod{n} \end{aligned}$$

So  $A \in \mathbb{Z}[\sqrt{d}]$  and  $A$  is a unit with norm 1 in  $\mathbb{Z}[\sqrt{d}]$ . □

**Theorem 4.30.** *Let  $\alpha \in \mathbb{R}$  be irrational. If  $\frac{a}{b} \in \mathbb{Q}$  with  $\left| \frac{a}{b} - \alpha \right| < \frac{1}{2b^2}$  then  $\frac{a}{b}$  is a convergent of  $\alpha$*

In order to solve this, we will state and prove the following lemma:

**Lemma 4.31.** *Let  $\alpha$  be an irrational real number  $\frac{h_n}{k_n}$  and the  $n^{\text{th}}$  convergent of  $\alpha$ . If  $\frac{a}{b}$  is any rational number with  $b > 0$  and  $b < k_{n+1}$  and  $\frac{a}{b}$  is not a convergent then*  
 $|a - b\alpha| > |h_n - k_n\alpha|$

*Proof.* Consider these simultaneous equations:

$$\begin{aligned} h_n x + h_{n+1} y &= a \\ k_n x + k_{n+1} y &= b \end{aligned}$$

The matrix  $\begin{pmatrix} h_n & h_{n+1} \\ k_n & k_{n+1} \end{pmatrix}$  has determinant  $\pm 1$  which means the solutions of  $x, y$  are integers  
 $x, y \neq 0$  because  $\frac{a}{b} \neq \frac{h_n}{k_n}, \frac{h_{n+1}}{k_{n+1}}$ . Plug  $x = 0$  or  $y = 0$  for a contradiction.

Also  $x, y$  have opposite signs because  $b < k_{n+1}$  and  $\alpha$  is between  $\frac{h_n}{k_n}$  and  $\frac{h_{n+1}}{k_{n+1}}$ .

Therefore  $\frac{h_n}{k_n} - \alpha$  and  $\frac{h_{n+1}}{k_{n+1}} - \alpha$  have opposite signs.

Therefore  $h_n - k_n\alpha$  and  $h_{n+1} - k_{n+1}\alpha$  have opposite signs.

Therefore  $x(h_n - k_n\alpha)$  and  $y(h_{n+1} - k_{n+1}\alpha)$  have the same sign.

$$\begin{aligned} |a - b\alpha| &= |(h_n x + h_{n+1} y) - (k_n x + k_{n+1} y)\alpha| \\ &= |x(h_n - k_n\alpha) + y(h_{n+1} - k_{n+1}\alpha)| \\ &= |x| * |h_n - k_n\alpha| + |y| * |h_{n+1} - k_{n+1}\alpha| \\ &> |h_n - k_n\alpha| \end{aligned}$$

□

*Proof.* Assume  $\frac{a}{b}$  is not a convergent to  $\alpha$ , choose an  $a$  such that  $k_n \leq b < k_{n+1}$ . By the

$$\text{lemma } |h_n - k_n \alpha| < \underbrace{|a - b\alpha|}_{< \frac{1}{2b}} = |b| * \underbrace{\left| \frac{a}{b} - \alpha \right|}_{< \frac{1}{2b^2}}$$

This means that  $\left| \frac{h_n}{k_n} - \alpha \right| < \frac{1}{2bk_n}$

$$\frac{a}{b} \neq \frac{h_n}{k_n} \implies \left| \frac{a}{b} - \frac{h_n}{k_n} \right| \geq \frac{1}{bk_n}$$

$$\begin{aligned} \therefore \frac{1}{bk_n} &\leq \left| \frac{a}{b} - \frac{h_n}{k_n} \right| = \left| \left( \frac{a}{b} - \alpha \right) + \left( \alpha - \frac{h_n}{k_n} \right) \right| \underbrace{\leq}_{\frac{1}{bk_n} < \frac{1}{bk_n} \text{ } \swarrow} \frac{1}{2b^2} + \underbrace{\frac{1}{2bk_n}}_{\frac{1}{2bk_n} + \frac{1}{2bk_n} = \frac{1}{bk_n}} \\ &= \frac{1}{bk_n} \end{aligned}$$

So  $\frac{a}{b}$  must be a convergent.

□