MA3H1 Topics in Number Theory
Lecture Notes

Soma Purkait

Contents

Chapter 1. Revision 6
1. Divisibility 6
2. Rings and Ideals 7
3. Greatest Common Divisor 7
4. Primes and Irreducibles 8
5. ord_p 9

Chapter 2. The ring $\mathbb{Z}/m\mathbb{Z}$, the unit group U_m, primitive roots 11
1. Congruences 11
2. Solving Linear Diophantine equations 13
3. Primitive Roots 16

Chapter 3. Quadratic Reciprocity 18
1. Quadratic Residues and Non-Residues 18
2. Law of Quadratic Reciprocity 19
3. Mersenne Numbers 24
4. A Diophantine Equation 25

Chapter 4. Algorithms 26
1. Tonelli-Shanks 26
2. Fermat's Factorization 28
3. Quadratic Sieve 29

Chapter 5. Introduction to Public Key Cryptography 32
1. RSA 33
2. Digital Signature Using RSA 34
3. Diffie-Hellman Key Exchange 34

Chapter 6. p-adic numbers 37
1. Congruences modulo p^m 37
2. p-adic Norm on $\mathbb{Q}$ 39
3. Sequences and Series 41
4. Construction of $\mathbb{Q}_p$ and Completeness 42
5. p-adic Digit Expansion 47
6. Hensel's Lemma over $\mathbb{Z}_p$ 48
7. Hasse Principle 52

Chapter 7. Geometry of Numbers 54

1. Two Squares Theorem 54
2. Areas and Volumes 56
3. Four Squares Theorem 57
4. Proof of Minkowski's Theorem 58
5. Quadratic Forms and Hasse-Minkowski 59

Chapter 8. Irrationality and Transcendence 63
1. Irrationality 63
2. Algebraic and Transcendental Numbers 64
3. Liouville's Theorem 65

Acknowlegdements

I would like to thank Prof. Samir Siksek and Dr. Alex Bartel for their support and for providing essential resources. A part of this lecture note is based on the previously taught lecture note of Prof. Samir Siksek. I would also like to thank my students for providing several corrections to earlier versions.

CHAPTER 1

Revision

1. Divisibility

Definition. Given two $a, b \in \mathbb{Z}$, we say that a divides b if $b = an$ for some $n \in \mathbb{Z}$. We write $a \mid b$.

It is clear from the above definition that the following holds for all $a, b, c \in \mathbb{Z}$:

(1) $a \mid b$.
(2) $a \mid b \Longrightarrow a \mid bc$.
(3) $a \mid b \Longrightarrow ac \mid bc$.
(4) $a \mid b$ and $b \mid c \Longrightarrow b \mid c$.
(5) $a \mid b$ and $b \mid a \Longleftrightarrow a = \pm b$.
(6) $a \mid b$ and $a \mid c \Longrightarrow a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.
(7) $(\pm 1) \mid a$.
(8) $a \mid (\pm 1) \Longrightarrow a = \pm 1$.
(9) $a \mid b$ and $b \neq 0 \Longrightarrow |a| \leq |b|$.

Example 1.1. $8 \mid (5^{2n} + 7)$ for all $n \geq 1$.

Proof. For $n = 1$, we have $8 \mid 32 = 5^2 + 7$. Now assume that it is true for $n = k$. Then

$$5^{2(n+1)} + 7 = 5^2(5^{2n} + 7) + (7 - 5^2 7).$$

Since $8 \mid 5^2(5^{2n} + 7)$ and $8 \mid (7 - 5^2 7) = -168$, it is proved by induction. □

Theorem 1.1. *Let a, $b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q, r such that $a = qb + r$ with $0 \leq r < b$.*

Proof. *Uniqueness*: Suppose $\exists\ q, r, q', r'$ with $0 \leq r, r' < b$ such that $a = qb + r = q'b + r'$. WLOG let $r' \geq r$. Then $(q - q')b = r' - r$. Since $0 \leq r' - r < b$, we have $r' = r$ and $q' = q$.
Existence: Consider $S = \{a - xb \mid x \in \mathbb{Z} \text{ and } a - xb \geq 0\} \subseteq \mathbb{N}$. Note that $S \neq \emptyset$ since $a - (-|a|)b \geq a + |a| \geq 0$. So applying well-ordering principle we get that S has the least element say, r and $r = a - qb$ for some $q \in \mathbb{Z}$. If $r \geq b$ then $a - (q + 1)b \in S$ but $a - (q + 1)b < a - qb = r$, a contradiction to r being the least element of S. So $0 \leq r < b$. □

Corollary 1.2. *Let a, $b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique q, $r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < |b|$.*

Proof. Apply Theorem 1.1 to a and $|b| > 0$. □

2. Rings and Ideals

Definition. A *ring* R is a set together with binary operations $+$, $\cdot$ such that

(i) $(R, +)$ is an abelian group.
(ii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.
(iii) $\exists\ 1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
(iv) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$

If $a \cdot b = b \cdot a$ for all $a, b \in R$ then R is called a *commutative ring*.

Example 1.2. $(\mathbb{Z}, +, \cdot)$ is a commutative ring.

From now on we will consider only commutative rings.

Definition. A *subring* $S \subseteq R$ is a subset that is a ring under the operations coming from R.

Definition. An *ideal* I is a subring of R such that $a \cdot i \in I$ for all $a \in R$, $i \in I$. we write $I \trianglelefteq R$.

Definition. For $a_1, a_2, \ldots a_k \in R$, the *ideal generated by* $a_1, a_2, \ldots a_k$ is $\langle a_1, a_2, \ldots a_k \rangle_R = \{\sum_{i=1}^{k} r_i a_i \mid r_i \in R\}$.

Definition. An ideal $I \trianglelefteq R$ is *principal* if $I = \langle a \rangle_R$ for some $a \in R$. An integral domain is called *Principal Ideal Domain* (PID) iff every ideal of R is principal.

Theorem 1.3. $(\mathbb{Z}, +, \cdot)$ *is a* PID.

Proof. Let $I \trianglelefteq \mathbb{Z}$. If $I = \{0\}$ then nothing to prove. Suppose $I \neq \{0\}$. Let $b \in I$ be a non-zero element with the smallest absolute value. We prove that $I = \langle b \rangle$. Clearly $\langle b \rangle \subseteq I$. Let $a \in I$. Then by Corollary 1.2, $a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq |r| < b$. If $r \neq 0$ then $r = a - qb \in I$, a contradiction to minimality of $|b|$. Thus $r = 0$ and $a \in \langle b \rangle$. □

Note. 1. $I = \langle b \rangle = \langle -b \rangle$, so can always take non-negative generator.
2. It follows from Theorem 1.1 that $\mathbb{Z}$ has an Euclidean function which is given by absolute value $|\cdot| : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, so $\mathbb{Z}$ is an Euclidean domain and hence a PID.
3. Other such examples of Euclidean domains are Gaussian integers $\mathbb{Z}[i]$, polynomial rings $K[x]$ over field K.

3. Greatest Common Divisor

Theorem 1.4. *Let* $a_1, a_2, \ldots a_n \in \mathbb{Z}$. *Then there exists a unique integer* $d \geq 0$ *satisfying*

(i) $d \mid a_i$ *for all* $i = 1, 2, \cdots n$.
(ii) *If* $c \mid a_i$ *for all* $i = 1, 2, \cdots n$, *then* $c \mid d$.
(iii) $d = u_1 a_1 + u_2 a_2 + \cdots + u_n a_n$.

The integer $d \geq 0$ is called the gcd of $a_1, a_2, \ldots a_n$ and we will denoted it by either $\gcd(a_1, a_2, \ldots a_n) = d$ or simply by $(a_1, a_2, \ldots a_n) = d$

PROOF. By Theorem 1.3 and the note above, there exists a unique $d \geq 0$ such that $\langle a_1, a_2, \ldots a_n \rangle = \langle d \rangle$. □

Note. 1. $\gcd(a, b) = 1 \Leftrightarrow ax + by = 1$ for some x and $y \in \mathbb{Z}$.
2. $\gcd(a_1, a_2, \ldots a_n) = d \Leftrightarrow \gcd(\frac{a_1}{d}, \frac{a_2}{d}, \ldots \frac{a_n}{d}) = 1$.

Corollary 1.5 (Euler's Lemma)**.** *If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.*

PROOF. $\gcd(a, b) = 1 \Rightarrow ax + by = 1$ for some x, $y \in \mathbb{Z} \Rightarrow acx + bcy = c \Rightarrow a \mid c$. □

Euclid's algorithm is based on following lemma

Lemma 1.6. *If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.*

PROOF. Clearly $\gcd(a, b) \mid \gcd(b, r)$ and $\gcd(b, r) \mid \gcd(a, b)$. Hence $\gcd(a, b) = \pm\gcd(b, r)$. Since gcd is non-negative, equality follows. □

Definition. $m_1, m_2, \ldots m_n \in \mathbb{Z}$ are coprime if $\gcd(m_1, m_2, \ldots m_n) = 1$; they are called pairwise coprime if $\gcd(m_i, m_j) = 1$ for all $i \neq j$.

Lemma 1.7. *Let $m_1, m_2, \ldots m_n \in \mathbb{Z}$ be pairwise coprime such that $m_i \mid x$ for all i. Then $M \mid x$ where $M = m_1 m_2 \cdots m_n$.*

PROOF. We prove for $n = 2$, the rest follows by induction. Let $m_1 \mid x$, $m_2 \mid x$. So $x = q_1 m_1$ for some $q_1 \in \mathbb{Z}$. Since $m_2 \mid x = q_1 m_1$ and $\gcd(m_2, m_1) = 1$ by Euler's lemma, $m_2 \mid q_1$. It follows that $x = q_1 q_2 m_1 m_2$ for some $q_2 \in \mathbb{Z}$. □

4. Primes and Irreducibles

Definition. Let R be a ring, $x \in R$ is called a *unit* iff $\exists\ x' \in R$ such that $xx' = 1$. We denote by $R^\times$ the group of units of R.

Definition. $p \in R \setminus (R^\times \cup \{0\})$ is called *prime* if whenever $p \mid ab$ then $p \mid a$ or $p \mid b$.

Definition. $p \in R \setminus (R^\times \cup \{0\})$ is called *irreducible* if whenever $p = ab$ then either a or b is a unit.

Recall that a *prime number* is a natural number > 1 that has no positive divisors other than 1 and itself. So prime numbers are the irreducible elements of $\mathbb{Z}$ that are > 1. *Composites* in $\mathbb{Z}$ are integers > 1 that are not primes.

Theorem 1.8. *In $\mathbb{Z}$, prime elements and irreducible elements are the same.*

PROOF. Let p be a prime. Let $p = ab$. So $p \mid a$ or b. WLOG let $p \mid a$. Since $a \mid p$ we get $a = \pm p$. But then $p = \pm pb$ and so $b = \pm 1$. Conversely let p be irreducible. Let $p \mid ab$. If $p \mid a$ we are done. If $p \nmid a$ then since p is irreducible we get that $\gcd(a, p) = 1$. Now by Euler's lemma $p \mid b$. □

Example 1.3. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. $2 \in R$ is irreducible since if $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ then taking complex conjugation and multiplying we obtain $4 = (a^2+5b^2)(c^2+5d^2)$ which implies that either $a + b\sqrt{-5} = \pm 1$ or $c + d\sqrt{-5} = \pm 1$. Note that $R^\times = \{\pm 1\}$. 2 is not prime since $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but $2 \nmid (1 \pm \sqrt{-5})$.

Theorem 1.9 (Fundamental theorem of arithmetic(FTA))**.** *Every non-zero integer n can be written uniquely (upto re-ordering and sign) as a finite product of primes.*

Proof. If $n < 0$ then write $n = -m$ for $m > 0$. We use induction to prove the above statement for positive integers n. If $n = 1$, it is a product of empty set of primes. If n is a prime, nothing to prove. If n is composite then $n = ab$ where $1 < a, b < n$. By induction hypothesis a, b can be written as a finite product of primes and so can be n. For uniqueness, use induction again! □

Theorem 1.10. *(Euclid)There are infinitely many primes.*

5. ord_p

Definition. For a prime p and $n \in \mathbb{Z} \setminus \{0\}$ define $\mathrm{ord}_p(n) = e$ if $p^e \| n$. Define $\mathrm{ord}_p(0) = \infty$.

Extend ord_p to $\mathbb{Q}$ by defining $\mathrm{ord}_p(\frac{a}{b}) = \mathrm{ord}_p(a) - ord_p(b)$. We can rephrase Theorem 1.9 as

Theorem 1.11 (FTA)**.** *For $\alpha \in \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\alpha = \pm \prod_{p \in \mathbb{P}} p^{\mathrm{ord}_p(\alpha)}$ where $\mathbb{P}$ denotes set of primes.*

Proof. Use Theorem 1.9 and $\mathrm{ord}_p(p^n) = n$. □

Corollary 1.12.

(i) $\alpha = \pm\beta \iff \mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta)$ *for all* $p \in \mathbb{P}$.
(ii) $\alpha \in \mathbb{Q}^\times$ *is square* $\iff \mathrm{ord}_p(\alpha)$ *is even for all* $p \in \mathbb{P}$.
(iii) *If* $\alpha \in \mathbb{Q}^\times$, *then* $\alpha = p^{\mathrm{ord}_p(\alpha)} \frac{u}{v}$ *where* $p \nmid u, v$.

Proof. **Exercise** (use FTA). □

Theorem 1.13 (Properties of ord_p)**.** *Let $\alpha, \beta \in \mathbb{Q}$. Then*

(i) $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$.
(ii) $\mathrm{ord}_p(\alpha + \beta) \geq min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\}$ *with equality if* $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$.

Note: the statement (ii) is not iff statement.

Proof. If either of α, β is zero then it clearly holds. Assume that $\alpha, \beta \in \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$. Then by Corollary 1.12,

$$\alpha = p^m \frac{a}{b} \qquad \text{and} \qquad \beta = p^n \frac{c}{d},$$

where $p \nmid a, b, c, d$ and $\mathrm{ord}_p(\alpha) = m$ and $\mathrm{ord}_p(\beta) = n$.
(i) Clearly $\mathrm{ord}_p(\alpha, \beta) = m + n$.
(ii) WLOG assume that $m \leq n$. We have

$$\alpha + \beta = p^m \frac{a}{b} + p^n \frac{c}{d} = p^m \left(\frac{a}{b} + p^{n-m} \frac{c}{d} \right) = p^m \left(\frac{ad + p^{n-m} c}{bd} \right).$$

Since $n \geq m$ we can write $ad + p^{n-m} c = p^t e$ where $t \geq 0$ and $\gcd(p, e) = 1$. Therefore

$$\alpha + \beta = p^{m+t} \frac{e}{bd} \qquad \text{where } p \nmid e, b, d,$$

and so $\mathrm{ord}_p(\alpha + \beta) = m + t \geq m = \min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\}$.

For the second part, suppose $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$. WLOG assume that $m < n$, i.e. $n - m \geq 1$. If $p \mid (ad + p^{n-m} c)$ then $p \mid ad$, a contradiction. Hence $t = 0$ in the above arguments and so $\mathrm{ord}_p(\alpha + \beta) = m = \min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\}$. $\square$

CHAPTER 2

The ring $\mathbb{Z}/m\mathbb{Z}$, the unit group U_m, primitive roots

1. Congruences

Definition. Let $a, b \in \mathbb{Z}$ and m be a positive integer. We say that a *is congruent to* b *modulo* m iff $m \mid (a-b)$. We write $a \equiv b \pmod{m}$.

It is easy to see that for $m \geq 1$, "congruence modulo m" denoted by $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

(i) *reflexive*: $a \equiv a \pmod{m}$ for all $a \in \mathbb{Z}$.
(ii) *symmetric*: If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.
(iii) *transitive*: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

By Theorem 1.1 given an integer a, we can write $a = qm + r$ for unique $q, r \in \mathbb{Z}$ with $0 \geq r < m$, i.e., $a \equiv r \pmod{m}$. Hence every integer is congruent modulo m to precisely one of $0, 1, \ldots m-1$. Thus the equivalence classes under the relation $\equiv_m$ can be represented precisely by the remainders $0, 1, \ldots m-1$.

Lemma 2.1 (Properties of $\equiv_m$)**.**

(a) *If* $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, *then* $a + b \equiv c + d \pmod{m}$, $ac \equiv bd \pmod{m}$.
(b) *If* $a \equiv b \pmod{m}$ *then* $a \equiv b \pmod{d}$ *for all divisor* $d \mid m$.
(c) *If* $a \equiv b \pmod{m}$ *then* $ac \equiv bc \pmod{m}$ *for all* $c \in \mathbb{Z}$.
(d) *If* $a \equiv b \pmod{m}$ *then* $\gcd(a, m) = \gcd(b, m)$ *(Euclid's algorithm).*
(e) *If* $ac \equiv bc \pmod{m}$ *then* $a \equiv b \pmod{\frac{m}{\gcd(m,c)}}$*; in particular if* $ac \equiv bc \pmod{m}$ *and* $\gcd(m, c) = 1$ *then* $a \equiv b \pmod{m}$.

Proof. (a), (b), (c) follow from properties of $\equiv_m$ and divisibility. (d) is Lemma 1.6. For (e), since $ac \equiv bc \pmod{m}$, we have $m \mid (ac - bc)$. Let $\gcd(m, c) = d$. Then $ac - bc = mt$ for some $t \in \mathbb{Z}$, so $\frac{ac}{d} - \frac{bc}{d} = \frac{m}{d}t$. Hence $\frac{m}{d} \mid \frac{c}{d}(a-b)$. Since $\gcd(\frac{m}{d}, \frac{c}{d}) = 1$, by Euler's lemma $\frac{m}{d} \mid (a-b)$. Hence $a \equiv b \pmod{\frac{m}{d}}$. □

Note that in (d), we cannot do cancellation unless $\gcd(m, c) = 1$.

Example 2.1. $8 \equiv 0 \pmod{8}$ but $4 \not\equiv 0 \pmod{8}$.

Definition. A *complete residue system (CRS) modulo* m is a set of m integers $\{a_1, a_2, \ldots a_m\}$ such that $a_i \not\equiv a_j \pmod{m}$ whenever $i \neq j$.

Example 2.2. The set of all remainders $\{0, 1, \ldots m-1\}$ after division by m.

It is easy to check that:

- If $\{a_1, a_2, \ldots a_m\}$ is CRS modulo m, then any integer is congruent to precisely one of a_i modulo m.
- If $\{a_1, a_2, \ldots a_m\}$ is CRS modulo m, then so is $\{x + ca_1,\ x + ca_2,\ \ldots,\ x + ca_m\}$ where $x, c \in \mathbb{Z}$ and $\gcd(c, m) = 1$.

Definition. Let $\mathbb{Z}/m\mathbb{Z}$ be the set of equivalence classes under $\equiv_m$,

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Define $+$ and $\cdot$ on $\mathbb{Z}/m\mathbb{Z}$ as follows:

$$\begin{aligned} [a]_m + [b]_m &:= [a+b]_m \\ [a]_m \cdot [b]_m &:= [ab]_m. \end{aligned}$$

Then check that $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring under $+$ and $\cdot$ as defined above and $[0]_m$ is the additive identity, $[1]_m$ is the multiplicative identity.

The next lemma gives a criterion for existence of inverse modulo m

Lemma 2.2. *Suppose $a, m \in \mathbb{Z}$ with $m \geq 1$. Then $\exists\ b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$ iff $\gcd(a, m) = 1$.*

Proof. $\gcd(a, m) = 1 \Leftrightarrow \exists\ b, c \in \mathbb{Z}$ such that $ab + mc = 1 \Leftrightarrow ab \equiv 1 \pmod{m}$. □

Hence $[a]_m$ is invertible (i.e. $\exists\ b \in \mathbb{Z}$ such that $[a]_m \cdot [b]_m = [ab]_m = [1]_m$) $\Longleftrightarrow \gcd(a, m) = 1$. Thus the *group of units modulo m* is

$$U_m := (\mathbb{Z}/m\mathbb{Z})^\times = \{[a]_m \in \mathbb{Z}/m\mathbb{Z} \mid gcd(a, m) = 1\}.$$

One can use Euclid's algorithm to compute an inverse modulo m.

Remark. For a prime p, $\mathbb{Z}/p\mathbb{Z} = \{[0]_p, [1]_p, \ldots, [p-1]_p\}$ is a commutative ring under $+$ and $\cdot$ defined above. Further $[a]_p$ is invertible iff $p \nmid a$, so every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is invertible. Hence $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field.

Definition. The *Euler's totient* φ is a function $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ defined by

$$\begin{aligned} \varphi(m) &= \#U_m = \#\{[a]_m \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\} \\ &= \#\{a \mid 0 \leq a < m \text{ and } \gcd(a, m) = 1\}. \end{aligned}$$

Definition. A *reduced residue system (RRS) modulo m* is a set of $\varphi(m)$ integers $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ such that $\gcd(a_i, m) = 1$ for all i and $a_i \not\equiv a_j \pmod{m}$ whenever $i \neq j$.

If $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ is RRS modulo m then so is $\{ca_1, ca_2, \ldots, ca_{\varphi(m)}\}$ whenever $\gcd(c, m) = 1$.

2. Solving Linear Diophantine equations

Lemma 2.3. *Let $a, b \in \mathbb{Z}$. Then*

(i) $\exists\ x_0 \in \mathbb{Z}$ *such that* $ax_0 \equiv b \pmod{m} \iff \gcd(a, m) \mid b$.
(ii) *If* $\gcd(a, m) \mid b$, *then* $\#\{[x]_m \in \mathbb{Z}/m\mathbb{Z} \mid ax \equiv b \pmod{m}\} = \gcd(a, m)$.

Proof. (i) $\exists\ x_0 \in \mathbb{Z}$ such that $ax_0 \equiv b \pmod{m} \iff \exists\ x_0, y_0 \in \mathbb{Z}$ such that $ax_0 - my_0 = b \iff \gcd(a, m) \mid b$.
(ii) Let $\gcd(a, m) = d$ and $d \mid b$. Then $b = ax_0 - my_0$ for some $x_0, y_0 \in \mathbb{Z}$. For any solution $x, y \in \mathbb{Z}$ we have $ax - my = b = ax_0 - my_0 \iff \frac{a}{d}(x - x_0) = \frac{m}{d}(y - y_0) \iff x = x_0 + \frac{m}{d}t$ and $y = y_0 + \frac{a}{d}t$ for some $t \in \mathbb{Z}$ (the last $\Leftrightarrow$ follows by Euler's lemma again as $\gcd(\frac{a}{d}, \frac{m}{d}) = 1$). Hence

$$\begin{aligned}
&\#\{[x]_m \in \mathbb{Z}/m\mathbb{Z} \mid ax \equiv b \pmod{m}\} \\
&= \#\{[x_0]_m + [\frac{mt}{d}]_m \in \mathbb{Z}/m\mathbb{Z} \mid ax_0 \equiv b \pmod{m},\ \ t \in \mathbb{Z}\} \\
&= \#\{t \in \mathbb{Z} \mid 0 \leq \frac{mt}{d} < m\} = d.
\end{aligned}$$

□

Theorem 2.4 (Chinese Remainder Theorem)**.** *Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and let $m_1, m_2, \ldots, m_n$ be pairwise coprime positive integers. Let $M = \prod_{i=1}^{n} m_i$. Then there exists a unique $[x]_M \in \mathbb{Z}/M\mathbb{Z}$ such that $x \equiv a_i \pmod{m_i}$ for all $i = 1, 2, \ldots n$.*

Proof 1. Consider the map

$$\begin{aligned}
\theta : \mathbb{Z}/M\mathbb{Z} &\longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \\
[a]_M &\longrightarrow ([a]_{m_1}, [a]_{m_2}, \ldots, [a]_{m_n}).
\end{aligned}$$

Note θ is a well-defined map since $[a]_M = [b]_M \Rightarrow a \equiv b \pmod{M} \Rightarrow a \equiv b \pmod{m_i}\ \forall\ i \Rightarrow [a]_{m_i} = [b]_{m_i}\ \forall\ i$. Check that θ is a ring homomorphism (i.e. $\theta([a+b]_M) = \theta([a]_M) + \theta([b]_M)$ and $\theta([ab]_M) = \theta([a]_M) \cdot \theta([b]_M)$ for all $[a]_M, [b]_M \in \mathbb{Z}/M\mathbb{Z}$ and $\theta([1]_M) = ([1]_{m_1}, \cdots [1]_{m_n})$. We first see that θ is injective since

$$\begin{aligned}
[x]_M \in \ker(\theta) &\iff [x]_{m_i} = [0]_{m_i} \text{ for all } i \\
&\iff x \equiv 0 \pmod{m_i} \text{ for all } i \\
&\iff m_i \mid x \text{ for all } i \\
&\iff M \mid x \text{ (since } m_i \text{ are pairwise coprime)} \\
&\iff [x]_M = [0]_M,
\end{aligned}$$

Hence

$$\begin{aligned}
M = \#\mathbb{Z}/M\mathbb{Z} = \#\mathrm{im}(\mathbb{Z}/M\mathbb{Z}) &\leq \#(\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}) \\
&= m_1 m_2 \cdots m_n = M.
\end{aligned}$$

Thus θ is injective and surjective and therefore a ring isomorphism. This gives CRT as follows:

Given $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, consider $([a]_{m_1}, [a]_{m_2}, \ldots, [a]_{m_n}) \in \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$. Since θ is an isomorphism, there exists a unique $[x]_M \in \mathbb{Z}/M\mathbb{Z}$ such that $[x]_{m_i} = [a_i]_{m_i}$ for all $i = 1, 2, \ldots, n$. □

This is existensial proof. Let us look at a constructive proof.

PROOF 2. Let $M_i = \prod_{j \neq i} m_j$. Since m_i's are pairwise coprime, we have $\gcd(M_i, m_i) = 1$ and so $\exists\ x_i \in \mathbb{Z}$ such that $M_i x_i \equiv 1 \pmod{m_i}$. Note that $M_i x_i \equiv 0 \pmod{m_j}$ for all $j \neq i$. Define

$$x = \sum_{i=1}^{n} a_i (M_i x_i),$$

then $x \equiv a_i \pmod{m_i}$ for all $i = 1, 2, \ldots, n$. If y is any other integer satisfying the congruence, then $y \equiv a_i \equiv x \pmod{m_i}$ for all i. So $m_i \mid (x-y)$ for all i which implies that $M \mid (x - y)$. Hence $x \equiv y \pmod{M}$. So $[x]_M \in \mathbb{Z}/M\mathbb{Z}$ is a unique such element. □

Corollary 2.5. *If* $\gcd(m, n) = 1$ *then* $\varphi(mn) = \varphi(m)\varphi(n)$.

PROOF 1. By CRT, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. So the unit groups are isomorphic, i.e., $U_{mn} \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \cong U_m \times U_n$. So we are done.
□

PROOF 2. Note that $\varphi(mn)$ is the number of positive integers less than mn that are coprime to m and n. Write $\{1, 2, \ldots mn\}$ as follows:

$$\begin{array}{ccccccc}
1 & m+1 & \cdots & (j-1)m+1 & \cdots & (n-1)m+1 \\
\vdots & \vdots & & \vdots & & \vdots \\
i & m+i & \cdots & (j-1)m+i & \cdots & (n-1)m+i \\
\vdots & \vdots & & \vdots & & \vdots \\
m & 2m & \cdots & jm & \cdots & nm
\end{array}$$

For each i where $1 \leq i \leq m$ we have $\gcd(i, m) = 1 \Leftrightarrow \gcd((j-1)m + i, m) = 1$ for all $1 \leq j \leq n$. So to choose elements that are coprime to m and n, need to only look at ith row such that $\gcd(i, m) = 1$. There are $\varphi(m)$ such rows.

Since $\gcd(m, n) = 1$, each such row is CRS modulo n and hence has precisely $\varphi(n)$ elements coprime to n. Hence we are done. □

Lemma 2.6. *If* p *is prime, then* $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

PROOF.

$$\begin{aligned}\varphi(p^r) &= \#\{m \mid 0 \le m < p^r \text{ and } \gcd(m, p^r) = 1\} \\ &= \#\{m \mid 0 \le m < p^r \text{ and } \gcd(m, p) = 1\} \\ &= \#(\mathbb{Z}/p^r\mathbb{Z}) - \#\{m \mid 0 \le m < p^r \text{ and } p \mid m\} \\ &= \#(\mathbb{Z}/p^r\mathbb{Z}) - \#\{pt \mid t \in \mathbb{Z} \text{ and } 0 \le pt < p^r\} \\ &= p^r - p^{r-1}.\end{aligned}$$

□

Corollary 2.7. *If $m = \prod_{i=1}^n p_i^{r_i}$, then $\varphi(m) = \prod_{i=1}^n p_i^{r_i-1}(p_i - 1)$.*

PROOF. Follows from Corollary 2.5 and Lemma 2.6. □

Corollary 2.8. *For any $n \in \mathbb{N}$, $\sum_{d|n} \varphi(d) = n$.*

PROOF. Partition $\{1, 2, \ldots, n\}$ into subsets as follows:

$$\begin{aligned}\{1, 2, \ldots, n\} &= \bigsqcup_{d|n} \{a \in \{1, 2, \ldots, n\} \mid \gcd(a, n) = d\} \\ &= \bigsqcup_{d|n} \{a \in \{1, 2, \ldots, n\} \mid a = da',\ \gcd(a', \frac{n}{d}) = 1\} \\ &= \bigsqcup_{d|n} \{a' \in \{1, 2, \ldots, \frac{n}{d}\} \mid \gcd(a', \frac{n}{d}) = 1\}\}.\end{aligned}$$

Hence $n = \#\text{LHS} = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$. □

Before moving further let us recall some basic facts from group theory that will be useful.

Lemma 2.9. *Let $(G, \cdot)$ be a group. Let $a \in G$.*

(i) *If order of a is d and $a^e = 1$ then $d \mid e$.*
(ii) *If order of a is d then order of a^h is $\frac{d}{\gcd(h,d)}$.*
(iii) *Let G be abelian group and $a, b \in G$ with orders m, n respectively. If $\gcd(m, n) = 1$ then order of ab is mn.*
(iv) (Lagrange's Theorem) *If G is a finite group and $H \le G$ is a subgroup then $\#H \mid \#G$. In particular if $a \in G$ and order of a is d then $d \mid \#G$.*
(v) *If $\#G$ is n and a is an element of order n then $G = \langle a \rangle$ is a cyclic group.*
(vi) *If G is cyclic group of order n, say $G = \langle a \rangle$, then for every divisor $d \mid n$, there are exactly $\varphi(d)$ elements of order d, namely*

$$\{a^{\frac{kn}{d}} \mid 0 \le k < d \text{ and } \gcd(k, d) = 1\}.$$

PROOF. **Exercise**. For (vi) use Corollary 2.8. □

Theorem 2.10 (Euler's Theorem)**.** *If a is coprime to m then $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

PROOF. If $\gcd(a,m)=1$ then $[a]_m \in U_m$. Since $\#U_m = \varphi(m)$, applying Lagrange's Theorem (Lemma 2.9 (iv)) to $[a]_m$ we have $[a]_m^{\varphi(m)} = [1]_m$, i.e., $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Theorem 2.11 (Fermat's Little Theorem (FLT))**.** *Let p be a prime and $a \in \mathbb{Z}$. Then*

$$a^{p-1} \equiv 1 \pmod{p} \qquad \text{if } p \nmid a.$$

Further,

$$a^p \equiv a \pmod{p} \qquad \text{for any } a \in \mathbb{Z}.$$

PROOF. Take $m = p$ in Theorem 2.10. Since $\varphi(p) = p-1$, we have $a^{p-1} \equiv 1 \pmod{p}$ for all $a \in \mathbb{Z}$ such that $\gcd(a,p)=1$. Multiply a on both sides to get the second statement. □

3. Primitive Roots

Definition. Let $m \in \mathbb{Z}$ such that $m \geq 1$. Let $a \in \mathbb{Z}$ such that $\gcd(a,m)=1$, then we define the *order of a modulo m* to be the order of $[a]_m$ in U_m.

Definition. Let $a \in \mathbb{Z}$ such that $\gcd(a,m)=1$. Then $a \in \mathbb{Z}$ is a *primitive root modulo m* if a has order $\varphi(m)$ modulo m.

Note. It follows by applying Lemma 2.9 (ii),(v),(vi) to the unit group U_m that
(i) A primitive root modulo m exists iff U_m is cyclic.
(ii) If a is a primitive root modulo m, then so is a^h if $\gcd(h,\varphi(m))=1$. There are precisely $\varphi(\varphi(m))$ distinct primitive roots modulo m in U_m.

Theorem 2.12 (Lagrange's Theorem)**.** *Let p be a prime and let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}/p\mathbb{Z}[x]$ be a non-zero polynomial of degree n (i.e., $p \nmid a_n$). Then $f(x) \equiv 0 \pmod{p}$ has at most n solutions in $\mathbb{Z}/p\mathbb{Z}$.*

PROOF. We prove it by induction. For $n=1$, $f(x) = a_1x + a_0$ such that $p \nmid a_1$. By Lemma 2.3(ii), $f(x)$ has exactly one solution in $\mathbb{Z}/p\mathbb{Z}$.

Assume true for $n=k$. Let $f(x) = \sum_{i=0}^{k+1} a_i x^i$ such that $p \nmid a_{k+1}$. If $f(x)$ has no solutions in $\mathbb{Z}/p\mathbb{Z}$, then we are done. Otherwise let $[r]_p \in \mathbb{Z}/p\mathbb{Z}$ such that $f(r) \equiv 0 \pmod{p}$. So

$$\begin{aligned} f(x) = f(x) - f(r) &= \sum_{i=0}^{k+1} a_i (x^i - r^i) \\ &= \sum_{i=1}^{k+1} a_i (x-r) \left(\sum_{j=0}^{i-1} x^{i-1-j} r^j \right) \\ &= (x-r) \sum_{i=1}^{k+1} a_i \left(\sum_{j=0}^{i-1} x^{i-1-j} r^j \right) \\ &= (x-r) g(x), \end{aligned}$$

where $\deg(g) = k$. By induction hypothesis, g has at most k solutions in $\mathbb{Z}/p\mathbb{Z}$. Since $x-r$ has precisely one solution in $\mathbb{Z}/p\mathbb{Z}$, $f(x)$ has at most $k+1$ solutions in $\mathbb{Z}/p\mathbb{Z}$. □

Remark. Same proof works if we take f to be a polynomial in $K[x]$ for any field K instead of $\mathbb{Z}/p\mathbb{Z}$.

Example 2.3. Above theorem does not hold over a ring that is not a field. Let $R = (\mathbb{Z}/8\mathbb{Z}, +, \cdot)$. Then the polynomial $x^2 - 1$ in $\mathbb{Z}/8\mathbb{Z}[x]$ has four roots in $\mathbb{Z}/8\mathbb{Z}$, namely $[1]_8, [3]_8, [5]_8$ and $[7]_8$. Note that $x^2 - 1 \equiv (x-1)(x-7) \equiv (x-3)(x-5) \pmod 8$.

Corollary 2.13. *Let p be a prime and let $d \geq 1$ such that $d \mid (p-1)$. Then $x^d \equiv 1 \pmod p$ has distinct d solutions in $\mathbb{Z}/p\mathbb{Z}$.*

PROOF. Since $d \mid (p-1)$, we have $p - 1 = kd$ for some $k \geq 1$. So

$$x^{p-1} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \cdots + 1).$$

Note that $x^{p-1} - 1$ has precisely $p-1$ distinct solutions in $\mathbb{Z}/p\mathbb{Z}$, namely $1, 2, \ldots, p-1$ by Fermat's little theorem. Also by Lagrange's theorem $x^{d(k-1)} + x^{d(k-2)} + \cdots + 1$ has at most $d(k-1) = p - 1 - d$ solutions. Hence $x^d - 1$ has at least d distinct solutions, so applying Lagrange's theorem again we see that $x^d - 1$ has precisely d distinct solutions in $\mathbb{Z}/p\mathbb{Z}$. □

Theorem 2.14. *If p is a prime then there exists a primitive root modulo p.*

PROOF. We want to find an integer a coprime to p such that a has order $p-1$ modulo p. One can write $p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$ where q_i are distinct primes. For each i, by Corollary 2.13, $x^{q_i^{e_i}} \equiv 1 \pmod p$ has exactly $q_i^{e_i}$ distinct solutions in $\mathbb{Z}/p\mathbb{Z}$ and $x^{q_i^{e_i-1}} \equiv 1 \pmod p$ has exactly $q_i^{e_i-1}$ distinct solutions in $\mathbb{Z}/p\mathbb{Z}$. Therefore there exist $a_i \in \mathbb{Z}$ such that ${a_i}^{q_i^{e_i}} \equiv 1 \pmod p$ but ${a_i}^{q_i^{e_i-1}} \not\equiv 1 \pmod p$, i.e., order of $[a_i]_p$ is $q_i^{e_i}$. Take $a = a_1 a_2 . \cdots a_r$. Then by applying Lemma 2.9(iii) to U_p we get that order of $[a]_p$ is $p-1$. □

Corollary 2.15.

(i) *U_p is a cyclic group of order $p-1$.*
(ii) *There are precisely $\varphi(p-1)$ distinct primitive roots modulo p.*

Theorem 2.16. *If F is a field and G is a finite subgroup of $F \setminus \{0\}$. Then G is a cyclic group.*

PROOF. Proof is similar to the proof of Theorem 2.14, essentially using Lagrange's Theorem 2.12 for general fields. □

CHAPTER 3

Quadratic Reciprocity

1. Quadratic Residues and Non-Residues

Definition. Let $\gcd(a, m) = 1$. We say that a is a *quadratic residue* modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution. Otherwise we say that a is a *quadratic non-residue* modulo m.

Example 3.1. Note that

$$1^2 \equiv 6^2 \equiv 1, \quad 2^2 \equiv 5^2 \equiv 4, \quad 3^2 \equiv 4^2 \equiv 2 \pmod{7}.$$

Hence the quadratic residues modulo 7 are 1, 2 and 4. The quadratic non-residues modulo 7 are 3, 5 and 6.

We will focus on quadratic residues modulo primes and return to quadratic residues modulo arbitrary positive integers later.

Lemma 3.1. *Let p be an odd prime and let g be a primitive root modulo p.*

- *The quadratic residues modulo p are of the form g^r where $0 \leq r \leq p-2$ and r is even.*
- *The quadratic non-residues are of the form g^r where $0 \leq r \leq p-2$ and r is odd.*

In particular, exactly half the non-zero residues are quadratic residues modulo p and the other half are quadratic non-residues.

Proof. Let g be a primitive root modulo p. Modulo p, the integers $1 \leq a \leq p-1$ are a rearrangement of the integers $1, g, \ldots, g^{p-2}$, since both lists are reduced residue systems. Note that g^r is certainly a quadratic residue modulo p for all even integers r. Let us prove the converse. Suppose that $g^r \equiv x^2 \pmod{p}$. Then we can write $x \equiv g^s \pmod{p}$ for some $0 \leq s \leq p-2$. Thus $g^{r-2s} \equiv 1 \pmod{p}$. As g is a primitive root, $p-1$ divides $r-2s$. But $p-1$ is even so $r-2s$ is even and so r is even. Thus we know that g^r is a quadratic residue modulo p if and only if r is even. Hence the quadratic residues modulo p are $1, g^2, g^4, \ldots, g^{p-3}$ and the quadratic non-residues are $g, g^3, g^5, \ldots, g^{p-2}$. This proves the lemma. □

Lemma 3.2. *Let p be an odd prime and g a primitive root modulo p. Then*

$$g^{(p-1)/2} \equiv -1 \pmod{p}.$$

Proof. Let $h = g^{(p-1)/2}$. Then $h^2 = g^{p-1} \equiv 1 \pmod{p}$. So $p \mid (h^2 - 1) = (h+1)(h-1)$. Hence $h \equiv \pm 1 \pmod{p}$. If $h \equiv 1 \pmod{p}$ then

$g^{(p-1)/2} \equiv 1 \pmod{p}$ contradicting the fact that the order of g (a primitive root) is exactly $p-1$. Hence $h \equiv -1 \pmod{p}$ which is what we want. □

Definition. Let p be an odd prime. Let

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 & \text{if } p \mid a. \end{cases}$$

The symbol $\left(\frac{a}{p}\right)$ is called a *Legendre symbol*.

The Legendre symbol is extremely convenient for discussing quadratic residues.

Example 3.2. From earlier example we have

$$\left(\frac{0}{7}\right) = 0, \qquad \left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1,$$

and

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Proposition 3.3. *Let p be an odd prime, and a, b integers.*

(i) *If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(ii) (Euler's Criterion) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

(iii) *For integers a, b we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Proof. (i) follows straightaway from the definition, and (iii) follows from (ii). Let's prove (ii). Let a be an integer. If $p \mid a$ then

$$\left(\frac{a}{p}\right) = 0 \equiv a^{(p-1)/2} \pmod{p}.$$

Hence suppose that $p \nmid a$. Let g be a primitive root modulo p. We know from Lemma 3.1 that $a \equiv g^r \pmod{p}$ for some $0 \leq r \leq p-2$ and that r is even if and only if a is a quadratic residue. Hence

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

by Lemma 3.2. This proves (ii). □

2. Law of Quadratic Reciprocity

The main theorem on quadratic reciprocity is the Law of Quadratic Reciprocity.

Theorem 3.4. *Let p and q be distinct odd primes. Then*

(a) (Law of Quadratic Reciprocity) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$.

(b) (First Supplement to the Law of Quadratic Reciprocity)
$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(c) (Second Supplement to the Law of Quadratic Reciprocity)
$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Remark. Note that we can rephrase the Law of Quadratic Reciprocity as follows:
$$\begin{cases} \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4 \end{cases}$$

Example 3.3. Is 94 a square modulo 257? One way to decide this is to run through the integers $x = 0, 1, \ldots, 256$ and see if $94 \equiv x^2 \pmod{257}$. It is much quicker to use Proposition 3.3 and the Law of Quadratic Reciprocity.

$$\begin{aligned}
\left(\frac{94}{257}\right) &= \left(\frac{2}{257}\right)\left(\frac{47}{257}\right) && \text{by Proposition 3.3} \\
&= \left(\frac{47}{257}\right) && \text{using the second supplement} \\
&= \left(\frac{257}{47}\right) && \text{since } 257 \equiv 1 \pmod 4 \\
&= \left(\frac{22}{47}\right) && 257 \equiv 22 \pmod{47} \\
&= \left(\frac{2}{47}\right)\left(\frac{11}{47}\right) \\
&= \left(\frac{11}{47}\right) && \text{using the second supplement} \\
&= -\left(\frac{47}{11}\right) && 11 \equiv 47 \equiv 3 \pmod 4 \\
&= -\left(\frac{3}{11}\right) \\
&= \left(\frac{11}{3}\right) && 3 \equiv 11 \equiv 3 \pmod 4 \\
&= \left(\frac{2}{3}\right) && 11 \equiv 2 \pmod 3 \\
&= -1 && \text{using the second supplement.}
\end{aligned}$$

Hence 94 is not a square modulo 47.

Exercise. Is 1729 a square modulo 2011?
The proof of the first supplement is straightforward.

Proof of the First Supplement. By Euler's Criterion,

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

Thus $\left(\frac{-1}{p}\right) = 1$ if and only if $(p-1)/2$ is even. This is the case if and only if $p \equiv 1 \pmod 4$. □

To prove the Law of Quadratic Reciprocity we need Gauss' Lemma.

Theorem 3.5 (Gauss' Lemma)**.** *Let p be an odd prime and write*

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

For integer n let $\widehat{n}$ be the unique integer satisfying $\widehat{n} \equiv n \pmod p$ and $-p/2 < \widehat{n} < p/2$. Let $p \nmid a$ and let

$$\widehat{aS} = \{\widehat{as} : s \in S\}.$$

Define $\mu(a)$ to be the number of **negative** *members of the set $\widehat{aS}$. Then*

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

Example 3.4. Let us determine $\left(\frac{3}{11}\right)$ using Gauss' Lemma. Note that

$$S = \{1, 2, 3, 4, 5\}$$

and

$$\widehat{3S} = \{\widehat{3}, \widehat{6}, \widehat{9}, \widehat{12}, \widehat{15}\} = \{3, -5, -2, 1, 4\}.$$

Thus $\mu(3) = 2$ and so $\left(\frac{3}{11}\right) = 1$.

Proof of Gauss' Lemma. We will show that $(-1)^{\mu(a)} a^{(p-1)/2} \equiv 1 \pmod p$. Gauss' Lemma will then follow from Euler's Criterion.

By definition, $\mu(a)$ is the number of negative elements in $\widehat{aS}$. Let $|\widehat{aS}| = \{|\widehat{as}| : s \in S\}$. We claim that $|\widehat{aS}| = S$. Let's assume this for the moment and use it to complete the proof. We will return to prove the claim later on.

Now

$$\begin{aligned}
\prod_{s\in S} s &= \prod_{t\in|\widehat{aS}|} t && \text{as } S = |\widehat{aS}| \\
&= \prod_{s\in S} |\widehat{as}| && \text{by definition of } |\widehat{aS}| \\
&= (-1)^{\mu(a)} \prod_{s\in S} \widehat{as} && \widehat{as} = -|\widehat{as}| \text{ for precisely } \mu(a) \text{ values of } s\in S \\
&\equiv (-1)^{\mu(a)} \prod_{s\in S} as && \text{since } as \equiv \widehat{as} \pmod p \\
&\equiv (-1)^{\mu(a)} a^{(p-1)/2} \prod_{s\in S} s \pmod p && \text{since } \#S = (p-1)/2.
\end{aligned}$$

Cancelling $\prod_{s\in S} s$ we obtain the desired conclusion that $(-1)^{\mu(a)} a^{(p-1)/2} \equiv 1 \pmod p$.

It remains to prove our claim that $|\widehat{aS}| = S$. Suppose $s \in S$. Then $-p/2 < \widehat{as} < p/2$ so $0 \le |\widehat{as}| < p/2$. But $\widehat{as} \neq 0$ since $p \nmid a$ and $p \nmid s$. Hence $\widehat{as} \in S$. This shows that $|\widehat{aS}| \subseteq S$. To show that the two sets are equal, we must show that the have the same number of elements. Suppose that s, $t \in S$ satisfy $|\widehat{as}| = |\widehat{at}|$. Then $as \equiv \pm at \pmod p$ and so $s \equiv \pm t \pmod p$. But $-p/2 < s, \pm t < p/2$, so their difference can't be divisible by p unless it is 0. Thus $s = \pm t$. But s, $t \in S$ so $s = t$. This shows that $|\widehat{aS}|$ has as many elements as S, completing the proof. □

Gauss' Lemma enables us to prove the second supplement to the Law of Quadratic Reciprocity.

Proof of the Second Supplement. We want to show that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Consider the case $p \equiv 1 \pmod 8$; the other cases are similar and are left as an exercise. Then $p = 8m+1$ for some integer m. Here $(p-1)/2 = 4m$. We will apply Gauss' Lemma to determine $\left(\frac{2}{p}\right)$. For this we need to compute $\widehat{2x}$ where $x = 1, 2, \ldots, 4m$. Now for $x = 1, 2, \ldots, 2m$ we have $0 < 2x < p/2$ and so $\widehat{2x} = 2x$ which is positive. However, for $x = 2m+1, 2m+2, \ldots, 4m$ we have $p/2 < 2x < p$ and $\widehat{2x} = 2x - p$ which is negative. Hence $\mu(2) = 2m$, so by Gauss' Lemma

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

□

PROOF OF THE LAW OF QUADRATIC RECIPROCITY. The first proof is due to Gauss and he altogether gave eight different proofs of LQR, and there are hundreds of published proofs. The proof we give is due to Eisenstein. It starts with the following trigonometric identity. Let m be an odd positive integer and let

$$S_m = \left\{1, 2, 3, \ldots, \frac{m-1}{2}\right\}.$$

Then

$$\frac{\sin mx}{\sin x} = (-4)^{(m-1)/2} \prod_{t \in S_m} \left(\sin^2 x - \sin^2 \frac{2\pi t}{m}\right). \tag{1}$$

Observe that if $u \equiv v \pmod p$ then $2\pi u/p$ and $2\pi v/p$ differ by a multiple of 2π and so $\sin(2\pi u/p) = \sin(2\pi v/p)$. Let $\operatorname{sgn}(u)$ denote the sign of u so that $u = \operatorname{sgn}(u)|u|$. Then $\sin(2\pi u/p) = \operatorname{sgn}(u)\sin(2\pi|u|/p)$. Now for $s \in S_p$,

$$qs \equiv \widehat{qs} \equiv \operatorname{sgn}(\widehat{qs})|\widehat{qs}| \pmod p.$$

Thus

$$\sin \frac{2\pi qs}{p} = \operatorname{sgn}(\widehat{qs}) \sin \frac{2\pi|\widehat{qs}|}{p}.$$

In the notation of Gauss' Lemma, exactly $\mu(q)$ of the $\widehat{qs}$ are negative. Hence

$$\left(\frac{q}{p}\right) = \prod_{s \in S_p} \operatorname{sgn}(\widehat{qs}).$$

From the last two equations,

$$\prod_{s \in S_p} \sin \frac{2\pi qs}{p} = \left(\frac{q}{p}\right) \prod_{s \in S_p} \sin \frac{2\pi|\widehat{qs}|}{p}.$$

However, from the proof of Gauss's Lemma, $\{|\widehat{qs}| : s \in S_p\} = |\widehat{qS_p}| = S_p$. Hence

$$\prod_{s \in S_p} \sin \frac{2\pi qs}{p} = \left(\frac{q}{p}\right) \prod_{s \in S_p} \sin \frac{2\pi s}{p},$$

which can be rewritten as

$$\left(\frac{q}{p}\right) = \prod_{s \in S_p} \frac{\sin(2\pi qs/p)}{\sin(2\pi s/p)}.$$

Using the identity (1) with $q = m$ and $x = 2\pi s/p$ we obtain

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{s \in S_p} (-4)^{(q-1)/2} \prod_{t \in S_q} \left(\sin^2(2\pi s/p) - \sin^2(2\pi t/q)\right) \\ &= (-4)^{(p-1)(q-1)/4} \prod_{s \in S_p, t \in S_q} \left(\sin^2(2\pi s/p) - \sin^2(2\pi t/q)\right),\end{aligned}$$

as S_p has $(p-1)/2$ members. Now interchanging p and q we have

$$\left(\frac{p}{q}\right) = (-4)^{(q-1)(p-1)/4} \prod_{s\in S_p, t\in S_q} \left(\sin^2(2\pi t/q) - \sin^2(2\pi s/p)\right).$$

The right-hand sides of the last two equations are identical except for a minus sign for each term in the product. But there are $(\#S_p)(\#S_q) = \frac{(p-1)}{2}\frac{(q-1)}{2}$ terms in the product. Thus

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

completing the proof. □

Next we are going to look at some applications of the Law of Quadratic Reciprocity.

3. Mersenne Numbers

You have met the Mersenne numbers $M_n = 2^n - 1$ in the homework, and know that if n is composite then so is M_n. What if $n = q$ is prime; is M_q necessarily prime? Computing the first few we find

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127,$$

which are all prime numbers. Now $M_{11} = 2047$. Is it a prime? The following theorem gives us a large supply of Mersenne numbers M_q where q is prime but M_q is composite.

Theorem 3.6. *Let $q \equiv 3 \pmod 4$ be a prime such that $p = 2q + 1$ is also prime. Then p divides M_q. In particular, for such $q > 3$, M_q is composite.*

Before proving Theorem 3.6 let us apply it with $q = 11$. Note that $q \equiv 3 \pmod 4$ and $p = 2q + 1 = 23$ is prime. Then according to the Theorem 3.6, p divides M_q and indeed we find that $M_{11} = 2047 = 23 \times 89$. You can use the same argument to find a factor of M_q for

$$q = 11, 23, 83, 131, 179, 191, 239, 251, 359, 419, 431, 443, 491, 659, \ldots$$

Proof of Theorem 3.6. Since $q \equiv 3 \pmod 4$, we have that $p = 2q + 1 \equiv 7 \pmod 8$. Hence

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

But by Euler's Criterion

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

Hence $M_q = 2^q - 1$ is divisible by p. To prove the last statement in Theorem 3.6, observe that M_q is composite if $M_q > p$. This is the same as $2^q - 1 > 2q + 1$ which is satisfied if $q > 3$. □

4. A Diophantine Equation

A Diophantine equation is one where we are interested in integer solutions. It can be very hard to determine all the solutions of a Diophantine equations (e.g. Fermat's Last Theorem). However, quadratic reciprocity can sometimes be used to show that there are no solutions. Here is an example.

Theorem 3.7. *The equation*

$$y^2 = x^3 - 5$$

has no solutions with x, $y \in \mathbb{Z}$.

PROOF. We proceed by contradiction. Suppose that x, $y \in \mathbb{Z}$ satisfy $y^2 = x^3 - 5$. If x is even then $y^2 \equiv -5 \equiv 3 \pmod 4$ which is impossible as the squares modulo 4 are 0 and 1. Thus x is odd. Now rewrite the equation as

$$y^2 + 4 = x^3 - 1 = (x-1)(x^2 + x + 1).$$

Note that $x^2 + x + 1 = \text{odd} + \text{odd} + \text{odd}$ and so is odd. Let p be a prime divisor of $x^2 + x + 1$. Then $p \mid (y^2 + 4)$ and so $y^2 \equiv -4 \pmod p$. Hence

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

Thus $p \equiv 1 \pmod 4$. As this is true of all prime divisors of $x^2 + x + 1$ we have

$$x^2 + x + 1 \equiv 1 \pmod 4.$$

If $x \equiv 1 \pmod 4$ then $x^2 + x + 1 \equiv 3 \pmod 4$ giving a contradiction. Hence $x \equiv 3 \pmod 4$. Hence $y^2 \equiv x^3 - 5 \equiv 3 - 5 \equiv 2 \pmod 4$, which is impossible. □

CHAPTER 4

Algorithms

In this section we will study algorithms to compute square roots modulo a given odd prime p. We will also study some factoring methods including Quadratic Sieve.

In previous chapters we have already seen some algorithms:

- Euclid's algorithm : (i) To compute gcd of two numbers, (ii) to compute inverse modulo n.
- Chinese Remainder Theorem: To solve simultaneous linear congruences.
- Primitive roots modulo prime p: Write $p-1 = q_1^{r_1} q_2^{r_2} \cdots q_k^{r_k}$. To compute primitive root modulo p either
  (i) For each $1 \leq i \leq k$ find an element g_i of order $q_i^{r_i}$ in U_p, then $\prod_{i=1}^{k} g_i$ is a primitive root; or
  (ii) Through a process of iteration find an element $g \in U_p$ such that $g^{\frac{p-1}{q_i}} \neq 1$ for all i. Then g is a primitive root.

Example 4.1. We find a primitive root modulo 19. Write $19-1 = 2 \times 3^2$. We need to find $g_1, g_2 \in U_{19}$ of order 2, 9 respectively. Take $g_1 = -1$, it has order 2. Note $2^9 = 512 \equiv -1 \pmod{19}$, hence 4 has order 9 modulo 19. Take $g_2 = 4$. Hence $-4 \equiv 15$ is a primitive root modulo 19.

In the previous chapter we proved LQR which is a powerful tool to decide whether a give integer is a square modulo a given prime. Note that every number is a square modulo 2.

One can easily see by using LQR and the second supplement that $\left(\frac{22}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{11}{97}\right) = \left(\frac{97}{11}\right) = \left(\frac{9}{11}\right) = 1$, so 22 is a square modulo 97. The question is to find square roots of 22 modulo 97, i.e. to find $x \in \mathbb{Z}$ such that $x^2 \equiv 22 \pmod{97}$. In order to this we will use algorithm of Tonell-Shanks.

1. Tonelli-Shanks

Let p be an odd prime. For integers a with $\left(\frac{a}{p}\right) = 1$, we want to find square roots of a modulo p. Write $p-1 = 2^e \cdot q$ with q odd. Since U_p is group of order $2^e \cdot q$, by Sylow's Theorem[1], U_p has a 2-Sylow subgroup, say H, of order 2^e. Since U_p is cyclic, H is also cyclic. Let $H = \langle z \rangle$ for

[1]Sylow's theorem: Let G be a finite group such that $p^k \| \#G$, then $\exists$ a subgroup H of G such that $\#H = p^k$. H is called p-Sylow subgroup of G.

some z of order 2^e. Note that squares in H are precisely the elements of order dividing 2^{e-1} and are also even powers of z. Since $\left(\frac{a}{p}\right) = 1$ by Euler's criterion $(a^q)^{2^{e-1}} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and so $b = a^q \pmod{p}$ is a square in H. Thus $1/b$ is a square in H and therefore there exists en even integer k with $0 \leq k < 2^e$ such that $1/b = z^k$, i.e., $a^q z^k = 1$ in H. Let $x = a^{\frac{q+1}{2}} z^{k/2}$. Then $x^2 = a^{q+1} z^k = a$ in H. Thus $x^2 \equiv a \pmod{p}$.

Thus we need to find (i) a generator z of H and (ii) exponent k.

Exercise: n is a quadratic non-residue modulo p iff n^q is a generator of H.

Algorithm 4.1 (Tonelli-Shanks algorithm)**.** Let p be a prime.

Step 1: Write $p - 1 = 2^e \cdot q$ where q is odd.

Step 2: Find a quadratic non-residue n modulo p.

Step 3: Let $z, x, b, r \in \mathbb{Z}$ be such that

$$\begin{aligned} z &\equiv n^q \pmod{p}, \\ x &\equiv a^{\frac{q+1}{2}} \pmod{p}, \\ b &\equiv a^q \pmod{p}, \\ r &= e. \end{aligned}$$

Step 4: If $b \equiv 1 \pmod{p}$, then output x and terminate the algorithm. Else iterate the following until we obtain $b \equiv 1 \pmod{p}$.

- Find the least $m \geq 1$ such that $b^{2^m} \equiv 1 \pmod{p}$. If $m = r$, then output the message "a is a quadratic non-residue" and stop. Else $m < r$.
- Let $t = z^{2^{r-m-1}} \pmod{p}$, and let

$$\begin{aligned} x &\leftarrow tx \pmod{p}, \\ b &\leftarrow bt^2 \pmod{p} \\ z &\leftarrow t^2 \pmod{p}, \\ r &\leftarrow m. \end{aligned}$$

(note: here "$a \leftarrow b$" denotes "replace a by b".)

Example 4.2. Find $x \in Z$ such that $x^2 \equiv 22 \pmod{97}$.

Step 1: Write $p - 1 = 96 = 2^5 \cdot 3$. Let $e = 5$, $q = 3$ and $a = 22$.

Step 2: We choose $n = 5$, since

$$\left(\frac{5}{97}\right) = \left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Step 3: Let

$$\begin{aligned} z &= 5^3 \equiv 28 \pmod{97}, \\ x &= 22^2 \equiv 96 \equiv -1 \pmod{97}, \\ b &= 22^3 \equiv -22 \equiv 75 \pmod{97}, \\ r &= 5. \end{aligned}$$

Step 4: Since $b \not\equiv 1 \pmod{97}$, we compute the least $m \geq 1$ such that $b^{2^m} \equiv 1 \pmod{97}$. Since

$$\begin{aligned} b^2 &= 22^6 = (22^2)^3 \equiv -1 \pmod{97}, \\ b^4 &\equiv 1 \pmod{97}, \end{aligned}$$

we have $m = 2 < 5 = r$. Thus we proceed the iteration. Let

$$\begin{aligned} t &= z^{2^{r-m-1}} = (28^2)^2 \equiv 28^4 \equiv 64 \pmod{97}, \\ x &\leftarrow tx = 64 \cdot 96 \equiv -64 \equiv 33 \pmod{97}, \\ b &\leftarrow bt^2 = 75 \cdot (64)^2 \equiv 1 \pmod{97}. \end{aligned}$$

Since $b \equiv 1 \pmod{97}$, the process terminates and we get that $x \equiv 33 \pmod{97}$ is a solution. Thus the two square roots are 33 and $-33 = 64$ modulo 97.

2. Fermat's Factorization

A naive way to find a factor of given number n is to check whether it is divisible by any prime p with $1 < p \leq \sqrt{n}$. The first improvement over this naive method was given by Fermat which is essentially based on the following lemma.

Lemma 4.2. *Every positive odd number n can be written as $n = x^2 - y^2$, where $x, y \in \mathbb{Z}$ and $x > y \geq 0$.*

Proof. Write $n = ab$ where $1 \leq b \leq a$. Then we can write

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

Since n is odd, both a and b are odd. Hence both $\frac{a+b}{2}$ and $\frac{a-b}{2}$ are integers. It is clear that $\frac{a+b}{2} > \frac{a-b}{2} \geq 0$. □

Exercise: Let n be a positive odd integer. Show that if $n = x^2 - y^2$ where $x, y \in \mathbb{Z}$ and $x > y \geq 0$, then $\lceil \sqrt{n} \rceil \leq x \leq \frac{n+1}{2}$.

Algorithm 4.3 (Fermet's factorization method)**.** Given a positive odd integer n, we want to find x and y such that $n = x^2 - y^2$. To do this we consider the values $x^2 - n$ as x varies between $\lceil \sqrt{n} \rceil$ and $\frac{n+1}{2}$ until we obtain a value of x such that $x^2 - n$ is a square.

Step 1: Let $s = \lceil \sqrt{n} \rceil$ (i.e. s is the smallest integer such that $s^2 \geq n$).

Step 2: Define $f(d) = (s+d)^2 - n$.

Step 3: Iterate $d = 0, 1, 2, \ldots$ until $f(d)$ is a square. Note that the process will stop once we have $s + d = \frac{n+1}{2}$, since then $f(d) = \left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$.

- If we find d such that $s + d < \frac{n+1}{2}$ and $f(d)$ is a square, say y^2, then $f(d) = (s+d)^2 - y^2 = (s+d-y)(s+d+y)$ gives a nontrivial factorization of n (by exercise above), showing that n is a composite.
- Otherwise, n is a prime.

Example 4.3. Let $n = 221$. Let $s = \lceil \sqrt{n} \rceil = 15$ (since $15^2 = 225$). So set $f(d) = (15+d)^2 - 221$. Then

$$f(0) = (15^2 + 0) - 221 = 225 - 221 = 4 = 2^2.$$

Thus $15^2 - 221 = 2^2$, i.e. $221 = 15^2 - 2^2 = (15-2)(15+2) = 13 \cdot 17$.

3. Quadratic Sieve

Let $n \geq 1$ be composite. In order to factor n, in Fermat's factorization method we look for integers x and y such that $n = x^2 - y^2$. In other words, we search for an integer x such that $x^2 - n$ is a square, where $\lceil \sqrt{n} \rceil \leq x \leq \frac{n+1}{2}$. But as n becomes large, this process becomes slow as we need to try many values of x. We can instead look for x and y such that $x^2 - y^2 \equiv 0 \pmod{n}$, i.e., $(x-y)(x+y) \equiv 0 \pmod{n}$. If $x \not\equiv \pm y \pmod{n}$, then it follows that $\gcd(x-y, n)$ and $\gcd(x+y, n)$ are proper divisors of n. Hence we obtain a nontrivial factorization of n. Using this idea, we have the following method.

Algorithm 4.4 (Quadratic sieve)**.** Let $n \geq 1$ be composite.

Step 1: Pick a set of primes $B = \{p_1, p_2, \cdots, p_r\}$ such that n is a square $\bmod p_i$ for all $i = 1, 2, \cdots, r$. Such a set B is called a *factor base*. A number is called *B-smooth* if all of its factors are in B.

Step 2: Let $s = \lceil \sqrt{n} \rceil$ and set $f(d) = (s+d)^2 - n$. Set a "sieve interval" $[-D, D]$. We will be looking at $f(d)$ for $-D \leq d \leq D$. Let $V = [f(-D), \cdots, f(0), \cdots f(D)]$. We want to find $\delta_1, \delta_2, \ldots \delta_t$ in $[-D, D]$ such that $f(\delta_1) f(\delta_2) \cdots f(\delta_t)$ is a square in $\mathbb{Z}$. For this we would first find entries of V that are B-smooth by process of sieving.

Step 3 (Sieve): For each p_i in B, apply Tonelli-Shanks algorithm to get solutions r_1 and r_2 to the congruence $x^2 \equiv n \pmod{p_i}$. Then

$$\begin{aligned} f(d) = (s+d)^2 - n &\equiv 0 \pmod{p_i} \\ &\iff d \equiv r_1 - s \text{ or } r_2 - s \pmod{p_i} \\ &\iff d \equiv a_1 \text{ or } a_2 \pmod{p_i}, \end{aligned}$$

where $a_1 = r_1 - s$, $a_2 = r_2 - s$. For $-D \leq d \leq D$, if $d \equiv a_1$ or $a_2 \pmod{p_i}$, then divide $f(d)$ by $p_i^{\operatorname{ord}_{p_i} f(d)}$ and record this power in a separate list.

After repeating this for each p_i, any entry of V that eventually becomes 1 or -1 is a B-smooth number, let us call them $f(d_1),\ f(d_2), \dots f(d_k)$. Since we recorded the powers earlier, we already know the factorization of $f(d_i)$, i.e., we know $\mathrm{ord}_{p_j} f(d_i)$ for each $j = 1, \dots, r$ and $i = 1, \dots, k$.

Step 4: Form a $k \times (r+1)$ matrix A such that (i,j)-th entry of A equals

$$\begin{cases} \mathrm{ord}_{p_j} f(d_i) \pmod 2 & \text{for } 1 \le j \le r, \\ \begin{cases} 1 & \text{if } f(d_i) < 0, \\ 0 & \text{if } f(d_i) > 0. \end{cases} & \text{for } j = r+1. \end{cases}$$

for $1 \le i \le k$. Consider the following system of linear equations over $\mathbb{Z}/2Z$,

$$A^T \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Check that rank of A^T is less than k and hence obtain a non-trivial solution, say $\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix}$ to the above system of equations. Then $\prod_{i=1}^k f(d_i)^{y_i}$ is a square in $\mathbb{Z}$, say Y^2. Also, let $X = \prod_{i=1}^k (s+d_i)^{y_i}$. Since $f(d_i) \equiv (s+d_i)^2 \pmod n$, we have $X^2 = \prod_{i=1}^k (s+d_i)^{2y_i} \equiv Y^2 \pmod n$. Compute $\gcd(X-Y, n)$ and $\gcd(X+Y, n)$ to find a proper divisor of n. If we do not find a proper divisor, then try different relations (or change B etc.) and repeat the process.

Example 4.4. Factorise 31309 using Quadratic Sieve.

To do this we first look for a factor base. Note that 2, 3, 5, 11 are first few primes such that 31309 is square modulo these primes. So let $B = \{2, 3, 5, 11\}$. Let $s = \lceil \sqrt{31309} \rceil = 177$ and $f(d) = (177+d)^2 - 31309$. Consider sieve interval $[0, 5]$ and let $V = [f(0),\ f(1),\ f(2),\ f(3),\ f(4),\ f(5)] = [20,\ 375,\ 732,\ 1091,\ 1452,\ 1815]$.

For $p = 2$, clearly 1 is only solution to $x^2 \equiv 31309 \pmod 2$. So $f(d) \equiv 0 \pmod 2 \Leftrightarrow d \equiv 1 - 177 \equiv 0 \pmod 2$. Dividing each even indexed entry of V by highest power of 2, we get $[5,\ 375,\ 183,\ 1091,\ 363,\ 1815]$.

Next for $p = 3$, we get 1 and 2 are square-roots of 31309 modulo 3. So $f(d) \equiv 0 \pmod 3 \Leftrightarrow d \equiv 1-177$ or $2-177 \equiv 1$ or $2 \pmod 3$. Dividing each such entry of V by highest power of 3, we get $[5,\ 125,\ 61,\ 1091,\ 121,\ 605]$.

Next for $p = 5$, we get 2 and 3 are square-roots of 31309 modulo 5. So $f(d) \equiv 0 \pmod 5 \Leftrightarrow d \equiv 2-177$ or $3-177 \equiv 0$ or $1 \pmod 5$. Dividing each such entry of V by highest power of 5 now, we get $[1,\ 1,\ 61,\ 1091,\ 121,\ 121]$.

Finally for $p = 11$, we get 5 and 6 are square-roots of 31309 modulo 5. So $f(d) \equiv 0 \pmod 5 \Leftrightarrow d \equiv 5 - 177$ or $6 - 177 \equiv 4$ or $5 \pmod{11}$.

Dividing each such entry of V by highest power of 11 now, we finally get $[1,\ 1,\ 61,\ 1091,\ 1,\ 1]$.

Thus $f(0),\ f(1), f(4)$ and $f(5)$ are B-smooth and

$$f(0) = 2^2 \cdot 5,\ f(1) = 3 \cdot 5^3,\ f(4) = 2^2 \cdot 3 \cdot 11^2,\ f(5) = 3 \cdot 5 \cdot 11^2$$

which we can record as the following table.

	2	3	5	11	-1
f(0)	2	0	1	0	0
f(1)	0	1	3	0	0
f(4)	2	1	0	1	0
f(5)	0	1	1	2	0

So we want to find a non-trivial solution for the following system:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Clearly rank of the LHS matrix above is less than 4 and $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$ is a non-trivial solution. Thus $f(1)f(5)$ is a square and $f(1)f(5) = 3^2 \cdot 5^4 \cdot 11^2$. Hence $3^2 \cdot 5^4 \cdot 11^2 = f(1)f(5) \equiv (1 + 177)^2(5 + 177)^2 \pmod{31309}$ and $\gcd(178 \cdot 182 + 3 \cdot 5^2 \cdot 11,\ 31309) = \gcd(33221, 31309) = 239$. Further $\gcd(178 \cdot 182 - 3 \cdot 5^2 \cdot 11,\ 31309) = \gcd(31571, 31309) = 131$. Indeed $31309 = 239 \cdot 131$.

Reading Suggestion: ***A Tale of Two Sieves, Carl Pomerance.*** This article is an excellent reading on history of factoring algorithms and provides a beautiful exposition of Quadratic and Number Field Sieve.

CHAPTER 5

Introduction to Public Key Cryptography

Aims of cryptography

(1) Privacy: Encryption and Decryption of a message.
(2) Authenticity: Digital Signature.

Suppose Alice wants to send Bob a secret message. One way is to use **symmetric key cryptography**:

$$\text{(key)} \quad \text{Alice} \quad \xrightarrow{\text{locked message}} \quad \text{Bob} \quad \text{(key)}$$

Here they share keys for the same lock. For this they need to share their keys in advance.

Another way is to use **Public key cryptography**. The following are the main steps:

Step 0 (KeyGen): Alice and Bob generate their own *public key* `PK` and *private key* `SK`. Public keys are known to everyone, but the private key is kept secretly to each person.

Now suppose Alice wants to send Bob a message `M`.

Step 1 (Encription): Alice obtains Bob's public key `PK`. Alice uses it to encrypt `M` and sends the ciphertext `C` to Bob.

Step 2 (Decryption): Bob uses his `SK` to decrypt `C` to obtain the original message `M`.

In other words, we need to have the system

$$\text{Decrypt}(\text{Encrypt}(\texttt{M}, \texttt{PK}), \texttt{SK}) = \texttt{M}.$$

Here Step 1 and Step 2 are for private communication, but there is a following problem. Since the public key `PK` is known to everyone, some third person may disguise as Alice to send a message to Bob. But Bob wants to make sure that the message is indeed sent by Alice. This leads to the use of **Digital signature**: Alice creates a signature `s` by using her `SK` and send it together with `C`. Bob then uses Alice's `PK` to authenticate the signature `s` and hence confirms that the ciphertext `C` is indeed sent by Alice.

We will look at the following two public key cryptosystem:

(1) RSA
(2) Diffie-Hellman key exchange

1. RSA

KeyGen: Each user chooses two large primes p and q of similar size. Let $N = pq$. Then $\varphi(N) = (p-1)(q-1)$. Choose $e \in \mathbb{Z}$ such that $\gcd(e, \varphi(N)) = 1$. Compute $d \in \mathbb{Z}$ such that $ed \equiv 1 \pmod{\varphi(N)}$. Here it generates

- Public key $\mathtt{PK} = (N, e)$,
- Private key $\mathtt{SK} = d$.

Encrypt$(\mathtt{M}, (N, e))$: Let (N, e) be the PK of the recipient, Bob. Let $\mathtt{M}$ be a message and assume $\mathtt{M} < N$. Compute $\mathtt{C} = \mathtt{M}^e \pmod{N}$ and transmit ciphertext $\mathtt{C}$.

Decrypt$(\mathtt{C}, d)$: Recipient Bob uses his SK d to compute $\mathtt{C}^d \pmod{N}$ and gets M, since

$$\mathtt{C}^e \equiv \mathtt{M} \pmod{N}$$

by Lemma 5.1 below and since $M < N$.

Lemma 5.1. *If* $\gcd(\mathtt{M}, N) = 1$, *then* $\mathtt{M}^{ed} \equiv \mathtt{M} \pmod{N}$. *If* $\gcd(\mathtt{M}, N) \neq 1$, *then also* $\mathtt{M}^{ed} \equiv \mathtt{M} \pmod{N}$.

Proof. If $\gcd(\mathtt{M}, N) = 1$, then we have $\mathtt{M}^{\varphi(N)} \equiv 1 \pmod{N}$. Since $ed \equiv 1 \pmod{\varphi(N)}$,

$$\begin{aligned} \mathtt{M}^{ed} &\equiv \mathtt{M}^{1+\varphi(N)t} \pmod{N} \qquad \text{for some } t \in \mathbb{Z} \\ &\equiv \mathtt{M}(\mathtt{M}^{\varphi(N)})^t \pmod{N} \\ &\equiv \mathtt{M} \pmod{N}. \end{aligned}$$

Now suppose $\gcd(\mathtt{M}, N) \neq 1$. Since $N = pq$, we have $\gcd(\mathtt{M}, N) = p, q$ or N. If $\gcd(\mathtt{M}, N) = N$, then clearly $\mathtt{M}^{ed} \equiv 0 \equiv \mathtt{M} \pmod{N}$. Thus WLOG assume that $\gcd(\mathtt{M}, N) = p$. Then we can write $\mathtt{M} = p\mathtt{M}_1$ for some $\mathtt{M}_1 \in \mathbb{Z}$ such that $\gcd(\mathtt{M}_1, q) = 1$. Hence

$$\begin{aligned} \mathtt{M}^{ed} - \mathtt{M} &\equiv p\mathtt{M}_1{}^{ed} - p\mathtt{M}_1 \pmod{N} \\ &\equiv p\mathtt{M}_1(p\mathtt{M}_1{}^{ed-1} - 1) \pmod{N} \\ &= p\mathtt{M}_1(p\mathtt{M}_1{}^{(p-1)(q-1)t} - 1) \pmod{N} \end{aligned} \tag{2}$$

for some $t \in \mathbb{Z}$, where the last equality follows since $ed - 1 \equiv 0 \pmod{\varphi(N) = (p-1)(q-1)}$. Now since $\gcd(\mathtt{M}_1, q) = 1$, we have $(p\mathtt{M})^{q-1} \equiv 1 \pmod{q}$. Thus

$$(p\mathtt{M}_1)^{(p-1)(q-1)t-1} \equiv 1 \pmod{q}. \tag{3}$$

From (2) and (3), it follows that $\mathtt{M}^{ed} - \mathtt{M} \equiv 0 \pmod{pq = N}$, i.e., $\mathtt{M}^{ed} \equiv \mathtt{M} \pmod{N}$. □

2. Digital Signature Using RSA

Suppose Alice is sending a message $\mathtt{M}$ to Bob. Alice sends her digital signature $\mathtt{s}$ together with $\mathtt{M}$. Let Alice's public key be (N, e) and her private key be d. She does the following:

sign$(\mathtt{M}, d)$:

- Compute $s = \mathtt{M}^d \pmod N$.
- Send $(\mathtt{C}, s)$ to Bob where $\mathtt{C} = \text{Encrypt}(\mathtt{M}, (N, e))$.

Once Bob receives $(\mathtt{C}, s)$, he does the following:

verify$((\mathtt{C}, s), (N, e))$: Decrypt $\mathtt{C}$ to obatin $\mathtt{M}$ using his $\mathtt{SK}$.

- Compute $s^e \pmod N$.
- Check if $\mathtt{M} \equiv s^e \pmod N$ or not. If yes, then the message is indeed sent by Alice.

Note:

- RSA security relies on the hardness of factorization of a number N that is a product of two very large primes p and q of similar size.
- In practise RSA is used mainly for transporting symmetric keys and digital signature.
- One would like to encrypt text message in alphabet. To do that we need to convert a text message to an integer $\mathtt{M}$. One standard procedure is to use the following assignment:

$$A = 00,\ B = 01,\ C = 03,\ \cdots Z = 25.$$

  The integer $\mathtt{M}$ so obtained will be most likely greater than N. So M is partitioned into smaller blocks: $\mathtt{M} = \mathtt{M_1M_2}...\mathtt{M_r}$ such that each $\mathtt{M_i} < N$.
- In 1994, RSA-129 (129-digit N) was factorized by using Quadratic sieve method with a factor base consisting 524339 primes, using 1600 computers.
- Commonly used RSA uses N that is ranging from 1024-bits to 2048-bits (i.e. $309 - 617$ decimal digits). In 2009, RSA-768 (768-bits N, i.e., 232-digit N) is broken. There is a US$ 200000 cash prize for breaking RSA-2048!!

3. Diffie-Hellman Key Exchange

Suppose Alice and Bob want to share a secret random key $\mathtt{K}$. Assume that they know a group G and $g \in G$ of order r.

- Alice chooses random $0 < a < r$ and sends $c_1 = g^a$ to Bob.
- Bob chooses random $0 < b < r$ and sends $c_2 = g^b$ to Alice.
- Alice compute $(c_2)^a = g^{ab}$ and Bob computes $(c_1)^b = g^{ab}$. Then $\mathtt{K} = g^{ab}$ will be their shared key.

Note that unlike RSA, all users share same group G and $g \in G$, but value of shared key K is randomised.

This is based on the **discrete logarithm problem**(DLP): given g and g^a, find a. In this case, the problem is to find g^{ab} given the triplet (g, g^a, g^b). Thus for Diffie-Hellman key exchange one needs to consider groups for which DLP is hard.

Note: 1. For $G = (\mathbb{Z}/p\mathbb{Z}, +)$ for some some prime p, DLP is easy since it is Euclidean algorithm.
2. If N is composite then DLP for $G = ((\mathbb{Z}/N\mathbb{Z})^\times, \cdot)$ is at least as hard as factoring.
Exercise. Suppose N is a product of two primes. Suppose you know DLP for $((\mathbb{Z}/N\mathbb{Z})^\times, \cdot)$ then find factors of N.

Elgamal Encryption System.

Suppose Alice wants to send message $\mathtt{M}$ to Bob.
KeyGen: Choose a prime p, and let $G = U_p = (\mathbb{Z}/p\mathbb{Z})^\times$. Compute the primitive root g of G. Bon chooses a random b such that $2 \leq b \leq p-2$ and compute $h \equiv g^b \pmod{p}$, and generates his

- Public key $\mathtt{PK} = (p, g, h)$,
- Private key $\mathtt{SK} = b$.

Encrypt($\mathtt{M}$, $\mathtt{PK}$): Let $\mathtt{M}$ be a message and assume that $\mathtt{M} \leq p-1$.

- Alice obtains Bob's $\mathtt{PK} = (p, g, h)$.
- Alice chooses a random $2 \leq a \leq p-2$ and computes $c_1 = g^a \pmod{p}$ and $c_2 = \mathtt{M}h^a \pmod{p}$.
- Alice sends ciphertext (c_1, c_2) to Bob.

Decrypt((c_1, c_2), b): Bob uses his secret key to compute $c_2 c_1^{p-1-b}$ to obtain $\mathtt{M}$ since

$$\begin{aligned} c_2 c_1^{p-1-b} &= \mathtt{M}h^a (g^a)^{p-1-b} \\ &= \mathtt{M}g^{ba} g^{a(p-1)-ab} \\ &\equiv \mathtt{M}(g^{(p-1)})^a \pmod{p} \\ &\equiv \mathtt{M} \pmod{p}. \end{aligned}$$

Note that Elgamal encryption is Diffie-Hellman key exchange followed by symmetric encryption. In the above both Alice and Bob computes shared key $\mathtt{K} = g^{ab}$ which is then used for symmetric encryption $\mathtt{M} \to \mathtt{MK}$ by Alice. Bob then computes $(\mathtt{MK})\mathtt{K}^{-1}$ to obtain $\mathtt{M}$. This is an example of hybrid encryption.

Digital signature using Elgamal: Bob wants to make sure that the message $\mathtt{M}$ is indeed coming from Alice. Alice uses her $\mathtt{PK} = (p, g, h')$ where $h' = g^a$ and $\mathtt{SK} = a$ to create a signature as follows.

- Alice chooses a random $1 \leq j \leq p-1$ such that $\gcd(j, p-1) = 1$.
- Compute $s = g^j$.

- Compute t such that $jt + as \equiv \mathtt{M} \pmod{p-1}$ with $1 \leq t \leq p-2$. The pair (s,t) is the signature for message $\mathtt{M}$.
- Alice sends Bob $(\mathtt{C}, (s,t))$ where $\mathtt{C}$ is a ciphertext for $\mathtt{M}$ that Alice obtains using Bob's PK.
- Bob decrypt $\mathtt{C}$ using his SK to get $\mathtt{M}$. He computes

$$V_1 = h'^s s^t \pmod{p},$$
$$V_2 = g^{\mathtt{M}} \pmod{p}.$$

The signature is verified when $V_1 = V_2$. Note that this equality should hold since

$$\begin{aligned} V_1 = h'^s s^t &= g^{as} g^{jt} \\ &= g^{as+jt} \\ &\equiv g^{\mathtt{M}+(p-1)t} \pmod{p} \qquad (\text{for some } t \in \mathbb{Z}) \\ &\equiv g^{\mathtt{M}} \pmod{p} \\ &= V_2. \end{aligned}$$

Example 5.1. Alice and Bob share a group $(\mathbb{Z}/p\mathbb{Z})^\times$ where $p = 43$ and $g = 3$. Bob's $\mathtt{PK}$ is $(43, 3, 22)$ and his $\mathtt{SK}$ is $b = 15$ (note that $3^{22} \equiv 15 \pmod{43}$). Alice wants to send "HELP" $= 07041115$ by separating into 4 blocks $B_1 = 07$, $B_2 = 04$, $B_3 = 11$ and $B_4 = 15$. Alice chooses a random $a = 23$ and calculates $c_1 = 3^{23} \equiv 34 \pmod{43}$. Then they have shared key $\mathtt{K} = 22^{23} \equiv 32 \pmod{43}$. Alice then computes $B_i\mathtt{K}$ for each i, so

$$B_1\mathtt{K} = 7 \cdot 32 \equiv 9 \pmod{43},$$
$$B_2\mathtt{K} = 4 \cdot 32 \equiv 42 \pmod{43},$$
$$B_3\mathtt{K} = 11 \cdot 32 \equiv 8 \pmod{43},$$
$$B_4\mathtt{K} = 15 \cdot 32 \equiv 7 \pmod{43}.$$

Alice sends $c_2 = (34, 9), (34, 42), (34, 8), (34, 7)$ to Bob. Bob then computes $34^{p-1-15} = 34^{27} \equiv 39 \pmod{43}$ and gets the message back;

$$9 \cdot 39 \equiv 7 \pmod{43},$$
$$42 \cdot 39 \equiv 4 \pmod{43},$$
$$8 \cdot 39 \equiv 11 \pmod{43},$$
$$7 \cdot 39 \equiv 15 \pmod{43}.$$

Finally, by concatinating the numbers Bob obtains 07041115 ="HELP".

CHAPTER 6

p-adic numbers

1. Congruences modulo p^m

We looked at congruences of the form

$$x^2 \equiv a \pmod{p}$$

where p is prime and $a \in \mathbb{Z}$, and we saw how to solve such congruences modulo p. We now consider congruences of the form

$$x^2 \equiv a \pmod{p^m} \qquad \text{for } m \geq 2,$$

i.e., modulo higher powers of p.

Example 6.1. Consider the polynomial $f(x) = x^2 + 1$. Note that there is no solution over $\mathbb{Z}$. Let us now look at $f(x)$ modulo 5. It is clear that

$$f(x) \equiv 0 \pmod{5} \iff x^2 \equiv -1 \pmod{5} \iff x \equiv 2 \text{ or } 3 \pmod{5}.$$

Now consider the congruence

$$x^2 \equiv -1 \pmod{5^2}.$$

Since any solution to the above congruence must also satisfy $x^2 \equiv -1 \pmod{5}$, it is of the form $x = 2 + 5t_1$ or $3 + 5t_1$ for some $t_1 \in \mathbb{Z}$.

Suppose $x = 2 + 5t_1$ for some $t_1 \in \mathbb{Z}$. Then

$$\begin{aligned} x^2 = (2 + 5t_1)^2 \equiv -1 \pmod{5^2} &\iff 4 + 20t_1 + (5t_1^2) \equiv -1 \pmod{5^2} \\ &\iff 5 + 20t_1 \equiv 0 \pmod{5^2} \\ &\iff 5(1 + 4t_1) \equiv 0 \pmod{5^2} \\ &\iff 1 + 4t_1 \equiv 0 \pmod{5} \\ &\iff t_1 \equiv 1 \pmod{5}. \end{aligned}$$

Similarly, if $x = 3 + 5t_1$ for some $t_1 \in \mathbb{Z}$, then we get $t_1 \equiv 3 \pmod{5}$. Therefore

$$x^2 \equiv -1 \pmod{5^2} \iff x \equiv 7 \text{ or } 18 \pmod{5^2}.$$

Now consider the congruence

$$x^2 \equiv -1 \pmod{5^3}.$$

Since any solution to this congruence must also satisfy $x^2 \equiv -1 \pmod{5^2}$, it is of the form $x = 7+25t_2$ or $18+25t_2$ for some $t_2 \in \mathbb{Z}$. Suppose $x = 7+25t_2$,

then

$$\begin{aligned} x^2 = (7+25t_2)^2 &\equiv -1 \pmod{5^3} \\ &\iff 49 + 2\cdot 7\cdot 25t_2 + (25t_2)^2 \equiv -1 \pmod{5^3} \\ &\iff 50 + 50\cdot 7t_2 \equiv 0 \pmod{5^3} \\ &\iff 5^2(2+14t_2) \equiv 0 \pmod{5^3} \\ &\iff 2 + 14t_2 \equiv 0 \pmod{5} \\ &\iff t_2 \equiv 2 \pmod{5}. \end{aligned}$$

Similarly, if $x = 18 + 25t_2$ then $t_2 \equiv 2 \pmod 5$. Therefore

$$x^2 \equiv -1 \pmod{5^3} \iff x \equiv 57 \text{ or } 68 \pmod{5^3}.$$

Note that if $x = 2 + 5t_1$, then

$$\begin{aligned} x &= 2 + 5t_1 \\ &= 2 + 5(1+5t_2) = 2 + 1\cdot 5 + 2\cdot 5^2 t_2 \\ &= 2 + 1\cdot 5 + 5^2(2+5t_3) \qquad (\text{for some } t_3 \in \mathbb{Z}) \\ &\equiv 2 + 1\cdot 5 + 2\cdot 5^2 \pmod{5^3}. \end{aligned}$$

Similarly, if $x = 3 + 5t_1$, then

$$x \equiv 3 + 3\cdot 5 + 2\cdot 5^2 \pmod{5^3}.$$

Thus we can iteratively find solutions to $f(x) = 0$ modulo higher power of 5, and from solutions at each stage we can, as above, form a power series in 5 with coefficients in $\{0, 1, 2, 3, 4\}$.

In the above example, we saw how to construct solutions modulo p^2, $p^3, \ldots$ etc. from solutions modulo p,. The following is the general statement.

Theorem 6.1 (Hensel's lemma)**.** *Let $f(x) \in \mathbb{Z}[x]$. Let p be a prime and $m \geq 1$ be an integer. Suppose there exists $a \in \mathbb{Z}$ such that*

$$f(a) \equiv 0 \pmod{p^m} \qquad \textit{and} \qquad f'(a) \not\equiv 0 \pmod{p}.$$

Then there exists $b \in \mathbb{Z}$ such that

$$b \equiv a \pmod{p^m} \qquad \textit{and} \qquad f(b) \equiv 0 \pmod{p^{m+1}}.$$

(We say that we *lift* a to a solution modulo p^{m+1}.)

Proof. By the Taylor's expansion for polynomials,

$$f(a+x) = f(a) + f'(a)x + \frac{f''(a)}{2!}x^2 + \cdots + \frac{f^{(n)}(a)}{n!}x^n$$

where $n = \deg(f)$.

We want to construct $b \in \mathbb{Z}$ such that $b \equiv a \pmod{p^m}$ and $f(b) \equiv 0 \pmod{p^{m+1}}$, so let $b = a + p^m t$ where t is an integer we will determine below.

Since $f(x) \in \mathbb{Z}[x]$ implies that $\frac{f^{(k)}(x)}{k!} \in \mathbb{Z}[x]$ for all $k \geq 1$ (**exercise!**), we have

$$\begin{aligned} f(b) &= f(a + p^m t) \\ &= f(a) + f'(a)p^m t + \frac{f''(a)}{2!}p^{2m}t^2 + \cdots \\ &= f(a) + f'(a)p^m t + p^{2m}K \end{aligned}$$

for some $K \in \mathbb{Z}$. Since $f(a) \equiv 0 \pmod{p^m}$ by assumption, write $f(a) = p^m s$ for some $s \in \mathbb{Z}$. So

$$f(b) = p^m(s + f'(a)t) + p^{2m}K.$$

Thus

$$f(b) \equiv 0 \pmod{p^{m+1}} \iff s + f'(a)t \equiv 0 \pmod{p}.$$

Since $f'(a) \not\equiv 0 \pmod{p}$, let $h = (f'(a))^{-1} \pmod{p}$. Now take $t = -hs$, then

$$f(b) = p^m(s + f'(a)t) + p^{2m}K \equiv 0 \pmod{p^{m+1}}$$

as required. □

Hence using Hensel's lemma (under certain hypothesis) repeatedly for solving a congruence modulo p^m starting from $m = 1$ we obtain a solution that is a power series of the form

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots,$$

where $0 \leq a_i \leq p - 1$, as we saw in the above example. But does this series in p-power converge? In order to make this power series converge we need a setting where p^m gets "smaller" in some sense as $m \to \infty$. This leads us to define a new norm.

2. p-adic Norm on $\mathbb{Q}$

First recall the function ord_p. For all $\alpha, \beta \in \mathbb{Q}$, we have:

(1) $\mathrm{ord}_p\left(p^n \frac{a}{b}\right) = n$ where $a, b \in \mathbb{Z}$ and $p \nmid a, b$, and $\mathrm{ord}_p(0) = \infty$.
(2) $\alpha \neq 0 \Longrightarrow \alpha = \pm \prod_{p \in \mathbb{P}} p^{\mathrm{ord}_p(\alpha)}$.
(3) $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$.
(4) $\mathrm{ord}_p(\alpha + \beta) \geq \min\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\}$, with equality if $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$.

Definition. The *p-adic absolute value (p-adic norm)* of $\alpha \in \mathbb{Q}$ is given by

$$|\alpha|_p = p^{-\mathrm{ord}(\alpha)} \quad \text{if } \alpha \neq 0, \quad \text{and} \qquad |0|_p = 0.$$

(Note that $|0|_p = p^{\mathrm{ord}_p(0)} = p^{-\infty} = 0$.)

The following are the basic properties of the p-adic norm.

Lemma 6.2. *Let p be a prime and $\alpha, \beta \in \mathbb{Q}$.*

(1) $|\alpha|_p \geq 0$ *and* $|\alpha|_p = 0 \iff \alpha = 0$.
(2) $|\alpha\beta|_p = |\alpha|_p\,|\beta|_p$.

(3) $|\alpha+\beta|_p \le \max\{|\alpha|_p, |\beta|_p\}$ *with equality if* $|\alpha|_p \ne |\beta|_p$.

The inequality in (3) is called the *ultrametric inequality*. It is stronger than the usual triangular inequality since (3) implies that $|\alpha+\beta|_p \le |\alpha|_p + |\beta|_p$.

PROOF. (1) Follows from the definition.
(2) Follows from the property (3) of ord_p.
(3) We have

$$\begin{aligned} |\alpha+\beta|_p &= p^{-\mathrm{ord}_p(\alpha+\beta)} \\ &\le p^{-\min\{\mathrm{ord}_p(\alpha),\mathrm{ord}_p(\beta)\}} \qquad \text{(by property (4) of } \mathrm{ord}_p) \\ &= \max\{p^{-\mathrm{ord}_p(\alpha)}, p^{-\mathrm{ord}_p(\beta)}\} \\ &= \max\{|\alpha|_p, |\beta|_p\}. \end{aligned}$$

Clearly equality holds if $\mathrm{ord}_p(\alpha) \ne \mathrm{ord}_p(\beta)$, i.e., $|\alpha|_p \ne |\beta|_p$. □

Hence the p-adic norm satisfies all the properties of a norm.

Note.

- $\{|\alpha|_p : \alpha \in \mathbb{Q}\} = \{0\} \cup \{p^n : n \in \mathbb{Z}\}$.
- $\forall n \in \mathbb{Z}, |n|_p \le |1|_p = 1$.
- Since $|p^r|_p = p^{-r}$, as r gets larger p^r gets smaller in the p-adic norm.

Example 6.2. Let $\alpha = -40/49$. Then $|\alpha|_2 = 2^{-3}$, $|\alpha|_5 = 5^{-1}$, $|\alpha|_7 = 7^2$, $|\alpha|_p = 1$ for $p \ne 2, 3, 5, 7$. Then $\prod_{p\in\mathbb{P}} |\alpha|_p = 49/40 = 1/|\alpha|$.

Lemma 6.3 (Product Formula)**.** *Let* $\alpha \in \mathbb{Q} \setminus \{0\}$. *Then* $|\alpha| \cdot \prod_{p\in\mathbb{P}} |\alpha|_p = 1$.

Note that above product is a finite product since $|\alpha|_p = 1$ for all but finitely many primes p.

PROOF. Let α has the prime factorization $\alpha = \pm\prod_{p\in\mathbb{P}} p^{\mathrm{ord}_p(\alpha)}$. Then

$$|\alpha| = \prod_{p\in\mathbb{P}} p^{\mathrm{ord}_p(\alpha)} = \prod_{p\in\mathbb{P}} 1/|\alpha|_p .$$

□

Let $\alpha \in \mathbb{Q}$. We define a disc of radius r centered at α by

$$D_r(\alpha) = \{\gamma \in \mathbb{Q} \ : \ |\gamma - \alpha|_p < r\}.$$

The ultrametric property of p-adic norm implies that any point inside such a disc is one of its center!

Lemma 6.4. *If* $\beta \in D_r(\alpha)$ *then* $D_r(\alpha) = D_r(\beta)$.

PROOF. Let $\gamma \in D_r(\alpha)$. Then

$$|\gamma - \beta|_p = |\gamma - \alpha + \alpha - \beta|_p \le \max\{|\gamma-\alpha|_p, |\alpha-\beta|_p\} < r$$

since $\beta, \gamma \in D_r(\alpha)$. Hence $\gamma \in D_r(\beta)$. Similarly $D_r(\beta) \subset D_r(\alpha)$. □

3. Sequences and Series

We have defined the p-adic norm and so we can talk about sequences and series, their convergence, cauchy property etc. with repect to this norm.

Definition. A sequence $(a_n)_n$ of rational numbers *converges p-adically* to a in $\mathbb{Q}$ if $\forall \epsilon > 0,\ \exists\ N_0 \in \mathbb{N}$ such that $n \geq N_0 \implies |a_n - a|_p < \epsilon$. Equivalently, $|a_n - a|_p \to 0$ as $n \to \infty$.

Definition. A series $\sum_{j=1}^{\infty} a_j$ of rational numbers converges p-adically if the sequence of partial sums $s_n = \sum_{j=1}^{n} a_j$ converges p-adically.

Definition. A sequence $(a_n)_n$ of rational numbers is called *p-adically null* if $|a_n|_p \to 0$ as $n \to \infty$.

Example 6.3. (1) Let $a \in \mathbb{Q}$. Then constant sequence $(a)_n$ converges to a p-adically.
(2) The sequence $(a + p^n)_n$ converges p-adically to a since

$$|a + p^n - a|_p = |p^n|_p = \frac{1}{p^n} \to 0 \qquad \text{as } n \to \infty.$$

(3) $(\frac{p^n}{p^n+1})_n \to_p 0$ with $|\cdot|_p$. Note this converges to 1 with the usual absolute value $|\cdot|$.
(4) Consider the series $1 + c + c^2 + \cdots$. If $|c|_p < 1$, then

$$1 + c + c^2 + \cdots \to_p \frac{1}{1-c}.$$

Proof. Let $s_n = 1 + c + c^2 + \cdots + c^{n-1} = \frac{1-c^n}{1-c}$. Then since $|c|_p \leq \frac{1}{p}$,

$$\left| s_n - \frac{1}{1-c} \right|_p = \left| \frac{-c^n}{1-c} \right|_p = |c|_p^n \leq \frac{1}{p^n} \to 0 \quad \text{as } m \to \infty.$$

□

What happens if $|c|_p \geq 1$?

Definition. A sequence $(a_n)_n$ is *p-adically cauchy* if $\forall \epsilon > 0$, $\exists N > 0$ such that $n, m \geq N \implies |a_n - a_m|_p < \epsilon$.

Proposition 6.5. *A sequence $(a_n)_n$ of rational numbers is p-adically cauchy iff the sequence $(b_n)_n := (a_{n+1} - a_n)_n$ is p-adically null, i.e., $|a_{n+1} - a_n|_p \to 0$ as $n \to \infty$.*

Example 6.4. This is not true for $(\mathbb{R}, |\cdot|)$ where $|\cdot|$ is the usual absolute value. For example consider the sequence $(a_n)_n = (\sqrt{n})_n$. Then

$$|a_{n+1} - a_n| = |\sqrt{n+1} - \sqrt{n}| = \left| \frac{1}{\sqrt{n+1}} + \frac{1}{\sqrt{n}} \right| \to 0 \quad \text{as } n \to \infty.$$

But clearly $(a_n)_n$ is not a cauchy sequence since $\sqrt{n} \to \infty$ as $n \to \infty$.

PROOF. ($\Longrightarrow$) Clear.
($\Longleftarrow$) Suppose $|a_{n+1} - a_n|_p \to 0$ as $n \to \infty$. Let $\epsilon > 0$ and let $N_0 \in \mathbb{N}$ be such that $n \geq N_0 \Longrightarrow |a_{n+1} - a_n|_p < \epsilon$. Then for $m > n \geq N_0$,

$$\begin{aligned} |a_m - a_n|_p &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + a_{m-2} + \cdots + a_{n+1} - a_n|_p \\ &\leq \max\{|a_m - a_{m-1}|_p, |a_{m-1} - a_{m-2}|_p, \cdots, |a_{n+1} - a_n|_p\} \\ &< \epsilon. \end{aligned}$$

Hence $(a_n)_n$ is p-adically cauchy. □

Lemma 6.6. *If a sequence $(a_n)_n$ where $a_n \in \mathbb{Q}$ is p-adically convergent, then it is p-adically cauchy.*

PROOF. Suppose $a_n \to_p a \in \mathbb{Q}$. Then

$$|a_m - a_n|_p = |a_m - a + a - a_n|_p \leq \max\{|a_m - a|_p, |a_n - a|_p\} \to 0$$

as $n, m \to \infty$. □

Does being p-adically cauchy imply being p-adically convergent in $\mathbb{Q}$? Recall the first example with $f(x) = x^2 + 1 \equiv 0 \pmod{5^m}$. Using Hensel's lemma repeatedly, we can construct a sequence

$$a_1 = 2, \quad a_2 = 2 + 1 \cdot 5, \quad a_3 = 2 + 1 \cdot 5 + 2 \cdot 5^2, \quad \cdots$$

which is 5-adically cauchy and $a_n^2 \to_5 -1$. Since $\sqrt{-1} \notin \mathbb{Q}$, $(a_n)_n$ does not converge 5-adically in $\mathbb{Q}$.

We have similar problems when we consider cauchy sequences of rational numbers and their convergence with respect to usual norm $|\cdot|$. Recall that the cauchy sequence $((1 + \frac{1}{n})^n)_n \to e \in \mathbb{R} \setminus \mathbb{Q}$. But what is e? Since e is the limit of $((1 + \frac{1}{n})^n)_n$, one way would be to think it as the cauchy sequence itself. But we also have $1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots \to e$. So e would also be equal to the sequence $(\sum_{k=0}^{n} \frac{1}{k!})_n$. To avoid ambiguity, we consider the sequences $((1 + \frac{1}{n})^n)_n$ and $(\sum_{k=0}^{n} \frac{1}{k!})_n$ to be equivalent! We will follow the same idea in the p-adic setting.

4. Construction of $\mathbb{Q}_p$ and Completeness

Let C be the set of p-adically cauchy sequence of rational numbers. Define $\sim$ on C by

$$(a_n)_n \sim (b_n)_n \Longleftrightarrow (b_n - a_n)_n \qquad \text{is } p\text{-adically null.}$$

This is clearly an equivalence relation:

- (reflexitive) $(a_n - a_n)_n = (0)_n \to 0$ as $n \to \infty$.
- (symmetic) $(a_n - b_n)_n \to 0 \Longrightarrow (b_n - a_n)_n \to 0$.
- (transitive) $(a_n - b_n)_n \to 0$ and $(b_n - c_n)_n \to 0 \Longrightarrow (a_n - c_n)_n \to 0$ by the triangle inequality.

Definition. Define the *p-adic numbers* $\mathbb{Q}_p$ to be the set of equivalence classes of C under $\sim$, i.e.,

$$\mathbb{Q}_p = C/\sim$$

and we denote the class of $(a_n)_n \in C$ by $[(a_n)_n]$.

Note.

(1) Both the zero sequence $(0)_n$ in $\mathbb{Q}$ and $(p^n)_n$ are p-adically null. Thus in $\mathbb{Q}_p$, $[(0)_n] = [(p^n)_n] = [\text{any } p\text{-adically null sequence}]$.
(2) Let $a \in \mathbb{Q}$ and consider the constant sequence $(a)_n$. Then $[(a)_n] \in \mathbb{Q}_p$. We can thus identify $\mathbb{Q}$ as a subset of $\mathbb{Q}_p$ via the injection $a \mapsto [(a)_n]$.
(3) Let $(a_n)_n \in C$ be such that $a_n \to_p a \in \mathbb{Q}$. Then $[(a_n)_n] = [(a)_n]$ in $\mathbb{Q}_p$, since $|a_n - a|_p \to 0$ as $n \to \infty$.

Now we define operations on $\mathbb{Q}_p$. Note that if $(a_n)_n,\ (b_n)_n \in C$ then so are $(a_n + b_n)_n$ and $(a_n b_n)_n$. Define $+, \cdot$ on $\mathbb{Q}_p$ as follows.

- Addition: $[(a_n)_n] + [(b_n)_n] := [(a_n + b_n)_n]$.
- Multiplication: $[(a_n)_n] \cdot [(b_n)_n] := [(a_n b_n)_n]$.
- Additive identity: $0 := [(0)_n]$
- Multiplicative identity: $1 := [(1)_n]$

Exercise. (1) For the above defined addition and multiplication to be well-defined check that if $(a_n)_n \sim (a'_n)_n$ and $(b_n)_n \sim (b'_n)_n$ then $(a_n + b_n)_n \sim (a'_n + b'_n)_n$ and $(a_n b_n)_n \sim (a'_n b'_n)_n$.
(2) Check that $\mathbb{Q}_p$ is a commutative ring with $+, \cdot$.

Next we want to define the division in $\mathbb{Q}_p$. That is, we want to define $[(a_n)_n]/[(b_n)_n]$ where $[(b_n)_n] \neq [(0)_n]$, i.e., $(b_n)_n$ is not p-adically null. Note that we cannot simply define $[(a_n)_n]/[(b_n)_n] := [(\frac{a_n}{b_n})_n]$ since some of the terms of $(b_n)_n$ may be zero. But we can show that such $(b_n)_n$ contains only finitely many zero terms. We start with the following lemma.

Lemma 6.7. *Let $(a_n)_n$ be a p-adically cauchy sequence of rational numbers. Then $(|a_n|_p)_n$ converges in the usual norm $|\cdot|$ in $\mathbb{R}$ to some element in $\{0\} \cup \{p^r \mid r \in \mathbb{Z}\}$.*

Proof. It is easy to see that any cauchy sequence whose terms are in $\{0\} \cup \{p^r \mid r \in \mathbb{Z}\}$ converges in $|\cdot|$ to some element in the same set (**exercise**). Thus it is enough to show that $(|a_n|_p)_n$ is cauchy sequence with the norm $|\cdot|$.

Since $(a_n)_n$ is p-adically cauchy, $\forall \epsilon > 0$, $\exists\ N_0 \in \mathbb{N}$ such that $m, n \geq N_0 \implies |a_m - a_n|_p < \epsilon$. Thus $\forall\ m, n \geq N_0$ we get

$$\big|\, |a_m|_p - |a_n|_p \,\big| \leq |a_m - a_n|_p < \epsilon,$$

where the first inequality follows from the triangular inequality of $|\cdot|_p$. Hence $(|a_n|_p)_n$ is cauchy. $\square$

Corollary 6.8. *Let $(b_n)_n$ be a p-adically cauchy sequence of rational numbers that is not p-adically null. Then $(b_n)_n$ contains only finitely many terms that are zero.*

PROOF. By Lemma 6.7, $(|b_n|_p)_n$ has a limit, and $(|b_n|_p)_n \not\to 0$ since $(b_n)_n \not\to_p 0$. If $(b_n)_n$ contains infinitely many zero terms, then $(|b_n|_p)_n$ also contains infinitely many zero terms. So $(|b_n|_p)_n$ has a subsequence that converges to 0, which is a contradiction to the fact $(|b_n|_p)_n$ converges to a nonzero limit. □

Now we are ready to define the division in $\mathbb{Q}_p$. Let $(a_n)_n, (b_n)_n \in \mathbb{Q}_p$ where $(b_n)_n$ is not p-adically null. Then by the corollary above, $\exists\ N_0 \in \mathbb{N}$ such that $b_n \neq 0$ for all $n \geq N_0$. Define

$$c_n := \begin{cases} \frac{a_n}{b_n} & \text{if } n \geq N_0, \\ x_n & \text{if } n < N_0 \qquad \text{(can take any } x_n \in \mathbb{Q}\text{)}. \end{cases}$$

Note that $[(b_n)_n] \cdot [(c_n)_n] = [(a_n)_n]$ since $(b_n c_n - a_n)_n \to_p 0$ as $n \to \infty$. Hence we can define

$$[(a_n)_n]/[(b_n)_n] := [(c_n)_n].$$

Thus we have shown that every non-zero element in $\mathbb{Q}_p$ has a multiplicative inverse and so we have the following theorem.

Theorem 6.9. *$(\mathbb{Q}_p, +, \cdot)$ is a field containing $\mathbb{Q}$ as a subfield.*

Now we extend the p-adic norm that we defined on $\mathbb{Q}$ to $\mathbb{Q}_p$.

Definition. Let $\alpha \in \mathbb{Q}_p$. Then $\alpha = [(a_n)_n]$ for some $(a_n)_n \in C$, the set of p-adically cauchy sequences of rational numbers. We define

$$|\alpha|_p := \lim_{n\to\infty} |a_n|_p$$

(Note that the limit is taken with the usual norm in $\mathbb{R}$).

By Lemma 6.7, the limit in RHS exists and is in $\{0\} \cup \{p^r \mid r \in \mathbb{Z}\}$. We need to show that the above definition of norm on $\mathbb{Q}_p$ is well-defined, i.e.,

$$\alpha = [(a_n)_n] = [(b_n)_n] \in \mathbb{Q}_p \implies \lim_{n\to\infty} |a_n|_p = \lim_{n\to\infty} |b_n|_p .$$

PROOF. We have

$$|a_n|_p = |a_n - b_n + b_n|_p \leq \max\{|a_n - b_n|_p , |b_n|_p\}.$$

Recall that $[(a_n)_n] = [(b_n)_n] \implies (|a_n - b_n|_p)_n \to 0$ as $n \to \infty$. So if $(|b_n|_p)_n \to 0$ as $n \to \infty$, then $(|a_n|_p)_n \to 0$ and we are done. Now suppose $(|b_n|_p)_n \not\to 0$ as $n \to \infty$ Then $\exists\ N_0 \in \mathbb{N}$ such that $\forall n \geq N_0$, $|a_n - b_n|_p < |b_n|_p$. Hence $|a_n|_p = |b_n|_p$ for all $n \geq N_0$ and we are done. □

Thus for any $\alpha \in \mathbb{Q}_p$, $|\alpha|_p = 0$ or p^n for some $n \in \mathbb{Z}$. One can check that $|\cdot|_p$ in $\mathbb{Q}_p$ is indeed a norm, i.e., for all $\alpha, \beta \in \mathbb{Q}_p$,

(1) $|\alpha|_p \geq 0$ and $|\alpha|_p = 0$ iff $\alpha = 0$.
(2) $|\alpha\beta|_p = |\alpha|_p\, |\beta|_p$.

(3) $|\alpha+\beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$ with equality if $|\alpha|_p \neq |\beta|_p$.

PROOF. **Exercise** (use Lemma 6.2 and definition of $|\cdot|_p$). □

Since we have now defined a norm in $\mathbb{Q}_p$, we can talk of cauchy or convergent sequences in $\mathbb{Q}_p$ with respect to this norm. In fact if $\alpha \in \mathbb{Q}_p$ is represented as $\alpha = [(a_n)_n]$ where $(a_n)_n \in C$, then we have $a_n \to_p \alpha$ as $n \to \infty$ with respect to above defined norm in $\mathbb{Q}_p$ since

$$|a_n - \alpha|_p = \lim_{m\to\infty} |a_n - a_m|_p \to 0 \text{ as } n \to \infty.$$

Now we can prove the following theorem.

Theorem 6.10. *$\mathbb{Q}_p$ is complete with $|\cdot|_p$. That is, a sequence in $\mathbb{Q}_p$ is cauchy if and only if the sequence is convergent in $\mathbb{Q}_p$.*

PROOF. ($\Longleftarrow$) Easy and left as an **exercise**.
($\Longrightarrow$) Let $(\alpha_n)_n$ be a cauchy sequence in $\mathbb{Q}_p$, i.e., $\alpha_n \in \mathbb{Q}_p$ for all n. Let $\alpha_n = [(a_{n,m})_m]$ where $(a_{n,m})_m$ is a p-adically cauchy sequence in $\mathbb{Q}$. We want to show that $\exists\ \alpha \in \mathbb{Q}_p$ such that $|\alpha_n - \alpha|_p \to 0$ as $n \to \infty$, where $|\cdot|_p$ is now the extended norm in $\mathbb{Q}_p$.

For each n, since $(a_{n,m})_m$ is a p-adically cauchy, $\exists\ N_n \in \mathbb{N}$ such that $r, s \geq N_n \Longrightarrow |a_{n,r} - a_{n,s}|_p < \frac{1}{n}$. Now let $m \geq N_n$, then

$$|\alpha_n - a_{n,m}|_p = \lim_{r\to\infty} |a_{n,r} - a_{n,m}| \leq \frac{1}{n}.$$

We now construct $\alpha := [(c_n)_n] \in \mathbb{Q}_p$ such that $\alpha_n \to_p \alpha$ with the norm in $\mathbb{Q}_p$.

For each n, choose $k(n) > N_n$ such that $k(1) < k(2) < k(3) \cdots$. Let $(c_n)_n$ be a sequence in $\mathbb{Q}$ such that $c_n = a_{n,k(n)}$.

We will show that $(c_n)_n$ is p-adically cauchy.

Given $\epsilon > 0$, since $(\alpha_n)_n$ is a cauchy sequence in $\mathbb{Q}_p$, $\exists\ N'$ such that $n_1, n_2 > N' \Longrightarrow |\alpha_1 - \alpha_2|_p < \epsilon$. Then by taking $N_0 = \max\{N', \frac{1}{\epsilon}\}$, for $n_1, n_2 > N_0$, we have

$$\begin{aligned}
|c_{n_1} - c_{n_2}|_p &= \left|a_{n_1,k(n_1)} - a_{n_2,k(n_2)}\right|_p \\
&\leq \max\{\left|a_{n_1,k(n_1)} - \alpha_{n_1}\right|_p, |\alpha_{n_1} - \alpha_{n_2}|_p, \left|\alpha_{n_2} - a_{n_2,k(n_2)}\right|_p\} \\
&\leq \max\{\frac{1}{n_1},\ |\alpha_{n_1} - \alpha_{n_2}|_p,\ \frac{1}{n_2}\} \\
&< \max\{\epsilon,\ \epsilon,\ \epsilon\} = \epsilon.
\end{aligned}$$

Therefore $(c_n)_n$ is p-adically cauchy.

Finally, it remains to show that $\alpha_n \to_p \alpha = [(c_n)_n]$ as $n \to \infty$ in $\mathbb{Q}_p$-norm.

Let $\epsilon > 0$. Since $(c_n)_n$ is p-adically cauchy, $\exists\ M_0 > 2/\epsilon$ such that $m, n > M_0 \Longrightarrow |c_m - c_n|_p < \epsilon/2$. Thus for all $n > M_0$ we have

$$|\alpha - c_n|_p = \lim_{m\to\infty} |c_m - c_n|_p \leq \epsilon/2 < \epsilon,$$

and $|c_n - \alpha_n|_p = \left|a_{n,k(n)} - \alpha_n\right|_p < 1/n < 1/M_0 < \epsilon/2$. Hence by ultrametric inequality for all $n > M_0$

$$|\alpha - \alpha_n|_p \leq \max\{|\alpha - c_n|_p, |c_n - \alpha_n|_p\} < \epsilon$$

and we are done. □

Note that if $\alpha_n \to_p \alpha$ in $\mathbb{Q}_p$ norm then $|\alpha_n|_p \to |\alpha|_p$ in the usual norm $|\cdot|$. Also you can show as before that a sequence $(\alpha_n)_n$ now in $\mathbb{Q}_p$ is p-adically cauchy if and only if the sequence $(\alpha_n - \alpha_{n-1})_n \to_p 0$ as $n \to \infty$.

We have now the following theorem for convergence of series in $\mathbb{Q}_p$.

Theorem 6.11. *A series $\sum_{n=1}^{\infty} \alpha_n$ where $\alpha_n \in \mathbb{Q}_p$ converges p-adically in $\mathbb{Q}_p$ iff $\alpha_n \to_p 0$ as $n \to \infty$ in $\mathbb{Q}_p$.*

PROOF. ($\Longrightarrow$) Same proof as with the usual norm and left as an **exercise**.
($\Longleftarrow$) To show $\sum_{n=1}^{\infty} \alpha_n$ converges p-adically in $\mathbb{Q}_p$, it is enough to show by completeness of $\mathbb{Q}_p$ (Theorem 6.10) that $\sum_{n=1}^{\infty} \alpha_n$ is p-adically cauchy in $\mathbb{Q}_p$. So we need to show that the sequence of partial sums $(s_n)_n = (\sum_{i=1}^{n} \alpha_i)_n$ is p-adically cauchy. Now

$$s_n - s_{n-1} = \alpha_n \to_p 0 \text{ as } n \to \infty$$

in $\mathbb{Q}_p$. Hence by the note above $(s_n)_n$ is p-adically cauchy in $\mathbb{Q}_p$. □

It is now easy to see for example that $\sum_{n=1}^{\infty} np^n$ converges in $\mathbb{Q}_p$.

Definition. The set of *p-adic integers* $\mathbb{Z}_p$ is the unit disc in $\mathbb{Q}_p$ centered at 0, that is,

$$\mathbb{Z}_p := \{\alpha \in \mathbb{Q}_p : \ |\alpha|_p \leq 1\}.$$

Proposition 6.12. *$\mathbb{Z}_p$ is a ring and contains $\mathbb{Z}$ as a subring. The group of units of $\mathbb{Z}_p$ is*

$$\mathbb{Z}_p^{\times} = \{\alpha \in \mathbb{Z}_p : \ |\alpha|_p = 1\}.$$

PROOF. Enough to show $\mathbb{Z}_p$ is closed under $+, \cdot$. Now for any $\alpha, \beta \in \mathbb{Z}_p$,

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} \leq 1, \qquad |\alpha \cdot \beta|_p = |\alpha|_p |\beta|_p \leq 1.$$

If $\alpha \in \mathbb{Z}$ then $\mathrm{ord}_p(\alpha) \geq 0$ and hence $|\alpha|_p \leq 1$. Hence $\mathbb{Z} \subset \mathbb{Z}_p$. Suppose $\alpha \in \mathbb{Z}_p$ is invertible then there exists $\beta \in \mathbb{Z}_p$ such that $\alpha \cdot \beta = 1$, hence $|\alpha|_p |\beta|_p = |\alpha \cdot \beta|_p = 1$. Since $|\alpha|_p \leq 1$ and $|\beta|_p \leq 1$, we must have $|\alpha|_p = |\beta|_p = 1$. □

Theorem 6.13. *An element $\alpha \in \mathbb{Q}_p$ is a p-adic integer iff it is a p-adic limit of a cauchy sequence of integers.*

PROOF. ($\Longleftarrow$) Suppose α be a p-adic limit of cauchy sequence of integers $(a_n)_n$. Since $|a_n|_p \leq 1$ for all n, we have

$$|\alpha|_p = \lim_{n \to \infty} |a_n|_p \leq 1$$

and so $\alpha \in \mathbb{Q}_p$.
($\Longrightarrow$) Suppose $\alpha \in \mathbb{Q}_p$ be a p-adic integer. Then $\alpha = [(a_n)_n]$ for some p-adically cauchy sequence $(a_n)_n$ of rational numbers. We need to construct a sequence $(b_n)_n$ of integers such that $(a_n)_n \sim (b_n)_n$ and hence $\alpha = [(b_n)_n]$ which is what we want. Since $a_n \to_p \alpha$ in $\mathbb{Q}_p$ we have $\lim_{n\to\infty} |a_n|_p = |\alpha|_p \leq 1$ and so $\exists\ N_0$ such that $\forall n \geq N_0,\ |a_n|_p \leq 1$, i.e., $\text{ord}_p(a_n) \geq 0$. If $a_n = u_n/v_n$ in the least form where $u_n, v_n \in \mathbb{Z}$ then $\forall n \geq N_0,\ p \nmid v_n$. Hence for each such n there exists $w_n \in \mathbb{Z}$ such that $v_n w_n \equiv 1 \pmod{p^n}$. Now for all $n \geq N_0$ let $b_n = u_n w_n \in \mathbb{Z}$. Then

$$a_n = u_n/v_n \equiv u_n w_n = b_n \pmod{p^n}\ \forall n \geq N_0$$

and hence $(a_n)_n \sim (b_n)_n$. □

In the above proof we can in fact choose $b_n \in \mathbb{Z}$ such that $b_n \geq 0$. Thus a p-adic integer is a p-adic limit of a cauchy sequence of non-negative integers.

5. p-adic Digit Expansion

We would now like to describe $\mathbb{Q}_p$ explicitly using *p-adic digit expansion*, that is given $\alpha \in \mathbb{Q}_p$ we want to write α as $\alpha_{-k}p^{-k} + \alpha_{1-k}p^{1-k} + \cdots + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$ where $0 \leq \alpha_i \leq p-1$.

First consider $\alpha \in \mathbb{Z}_p$. By Theorem 6.13 there exists a sequence of non-negative integers $(b_n)_n$ such that $|\alpha - b_n|_p \to 0$ as $n \to \infty$. Let $B_0 := b_{n_0}$ be such that $|\alpha - B_0|_p < 1$. We can write $B_0 = pC_0 + \alpha_0$ for some $C_0,\ \alpha_0 \in \mathbb{Z}$ such that $0 \leq \alpha_0 \leq p-1$. Then $|\alpha - \alpha_0|_p \leq \max\{|\alpha - B_0|_p, |pC_0|_p\} < 1$. Thus we can find α_0 satisfying $0 \leq \alpha_0 \leq p-1$ such that

$$|\alpha - \alpha_0|_p \leq \frac{1}{p} < 1$$

and so

$$\frac{\alpha - \alpha_0}{p} \in \mathbb{Z}_p.$$

Repeating the above steps we can now find α_1 such that $0 \leq \alpha_1 \leq p-1$ such that

$$\left|\frac{\alpha - \alpha_0}{p} - \alpha_1\right|_p < 1 \qquad \text{i.e., } |\alpha - (\alpha_0 + p\alpha_1)|_p < \frac{1}{p}.$$

Repeating this process we get a sequence $\alpha_n \in \mathbb{Z}$ such that $0 \leq \alpha_n \leq p-1$ and

$$\left|\alpha - (\alpha_0 + \alpha_1 + \alpha_2 p^2 + \cdots + \alpha_n p^n)\right|_p < \frac{1}{p^n}.$$

Hence $\sum_{i=0}^{\infty} \alpha_i p^i \to_p \alpha$ in $\mathbb{Q}_p$ and we can write

$$\alpha = \alpha_0 + \alpha_1 + \alpha_2 p^2 + \cdots$$

and we call it the p-adic expansion of $\alpha \in \mathbb{Z}_p$. Now consider $\alpha \in \mathbb{Q}_p$ such that $|\alpha|_p = p^k$ for some $k > 0$. Let $\beta = p^k\alpha$ then $|\beta|_p = 1$ and so $\beta \in \mathbb{Z}_p$ and has p-adic expansion

$$\beta = \beta_0 + \beta_1 + \beta_2 p^2 + \cdots, \qquad 0 \leq \beta_i \leq p-1.$$

Hence

$$\alpha = \beta_0 p^{-k} + \beta_1 p^{-k+1} + \beta_2 p^{-k+2} + \cdots.$$

So we have proved the following theorem except for the uniqueness that is left as an **exercise**!

Theorem 6.14. *Every p-adic number $\alpha \in \mathbb{Q}_p$ has a unique p-adic expansion*

$$\alpha = \alpha_{-k}p^{-k} + \alpha_{1-k}p^{1-k} + \cdots + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots, \qquad 0 \leq \alpha_i \leq p-1.$$

If $\alpha \in \mathbb{Z}_p$ then $\alpha_{-r} = 0$ for all $r > 0$.

So in order to compute a p-adic digit expansion of $\alpha \in \mathbb{Z}_p$ we need to compute α modulo higher powers of p repeatedly. For example, 3-adic expansion of -1 is

$$-1 = 2 + 2.3 + 2.3^2 + 2.3^3 + \cdots.$$

In fact after computing $-1 \pmod{3^m}$ for first few m, we check that indeed $2+2.3+2.3^2+\cdots \to_3 \frac{2}{1-3} = -1$, which proves that it is the 3-adic expansion of -1. Here is another way of getting this!

$$\begin{aligned} &1 + (2 + 2.3 + 2.3^2 + \cdots) \\ &= 0 + 1.3 + 2.3 + 2.3^2 + \cdots \\ &= 0 + 0 + 1.3^2 + 2.3^2 + \cdots = \cdots = 0. \end{aligned}$$

6. Hensel's Lemma over $\mathbb{Z}_p$

We need the following lemma which is an analogue of polynomials in $\mathbb{Z}[x]$.

Lemma 6.15. *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial of degree n. Note that if $f(x) = \sum_{k=0}^{n} a_k x^k$ then derivative of $f(x)$ is $f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$. Thus one can recursively define $f^{(r)}(x)$.*

(a) *For $b \in \mathbb{Z}_p$ show that $f(b+x) = \sum_{k=0}^{n} \frac{f^{(k)}(b)x^k}{k!}$.*
(b) *Show that $\frac{f^{(r)}(x)}{r!} \in \mathbb{Z}_p[x]$.*

Proof. The proof is left as an **exercise**! You can first give an algebraic proof for the statements for $f(x) \in \mathbb{Z}[x]$ and observe that exactly same steps work for $f(x) \in \mathbb{Z}_p[x]$. We only need that $\mathbb{Z}_p$ is a commmutative ring with unity and has zero characteristic (i.e., $\underbrace{1+1+\cdots+1}_{n \text{ times}} \neq 0$ in $\mathbb{Z}_p$ for all $n \in \mathbb{N}$). □

Theorem 6.16 (Hensel's Lemma)**.** *Let $f(x) \in \mathbb{Z}_p[x]$. Let $\alpha_0 \in \mathbb{Z}_p$ be such that*

$$|f(\alpha_0)|_p \leq \frac{1}{p} \qquad \text{and} \qquad \left|f'(\alpha_0)\right|_p = 1.$$

Then there exists a sequence $(\alpha_n)_n$ given by

$$\alpha_{n+1} = \alpha_n - f'(\alpha_0)^{-1} f(\alpha_n)$$

such that for all $n \in \mathbb{N}$, we have

(1) $\alpha_n \in \mathbb{Z}_p$.
(2) $|\alpha_n - \alpha_0|_p < 1$.
(3) $|f(\alpha_n)|_p < \frac{1}{p^n}$.

Moreover, if $\alpha \in \mathbb{Z}_p$ is the p-adic limit of the p-adically cauchy sequence $(\alpha_n)_n$, then $f(\alpha) = 0$.

Before getting into the proof of the theorem let us look at how to use this theorem.

First note that Theorem 6.16 can be applied to polynomials in $\mathbb{Z}[x]$ since $\mathbb{Z} \subset \mathbb{Z}_p$. When applied to $f(x) \in \mathbb{Z}[x]$, it says that if $\exists\ \alpha_0 \in \mathbb{Z}$ such that $f(\alpha_0) \equiv 0 \pmod{p}$ and $f'(\alpha_0) \not\equiv 0 \pmod{p}$ then one can construct a p-adically cauchy sequence $(\alpha_n)_n$ of integers such that $f(\alpha_n) \equiv 0 \pmod{p^n}$ and $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$. Let $\alpha_n \to_p \alpha \in \mathbb{Z}_p$ then $f(\alpha) = 0$.

Corollary 6.17. *Let $b \in \mathbb{Z}$ such that $b \neq 0$. Let p be an odd prime. Then b is a square in $\mathbb{Z}_p$ iff $b = p^{2r}c$ where $c \in \mathbb{Z}$ such that $\left(\frac{c}{p}\right) = 1$.*

Proof. ($\Longleftarrow$) Let $b = p^{2r}c$ where $\left(\frac{c}{p}\right) = 1$. Consider $f(x) = x^2 - c \in \mathbb{Z}[x]$. Since $\left(\frac{c}{p}\right) = 1$, there exists a such that $\gcd(a, p) = 1$ and $a^2 \equiv c \pmod{p}$, i.e., $f(a) \equiv 0 \pmod{p}$. Also $f'(a) = 2a \not\equiv 0 \pmod{p}$ as p is odd and $\gcd(a, p) = 1$. So by Hensel's lemma there exists $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$, i.e., $\alpha^2 = c$. So $b = (p^r\alpha)^2$ is a square in $\mathbb{Z}_p$.
($\Longrightarrow$) Let $b = \beta^2$ for some $\beta \in \mathbb{Z}_p$. Also we can write $b = p^s c$ where $s \geq 0$ and $\gcd(c, p) = 1$. Now $|b|_p = p^{-s} = |\beta|_p^2$ is an even power of p. Hence s is even, say $s = 2r$. So $c = \frac{b}{p^{2r}} = (\frac{\beta}{p^r})^2$ is a square in $\mathbb{Q}_p$, say $c = \gamma^2$ for some $\gamma \in \mathbb{Q}_p$. Now $|\gamma|_p^2 = |c|_p = 1$, so $\gamma \in \mathbb{Z}_p$. Let $(\gamma_n)_n$ be a sequence of integers such that $\gamma_n \to_p \gamma$. Hence $\gamma_n^2 \to_p \gamma^2 = c$ and so there exists n_0 such that $\left|\gamma_{n_0}^2 - c\right|_p \leq \frac{1}{p}$, i.e., $\gamma_{n_0}^2 \equiv c \pmod{p}$. Hence $\left(\frac{c}{p}\right) = 1$. □

Proof of Theorem 6.16. Since $f'(x) \in \mathbb{Z}_p(x)$ and $\alpha_0 \in \mathbb{Z}_p$, we have $f'(\alpha_0) \in \mathbb{Z}_p$. Now since $|f'(\alpha_0)|_p = 1$, $f'(\alpha_0) \in \mathbb{Z}_p^\times$. So there exists $h := -(f'(\alpha_0))^{-1} \in \mathbb{Z}_p^\times$ with $|h|_p = 1$. We will prove that α_n satisfies the above equations (1), (2), (3) for all n using induction.

$\underline{n = 1}$: Since $\alpha_1 = \alpha_0 + hf(\alpha_0)$, clearly $\alpha_1 \in \mathbb{Z}_p$. Also,

$$|\alpha_1 - \alpha_0|_p = |hf(\alpha_0)|_p = |f(\alpha_0)|_p < 1.$$

Moreover using Lemma 6.15, we get that if $\deg(f) = t$ then

$$\begin{aligned} f(\alpha_1) &= f(\alpha_0 + hf(\alpha_0)) \\ &= f(\alpha_0) + f'(\alpha_0)hf(\alpha_0) + \frac{f''(\alpha_0)}{2!}h^2 f(\alpha_0)^2 + \cdots + \frac{f^{(t)}(\alpha_0)}{t!}h^t f(\alpha_0)^t \\ &= f(\alpha_0)(1 + f'(\alpha_0)h) + f(\alpha_0)^2 K \\ &= f(\alpha_0)^2 K \qquad\qquad (\text{as } 1 + f'(\alpha_0)h = 0) \end{aligned}$$

where $K \in \mathbb{Z}_p$. So

$$|f(\alpha_1)|_p = \left|f(\alpha_0)^2 K\right|_p < \frac{1}{p}$$

since $\left|f(\alpha_0)^2\right|_p \leq \frac{1}{p^2}$.

Induction hypothesis: Assume that α_{k-1} satisfies (1), (2), (3) above where $k \geq 2$.

Clearly $\alpha_k = \alpha_{k-1} + hf(\alpha_{k-1}) \in \mathbb{Z}_p$ since $\alpha_{k-1} \in \mathbb{Z}_p$. Moreover,

$$\begin{aligned} |\alpha_k - \alpha|_p &\leq \max\{|\alpha_k - \alpha_{k-1}|_p, |\alpha_{k-1} - \alpha|_p\} \\ &= \max\{|hf(\alpha_{k-1})|_p, |\alpha_{k-1} - \alpha|_p\} \\ &< 1 \end{aligned}$$

since $|hf(\alpha_{k-1})|_p < \frac{1}{p^{k-1}}$ and $|\alpha_{k-1} - \alpha|_p < 1$. Further using Lemma 6.15, we have

$$\begin{aligned} f(\alpha_k) &= f(\alpha_{k-1} + hf(\alpha_{k-1})) \\ &= f(\alpha_{k-1}) + f'(\alpha_{k-1})hf(\alpha_{k-1}) + f(\alpha_{k-1})^2 K_1 \\ &= f(\alpha_{k-1})(1 + f'(\alpha_{k-1})h) + f(\alpha_{k-1})^2 K_1 \end{aligned}$$

where $K_1 \in \mathbb{Z}_p$.

Since $|\alpha_{k-1} - \alpha_0|_p < 1$, we can write $\alpha_{k-1} = \alpha_0 + pt$ where $t \in \mathbb{Z}_p$. Thus

$$\begin{aligned} f'(\alpha_{k-1}) &= f'(\alpha_0 + pt) \\ &= f'(\alpha_0) + pK_2 \qquad (\text{applying Lemma 6.15 to } f') \end{aligned}$$

for some $K_2 \in \mathbb{Z}_p$. Hence

$$1 + hf'(\alpha_{k-1}) = 1 + hf'(\alpha_0) + phK_2 = phK_2$$

and so

$$\left|1 + hf'(\alpha_{k-1})\right|_p \leq \frac{1}{p}.$$

Hence it follows that

$$|f(\alpha_k)|_p \leq \max\{\left|f(\alpha_{k-1})(1 + f'(\alpha_{k-1})h)\right|_p, \left|f(\alpha_{k-1})^2 K_1\right|_p\} < \frac{1}{p^k}.$$

Clearly $(\alpha_n)_n$ is p-adically cauchy sequence in $\mathbb{Z}_p$ and so has a limit, say $\alpha \in \mathbb{Z}_p$. Therefore,

$$f(\alpha) = f(\lim_{n\to\infty} \alpha_n) = \lim_{n\to\infty} f(\alpha_n) = 0,$$

since $|f(\alpha_n)|_p < \frac{1}{p} \to 0$ as $n \to \infty$. Note that the middle equality is true since limit of sums and products are respectively sums and products of limits!. □

Theorem 6.18 (Hensel's Lemma - Strong version)**.** *Let $f(x) \in \mathbb{Z}_p[x]$. Let $\alpha_1 \in \mathbb{Z}_p$ be such that $|f(\alpha_1)|_p \leq \frac{1}{p^{2k+1}}$ and $|f'(\alpha_1)|_p = \frac{1}{p^k}$. Then there is a sequence $(\alpha_n)_n \in \mathbb{Z}_p$ such that*

$$(i)\ |\alpha_{n+1} - \alpha_n|_p \leq \frac{1}{p^{n+k}}, \qquad (ii)\ |f(\alpha_n)|_p \leq \frac{1}{p^{n+2k}}.$$

If $\alpha \in \mathbb{Z}_p$ is the p-adic limit of α_n, then $f(\alpha) = 0$.

Proof. Given $\alpha_1 \in \mathbb{Z}_p$ satisfying $|f(\alpha_1)|_p \leq \frac{1}{p^{2k+1}}$ and $|f'(\alpha_1)|_p = \frac{1}{p^k}$, we can construct the following sequence $(\alpha_n)_n$ given by

$$\alpha_{n+1} = \alpha_n - f'(\alpha_1)^{-1} f(\alpha_n)$$

such that for all $n \in \mathbb{N}$, we have

(1) $\alpha_n \in \mathbb{Z}_p$.
(2) $|\alpha_n - \alpha_1|_p \leq \frac{1}{p^{1+k}}$.
(3) $|f(\alpha_n)|_p < \frac{1}{p^{n+2k}}$.

Note that unlike Theorem 6.16, $f'(\alpha_1)^{-1} \in \mathbb{Q}_p \setminus \mathbb{Z}_p$, but since $|f(\alpha_1)|_p \leq \frac{1}{p^{2k+1}}$ we have

$$\left|f'(\alpha_1)^{-1} f(\alpha_1)\right|_p = \left|f'(\alpha_1)^{-1}\right|_p \cdot |f(\alpha_1)|_p \leq p^k \cdot \frac{1}{p^{2k+1}} = \frac{1}{p^{k+1}}.$$

So $f'(\alpha_1)^{-1} f(\alpha_1) \in \mathbb{Z}_p$ and hence $\alpha_2 = \alpha_1 - f'(\alpha_1)^{-1} f(\alpha_1) \in \mathbb{Z}_p$ and so for α_2, (1) and (2) holds. Now by Lemma 6.15,

$$\begin{aligned} f(\alpha_2) &= f(\alpha_1 + (-f'(\alpha_1)^{-1} f(\alpha_1))) \\ &= f(\alpha_1) - f'(\alpha_1) f'(\alpha_1)^{-1} f(\alpha_1) + p^{2k+2} K = p^{2k+2} K \end{aligned}$$

for some $K \in \mathbb{Z}_p$. Hence $|f(\alpha_2)|_p < \frac{1}{p^{2+2k}}$.

Now by proceeding the step of induction hypothesis as in Theorem 6.16 one obtains the strong version of Hensel's Lemma. Note that by construction of α_{n+1} we have

$$|\alpha_{n+1} - \alpha_n|_p = \left|f'(\alpha_1)^{-1} f(\alpha_n)\right|_p \leq p^k \cdot \frac{1}{p^{2k+n}} = \frac{1}{p^{n+k}},$$

at each step. □

Corollary 6.19. *Let $b \in \mathbb{Z}$ such that $b \neq 0$. Then b is a square in $\mathbb{Z}_2$ iff $b = 2^{2r} c$ for some $r \in \mathbb{N}$ where $c \equiv 1 \pmod 8$.*

Proof. ($\Longleftarrow$) Consider $f(x) = x^2 - c \in \mathbb{Z}[x]$. Since $c \equiv 1 \pmod 8$, we get that $f(c) \equiv 0 \pmod 8$, i.e. $|f(c)|_2 \leq \frac{1}{2^3}$. Moreover, since $f'(c) = 2c$ and c must be odd, we have $|f'(c)|_2 = \frac{1}{2}$. So by applying (a) with $k = 1$, there

exists $\alpha \in \mathbb{Z}_2$ such that $f(\alpha) = 0$, i.e. $\alpha^2 = c$. Hence $b = (2^r\alpha)^2$ is a square in $\mathbb{Z}_2$.

($\Longrightarrow$) Suppose $b = \beta^2$ for some $\beta \in \mathbb{Z}_2$. Also we can write $b = 2^s c$ where $\gcd(c, 2) = 1$. Now $|b|_2 = 2^{-s} = |\beta|^2$ is an even power of 2. Hence s is even, say $s = 2r$. Hence c is a square in $\mathbb{Z}_2$, say $c = \gamma^2$ where $|\gamma|_2 = 1$. So γ has 2-adic expansion

$$\gamma = 1 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots, \qquad a_i = 0 \text{ or } 1$$

After squaring γ one obtains 2-adic expansion

$$\gamma^2 = 1 + b_1 \cdot 2^3 + b_2 \cdot 2^4 + \cdots, \qquad b_i = 0 \text{ or } 1$$

Hence $c = \gamma^2 \equiv 1 \pmod 8$. □

7. Hasse Principle

Let $f(x_1, x_2, \ldots x_n) \in \mathbb{Z}[x_1, x_2, \ldots x_n]$. We want to know if $f = 0$ has solutions in integers. Since $\mathbb{Z} \subset \mathbb{Z}_p$ for all primes p and $\mathbb{Z} \subset \mathbb{R}$, we know that

$$f = 0 \text{ has solution in } \mathbb{Z}^n \Longrightarrow f = 0 \text{ has solution in } \mathbb{Z}_p^n \text{ for all primes } p \text{ and } f = 0 \text{ has solution in } \mathbb{R}^n.$$

So to show a diophantine equation has no integer solutions, it is enough to find a prime p such that it has no solutions in $\mathbb{Z}_p$.

Exercise. Show that the Diophantine equation

$$x^2 + 7y^4 = 3z^2.$$

has no non-trivial solution in integers by showing it has no non-trivial solution in $\mathbb{Z}_7$.

Suppose $f = 0$ has solution in $\mathbb{Z}_p^n$ for all primes p and has solution in $\mathbb{R}$. Then does $f = 0$ has solution in integers? This statement is called *Hasse Principle* and if it is true for f we say Hasse principle holds for f. Hasse principle holds for many polynomials. In particular we have

Theorem 6.20. *(Hasse-Minkowski) Let $f(x) \in \mathbb{Z}[x_1, x_2, \ldots x_n]$ be homogeneous degree 2 polynomial (i.e. each term of f has degree 2). Then Hasse principle holds for f.*

There are many polynomials for which Hasse principle fails! Here is a simple counterexample.

Example 6.5. Let $f(x) = (x^2-2)(x^2-17)(x^2-34)$. Clearly only solutions to $f(x) = 0$ in $\mathbb{R}$ are $\pm\sqrt{2}$, $\pm\sqrt{17}$, $\pm\sqrt{34}$. So it has no solutions in $\mathbb{Z}$. Now $17 \equiv 1 \pmod 8$, so by Corollary 6.19 we get that $x^2 - 17$ has a solution in $\mathbb{Z}_2$. Also $\left(\frac{2}{17}\right) = 1$, So $x^2 - 2$ has a solution in $\mathbb{Z}_{17}$. Thus $f(x) = 0$ has solution in $\mathbb{Z}_2$ and $\mathbb{Z}_{17}$. Suppose p be a prime such that $p \neq 2, 17$. We want to show $f(x) = 0$ has a solution in $\mathbb{Z}_p$. So enough to show that either 2 or 17 or 34 is a square modulo p in order to apply Hensel's lemma. If

$\left(\frac{2}{p}\right) = 1$ or $\left(\frac{17}{p}\right) = 1$ then we are done. Suppose $\left(\frac{2}{p}\right) = \left(\frac{17}{p}\right) = -1$. Then $\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = 1$ and so we are done.

Example 6.6. The polynomial $f(x, y) = 2y^2 - x^4 + 17$ is another counterexample to the Hasse Principle. Note that $f(x, y) = 0$ has solutions over $\mathbb{R}$, namely $(\sqrt[4]{17}, 0)$. Moreover it has solutions in $\mathbb{Z}_p$ for all primes p, the proof of which is not easy. Use quadratic reciprocity to check that $f(x, y) = 0$ has no integer solutions.

CHAPTER 7

Geometry of Numbers

Let n be a positive integer. Consider the group $(\mathbb{R}^n, +)$.

Definition. A subgroup of $\mathbb{R}^n$ is called a *(full) lattice* in $\mathbb{R}^n$ if $L = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdot + \mathbb{Z}v_n$ for some linearly independent vectors v_1, $v_2 \ldots v_n$ of $\mathbb{R}^n$. For example, $\mathbb{Z}^n$ is lattice in R^n.

Definition. A *sublattice* of $\mathbb{Z}^n$ is a subgroup of finite index.

Example 7.1. $2\mathbb{Z}^2$ is a sublattice of $\mathbb{Z}^2$ of index 4 since

$$\mathbb{Z}^2/2\mathbb{Z}^2 = \{(0,0),\ (1,0), (0,1), (1,1)\}.$$

Definition. A subset S of $\mathbb{R}^n$ is *symmetric* if for every $\underline{x} \in S$, $-\underline{x} \in S$.

Definition. A subset S of $\mathbb{R}^n$ is *convex* if for every pair of points $\underline{x}, \underline{y} \in S$, the line joining $\underline{x}$ and $\underline{y}$ is contained in S, i.e., $\lambda\underline{x} + (1-\lambda)\underline{y} \in S$ for all $\lambda \in [0,1]$.

Note that $\underline{0} \in S$ for every convex, symmetic subset S of $\mathbb{R}^n$.

Theorem 7.1 (Minkowski's Theorem)**.** *Let Λ be a sublattice of $\mathbb{Z}^n$ of index m. Let C be a convex symmetric subset of $\mathbb{R}^n$ having volume $V(C)$ such that $V(C) > 2^n m$. Then $C \cap \Lambda$ contains a point other than $\underline{0}$.*

Let us see some applications of Minkowski's Theorem.

1. Two Squares Theorem

Theorem 7.2. *Let $n = N^2 m$ be a positive integer where m is a square-free, i.e., $\mathrm{ord}_p(m) = 0$ or 1 for all primes $p \in \mathbb{P}$. Then, n is a sum of two squares iff m has no prime factor congruent to $3 \pmod 4$.*

Before we continue with the proof consider the following easy lemma

Lemma 7.3. *If m and n are each sum of two squares then so is mn.*

Proof. The proof follows from the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

□

Also note that $2 = 1^2 + 1^2$. So to prove the theorem we need to prove the following statement:
A square-free m is a sum of two squares iff any odd prime divisor of m is congruent to $1 \pmod 4$.

PROOF. ($\Longrightarrow$): Let $m = (a^2 + b^2)$. Let p be an odd prime divisor of m. If $p \mid a$ and $p \mid b$ then $p^2 \mid (a^2 + b^2) = m$, a contradiction to m square-free. So WLOG we may assume that $p \nmid b$. Let $d \in \mathbb{Z}$ such that $bd \equiv 1 \pmod{p}$. Then we have

$$(a^2+b^2) \equiv 0 \pmod{p} \Longleftrightarrow a^2 \equiv -b^2 \pmod{p} \Longleftrightarrow (a^2d^2) \equiv -1 \pmod{p}$$

$$\Longleftrightarrow \left(\frac{-1}{p}\right) = 1 \Longleftrightarrow p \equiv 1 \pmod{4}.$$

($\Longleftarrow$): Let $m = 2^\alpha p_1 p_2 \cdots p_k$ where p_i are distinct odd primes congruent to 1 (mod 4) and $\alpha = 0$ or 1. By Proposition 7.4 below it follows that p_i is a sum of two squares and hence so is m using Lemma 7.3. □

Proposition 7.4. *An odd prime p is a sum of two squares iff $p \equiv 1 \pmod{4}$.*

PROOF. ($\Longrightarrow$): Since sum of two squares is congruent to 0, 1 or 2 modulo 4.
($\Longleftarrow$): Since $p \equiv 1 \pmod{4}$ we know that $\left(\frac{-1}{p}\right) = 1$. Let $\ell \in \mathbb{Z}$ be such that $\ell^2 \equiv -1 \pmod{p}$. Let

$$\Lambda = \{(x, y) \in \mathbb{Z}^2 : x \equiv \ell y \pmod{p}\}.$$

Consider the map $\Theta : \mathbb{Z}^2 \to \mathbb{Z}/p\mathbb{Z}$ given by $(x, y) \mapsto [x - \ell y]_p$. It is easy to see that Θ is a group homomorphism and it is clear from the definition of Λ that $\mathrm{Ker}(\Theta) = \Lambda$. So Λ is a subgroup of $\mathbb{Z}^2$. Further for any $[a]_p \in \mathbb{Z}/p\mathbb{Z}$ we have $\Theta((a, 0)) = [a]_p$, hence Θ is surjective. So by First Isomorphism Theorem we get that

$$\mathbb{Z}^2/\Lambda \cong \mathbb{Z}/p\mathbb{Z}.$$

Thus $\#\mathbb{Z}^2/\Lambda = p$ and so Λ has index p in $\mathbb{Z}^2$. Consider the disc centered at $(0, 0)$ with radius $\sqrt{2p}$

$$C = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 2p\}.$$

This is clearly convex and symmetric with volume

$$V(C) = \mathrm{Area}(C) = 2\pi p > 2^2 p.$$

So applying Minkowski's Theorem to Λ and C we obtain a point $(x, y) \in C \cap \Lambda$ such that $(x, y) \neq (0, 0)$. Hence we have $0 < x^2 + y^2 < 2p$. Also $(x, y) \in \Lambda$ implies that

$$x^2 + y^2 \equiv \ell^2 y^2 + y^2 \equiv (\ell^2 + 1)y^2 \equiv 0 \pmod{p}.$$

Thus $x^2 + y^2$ is a multiple of p strictly between 0 and $2p$ and so $x^2 + y^2 = p$. □

We will next apply Minkowski's theorem to show that every positive integer can be written as sum of four squares! Before that we compute some areas and volumes.

2. Areas and Volumes

Let S be a subset of R^n. Let χ_S be the *characteristic* function of S defined by

$$\chi_S(\underline{x}) = \begin{cases} 1 & \text{if } \underline{x} \in S \\ 0 & \text{if } \underline{x} \notin S. \end{cases}$$

Then volume of S, denoted by $V(S)$, is defined to be

$$V(S) := \int_S \underline{dx} = \int_{\mathbb{R}^n} \chi_S(\underline{x})\ \underline{dx}.$$

Note that if we consider the coordinate system $x_1, x_2, \ldots x_n$ for $S \subset \mathbb{R}^n$ then $\underline{dx}$ is simply $dx_1 dx_2 \cdots dx_n$.

Example 7.2. Consider the ellipse

$$E_{a,b} = \left\{ (x,y) \in \mathbb{R}^2 : \frac{x^2}{a^2} + \frac{y^2}{b^2} < 1 \right\},$$

where a and b are positive integers. Then

$$V(E_{a,b}) = \iint_{E_{a,b}} 1 dxdy.$$

Consider the substitution $x/a = u$ and $y/b = v$. Then the ellipse $E_{a,b}$ in the xy-plane becomes the unit disc

$$D = \{(u,v) \in \mathbb{R}^2 : u^2 + v^2 < 1\}$$

in the uv-plane. Further $dx = adu$ and $dy = bdv$. Hence

$$V(E_{a,b}) = \iint_D abdudv = ab \iint_D 1 dudv = abV(D) = ab\pi.$$

Example 7.3. Consider the ellipsoid

$$E_{a,b,c} = \left\{ (x,y,z) \in \mathbb{R}^3 : \frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} < 1 \right\}.$$

Show that $V(E_{a,b}) = \pi abc$.

Example 7.4. We will next compute volume of Ball of radius r in 4-dimensions.

$$B_r = \{(x,y,z,w) \in R^4 : x^2 + y^2 + z^2 + w^2 < r^2\}.$$

Then

$$V(B_r) = \iiiint_{x^2+y^2+z^2+w^2<r^2} dxdydzdw.$$

Note that $-r < w < r$, so we can rewrite the integral as

$$V(B_r) = \int_{w=-r}^{w=r} \left(\iiint_{x^2+y^2+z^2<r^2-w^2} dxdydz \right) dw.$$

However $x^2+y^2+z^2 < r^2-w^2$ is a sphere in xyz-space of radius $\sqrt{r^2-w^2}$, so

$$\iiint_{x^2+y^2+z^2<r^2-w^2} dxdydz = \frac{4\pi}{3}(r^2-w^2)^{3/2}.$$

Hence

$$V(B_r) = \frac{4\pi}{3}\int_{w=-r}^{w=r}(r^2-w^2)^{3/2}dw = \frac{8\pi}{3}\int_{w=0}^{w=r}(r^2-w^2)^{3/2}dw.$$

Now substitute $w = r\sin\theta$, so $dw = r\cos\theta d\theta$. So

$$V(B_r) = \frac{8\pi}{3}\int_{\theta=0}^{\theta=\pi/2}(r^2 cos^2\theta)^{3/2} r\cos\theta d\theta = \frac{8\pi r^4}{3}\int_0^{\pi/2}\cos^4\theta d\theta.$$

Writing $\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2}$ and using binomial expansion we obtain that

$$\cos^4\theta = \frac{1}{8}\cos 4\theta + \frac{1}{2}\cos 2\theta + \frac{3}{8}.$$

Hence

$$V(B_r) = \frac{8\pi r^4}{3}\int_0^{\pi/2}\cos^4\theta d\theta = \frac{8\pi r^4}{3}\cdot\frac{3\pi}{16} = \frac{\pi^2 r^4}{2}.$$

3. Four Squares Theorem

Theorem 7.5. *Every positive integer n can be written as the sum of four integer squares.*

We need the following lemma.

Lemma 7.6. *(Euler's identity) If m and n are each sum of four squares then so is mn.*

Proof. The proof follows from the following identity

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = \\ (ax-by-cz-dw)^2 + (ay+bx+cw-dz)^2 \\ + (az-bw+cx+dy)^2 + (aw+bz-cy+dx)^2.\end{aligned}$$

□

Proof of Theorem 7.5. Since 2 is a sum of four squares and by above lemma it is enough to prove the statement of the theorem for odd primes. By Problem 9 Assignment 2, we know that there exists integers a, b such that $a^2+b^2+1 \equiv 0 \pmod p$. Consider

$$\Lambda = \{(x,y,z,w)\in\mathbb{Z}^4 : x \equiv az+bw \pmod p, \quad y \equiv bz-aw \pmod p\}.$$

By considering the homomorphism $\Theta : \mathbb{Z}^2 \to \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ given by $(x,y)\mapsto([x-az-bw]_p,\ [y-bz+aw]_p)$, it is easy to see that Λ is a subgroup of $\mathbb{Z}^4$ of index p^2. Consider the following ball of radius $\sqrt{2p}$

$$C = \{(x,y,z,w)\in\mathbb{R}^4 : x^2+y^2+z^2+w^2 < 2p\}.$$

C is clearly convex and symmetric and by the above example we know that

$$V(C) = \frac{\pi^2}{2}(\sqrt{2p})^4 = 2\pi^2 p^2 > 2^4 p^2.$$

Hence we can apply Minkowski's Theorem to obtain $(x, y, z, w) \in C \cap \Lambda$ such that $(x, y, z, w) \neq (0, 0, 0, 0)$. So we have $0 < x^2 + y^2 + z^2 + w^2 < 2p$. Further $(x, y, z, w) \in \Lambda$ implies that

$$\begin{aligned} x^2 + y^2 + z^2 + w^2 &\equiv (az + bw)^2 + (bz - aw)^2 + z^2 + w^2 \\ &= (a^2 + b^2 + 1)(z^2 + w^2) \equiv 0 \pmod{p}. \end{aligned}$$

Hence $x^2 + y^2 + z^2 + w^2$ is a multiple of p strictly between 0 and $2p$ and so $x^2 + y^2 + z^2 + w^2 = p$. □

4. Proof of Minkowski's Theorem

Theorem 7.7 (Blichfeldt's Theorem)**.** *Let $m \geq 1$ be an integer. Let S be a subset of $\mathbb{R}^n$ such that volume $V(S) > m$. Then there exists $m + 1$ distinct points $\underline{x}_0, \ldots, \underline{x}_m \in S$ such that*

$$\underline{x}_j - \underline{x}_i \in \mathbb{Z}^n, \qquad \text{for } 0 \leq i, j \leq m.$$

Proof. Let W be the unit cube:

$$W = \{(x_1, \ldots, x_n) : 0 \leq x_i < 1\}.$$

Clearly volume of W is 1. Every vector $\underline{x} \in \mathbb{R}^n$ can be decomposed uniquely as $\underline{x} = \underline{z} + \underline{w}$ where $\underline{z} \in \mathbb{Z}^n$ and $\underline{w} \in W$ (note that every x in $\mathbb{R}$ can be uniquely written as $\lfloor x \rfloor + \theta$ for some $0 \leq \theta < 1$). Thus

$$\mathbb{R}^n = \bigcup_{\underline{z} \in \mathbb{Z}^n} (\underline{z} + W),$$

where $\underline{z} + W = \{\underline{z} + \underline{w} : \underline{w} \in W\}$. Hence,

$$V(S) = \int_{\mathbb{R}^n} \chi_S(\underline{x})\ \underline{dx} = \sum_{\underline{z} \in \mathbb{Z}^n} \int_{\underline{w} \in W} \chi_S(\underline{z} + \underline{w})\ \underline{dw}.$$

Interchanging the summation and integration (note that if S is bounded set then the summation is a finite sum and we can exchange the sum and integral, in the general case one can use results from measure theory to justify this interchange! It's a good place to note that all the subset of R^n that we are dealing with are actually Lebesgue-measurable),

$$V(S) = \int_{\underline{w} \in W} \left(\sum_{\underline{z} \in \mathbb{Z}^n} \chi_S(\underline{z} + \underline{w}) \right) \underline{dw}.$$

Write $f(\underline{w}) = \sum_{\underline{z} \in \mathbb{Z}} \chi_S(\underline{z} + \underline{w})$. If $f(\underline{w} \leq m$ for all $\underline{w} \in W$ then $V(S) = \int_{\underline{w} \in W} f(\underline{w}) \underline{dw} \leq \int_{\underline{w} \in W} m \underline{dw} = mV(W) = m$, a contradiction to our assumption that $V(S) > m$. Hence there is some point $\underline{w_0} \in W$ such that $f(\underline{w_0}) > m$; i.e. $\sum_{\underline{z} \in \mathbb{Z}^n} \chi_S(\underline{z} + \underline{w_0}) > m$. But $\chi_S(\underline{z} + \underline{w_0})$ are either zeros or

ones, so there are $m+1$ distinct $\underline{z}_0, \ldots, \underline{z}_m \in \mathbb{Z}^n$ such that $\chi_S(\underline{z}_i + \underline{w}) = 1$. Let $\underline{x}_i = \underline{z}_i + \underline{w_0}$, so the $\underline{x}_i$ are distinct elements in S. Finally

$$\underline{x}_j - \underline{x}_i = (\underline{z}_j + \underline{w}) - (\underline{z}_i + \underline{w}) = \underline{z}_j - \underline{z}_i \in \mathbb{Z}^n.$$

□

Theorem 7.8 (Minkowski's Theorem)**.** *Let Λ be a sublattice of $\mathbb{Z}^n$ of index m. Let C be a convex symmetric subset of $\mathbb{R}^n$ having volume $V(C)$ such that $V(C) > 2^n m$. Then $C \cap \Lambda$ contains a point other than $\underline{0}$.*

Proof. Let

$$S = \frac{1}{2}C = \left\{ \frac{1}{2}\underline{x} : \underline{x} \in C \right\}.$$

The volume of S is

$$V(S) = \frac{1}{2^n}V(C) > m.$$

By Blichfeldt's Theorem, there are $m+1$ distinct points $\underline{x}_0, \ldots, \underline{x}_m \in S$ such that

$$\underline{x}_j - \underline{x}_i \in \mathbb{Z}^n, \qquad \text{for } 0 \le i, j \le m.$$

Let $\underline{y}_j = \underline{x}_j - \underline{x}_0 \in \mathbb{Z}^n$ for $j = 0, \ldots, m$. These are $m+1$ distinct points in $\mathbb{Z}^n$. Since Λ has index m in $\mathbb{Z}^n$, it has m cosets and so there exists $0 \le i \ne j \le m$ such that $\underline{y}_i, \underline{y}_j$ lie in the same coset of Λ, i.e., $0 \ne \underline{y}_j - \underline{y}_i \in \Lambda$. Hence $\underline{x}_j - \underline{x}_i = \underline{y}_j - \underline{y}_i$ is a non-zero element of Λ. Next we will show that $\underline{x}_j - \underline{x}_i \in C$.

Since $\underline{x}_j, \underline{x}_i \in S$ we have $\underline{x}_j = \frac{1}{2}\underline{c}$ and $\underline{x}_i = \frac{1}{2}\underline{c}'$ for some $\underline{c}$ and $\underline{c}'$ are in C. Now C is symmetric so, $\frac{1}{2}\underline{c} - \frac{1}{2}\underline{c}'$ is the mid-point between $\underline{c}$ and $-\underline{c}'$, so it must be in C. Hence $\underline{x}_j - \underline{x}_i \in C$. So $\underline{x}_j - \underline{x}_i$ is a non-zero element in $C \cap \Lambda$. □

5. Quadratic Forms and Hasse-Minkowski

Definition. A *quadratic form* over a commutative ring R in n variables is a homogeneous polynomial of degree 2 in $R[x_1, x_2, \ldots x_n]$.

Example 7.5.
(1) $f(x) = ax^2 \in R[x]$ is a quadratic form in one variable.
(2) $f(x) = ax^2 + bxy + cy^2 \in R[x, y]$ is a quadratic form in two variables. These are called *binary* quadratic forms.
(3) $f(x) = ax^2 + by^2 + cz^2 + dxy + exz + fyz \in R[x, y, z]$ is a quadratic form in three variables. These are called *ternary* quadratic forms.

Definition. A *diagonal* quadratic form over ring R in n variables is a quadratic form that looks like $a_1x_1^2 + a_2x_2^2 + \cdots + \cdots a_nx_n^2$.

Fact. Every quadratic form over a field F where $2 \ne 0$, i.e. characteristic not equal to 2 can be represented by a diagonal form after a suitable *invertible* linear change of variables over F.

In the case of binary quadratic form $ax^2 + bxy + cy^2$ where $a \neq 0$ one uses the change of variables $z = x + \frac{b}{2a}y$ and $w = y$, to get a diagonal form $az^2 + (c - \frac{b^2}{4a^2})w^2$. Note that this change of variable is invertible, i.e., we can write x, y in terms of z, w. Similarly we can get a digaonal form in the cases $c \neq 0$ or if $a = c = 0,\ b \neq 0$. For example, $x^2 + 2xy - 3y^2$ can be represented as $z^2 - 4w^2$ where $z = x + y$ and $w = y$.

Theorem 7.9 (Hasse-Minkowski for binary forms)**.** *A binary quadratic form $f(x, y)$ in $\mathbb{Q}[x, y]$ has a non-trivial zero in rationals iff it has non-trivial zeros in $\mathbb{Q}_p$ for all primes p and in $\mathbb{R}$.*

Proof. ($\Longrightarrow$:)Clearly having solutions in $\mathbb{Q}^2$ implies having solutions in $\mathbb{Q}_p^2$ for all primes p and in $\mathbb{R}^2$.
($\Longleftarrow$:) As shown above we can represent the given binary form $f(x, y)$ by a diagonal form $az^2 - bw^2$ after an invertible linear change of variables over $\mathbb{Q}$. Now note that since the change of variables is invertible,

$$\begin{aligned} & f(x,y) = 0 \text{ has a non-trivial solution in } \mathbb{Q}^2 \text{ or } \mathbb{Q}_p^2 \text{ or } \mathbb{R}^2 \\ \iff & az^2 - bw^2 = 0 \text{ has a non-trivial solution in } \mathbb{Q}^2 \text{ or } \mathbb{Q}_p^2 \text{ or } \mathbb{R}^2 \end{aligned} \tag{4}$$

So if $a = 0$ or $b = 0$ there is a non-trivial rational solution, say if $a = 0$ then $(1, 0)$ is a non-trivial solution to $az^2 - bw^2 = 0$. So we may assume $a \neq 0$, $b \neq 0$. Then (4) is equivalent to $z^2 - cw^2 = 0$ having a non-trivial solution in $\mathbb{Q}^2$ or $\mathbb{Q}_p^2$ or $\mathbb{R}^2$, where $c = b/a \in \mathbb{Q}^\times$. Let $c = \pm \prod_{p \in \mathbb{P}} p^{c_p}$ where $c_p \in \mathbb{Z}$.

Since by assumption $z^2 - cw^2 = 0$ has a non-trivial solution in $\mathbb{Q}_p^2$ for all primes p and in $\mathbb{R}^2$ we get that c is a square in $\mathbb{Q}_p$ for all primes p and c is a square in $\mathbb{R}$. Hence we must have $c > 0$ and c_p is even for all primes p. Hence c is a square in $\mathbb{Q}$ and thus $z^2 - cw^2 = 0$ has a non-trivial solution over rationals which completes the proof. □

Theorem 7.10 (Hasse-Minkowski for ternary forms)**.** *A ternary quadratic form over $\mathbb{Q}$ has a non-trivial zero in rationals iff it has non-trivial zeros in $\mathbb{Q}_p$ for all primes p and in $\mathbb{R}$.*

As before one way is easy! For the proof of the converse part, as before we can represent the given ternary form by a diagonal form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ after an invertible linear change of variables over $\mathbb{Q}$. We may assume that $a_1,\ a_2,\ a_3$ are all nonzero rationals since otherwise there will always be a non-trivial solution over rationals. We now have following lemmas.

Lemma 7.11. *Let $f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \in \mathbb{Q}[x_1, x_2, x_3]$ where $a_1a_2a_3 \neq 0$. Then there is an $\alpha \in \mathbb{Q}^\times$ such that*

$$g = \alpha f = b_1y_1^2 + b_2y_2^2 + b_3y_3^2 \tag{5}$$

where $b_1, b_2, b_3 \in \mathbb{Z}$ and $b_1b_2b_3$ is square-free.

PROOF. First we can multiply f by LCM of denominators of a_1, a_2, a_3 to get coefficients in integers, to obtain a form that looks like

$$a_1'(c_1x_1)^2 + a_2'(c_2x_2)^2 + a_3'(c_3x_3)^2$$

where $a_i',\ c_i \in \mathbb{Z}$ and a_i' are square-free. Let $z_i = c_ix_i$ and so our new form looks like

$$a_1'z_1^2 + a_2'z_2^2 + a_3'z_3^2.$$

Finally if there is a prime p such that p divides at least two of the coefficients, say $p \mid a_1'$ and $p \mid a_2'$ then dividing the above form by p we obtain

$$\frac{a_1'}{p}z_1^2 + \frac{a_2'}{p}z_2^2 + pa_3'\left(\frac{z_3}{p}\right)^2,$$

which can be written as

$$a_1''w_1^2 + a_2''w_2^2 + a_3''w_3^2,$$

where $a_1'' = \frac{a_1'}{p},\ a_2'' = \frac{a_2'}{p},\ a_3'' = pa_3'$ are integers and by change of variables $w_1 = z_1,\ w_2 = z_2,\ w_3 = \frac{z_3}{p}$.

We can continue this process to finally obtain a form of type (5) (note that this process should eventually stop as we are decreasing the absolute value of product of coefficients at every step). □

Lemma 7.12. *Let g be of the form* (5)*. Then*

(a) *Suppose $g = 0$ has a non-trivial solution in $\mathbb{Q}_p$. If p is an odd prime dividing $b_1b_2b_3$, say $p \mid b_3$ then there is an integer r_p such that $b_1r_p^2 + b_2 \equiv 0 \pmod{p}$.*

(b) *Suppose $g = 0$ has a non-trivial solution in $\mathbb{Q}_2$. Then*

  (i) *If $2 \nmid b_1b_2b_3$ then after permuting the indices we may assume that $b_1 + b_2 \equiv 0 \pmod 4$.*

  (ii) *Suppose $2 \mid b_3$. Then $b_1 + b_2 + b_3s^2 \equiv 0 \pmod 8$ where $s =$ 0 or 1.*

PROOF. For part (a), let $m_1, m_2, m_3 \in \mathbb{Q}_p$ not all zero be such that

$$b_1m_1^2 + b_2m_2^2 + b_3m_3^2 = 0. \tag{6}$$

We may assume, by multiplying a suitable power of p, that $m_1,\ m_2\, m_3 \in \mathbb{Z}_p$ and $\max\{|m_1|_p, |m_2|_p, |m_3|_p\} = 1$. Now $\left|b_3m_3^2\right|_p < 1$. We claim that $|m_1|_p = |m_2|_p = 1$. Suppose $|m_1|_p < 1$ Then $\left|b_2m_2^2\right|_p = \left|b_1m_1^2 + b_3m_3^2\right|_p < 1$. Since $p \nmid b_2$, we get $|m_2|_p < 1$. But then $\left|b_3m_3^2\right|_p = \left|b_1m_1^2 + b_2m_2^2\right|_p \leq 1/p^2$ which implies $|m_3|_p < 1$ contradicting $\max\{|m_1|_p, |m_2|_p, |m_3|_p\} = 1$. Hence $|m_1|_p = |m_2|_p = 1$. Let $r_p = m_1/m_2 \in \mathbb{Z}_p$. Then it follows from (6) that $b_1r_p^2 + b_2 \equiv 0 \pmod p$.

For part(b), let $m_1, m_2, m_3 \in \mathbb{Q}_2$ not all zero be a solution and we may assume as before that $\max\{|m_1|_2, |m_2|_2, |m_3|_2\} = 1$.

For part (i) let $2 \nmid b_1b_2b_3$. Then one can show as before if one of m_i has norm less than 1, then the other two are units in $\mathbb{Z}_2$. Also if any two of

them are units in $\mathbb{Z}_2$, say $|m_1|_2 = |m_2|_2 = 1$, then both $b_1m_1^2$ and $b_2m_2^2$ are 2-adic units and so their 2-adic expansion starts with 1. Hence $|b_3m_3^2|_2 = |b_1m_1^2 + b_2m_2^2|_2 \leq 1/2$ showing $|m_3|_2 < 1$. So precisely two of the m_i's are units in $\mathbb{Z}_2$, say $m_1,\ m_2$. Then $m_1^2 \equiv m_2^2 \equiv 1 \pmod 4$ giving $b_1 + b_2 \equiv 0 \pmod 4$.
For part(ii), let $2 \mid b_3$. As in part (a) we obtain $|m_1|_2 = |m_2|_2 = 1 > |b_3m_3^2|_2$ and so $m_1^2 \equiv m_2^2 \equiv 1 \pmod 8$. If $|m_3|_2 = 1$, we get $b_1+b_2+b_3 \equiv 0 \pmod 8$, else $|m_3|_2 < 1$ and we get $b_1 + b_2 \equiv 0 \pmod 8$. □

Proof of Theorem 7.10. Let $g = 0$ has solution in $\mathbb{Q}_p$ for all primes p and in $\mathbb{R}$. So Lemma 7.12 applies to g. The rest of the proof is an application of Minkowski's Theorem. Let Λ be a subgroup in $\mathbb{Z}^3$ consisting of $(n_1, n_2, n_3) \in \mathbb{Z}^3$ satisfying the following set of linear congruences:

(i) For each odd prime $p \mid b_3$ impose the condition $n_1 \equiv r_p n_2 \pmod p$. In this case, indeed we have $g(n_1, n_2, n_3) = b_1n_1^2 + b_2n_2^2 + b_3n_3^2 \equiv (b_1r_p^2 + b_2)n_2^2 \equiv 0 \pmod p$. Similarly for each odd prime $p \mid b_1$ or $p \mid b_2$ impose the respective conditions.
(ii) If $2 \mid b_3$, impose the conditions $n_1 \equiv n_2 \pmod 4$ and $n_3 \equiv sn_2 \pmod 2$ where $s = 0$ or 1 as in part(ii) of Lemma 7.12. Then one can check $g(n_1, n_2, n_3) \equiv 0 \pmod 8$. Impose similar conditions if $2 \mid b_1$ or $2 \mid b_2$.
(iii) If $2 \nmid b_1b_2b_3$ and $b_1 + b_2 \equiv 0 \pmod 4$, then impose the conditions $n_1 \equiv n_2 \pmod 2$ and $n_3 \equiv 0 \pmod 2$.

If (n_1, n_2, n_3) satisfies all the above imposed congruences then

$$g(n_1, n_2, n_3) \equiv 0 \pmod{|4b_1b_2b_3|}.$$

Let $\beta = |4b_1b_2b_3|$. Then it is clear that Λ is a sublattice in $\mathbb{Z}^3$ of index β. Let C be an ellipsoid given by

$$C = \{(r_1, r_2, r_3) \in \mathbb{R}^3 : |b_1|r_1^2 + |b_2|r_2^2 + |b_3|r_3^2 < |4b_1b_2b_3|\}.$$

In the above $|\cdot|$ is usual norm on $\mathbb{R}$. Now volume of the ellipsoid S is

$$V(C) = \frac{\pi}{3} \cdot 2^3 \cdot |4b_1b_2b_3| > 2^3\beta.$$

So applying Minkowski's theorem we obtain $(R_1, R_2, R_3) \in C \cap \Lambda$ such that $(R_1, R_2, R_3) \neq (0, 0, 0)$. Since $(R_1, R_2, R_3) \in \Lambda$ we get that

$$b_1R_1^2 + b_2R_2^2 + b_3R_3^2 \equiv 0 \pmod \beta.$$

Also $(R_1, R_2, R_3) \in C$ non-zero implies that

$$|b_1R_1^2 + b_2R_2^2 + b_3R_3^2| \leq |b_1|R_1^2 + |b_2|R_2^2 + |b_3|R_3^2 < \beta.$$

It follows now $b_1R_1^2 + b_2R_2^2 + b_3R_3^2 = 0$ concluding the proof. □

CHAPTER 8

Irrationality and Transcendence

1. Irrationality

A number in $\mathbb{R}$ is called *irrational* if it does not belong to $\mathbb{Q}$.

Example 8.1. $\sqrt{2}$ is irrational. Since if $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, then squaring both sides we get $2b^2 = a^2$ which implies 2 divides both a and b giving a contradiction to $\gcd(a, b) = 1$.

Theorem 8.1. *(Gauss) Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ be a monic polynomial with integer coefficients and degree $n \geq 1$. The only possible rational roots of f are integers which divide a_0.*

Proof. Let $r = \frac{c}{d}$ be a rational root of f where $c, d \in \mathbb{Z}$ with $\gcd(c, d) = 1$. Thus

$$a_0 + a_1\frac{c}{d} + \cdots + a_{n-1}\frac{c^{n-1}}{d^{n-1}} + \frac{c^n}{d^n} = 0. \tag{7}$$

Multiplying by d^n and rearranging we have

$$d(-a_0 d^{n-1} - a_1 c d^{n-2} - \cdots - a_{n-1}c^{n-1}) = c^n.$$

Thus $d \mid c^n$. We claim that $d = 1$. Suppose $d > 1$ and let p be any prime factor of d. Then $p \mid d$, so $p \mid c^n$ and hence $p \mid c$, giving a contradiction to $\gcd(c, d) = 1$. Hence $d = 1$. Therefore $r = c \in \mathbb{Z}$. Moreover, by (7) we have

$$c(-a_1 - a_2 c - \cdots - a_{n-1}c^{n-2}) = a_0,$$

hence $c \mid a_0$. Thus any rational root of f must be an integer dividing a_0. □

Corollary 8.2. *Let $n > 1$ be a positive integer. Suppose that d is a positive integer that is not an n-th power. Then $\sqrt[n]{d}$ is irrational.*

Proof. Let $f(x) = x^n - d$. Suppose $\sqrt[n]{d}$ is rational. By Gauss' Theorem, $\sqrt[n]{d}$ is an integer, say $\sqrt[n]{d} = c \in \mathbb{Z}$. Then $d = c^n$ is an n-th power, giving a contradiction. □

So far the only irrational numbers we have seen are roots of polynomials with integer coefficients. It is natural to wonder about the irrationality of naturally occuring numbers such as $e = \exp(1)$. In fact Euler proved that e is irrational by considering the expansion $e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots$. It is a hard fact that e is not a root of any polynomial with integer coefficients.

2. Algebraic and Transcendental Numbers

Definition. A number $\alpha \in \mathbb{C}$ is *algebraic* if there is some $n \geq 1$ and integers $a_0, a_1, \ldots, a_n$, not all zero, such that α is a root of the polynomial

$$a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x].$$

A number $\alpha \in \mathbb{C}$ is *transcendental* if it is not algebraic.

Example 8.2.

- Any rational number $\frac{p}{q}$ where $p, q \in \mathbb{Z}$ is algebraic since it is a root of $qx - p \in \mathbb{Z}[x]$.
- For any integer d, $\sqrt[n]{d}$ is algebraic since it is a root of $x^n - d \in \mathbb{Z}[x]$. Thus $\sqrt{2}$, i are algebraic.
- **Fact.** Sums and products of algebraic numbers are algebraic.
- **Hard Fact.** e and π are transcendental, i.e, e, π are not roots of any polynomial with integer coefficients.

Lemma 8.3. *The set of algebraic numbers is countable. Hence the set of transcendentals is uncountable.*

Proof. It is easy to see that the set of polynomial with integer coefficiets is countable (countable union of countable sets!). Also each such polynomial has finitely many roots. Hence the set of roots of polynomials with integer coefficients, which by definition is the set of algebraic numbers, is countable. Since $\mathbb{R}$ and hence $\mathbb{C}$ are uncountable, it follows that the set of transcendental is uncountable. □

Hence 'almost all' real and complex numbers are transcendental. However in general it is very hard to show that a given number is transcendental. The number e is transcendental was proved by Charles Hermite in 1872. In 1882 Lindemann showed that e^α is transcendental for α any non-zero algebraic number and hence $i\pi$ is transcendental since $e^{i\pi} = -1$. Since product of two algebraic numbers is algebraic it follows that π is transcendental.

In 1934, Gelfond and Schneider proved the following theorem.

Theorem 8.4. *If a and b are algebraic numbers that are not zero or one and b is not a rational number then a^b is transcendental.*

This theorem allows us to prove trancendence for many numbers. For example, $\sqrt{2}^{\sqrt{2}}$ is transcendental. Also $e^\pi = (e^{i\pi})^{-i}$ and hence transcendental. There are still many numbers

$$e + \pi,\ \pi e,\ \pi^e,\ e^e,\ \pi^\pi,\ e^{e^2},\ \pi^{\pi^2}, \cdots$$

that are expected to be transcendental but it is not even known whether they are rational or not!

Definition. Let α be an algebraic number. The *degree* of α is the smallest positive integer d such that there is a polynomial $f \in \mathbb{Z}[x]$ of degree d with $f(\alpha) = 0$.

Lemma 8.5. *Let α be an algebraic number of degree d. Then it is a root of an irreducible polynomial $f \in \mathbb{Z}[x]$ with degree d.*

PROOF. By definition of degree d, there is a polynomial $f \in \mathbb{Z}[x]$ of degree d such that $f(\alpha) = 0$. We show that f is irreducible. Suppose f is reducible, then we can write $f(x) = g(x)h(x)$ with $g(x)$, $h(x) \in \mathbb{Z}[x]$ having degree smaller than d. Now $f(\alpha) = 0$ implies either $g(\alpha) = 0$ or $h(\alpha) = 0$. This contradicts the mimimality of d. □

3. Liouville's Theorem

Theorem 8.6 (Liouville's Theorem)**.** *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree d. Then there is a constant $C > 0$, depending on α, so that for all rational numbers p/q,*

$$\text{either} \quad \alpha = \frac{p}{q}, \qquad \text{or} \quad \left|\frac{p}{q} - \alpha\right| \geq \frac{C}{q^d}.$$

PROOF. We know that $f(\alpha) = 0$ for some irreducible polynomial $f \in \mathbb{Z}[x]$ of degree $d \geq 1$. Write

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d.$$

Then for any rational number p/q,

$$\begin{aligned} f\left(\frac{p}{q}\right) &= a_0 + a_1 \frac{p}{q} + \cdots a_d \frac{p^d}{q^d} \\ &= \frac{N}{q^d} \end{aligned}$$

where $N = a_0 q^d + a_1 p q^{d-1} + \cdots + a_d p^d \in \mathbb{Z}$. Suppose that $N = 0$. Then $f(p/q) = 0$, so $qx - p$ is a factor of the irreducible polynomial f. Hence f is equal to $qx - p$ up to multiplication by a non-zero constant and hence degree 1. Now $f(\alpha) = 0$ implies that $q\alpha - p = 0$ so $\alpha = p/q$.

What happens if $\alpha \neq p/q$. Well, for a start $N \neq 0$. As N is an integer, $|N| \geq 1$. So

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}.$$

Now we note that

$$\begin{aligned} \frac{1}{q^d} &\leq \left|f\left(\frac{p}{q}\right)\right| \\ &= \left|f(\alpha) - f\left(\frac{p}{q}\right)\right| \qquad \text{since } f(\alpha) = 0 \\ &= f'(\eta)\left|\alpha - \frac{p}{q}\right|, \end{aligned} \tag{8}$$

by the Mean Value Theorem, where η is some number between α and p/q.

Let

$$C' = \sup\left\{|f'(t)| : \alpha - 1 \leq t \leq \alpha + 1.\right\}.$$

Let

$$C = \min\left\{1, \frac{1}{C'}\right\}.$$

We shall show that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^d},$$

which proves the theorem. If $\alpha - 1 \leq p/q \leq \alpha + 1$, then η is also in the interval $[\alpha - 1, \alpha + 1]$. So $f'(\eta) \leq C'$. Hence by (8),

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{C'}\frac{1}{q^d} \geq \frac{C}{q^d},$$

which is what we want. Now all we have to worry about is the case when p/q is outside the interval $[\alpha - 1, \alpha + 1]$. But this is easy:

$$\left|\alpha - \frac{p}{q}\right| \geq 1 \geq \frac{1}{q^d} \geq \frac{C}{q^d},$$

which completes the proof. □

Joseph Liouville was the first to construct transcendental numbers in 1844. Here is his example.

Corollary 8.7. *Let*

$$\alpha = \sum_{i=0}^{\infty} \frac{1}{10^{i!}}.$$

Then α is transcendental.

Proof. We prove this using contradiction. Suppose that α is algebraic of degree d. Let $n \geq 1$ and let $q = 10^{n!}$. Let

$$p = q \cdot \sum_{i=0}^{n} \frac{1}{10^{i!}}.$$

Note that p, q are positive integers, and that

$$\begin{aligned}
0 &< \alpha - \frac{p}{q} \\
&= \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+2)!}} + \cdots \\
&= \frac{1}{10^{(n+1)!}}\left(1 + \frac{1}{10^{(n+2)!-(n+1)!}} + + \frac{1}{10^{(n+3)!-(n+1)!}} + \cdots\right) \\
&< \frac{1}{10^{(n+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \cdots\right) \quad \text{since } (n+k)! - (n+1)! > (k-1) \\
&= \frac{10}{9 \cdot 10^{(n+1)!}}.
\end{aligned}$$

By the first inequality $\alpha \neq p/q$. Hence by Liouville's Theorem there exists a positive constant C such that

$$\frac{10}{9 \cdot 10^{(n+1)!}} > \alpha - \frac{p}{q} > \frac{C}{q^d} = \frac{C}{10^{d \cdot n!}}.$$

Hence

$$\frac{10}{9C} > 10^{(n+1)! - d \cdot n!}.$$

Note that here d and C are fixed, where as we can choose n as large as we like. Making n very large gives a contradiction. $\square$