Introduction to Number Theory Notes

Francesco Chotuck

Abstract

This is KCL undergraduate module 5CCM224A, instructed by Dr Stephen Lester. The formal name for this class is "Introduction to Number Theory".

Contents

1 Divisibility

1.1 GCD & Euclidean algorithm

Definition 1.1. Let a and b be two integers. We say that b **divides** a if there exists an integer q such that $a = qb$. If b divides a, we write $b \mid a$.

Theorem 1.1

Some basic properties of divisibility, let $a, b, c \in \mathbb{Z}$:

1. If $a \mid b$ and $b \mid c$, then $a \mid c$.
2. If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.
3. If $a \mid 1$ then $a = \pm 1$.
4. If $a \mid b$ and $b \mid a$ then $a = \pm b$.
5. Suppose $c \neq 0$ then, $a \mid b$ if and only if $ac \mid bc$.

Example 1.1. Prove $\gcd(a, b) = \gcd(a + b, b)$.
Solution: Let d be a divisor of a and $(a + b)$ then,

$$\begin{aligned} d \mid a \quad &\text{and} \quad d \mid (a+b) \\ \Rightarrow d \mid &\underbrace{(a + b - a)}_{b} \end{aligned}$$

Theorem 1.1 (Division algorithm)**.** Let $a \in \mathbb{Z}$ and $b \in N$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that

$$a = qb + r$$

and $0 \leq r < b$.

Definition 1.2. Let a and b be integers. If d is another integer such that $d \mid a$ and $d \mid b$ then we call d a **common divisor** of a and b.

Definition 1.3. If at least one of a and b are non-zero then we define the **greatest common divisor** of a and b to be the largest positive integer d which is a common divisor of a and b. This is usually denoted as $\gcd(a, b)$.

Lemma 1.1 (Euclidean algorithm)**.** If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.

Example 1.1

Let $a = 1492$ and $b = 1066$. Then applying the Euclidean algorithm:

$$\begin{aligned}
1492 &= 1 \cdot 1066 + 426 \\
1066 &= 2 \cdot 426 + 214 \\
426 &= 1 \cdot 214 + 212 \\
214 &= 1 \cdot 212 + 2 \\
212 &= 106 \cdot 2 + 0.
\end{aligned}$$

The last non-zero remainder is 2, so $\gcd(1492, 1066) = 2$.

Remark 1.1. Why the Euclidean algorithm works:

- Algorithm always terminates since the remainder strictly decreases;
- Refer to Lemma 1.1 – each iteration of the algorithm does not change the gcd of the original pair;
- $\gcd(0, r) = r$ for $r \in \mathbb{Z}$.

1.2 Bezout's lemma

Theorem 1.2 (Bezout's lemma)

Let a and b be integers (not both 0). Then there exists integers x and y such that

$$\gcd(a, b) = ax + by.$$

Example 1.2

Using the information from Example 1.1 we can 'reverse' the Euclidean algorithm to find the integers x, y such that $\gcd(1492, 1066) = 2 = 1492x + 1066y$. So, we have:

$$\begin{aligned}
\gcd(1492, 1066) &= 2 \\
&= 214 - 1 \cdot 212 \\
&= 214 - 1 \cdot (426 - 1 \cdot 214) \\
&= -1 \cdot 426 + 2 \cdot 214 \\
&= -1 \cdot 426 + 2(1066 - 2 \cdot 426) \\
&= 2 \cdot 1066 - 5 \cdot 426 \\
&= 2 \cdot 1066 - 5(1492 - 1 \cdot 1066) \\
&= -5 \cdot 1492 + 7 \cdot 1066.
\end{aligned}$$

Therefore, $(x, y) = (-5, 7)$.

Proposition 1.1. Let a, b be integers, not both zero, and consider the set

$$S = \{ax + by : x, y \in \mathbb{Z}\}.$$

Let $d > 0$ be the smallest positive integer in S. Then $d = \gcd(a, b)$.

Remark 1.2. A consequence of Proposition 1.1:
$\gcd(a, b) = 1$ if and only if there are integers x, y such that

$$1 = ax + by.$$

Corollary 1.1. Let a, b be integers, not both zero and consider the set

$$S = \{ax + by : x, y \in \mathbb{Z}\};$$

we can also consider the set

$$S' = \{n \gcd(a, b) : n \in \mathbb{Z}\}.$$

Then the two sets of integers S, S' are equal.

Note 1.1. Interpretation of Corollary 1.1: linear combinations (over $\mathbb{Z}$) of a, b are precisely the multiples of $\gcd(a, b)$.

Corollary 1.2. Let a, b be integers, not both zero. Let c be an integer. Then c is a common divisor of a and b if and only if $c \mid \gcd(a, b)$.

Definition 1.4. Two integers a, b are said to be **coprime** or **relatively prime** if

$$\gcd(a, b) = 1.$$

Lemma 1.1

Suppose a, b are coprime:

1. If $a \mid c$ and $b \mid c$ then $(ab) \mid c$;
2. if $a \mid (bc)$ then $a \mid c$;
3. if a and c are also coprime, then a and bc are coprime.

Proof.
1. We have $ax + by = 1$ for some integers x, y. Since $a \mid c$ and $b \mid c$ then we can write $c = aj$ and $c = bk$. Multiplying the first equation by c we get

$$\begin{aligned} cax + cby &= c \\ (bk)ax + (aj)by &= c \\ ab(kx) + ab(jy) &= c \\ ab(kx + by) &= c. \end{aligned}$$

   So, $(ab) \mid c$.

2. We have $c = cax + cby$. Since $a \mid (bc)$ and $a \mid a$ we get that $a \mid [a(cx) + (bc)y] = c$.

3. We have
$$1 = au + bv \quad \text{and} \quad 1 = ax + cy.$$
Multiplying the equations together gives
$$\begin{aligned} 1 &= (au + bc)(ax + cy) \\ &= a(uax + ucy + bvx) + bc(vy). \end{aligned}$$
It follows that $\gcd(a, bc) = 1$.

□

1.3 LCM & Linear Diophantine Equations

Definition 1.5. If a, b are integers, then a **common multiple** of a and b is an integer c such that $a \mid c$ and $b \mid c$.

Definition 1.6. If a and b are both non-zero, the **least common multiple** of a and b is defined to be the **smallest** (positive) integer $\operatorname{lcm}(a, b)$ which is a common multiple of a and b.

Proposition 1.2. Let a, b be non-zero integers. Then
$$\gcd(a, b)\operatorname{lcm}(a, b) = |ab|$$

Corollary 1.3. Let $a, b \in \mathbb{N}$. Suppose $\gcd(a, b) = 1$ then $\operatorname{lcm}(a, b) = ab$

> **Remark 1.3.** The $\operatorname{lcm}(a, b) \leq ab$ for $a, b > 0$.

Definition 1.7. Linear Diophantine equations where $a, b, c \in \mathbb{Z}$ are equations of the form
$$ax + by = c,$$
has integer solutions for (x, y).

> **Note 1.2.** In general, **Diophantine equations** are equations in one or more variables, for which we seek integer valued solutions.

Theorem 1.2. Let a, b, c be integers, with a and b not both 0 and let $g = \gcd(a, b)$. The equation
$$ax + by = c$$
has an integer solution (x, y) if and only if $\gcd(a, b) \mid c$.

Theorem 1.3

Assume $\gcd(a, b) \mid c$. Let x_0 and y_0 be solutions to $ax_0 + by_0 = g$. Then the solutions to
$$ax + by = c$$
are given by $(x_n, y_n)_{n \in \mathbb{Z}}$, where
$$\begin{aligned} x_n &= \frac{c}{g}x_0 + \frac{b}{g}n, \\ y_n &= \frac{c}{g}y_0 - \frac{a}{g}n. \end{aligned}$$

2 Prime numbers & modular arithmetic

2.1 Prime numbers

Definition 2.1. An integer $p > 1$ is called a **prime number** or a **prime** if it has no positive divisors other than 1 and p.
An integer $n > 1$ is called **composite** if it is not prime.

Theorem 2.1 (Fundamental theorem of arithmetic)**.**
Every integer $n > 1$ can be expressed uniquely (up to reordering) as a product of primes.

Corollary 2.1. There exists primes $p_1, p_2, \dots, p_r$ and non-negative integers, $a_1, a_2, \dots, a_n$ with

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

Lemma 2.1 (Euclid's Lemma)**.**

1. Let p be a prime number and let a, b be integers. Suppose $p \mid ab$, then $p \mid a$ or $p \mid b$.
2. If we have integers $a_1, a_2, \dots, a_n$ and $p \mid (a_1, a_2, \dots, a_n)$ then $p \mid a_i$ for some i.

Lemma 2.1

Let

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

with the p_i distinct primes and the a_i positive integers. Then,

1. $d > 0$ is a divisor of n if and only if

$$d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

   with $0 \leq b_i \leq a_i$ for each i.
2. The number of positive divisors of n is $\prod_{i=1}^{r}(a_i + 1)$.

Example 2.1. How many divisors does 200 have?
Solution: The prime factorisation of $200 = 2^3 \cdot 5^2$ therefore, 200 has $(3+1)(2+1) = 12$ divisors.

Example 2.1

How many positive divisors of $999 = 3^3 \cdot 37$ are multiples of 9?
Solution: We have that any divisor of 999 is of the form $d = 3^a \cdot 37^b$ for $0 \leq a \leq 3$ and $0 \leq b \leq 1$. For d to be a multiple of 9 we need $9 \mid d \iff a \geq 2$. Hence, $2 \leq a \leq 3 \Rightarrow 2$ choices and $0 \leq b \leq 1 \Rightarrow 2$ choices; we then have $2 \cdot 2 = 4$ choices in total, i.e. 4 such divisors.

Proposition 2.1. For $n \in \mathbb{N}$, then the $\gcd(n, n+1) = 1$.

Proof. If $d \mid n$ and $d \mid (n+1)$ then $d \mid (n+1-n) = d \mid 1$ (i.e. any linear combination of n and $n+1$) so, $d = \pm 1$. Since $d > 0$ to be the gcd we have that $d = 1$. □

Lemma 2.2. Let m, n be two positive integers with

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$
$$n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

where $a_i, b_i \geq 0$ are integers. Then,

1. $\gcd(m, n) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where $e_i = \min(a_i, b_i)$.
2. $\operatorname{lcm}(m, n) = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ where $f_i = \max(a_i, b_i)$.

Theorem 2.2 (Euclid)**.** There are infinitely many primes.

2.2 Infinite primes

Proposition 2.2. There are infinitely many primes of the form $4k + 3$, with $k \in \mathbb{N}$.

Proof. We will be using the following facts:

1. For $n \in \mathbb{N}$ we have that $n = 4k, 4k + 1, 4k + 2$, or $4k + 3$ for some $k \in \mathbb{Z}$. [This follows from the division algorithm applied to 4 and n].
2. If $a, b \in \mathbb{Z}$ with $a = 4k + 1$ and $b = 4j + 1$ for some $k, j \in \mathbb{Z}$ then $ab = (4k + 1)(4j + 1) = 4\underbrace{(4kj + k + j)}_{k'} + 1 = 4k' + 1$. I.e. numbers of this form are closed under multiplication.

We will use a proof by contradiction. Suppose, $p_1, p_2, \ldots, p_r$ are all primes of the form $4k + 3$. Consider

$$N = 4(p_1 p_2 \cdots p_r - 1) + 3$$
$$N = 4p_1 p_2 \cdots p_r - 1$$

This number is of the form $4k + 3$, we suppose N is not prime, so there must exist a prime which divides N. If $p \mid N$ then p is odd since N is odd. Using Fact (1) we have that $p \neq 4k, 4k + 2$ for any $k \in \mathbb{Z}$ since N is odd. Also since $p \mid N$ and $p \mid p_1 p_2 \cdots p_r$ we know that $p \nmid p_1 p_2 \cdots p_r$ since

$$N - 4p_1 p_2 \cdots p_r = 1$$

so $p \neq p_j$ for any $j = 1, 2, \ldots, r$ [from divisibility facts we know that p must divide any linear combination of N and $p_1 p_2 \cdots p_r$ so, we choose our linear combination to be $N - 4p_1 p_2 \cdots p_r = 1$]. This tells us that $p \neq 4k + 3$ for any $k \in \mathbb{Z}$. By Fact [1] $p = 4k + 1$ for $k \in \mathbb{Z}$, because there is no $k \in \mathbb{Z}$ for which $4k + 3 = 1$. By Fact [2] we have that N is also of the form $4k + 1$, i.e. $N = 4k' + 1$ for some $k' \in \mathbb{Z}$.

$$\begin{aligned} 4k' + 1 = N &= 4p_1 p_2 \cdots p_r - 1 \\ &= 4(p_1 p_2 \cdots p_r - 1 - k') = 2 \\ &\Rightarrow 4 \mid 2. \end{aligned}$$

We have arrived at a contradiction. $\square$

Theorem 2.1

Let $a \in \mathbb{Z}$ and $q \in \mathbb{N}$. Suppose that $\gcd(a, q) = 1$. Then there are infinitely many primes of the form $qk + a$ with k a positive integer.

2.3 Congruence

Definition 2.2. Let m be a non-zero integer and let $a, b \in \mathbb{Z}$. We say that a is **congruent** to b **modulo** m if $m \mid (a - b)$. If a is congruent to b modulo m, we write

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

Remark 2.1. The definition of congruence also implies that

1. $a = b + km$ for some $k \in \mathbb{Z}$;
2. a and b have the same remainder on division by m.

Theorem 2.2

Some properties of congruences:

1. $a \equiv b \pmod{m} \iff b \equiv a \pmod{m} \iff a - b \equiv 0 \pmod{m}$.
2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$ and $ax + cy \equiv bx + dy \pmod{m}$ for all $x, y \in \mathbb{Z}$.
4. For $n \geq 1$ we have $a^n \equiv b^n \pmod{m}$.
5. If $a \equiv b \pmod{m}$ and $d \mid m$, then $a \equiv b \pmod{d}$.
6. Suppose $c \neq 0$, $a \equiv b \pmod{m}$ if and only if $ac \equiv bc \pmod{mc}$.

Example 2.2. Example of Property 5:

$$8x \equiv 2 \pmod{10} \Rightarrow 4x \equiv 1 \pmod{5}.$$

Note 2.1. Some of these properties are inherent from congruences being an **equivalence** relation.

Definition 2.3. Let m be a non-zero integer and $a \in \mathbb{Z}$. The **residue class** or **congruence class** of a is the set

$$\begin{aligned} [a]_m &= \{b \in \mathbb{Z} : b \equiv a \pmod{m}\} \\ &= \{a + mk : k \in \mathbb{Z}\}. \end{aligned}$$

Remark 2.2. Congruence classes modulo m can be thought of all the integers that have a common remainder when divided by m.

Note 2.2. If the modulo m is not specified then write $[a]$.

Lemma 2.3.

$$[a]_m = [b]_m \iff a \equiv b \pmod{m}.$$

Definition 2.4. For a positive integer m, the set $\mathbb{Z}_m$ denotes the set of congruence classes modulo m. That is

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

Remark 2.3. If $\{x_1, x_2, \ldots, x_m\}$ is **any** complete residue system modulo m then the set

$$\mathbb{Z}_m = \{[x_1]_m, [x_2]_m, \ldots, [x_m]_m\}.$$

Definition 2.5. For $m \neq 0$ and $a, b \in \mathbb{Z}$ the operations of addition and multiplication on $\mathbb{Z}_m$ are defined by:

$$[a]_m + [b]_m = [a+b]_m$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m.$$

Definition 2.6. Let m be a positive integer. A set $\{x_1, x_2, \ldots, x_r\}$ is called a **complete residue system** modulo m (CRS) if for every integer y there is exactly one x_i such that

$$y \equiv x_i \pmod{m}.$$

Remark 2.4. In general, every complete residue system modulo m has size m.

Note 2.3. We can reformulate the definition of a CRS as: all the elements of the group $\mathbb{Z}_m$.

Example 2.3. Let m be a positive integer. Then $\{0, 1, 2, \ldots m-1\}$ is a complete residue system modulo m.

2.4 Solving equations in $\mathbb{Z}_m$

Lemma 2.2

Let m be a positive integer and let $a \in \mathbb{Z}$. If $\gcd(a, m) = 1$ then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$.
We call such ab **inverse** of a modulo m, where the residue class $[b]_m$ by $[a]_m^{-1}$.

Remark 2.5. Reformulation: $[a]_m \in \mathbb{Z}_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.

Proof. Proof of converse($\Leftarrow$):
Suppose $\gcd(a, m) = 1$ then we want to show $\exists u \in \mathbb{Z}$ with $au = 1 \pmod{m}$, i.e. $[u]_m = [a]_m^{-1}$. By Bezout's lemma $\exists u \in \mathbb{Z}$ such that

$$au + mv = 1$$
$$\Rightarrow m \mid 1 - au$$
$$\Rightarrow au \equiv 1 \pmod{m}.$$

Proof of ($\Rightarrow$):
Suppose $\exists [b]_m \in \mathbb{Z}_m$ with $[a]_m \cdot [b]_m = [1]_m$ i.e.

$$\begin{aligned} ab &\equiv 1 \pmod m \\ \Rightarrow m &\mid ab - 1 \\ \Rightarrow mv &= ab - 1. \end{aligned}$$

If $d \mid m$ and $d \mid a$ then $d \mid \underbrace{(mv - ab)}_{-1}$ therefore $d \mid \pm 1 \Rightarrow \gcd(a, m) = 1$. □

Proposition 2.1
Let $a, b, m \in \mathbb{Z}$ and $m \neq 0$ then

$$ax \equiv b \pmod m$$

has solutions in the integers if and only if $\gcd(a, m) \mid b$.

Remark 2.6. Reformulation: $[ax]_m = [b]_m$ has integer solutions if and only if $\gcd(a, m) \mid b$.

Example 2.4. The linear case. Solve $48x + 14 \equiv 0 \pmod{85}$ for $x \in \mathbb{Z}$. Note that $\gcd(48, 85) = 1$.
Solution: By the Euclidean algorithm we have that

$$85(13) + 48(-23) = 1.$$

Now we need to find $u \in \mathbb{Z}$ with $48u \equiv 1 \pmod{85}$. Notice that

$$\begin{aligned} 85(13) &= 1 - 48(-23) \\ &\Rightarrow 85(1 - 48(-23)) \\ &\Rightarrow 48(-23) \equiv 1 \pmod{85} \end{aligned}$$

Since $-14 \equiv -14 \pmod{85}$ by the addition law of modular arithmetic we can rewrite the original congruence as

$$\begin{aligned} 48x + 14 - 14 &\equiv -14 \pmod{85} \\ 48x &\equiv -14 \pmod{85}. \end{aligned}$$

So $u = -23$ and if we multiply the original congruence by u we have that

$$\begin{aligned} (-23)(48)x &\equiv (-14)(-23) \pmod{85} \\ 1x &\equiv 67 \pmod{85} \\ x &\equiv 67 \pmod{85}. \end{aligned}$$

Lemma 2.3
Let $f(x) = a_0 + a_1 x + \cdots a_n x^n$ be a polynomial with integer coefficients $a_i \in \mathbb{Z}$. If $a \equiv b \pmod m$ then $f(a) \equiv f(b) \pmod m$.

Corollary 2.2. Suppose $x \equiv y \pmod m$ then $f(x) \equiv 0 \pmod m$ if and only if $f(y) \equiv 0 \pmod m$.

Remark 2.7. To solve $f(x) \equiv 0 \pmod{m}$ it suffices to find all the solutions among a complete residue system modulo m.

Note 2.4. When the modulo, m, is very large obviously this method is not recommended being used.

Example 2.2
Find all the solutions to
$$x^8 + 3 \equiv 0 \pmod{4}.$$

Solution: By trial and error we can consider the complete residue system of modulo 4. Therefore, consider the CRS $\{-1, 0, 1, 2\}$:

- $x = -1 \Rightarrow (-1)^8 + 3 = 4 \equiv 0 \pmod{8}$;
- $x = 0 \Rightarrow 0^8 + 3 = 3 \not\equiv 0 \pmod{8}$;
- $x = -1 \Rightarrow 1^8 + 3 = 4 \equiv 0 \pmod{8}$;
- $x = -1 \Rightarrow 2^8 + 3 = 259 \not\equiv 0 \pmod{8}$;

Therefore, $x \equiv -1 \pmod{4}$ or $x \equiv 1 \pmod{4}$.

3 Multiplicative group of integers modulo m

Definition 3.1. Given a commutative ring R with an identity element 1_R we say that $a \in R$ is a **unit** provided there exists $b \in R$ such that $a \cdot b = 1_R$.

Note 3.1. Being a unit means the same as having a multiplicative inverse in the ring R.

Definition 3.2. We write $\mathbb{Z}_m^\times$ for the **multiplicative group** of integers modulo m of the **group of units** modulo m, which are defined by

$$\begin{aligned}\mathbb{Z}_m^\times &= \{[a]_m \in \mathbb{Z}_m : [a]_m \text{ is a unit}\} \\ &= \{[a]_m \in \mathbb{Z}_m : \gcd(a, m) = 1\}.\end{aligned}$$

Example 3.1. Consider $\mathbb{Z}_6$ which are the units?

- $[5]_6$, we know that $5 \cdot 5 \equiv 1 \pmod{6}$ therefore $[5]_6^{-1} = [5]_6$;
- $[2]_6$ is not a unit because there is no solution x to the congruence $2x \equiv 1 \pmod{6}$.

Definition 3.3. Let m be a non-zero integer. A set $\{x_1, x_2, \ldots, x_r\}$ is called a **reduced residue system** modulo m if for every integer y with $\gcd(y, m) = 1$ there is exactly one x_i such that
$$y \equiv x_i \pmod{m}.$$

Note 3.2. We can think of a reduced residue system as all the elements of the group $(\mathbb{Z}_m^\times, \times)$.

4 The Chinese Remainder Theorem

Theorem 4.1 (Chinese Remainder Theorem)**.** Let $m_1, m_2, \ldots, m_r$ be positive integers with $\gcd(m_i, m_j) = 1$ for all $i \neq j$. Set $m = m_1 m_2 \cdots m_r$ then, the map

$$\mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$$

given by

$$[a]_m \mapsto ([a]_{m_1}, [a]_{m_2}, \cdots, [a]_{m_r})$$

is a bijection.

Proposition 4.1

Suppose $\gcd(m, n) = 1$. The image of the map $\mathbb{Z}_{mn}^\times \to \mathbb{Z}_m \times \mathbb{Z}_n$ given by

$$([a]_{mn}) \mapsto ([a]_m, [a]_n)$$

equals $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$.

Note 4.1. Suppose $\gcd(m, n) = 1$ there exists an isomorphism $\psi : \mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ given by the map

$$[a]_{mn} \mapsto ([a]_m, [a]_n) .$$

Theorem 4.1 (CRT Reformulation)

Let $m_1, m_2, \ldots, m_r$ be positive integers with $\gcd(m_i, m_j) = 1$ for all $i \neq j$. Let $a_1, a_2, \ldots, a_r$ be integers then, the solutions of the simultaneous congruence equations

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

are given by the integers x lying in a single congruence class $\pmod{m_1 m_2 \cdots m_r}$.

4.1 How to use the CRT

4.1.1 Method I: Euclidean Algorithm

The CRT does not explicitly outline how to find a solution to x in practice. Suppose we are solving the simultaneous congruence of

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n} .$$

To solve such system we use the Euclidean algorithm to find $r, s \in \mathbb{Z}$ such that $mr + ns = 1$. Then the general solution is

$$x \equiv bmr + ans \pmod{mn}.$$

> **Remark 4.1.** To solve a system of congruence with 3 or more congruences, solve a pair first with the CRT. Then use the solution to form a pair so that the CRT can be invoked again and vice versa.

Example 4.1. Use the Chinese Remainder Theorem to find all integers x such that

$$x \equiv 11 \pmod{47} \quad \text{and} \quad x \equiv 3 \pmod{31}.$$

Solution:
First we check if 47 and 31 are relatively prime. They are since $\gcd(47, 31) = 1$. We use the Euclidean Algorithm to solve find $r, s \in \mathbb{Z}$ such that $47r + 31s = 1$. We begin as such:

$$\begin{aligned} 47 &= 1 \cdot 31 + 16 \\ 31 &= 1 \cdot 16 + 15 \\ 16 &= 1 \cdot 15 + 1. \end{aligned}$$

Furthermore, we can "unwind" the system of equations:

$$\begin{aligned} 1 &= 16 - 15 \\ &= 16 - (31 - 16) \\ &= 2 \cdot 16 - 31 \\ &= 2(47 - 31) - 31 \\ &= 2 \cdot 47 - 3 \cdot 31. \end{aligned}$$

Therefore, we have that $r = 2$ and $s = -3$. The general solution of the system of congruences

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}$$

is given by

$$x \equiv bmr + ans \pmod{mn}.$$

Hence, the solution to our system of congruences is:

$$\begin{aligned} x &\equiv (3)(47)(2) + (11)(31)(-3) \pmod{47 \times 31} \\ x &\equiv 282 - 1023 \pmod{47 \times 31} \\ x &\equiv -741 \pmod{47 \times 31} \\ x &\equiv 716 \pmod{47 \times 31} \end{aligned}$$

This means that,

$$\begin{aligned} x - 716 &= 1457k \\ x &= 716 + 1457k \quad \text{for } k \in \mathbb{Z}. \end{aligned}$$

4.1.2 Method II: Multiplicative inverses

In the general case, suppose we are solving the simultaneous congruence of

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}.$$

We note that to solve such system $\gcd(m, n) = 1$ therefore, by Bezout's lemma $\exists r, s \in \mathbb{Z}$ such that $mr + ns = 1$; by such a relation we notice that

$$mr \equiv 1 \pmod{n} \quad \text{and} \quad ns \equiv 1 \pmod{m}$$

therefore we have that r, s are the multiplicative inverses of the system of congruences respectively. As such we need to find these multiplicative inverses and then set the solution

$$x \equiv bmr + ans \pmod{mn}.$$

Example 4.2. Let us reconsider the same example from before:
find all integers x such that

$$x \equiv 11 \pmod{47} \quad \text{and} \quad x \equiv 3 \pmod{31}.$$

Solution:
As checked previously, 47 and 31 are coprime, so we can apply the CRT. By Bezout's lemma we have that $\exists r, s \in \mathbb{Z}$ such that $47r + 31s = 1$ therefore,

$$47r \equiv 1 \pmod{31} \quad \text{and} \quad 31s \equiv 1 \pmod{47}.$$

The values r and s are the multiplicative inverse of the congruence respectively; we have that $r = [47]_{31}^{-1} = [2]_{31}$ and $s = [31]_{47}^{-1} = [44]_{47}$. Hence, the solution to the problem is

$$\begin{aligned}
x &\equiv (3)(47)(2) + (11)(31)(44) \pmod{47 \times 31} \\
x &\equiv 282 + 15004 \pmod{1457} \\
x &\equiv 15286 \pmod{1457} \\
x &\equiv 716 \pmod{1457}.
\end{aligned}$$

4.2 The CRT for polynomials in $\mathbb{Z}_m$

Example 4.3. Find all solutions in $\mathbb{Z}_{15}$ to $f(x) \equiv 0 \pmod{15}$ for $f(x) = 2x^3 + 5x + 2$.
Key idea: $f(x) \equiv 0 \pmod{15} \iff 15 \mid f(x)$ that is

$$\begin{aligned}
f(x) \equiv 0 \pmod{3} &\iff 3 \mid f(x) \\
f(x) \equiv 0 \pmod{5} &\iff 5 \mid f(x).
\end{aligned}$$

Solution: now we solve two equations

1. $f(x) \equiv 0 \pmod{3}$;
2. $f(x) \equiv 0 \pmod{5}$.

Now we can just use trial and error to find the solutions:

- $x = 0, f(0) = 2 \not\equiv 0 \pmod{3}$;

- $x = 1, f(1) = 2 + 5 + 2 \equiv 0 \pmod 3$;
- $x = -1, f(-1) = -2 - 5 + 2 \not\equiv 0 \pmod 3$.

So our only solution for this congruence is

$$x \equiv 1 \pmod 3 .$$

By a similar process for the second congruence the solution is

$$x \equiv 4 \pmod 5 .$$

Applying the CRT to the congruences:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 4 \pmod 5 . \end{aligned}$$

We have that

$$\begin{aligned} x &\equiv (1)(5)(-1) + (4)(3)(2) \pmod{15} \\ &\equiv -5 + 24 \pmod{15} \\ &\equiv 19 \pmod{15} \\ &\equiv 4 \pmod{15} . \end{aligned}$$

Example 4.4. How many solutions does the congruence

$$x^2 \equiv 4 \pmod{15}$$

have in $\mathbb{Z}_{15}$?
Solution: Consider

$$\begin{aligned} x^2 &\equiv 4 \pmod 3 \Rightarrow 2 \text{ solutions} \\ x^2 &\equiv 4 \pmod 5 \Rightarrow 2 \text{ solutions} \end{aligned}$$

Therefore there are $2 \times 2 = 4$ pairs of solutions.

5 Hensel's Lemma

Theorem 5.1. Let p be a prime and let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial degree $\leq n$ with integer coefficients (we allow the possibility that $a_n = 0$). We suppose that $a_i \not\equiv 0 \pmod p$ for some i. Then the congruence equation

$$f(x) \equiv 0 \pmod p$$

has **at most** n solutions in $\mathbb{Z}_p$.

Theorem 5.1 (Hensel's Lemma)
Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial with integer coefficients, let p be a prime and let r be a positive integer. We let $f'(x)$ be the derivative of $f(x)$ so, $f'(x) = a_1 + 2a_2 x + \ldots + na_n x^{n-1}$. Suppose x_r is an integer with

$$f(x_r) \equiv 0 \pmod{p^r}$$

and

$$f'(x_r) \not\equiv 0 \pmod{p}.$$

Then there exists $x_{r+1} \in \mathbb{Z}$ satisfying

$$f(x_{r+1}) \equiv 0 \pmod{p^{r+1}} \quad \text{and} \quad x_{r+1} \equiv x_r \pmod{p^r}$$

Moreover, the x_{r+1} satisfying these properties is **unique** modulo p^{r+1}, and we can take

$$x_{r+1} = x_r - uf(x_r)$$

where u is an inverse of $f'(x_r)$ modulo p.

Example 5.1. How many solutions does

$$f(x) = x^{10} + x^3 + 1 \equiv 0 \pmod{9}$$

have?
Solution:

1. Solve $f(x) \equiv 0 \pmod{3} \Rightarrow x \equiv 1 \pmod{3}$;
2. Check if $f'(1) \equiv 0 \pmod{3}$; we have that $f'(1) = 13 \not\equiv 0 \pmod{3}$.

Therefore, the conditions Hensel's lemma are met, so there is a solution which is **unique**. The congruence has only one solution.

Example 5.1

Let $f(x) = x^2 + x + 5$. Find all solutions to $f(x) \equiv 0 \pmod{11^2}$.
Solution:

1. Solve $f(x) \equiv 0 \pmod{11}$ by trial and error, so we have $x = 2, 8 \pmod{11}$;

2. for each solution x_1 check if $f'(x_1) \equiv 0 \pmod{11}$ i.e.

   - $x_1 = 2 \Rightarrow f'(x_1) = 5 \not\equiv 0 \pmod{11}$;
   - $x_1 = 8 \Rightarrow f'(x_1) = 17 \not\equiv 0 \pmod{11}$;

3. Find the multiplicative inverse, u, to $f'(x_1) \pmod{11}$ i.e. find u such that $uf'(x_1) \equiv 1 \pmod{11}$:

   - for $x_1 = 2$ we need to find u such that $uf'(2) = 5u \equiv 1 \pmod{11}$ which implies $u = -2$;
   - for $x_1 = 8$ we have $u = 2$

4. Apply Hensel's lemma to $x_1 = 2, 8$ for which we have a formula:

$$\begin{aligned} x_2 &= x_1 - uf(x_1) \\ \Rightarrow x_1 &= 2 \Rightarrow x_2 \equiv 24 \pmod{121} \\ \Rightarrow x_1 &= 8 \Rightarrow x_2 \equiv 96 \pmod{121}. \end{aligned}$$

Lemma 5.1. For $t \in \mathbb{Z}$ and a positive integer r, we have

$$f(x + tp^r) \equiv f(x) + tf'(x)p^r \pmod{p^{r+1}},$$

where we view both sides as polynomials in x, and we mean that all the coefficients of these two polynomial are congruent modulo p^{r+1}.

Theorem 5.2

With regard to Hensel's lemma if $f'(x_r) \equiv 0 \pmod{p}$ then each of the following holds:

1. if $p^{r+1} \mid f(x_r)$ then $f(x_r + tp^r) \equiv 0 \pmod{p^{r+1}}$ for each $t \pmod{p}$ i.e. $t \in \{1, 2, \ldots, p\}$.

2. If $p^{r+1} \nmid f(x_r)$ then there are **no** solutions x_{r+1} to $f(x) \equiv 0 \pmod{p^{r+1}}$ **with** $x_{r+1} \equiv x_r \pmod{p^r} \Rightarrow x_{r+1} = x_r + tp^r$.

Remark 5.1. In Case 1. If **ONE** of the $t \in \{1, 2, \ldots, p\}$ are roots of $f(x) \equiv 0 \pmod{p}$ then **ALL** $t \in \{1, 2, \ldots, p\}$ are roots of the congruence.

Note 5.1. That is, suppose x_r is a solution to the congruence $f(x) \equiv 0 \pmod{p^r}$ but, Hensel's lemma's condition are not satisfied i.e. $f'(x_r) \equiv 0 \pmod{p}$. Then we need to compute $f(x_r) \pmod{p^{r+1}}$:

- if $f(x_r) \equiv 0 \pmod{p^{r+1}}$ then $x_r + tp^r$ are solutions for all $t \in \{1, 2, \ldots p\}$;
- if $f(x_r) \not\equiv 0 \pmod{p^{r+1}}$ then there are no solutions modulo p^{r+1}.

Example 5.2. Solve $x^3 + 1 \equiv 0 \pmod{9}$.

1. Solve $f(x) = x^3+1 \equiv \pmod{3}$ by trial and error, which implies that $x \equiv 2 \pmod{3}$;
2. Check if $3 \mid f'(2)$. We have that $f'(2) = 3 \cdot 2^2 \equiv 0 \pmod{3}$. So, Hensel's lemma does not apply.
3. Check if $9 \mid f(2)$, we have that $f(2) = 9$ so yes.
4. We can conclude that this will have 3 solutions i.e. $x_1 = 2 \Rightarrow x_1+tp$ for $t \in \{1, 2, 3\}$ which leads to $x \equiv 2, 5, 8 \pmod{5}$.

6 The structure of $\mathbb{Z}_m^\times$

6.1 Euler's ϕ Function

Definition 6.1. Let m be a positive integer. We define $\phi : \mathbb{N} \to \mathbb{N}$ given by $\phi(m)$ to be the number of integers a such that $1 \leq a \leq m$ and $\gcd(a, m) = 1$ i.e.

$$\phi(m) = \left|\{1 \leq a \leq m : \gcd(a, m) = 1\}\right|.$$

Note 6.1. The ϕ function tells us how many numbers are coprime to m.

Theorem 6.1. Equivalently $\phi(m) = |\mathbb{Z}_m^\times|$, the cardinality of the multiplicative group $\mathbb{Z}_m^\times$.

Lemma 6.1. Let m, n be coprime positive integers then, $\phi(mn) = \phi(m)\phi(n)$.

Lemma 6.1

Let p be prime and n a positive integer. Then

$$\phi(p^n) = p^{n-1}(p-1) = p^n - p^{n-1}.$$

Remark 6.1. Notice that $\phi(p) = p - 1$.

6.2 The Fermat-Euler theorem

Proposition 6.1. Let m be a positive integer then

$$\sum_{d|m} \phi(d) = F(m) = m$$

for $d > 0$. Note that we are summing over positive divisors of m.

Note 6.2. We can interpret $F(m)$ as the sum of the ϕ of all the positive divisors of m.

Remark 6.2. If m, n are coprime then $F(mn) = F(m)F(n)$

Example 6.1. Find

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

Theorem 6.1 (Fermat-Euler theorem)
Let $a \in \mathbb{Z}$ and let m be a positive integer. Suppose $\gcd(a, m) = 1$ then,

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

Definition 6.2. Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. The **order** of $[a]_m \in \mathbb{Z}_m^\times$ is the smallest positive integer d with $[a]_m^d = [1]_m$.

Note 6.3. Notation: $o\left([a]_m\right)$ means the order of $[a]_m$.

Corollary 6.1. By the Euler-Fermat theorem $o([a]_m) \leq \phi(m)$ for $\gcd(a, m) = 1$. In particular the order of $[a]_m$ divides $\phi(m)$ i.e. $o([a]_m) \mid \phi(m)$.

Example 6.2. Find the order of $2 \pmod 9$.
Solution: We know the order of $[2]_9$ divides $\phi(9) = 6$. So, $o([2]_9) \in \{1, 2, 3, 6\}$ i.e. the divisors of 6. Note $[1]_9$ has order 1 so check

- $2^2 \equiv 4 \pmod 9$;
- $2^3 \equiv 8 \pmod 9$.

Therefore, the order of $[2]_9$ is 6.

Corollary 6.1 (Fermat's Little theorem)
Suppose that p is a prime number and a is an integer.

1. $a^p \equiv a \pmod{p}$;
2. if $\gcd(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$.

Example 6.1

What is $10^{4035} \pmod{2017}$? (2017 is a prime number)

Solution: Since 2017 is prime we can use Fermat's Little Theorem which implies $10^{2016} \equiv 1 \pmod{2017}$. Since $4035 = 2 \cdot 2016 + 3$ we have

$$\begin{aligned} 10^{4035} &\equiv 10^{2 \cdot 2016 + 3} \pmod{2017} \\ &\equiv \left(10^{2016}\right)^2 \cdot 10^3 \pmod{2017} \\ &\equiv 1 \cdot 1000 \pmod{2017}. \end{aligned}$$

Therefore, $10^{4035} \pmod{2017}$ is $1000 \pmod{2017}$.

6.3 Primitive roots

The motivation behind this section is to find the positive integers m for which $\mathbb{Z}_m^\times$ is a cyclic group.

Definition 6.3. Let m be a positive integer. If g is an integer which is coprime to m, such that the order of g modulo m is $\phi(m)$. Then we say that g is a **primitive root** modulo m.

Note 6.4. We can reformulate this definition as: if $\gcd(g, m) = 1$ such that $o([g]_m) = \phi(m)$ then we say g is a **primitive root** modulo m.

Remark 6.3. By this definition if a primitive root exists within $\mathbb{Z}_m^\times$ then it is a cyclic group because, the order of the primitive root is equal to the order of the group. Therefore, a primitive root is a generator of $\mathbb{Z}_m^\times$.

Lemma 6.2 (Primitive Root Test)

Let $m \geq 3$ be a positive integer and let g be coprime to m. Then g is a primitive root modulo m if and only if

$$g^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod{m}$$

for all prime divisors p of $\phi(m)$ i.e. all the primes, p, for which $p \mid \phi(m)$.

Note 6.5. We are determining that the only possible choice for the order of g is $\phi(m)$.

Example 6.3. Find a primitive root modulo 7.
Solution:

1. Compute $\phi(7) = 7 - 1 = 6$.

2. Use trial and error, try $g = 2$, we have that the prime divisors of 6 are 2 and 3 so now with primitive root test:

- $2^{\frac{6}{3}} = 2^2 \equiv 4 \pmod 7$;
- $2^{\frac{6}{2}} = 2^3 \equiv 1 \pmod 7$.

So, 2 is not a primitive root modulo 7.

3. Try a different number, $g = 3$.

- $3^{\frac{6}{3}} = 3^2 \equiv 2 \pmod 7$;
- $3^{\frac{6}{2}} = 3^3 \equiv 6 \pmod 7$.

So, the primitive root test implies that 3 **IS** a primitive root modulo 7.

Lemma 6.2. Let p be a prime number. For $d \mid (p-1)$ let

$$W_d = \{[a] \in \mathbb{Z}_p^\times : [a] \text{ has order } d\}$$

and $w_d = |W_d|$. Then $w_d \leq \phi(d)$, for each $d \mid (p-1)$.

Theorem 6.2. For each divisor of $p-1$ i.e. $d > 0$ such that $d \mid (p-1)$, there are $\phi(d)$ elements of order d in $\mathbb{Z}_p^\times$.

Corollary 6.2

There are $\phi(p-1)$ primitive roots modulo p.

> **Remark 6.4.** Therefore, $\mathbb{Z}_p^\times$ is cyclic as there are $\phi(p-1)$ elements of $p-1$ i.e. the primitive roots.

Corollary 6.3

There always exists a primitive root modulo p.

Example 6.4. How many primitive roots are there modulo 23?
Solution: There are $\phi(23-1) = \phi(22) = \phi(2)\phi(11) = 10$.

Example 6.2

Show there is no primitive root modulo 15.
Solution: We have $\phi(15) = \phi(3)\phi(5) = 8$. Observe for any $g \pmod{15}$, by the CRT, we have

$$\begin{aligned} g^d \equiv 1 \pmod{15} &\iff g^d \equiv 1 \pmod 3 \text{ and} \\ &\iff g^d \equiv 1 \pmod 5 . \end{aligned}$$

By Fermat's Little Theorem we obtain $g^4 \equiv 1 \pmod 3$ and $g^4 \equiv 1 \pmod 5$ so, $g^4 \equiv 1 \pmod{15}$. Hence, the order of g is at most 4. We are done because for g to be a primitive root, it needs to have order 8, but it has only at most order 4.

Proposition 6.1

If g is a primitive root modulo p then

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

Proof. Suppose g is a primitive root modulo p. Let $x = g^{\frac{p-1}{2}}$. Then

$$x^2 = g^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem. Hence, $x \equiv 1$ or $-1 \pmod{p}$. Since, g is a primitive root, we know $o([g]_p) = \phi(p) = p - 1$ therefore

$$x \not\equiv 1 \pmod{p}.$$

The only possibly choice is

$$x = g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

□

6.4 Order of an element

Proposition 6.2

For G a finite group $g \in G$ and $o(g) = d$ we have

$$o(g^k) = \frac{d}{\gcd(k, d)}.$$

Example 6.5. Show 4 is not a primitive root modulo m for $m \geq 3$.
Solution: Write $d = o([2]_m)$ (assuming $\gcd(m, 2) = 1$).

- If d is even then $4 = 2^2$ so

$$o([2^2]_m) = \frac{d}{\gcd(2, d)} = \frac{d}{2} \leq \frac{\phi(m)}{2} \leq \phi(m).$$

- If d is odd then

$$o([4]_m) = o([2]_m) = d < \underbrace{\phi(m)}_{\text{even}}.$$

Proposition 6.3

Suppose p and q are distinct prime numbers. Then the maximum order of an element in $\mathbb{Z}_{pq}^{\times}$ is given by the $\operatorname{lcm}(p-1, q-1)$.

6.5 Applications of primitive roots

Lemma 6.3

Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ with $\gcd(a, m) = 1$. Then $a^n \equiv 1 \pmod{m}$ if and only if $o([a]_m)$ divides n.

Remark 6.5. Reformulation of lemma from lecture notes:
Let G be a finite group with identity element e. Then for $g \in G$ we have that $g^n = e$ if and only if $o(g)$ divides n.

Note 6.6. In practice this lemma will be used when $G = \mathbb{Z}_m^\times$, in which case the lemma states: for $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$ we have that

$$([a]_m)^n = 1 \iff o([a]_m) \mid n.$$

Example 6.3

Find all solutions in $\mathbb{Z}_{19}$ to

$$4x^5 \equiv 7 \pmod{19}.$$

Solution:

1. Find a primitive root modulo 19. With trial and error in combination with primitive root test we have that 2 is a primitive root modulo 19.

2. Since we know 2 is a primitive root we can write:
   - $x = 2^i$ for some i;
   - $4 = 2^2$;
   - (by trial and error) $7 \equiv 2^6 \pmod{19}$.

3. Now the original problem becomes

$$\begin{aligned} 2^2 2^{5i} &\equiv 2^6 \pmod{19} \\ 2^{5i-4} &\equiv 1 \pmod{19} \end{aligned}$$

   Recall 2 is a primitive root modulo 19 so $o([2]_{19}) = \phi(19) = 18$ therefore, by the lemma above we have $18 \mid 5i - 4 \Rightarrow 5i \equiv 4 \pmod{18}$.

4. Solve $5i \equiv 4 \pmod{18}$ so, $i \equiv 8 \pmod{18}$ which implies $i = 8 + 18k$ for some $k \in \mathbb{Z}$.

5. Notice, $2^{18k} \equiv 1 \pmod{19}$ so, $2^{8+18k} = 2^8 \cdot 2^{18k} \equiv 2^8 \cdot 1 \pmod{19}$. Therefore, by substituting i into x we have the solution

$$x = 2^8 \equiv 9 \pmod{19}.$$

Example 6.6. Find all integer x with $4^x \equiv 9 \pmod{19}$.
Solution:

1. Find a primitive root modulo 19: we have 2 is a primitive root modulo 19.
2. Write:
   - $4 = 2^2$;
   - (by trial and error) $9 \equiv 2^8 \pmod{19}$

   so,
   $$2^{2x} \equiv 2^8 \pmod{19} \Rightarrow 2^{2x-8} \equiv 1 \pmod{18}.$$
3. Recall $o([2]_{19}) = \phi(19) = 18$, by the lemma above we know,
   $$\begin{aligned}&18 \mid (2x-8)\\ &\Rightarrow 2x \equiv 8 \pmod{18}\\ &\Rightarrow x \equiv 4 \pmod{9}\end{aligned}$$
   Our answer is therefore, $x \equiv 4 \pmod 9$.

6.5.1 Primitive roots of prime powers

Proposition 6.4
Let p be a prime. Suppose g is a primitive root modulo p. Then g or $g + p$ is a primitive root modulo p^2.

Remark 6.6. The group $\mathbb{Z}_{p^2}^{\times}$ is a cyclic group.

Note 6.7. This proposition helps us 'lift' primitive roots to higher powers of p.

Note 6.8. To determine which of g or $g+p$ is a primitive root modulo p^2, we need to compute $g^{p-1} \pmod{p^2}$. If $g^{p-1} \equiv 1 \pmod{p^2}$ then $g+p$ is a primitive root modulo p^2, otherwise g is a primitive root modulo p^2.
Since g is a primitive root modulo p it has order $\phi(p) = p - 1$. Suppose g is a primitive root modulo p^2, in this case g would have order $\phi(p^2)$ therefore, if $g^{p-1} \equiv 1 \pmod{p^2}$ then it **cannot** be a primitive root modulo p^2 as this would imply g has order $\phi(p) \neq \phi(p^2)$. Then it follows that $g + p$ is the primitive root.

Example 6.4

Find two primitive roots modulo 25.
Solution:

1. Find a primitive root modulo 5. By trial and error we have 2 is a primitive root modulo 5.

2. Compute $2^{5-1} \pmod{5^2}$.

   - If $2^{5-1} \equiv 1 \pmod{5^2}$ then $2 + 5 = 7$ is a primitive root modulo 25.
   - If $2^{5-1} \not\equiv 1 \pmod{5^2}$ then 2 is a primitive root modulo 25.

3. We have $2^4 = 16 \not\equiv 1 \pmod{25}$. So, we conclude 2 is a primitive root modulo 25.

4. Since 2 and 7 are primitive roots modulo 5 we can compute

$$7^{5-1} = 7^4 = 2401 \equiv 1 \pmod{25}.$$

   So we conclude $7 + 5 = 12$ is a primitive root modulo 25.

Proposition 6.5

Let $p > 2$ be a prime. Suppose g is a primitive root modulo p^2 then g is a primitive root modulo p^n for all $n \geq 2$.

Remark 6.7. The group $\mathbb{Z}_{p^n}^\times$ is cyclic whenever $p \neq 2$.

Proposition 6.6

The group $\mathbb{Z}_m^\times$ is cyclic if and only if $m = 1, 2, 4, p^n, 2p^n$ for $p > 2$ and $n \geq 1$.

Proposition 6.7

Suppose $m > 0$ is a positive integer and suppose that $\mathbb{Z}_m^\times$ has a primitive root. Then the number of primitive roots in $\mathbb{Z}_m^\times$ is $\phi(\phi(m))$.

6.6 Quadratic residues

Definition 6.4. Let $p > 2$ and $b \in \mathbb{Z}$ with $\gcd(b, p) = 1$. We say that b is a **quadratic residue** (QR) modulo p if the equation

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

has a solution. Otherwise, we say that b is a **quadratic non-residue** (QNR) modulo p.

Note 6.9. We can think of quadratic residues as the 'square numbers' modulo p.

Remark 6.8. If $p \mid b$ then $x \equiv 0 \pmod p$ is the only solution. Also, if $p = 2$ and a is odd then the only other possibility is $b \equiv 1 \pmod 2$. Therefore, from now on we assume that p is odd and b is coprime to p.

Remark 6.9. In this course 0 is neither a quadratic residue nor a quadratic non-residue.

Corollary 6.2. If $a \equiv b \pmod p$ then a is a QR modulo p if and only if b is a QR modulo p.

Example 6.5

Find all QR modulo 7.
Solution: We write an exhaustive table.

$a \pmod 7$	$a^2 \pmod 7$
1	$1^2 = 1$
2	$2^2 = 4$
3	$3^2 \equiv 2$
$4 \equiv -3$	2
$5 \equiv -2$	4
$6 \equiv -1$	1

Remark 6.10. The QR are the numbers that we get on the RHS of the table.

The QR modulo 7 are all the squares modulo 7 i.e. all the numbers that are equal to a square modulo 7. By looking at the right-hand column of the table we have all the numbers that satisfy such property. Therefore,

- the QR are: $1, 2, 4$ modulo 7;
- the QNR are $3, 5, 6$ modulo 7.

Proposition 6.8

Let $g \in \mathbb{Z}$ be a primitive root modulo p. Then $[g^k]_p$ is a quadratic residue if and only if k is even.

Corollary 6.3. There are $\frac{(p-1)}{2}$ quadratic residues and $\frac{(p-1)}{2}$ quadratic non-residues in $\mathbb{Z}_p^\times$.

Theorem 6.2

We have -1 is a quadratic residue modulo p if $p \equiv 1 \pmod 4$ and a quadratic non-residue if $p \equiv 3 \pmod 4$.

Proof. Let g be a primitive root modulo p and let $x = g^{\frac{(p-1)}{2}}$. We have

$$x^2 = g^{p-1} \equiv 1 \pmod p$$

and $x \not\equiv 1 \pmod p$, since g is a primitive root. The equation $x^2 \equiv 1 \pmod p$ has only two solutions, so we have $x \equiv -1 \pmod p$. We deduce that -1 is a quadratic residue if and only if $\frac{p-1}{2}$ is even i.e.

$$\begin{aligned} \frac{p-1}{2} &\equiv 0 \pmod 2 \\ \Rightarrow p - 1 &\equiv 0 \pmod 4 \\ \Rightarrow p &\equiv 1 \pmod 4 . \end{aligned}$$

□

7 Euler's criterion

Theorem 7.1. There are infinitely many primes, p, with $p \equiv 1 \pmod 4$ i.e. primes of the form $4k + 1$.

Proof. For sake of contradiction suppose $p_1, p_2, \ldots, p_n$ are **all** the primes congruent to 1 modulo 4. Consider

$$x = 2p_1p_2 \cdots p_n \quad \text{and} \quad N = x^2 + 1.$$

Suppose $p \mid N$, then $x^2 + 1 \equiv 0 \pmod p$. Since $x^2 \equiv -1 \pmod p$ then -1 is a quadratic residue modulo p we have that $p \equiv 1 \pmod 4$ by Theorem 6.2. Hence, $p \mid x$; by assumption, p must be one of the primes $p_1, p_2, \ldots p_n$. This is a contradiction since $q \nmid N - x^2 = 1$. □

Theorem 7.1 (Euler's Criterion)

Let $b \in \mathbb{Z}$ and $p > 2$ with $\gcd(b, p) = 1$. Then each of the following holds:

1. b is a **quadratic residue** if and only if

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

2. b is a **quadratic non-residue** if and only if

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

7.1 Application to solving $x^2 \equiv b \pmod p$

Proposition 7.1

Suppose b is a quadratic residue modulo p and $p \equiv 3 \pmod 4$. Then

$$x_0 = b^{\frac{p+1}{4}}$$

is a solution to $x^2 \equiv b \pmod p$.

Example 7.1
Given that 5 is a quadratic residue modulo 139. Find **all** solutions in $\mathbb{Z}_{139}$ to

$$x^2 \equiv 5 \pmod{139}.$$

Solution: We have that 139 is prime and $139 \equiv 3 \pmod 4$ so take

$$x_0 = 5^{\frac{139+1}{4}} = 5^{35}.$$

Now we compute $5^{35} \pmod{139}$ (using the method of repeated squaring) and we have

$$5^{35} \equiv 137 \pmod{139}.$$

Notice $(x_0)^2 \equiv b \pmod p \iff (-x_0)^2 \equiv 0 \pmod p$. Therefore, our solutions are

$$x \equiv 127 \pmod{139} \quad \text{and} \quad x \equiv -127 \equiv 12 \pmod{139}.$$

8 Legendre symbol

Definition 8.1. Let $b \in \mathbb{Z}$ and $p > 2$. The **Legendre symbol**, $\left(\frac{b}{p}\right)$ is given by

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

Remark 8.1. For each prime $p > 2$ we can think of the Legendre symbol as a function:

- $$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{-1, 0, 1\}.$$
- $$\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p \to \{-1, 0, 1\}.$$
- $$\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p^\times \to \{-1, 1\}.$$

Proposition 8.1. Some properties of the Legendre symbol:

- $\left(\frac{1}{p}\right) = 1$ **always** because 1 is a quadratic root modulo p.
- $\left(\frac{b^2}{p}\right) = 1$ if $p \nmid b$ because $x^2 \equiv b^2 \pmod p \iff x \equiv \pm b \pmod p$.
- If $a \equiv b \pmod p$ then
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$
because a is a quadratic residue if and only if b is a quadratic residue.

Lemma 8.1 (Periodicity)
The Legendre symbol is periodic i.e.

$$\left(\frac{a+dp}{p}\right) = \left(\frac{a}{p}\right).$$

Example 8.1
Compute $\left(\frac{2022}{7}\right)$.
Solution: We have $2022 \equiv 6 \equiv -1 \pmod 7$, which implies

$$\left(\frac{2022}{7}\right) = \left(\frac{-1}{7}\right).$$

Since $7 \equiv 3 \pmod 4$ then -1 is a quadratic non-residue modulo 7. Therefore,

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

Lemma 8.2
Let $b \in \mathbb{Z}$ and $p > 2$. The number of solutions in $\mathbb{Z}_p$ to

$$x^2 \equiv b \pmod p$$

is equal to $1 + \left(\frac{b}{p}\right)$.

Proof. We have three cases to consider.

- If $p \mid b$ the only solution is $x = [0]$, and $1 = 1 + 0 = 1 + \left(\frac{b}{p}\right)$.
- If b is QNR then, by definition there are no solutions to the congruence hence, we $0 = 1 - 1 = 1 + \left(\frac{b}{p}\right)$.
- If b is a QR, we have one solution x and another solution given by $(-x)$ since, it is an even polynomial thus, we have $2 = 1 + 1 = 1 + \left(\frac{b}{p}\right)$ solutions.

□

Example 8.2
How many solutions does the equation

$$3x^2 + 6x + 2 \equiv 0 \pmod{23}$$

have in $\mathbb{Z}_{23}$?

Solution. We have $3x^2 + 6x + 2 = 3(x+1)^2 - 1$, so we have to solve

$$3(x+1)^2 \equiv 1 \pmod{23}\,.$$

Note that, $[8]_{23} = [3]_{23}^{-1}$ thus, we are solving

$$(x+1)^2 \equiv 8 \pmod{23}\,.$$

The question is now if, 8 is a QR modulo 23, which indeed it is. Hence, we have two solutions.

8.1 Properties of the Legendre symbol

Theorem 8.1. Reformulation of Euler's criterion with the Legendre symbol. Let $b \in \mathbb{Z}$ and $p > 2$ with $\gcd(b, p) = 1$. Then we have

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

Remark 8.2. This reformulation also holds true when $b \mid p$ as both sides are 0 therefore, they are congruent modulo p.

Lemma 8.1 (Multiplicative property)**.** Let a, b be integers then

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

Remark 8.3. Reformulation of Euler's criterion in terms of the Legendre symbol. If $[a] \in \mathbb{Z}_p^\times$ then we have

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

If $p \mid a$ we also have

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

because in this case both sides are $0 \pmod{p}$.

Lemma 8.2 (The rule for -1)**.** Let $p > 2$. We have that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}\,. \end{cases}$$

Proposition 8.2 (The rule of 2)**.** Let $p > 2$ then

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

Example 8.3

Compute $\left(\frac{51}{53}\right)$.

Solution: Observe $51 \equiv -2 \pmod{53}$, $53 \equiv 1 \pmod 4$ and $53 \equiv 3 \pmod 8$ then by periodicity

$$\begin{aligned} \left(\frac{51}{53}\right) &= \left(\frac{-2}{53}\right) \\ &= \left(\frac{-1 \cdot 2}{53}\right) \\ &= \left(\frac{-1}{53}\right)\left(\frac{2}{53}\right) \\ &= 1 \cdot (-1) \\ &= -1. \end{aligned}$$

Theorem 8.2. Let $p > 2$ then

$$\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0.$$

8.2 Quadratic reciprocity

Theorem 8.1 (The Law of Quadratic reciprocity)

Let $p, q > 2$ be two distinct primes. Then

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \textbf{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Remark 8.4. Quadratic reciprocity is transformative, in the following way

$$\underbrace{\left(\frac{p}{q}\right)}_{\text{Arithmetic in } \mathbb{Z}_q} = \underbrace{(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)}_{\text{Arithmetic in } \mathbb{Z}_p}.$$

Example 8.1. Compute $\left(\frac{5}{8171}\right)$ (8171 is a prime).

Solution: Using quadratic reciprocity:

$$\left(\frac{5}{8171}\right) = \left(\frac{8171}{5}\right)$$

As $5 \equiv 1 \pmod 4$ we do not include the -1. Then by periodicity

$$\left(\frac{8171}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

As $8171 \equiv 1 \pmod 5$.

Example 8.4

Show that $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv 1$ or $4 \pmod 5$. (That is, show that 5 is a quadratic residue modulo 5).
Solution: Notice, $5 \equiv 1 \pmod 4$. Observe by quadratic reciprocity

$$\begin{aligned} 1 &= \left(\frac{5}{p}\right) \\ &= \left(\frac{p}{5}\right). \end{aligned}$$

The statement holds if and only if p is a quadratic residue modulo 5. We then list the quadratic residues modulo 5.

$a \pmod 5$	$a^2 \pmod 5$
± 1	1
± 2	4

Which means $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$.

Example 8.2. Compute $\left(\frac{21}{67}\right)$.
Solution: Observe, $67 \equiv 7 \equiv 3 \pmod 4$, $67 \equiv 4 \pmod 4$ and $67 \equiv 1 \pmod 3$.

$$\begin{aligned} \left(\frac{21}{67}\right) &= \left(\frac{3}{67}\right)\left(\frac{7}{67}\right) \\ &= (-1)\left(\frac{67}{3}\right)(-1)\left(\frac{67}{7}\right) \\ &= (-1)\left(\frac{1}{3}\right)(-1)\left(\frac{4}{7}\right) \\ &= (-1)(1)(-1)(1) \\ &= 1. \end{aligned}$$

Remark 8.5. General strategy for computing $\left(\frac{a}{p}\right)$.

1. If $|a| > p$ use the periodicity rule.
2. Factor a and then use the multiplicative rule.
3. Apply quadratic reciprocity.

Repeat the process if necessary.

Theorem 8.2
If $p, q > 2$ and p and q are distinct primes then for $b \in \mathbb{N}$

$$\left(\frac{q^b}{p}\right) = \left(\frac{q}{p}\right)^b = \begin{cases} +1 & \text{if } b \text{ is even} \\ \left(\frac{q}{p}\right) & \text{if } b \text{ is odd.} \end{cases}$$

8.3 Rules for computing the Legendre symbol

Theorem 8.3
Let p, q be distinct odd primes and $a, b \in \mathbb{Z}$.

R0. Periodicity: $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod p$.

R1. Multiplicativity: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

R2. Rule for 2:
$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

R3. Rule for -1:
$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

R4. Quadratic reciprocity:
$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \textbf{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Theorem 8.4
Let p be an odd prime. Given integers a, b, c with $\gcd(1, p) = 1$; the quadratic equation
$$ax^2 + bx + c \equiv 0 \pmod p$$
has (in $\mathbb{Z}_p$):

- 0 solutions if $b^2 - 4ac$ is a quadratic non-residue modulo p.
- 1 solution if $b^2 - 4ac \equiv 0 \pmod p$.
- 2 solutions $b^2 - 4ac$ is a quadratic residue modulo p.

Example 8.5

Determine the number of solutions to $5x^2 + 2x + 4 \equiv 0 \pmod{29}$.

Solution: Consider the congruence equation $ax^2 + bx + c \equiv 0 \pmod{p}$, if $p \nmid a$ then the number of solutions is given by $1 + \left(\frac{b^2-4ac}{p}\right)$. We are computing

$$1 + \left(\frac{2^2 - 4(5)(4)}{2(5)}\right).$$

We compute the Legendre symbol first

$$\begin{aligned}\left(\frac{2^2 - 4(5)(4)}{2(5)}\right) &= \left(\frac{-76}{29}\right) \\ &= \left(\frac{-1}{11}\right) \\ &= -1.\end{aligned}$$

Therefore, there are $1 - 1$ solutions i.e. there are no solutions.

9 Gauss sums

Definition 9.1. An n^{th} **root of unity** is a complex number, z, such that $z^n = 1$ for $n \in \mathbb{N}$.

Note 9.1. Suppose $z \in \mathbb{C}$, the roots of unity are the solutions to $z^n = 1$. Now we write the number 1 in polar form

$$\begin{aligned}z^n &= 1 \\ &= e^{2\pi k i} \\ &= \cos(2\pi k) + i\sin(2\pi k).\end{aligned}$$

Therefore, by De Moivre's theorem

$$\begin{aligned}z &= 1^{\frac{1}{n}} \\ &= e^{\frac{2\pi k}{n}i} \\ &= (\cos(2\pi k) + i\sin(2\pi k))^{\frac{1}{n}} \\ &= \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)\end{aligned}$$

Definition 9.2. We will define the notation. Given $p > 2$ and $b \in \mathbb{Z}$ then

$$e_p(b) := e^{\frac{2\pi b}{p}i} = \cos\left(\frac{2\pi b}{p}\right) + i\sin\left(\frac{2\pi b}{p}\right).$$

Theorem 9.1. Properties of the roots of unity; let $a, b \in \mathbb{Z}$.

- $e_p(ab) = e_p(a)^b$.

- If $a \equiv b \pmod{p}$ then $e_p(a) = e_p(b)$.
- $e_p(a)^p = e_p(ap) = e_p(0) = 1$. Therefore, $e_p(a)$ is a p^{th} root of unity.

Definition 9.3. Let $p > 2$ be a prime and $b \in \mathbb{Z}$. The **Gauss sum** associated to b modulo p is given by

$$g_b = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e_p(bn).$$

Example 9.1. If $p = 5$ and $b = 2$ then the Gauss sum of 2 modulo 5 is given by

$$\begin{aligned} g_2 &= \sum_{n=1}^{4} \left(\frac{n}{5}\right) e_5(2n) \\ &= \left(\frac{1}{5}\right) e_5(2) + \left(\frac{2}{5}\right) e_5(4) + \left(\frac{3}{5}\right) e_5(6) + \left(\frac{4}{5}\right) e_5(8) \\ &= (1)e_5(2) + (-1)e_5(4) + (-1)e_5(6) + (1)e_5(8) \\ &= e_5(2) - e_5(4) - e_5(1) + e_5(3) \\ &= -\sqrt{5}. \end{aligned}$$

Proposition 9.1

Let $p > 2$ and $b \in \mathbb{Z}$ with $\gcd(b, p) = 1$. Then

$$g_b^2 = p(-1)^{\frac{p-1}{2}}.$$

Lemma 9.1. Let $p > 2$ and $b \in \mathbb{Z}$. Then

$$g_b = \left(\frac{b}{p}\right) g_1.$$

Lemma 9.2. Let $m, m \in \mathbb{Z}$. Then

$$\sum_{b=0}^{p-1} e_p(b(m-n)) = \begin{cases} p & \text{if } m \equiv n \pmod{p} \\ 0 & \text{otherwise.} \end{cases}$$

9.1 Proof of quadratic reciprocity

9.1.1 Preliminaries

Definition 9.4. The set $\mathbb{Z}[x]$ is the ring of polynomials with integer coefficients.

Definition 9.5. The set $\mathbb{Z}[e_p]$ is defined as

$$\begin{aligned} \mathbb{Z}[e_p] &= \{f(e_p) : f \in \mathbb{Z}[x]\} \\ &= \{c_{p-1}e_p^{p-1} + c_{p-2}e_p^{p-2} + \cdots + c_1 e_p + c_0 : c_{p-1}, \cdots, c_0 \in \mathbb{Z}\}. \end{aligned}$$

Remark 9.1. Let $\alpha, \beta \in \mathbb{Z}[e_p]$ and q be a prime then,

$$(\alpha+\beta)^q \equiv \alpha^q + \beta^q \pmod{q}.$$

Remark 9.2. From now on the notation $e_p := e_p(1)$.

Definition 9.6. Let $\gamma, \alpha, \beta \in \mathbb{Z}[x]$. We say α **divides** β if there exists $\delta \in \mathbb{Z}[x]$ with $\alpha = \delta\beta$.

Definition 9.7. We say α is **congruent** to β modulo γ if $\gamma \mid (\alpha - \beta)$.

Theorem 9.2. If p is prime and $\alpha, \beta \in \mathbb{Z}[e_p]$ the

$$(\alpha+\beta)^p \equiv \alpha^p + \beta^p \pmod{p}.$$

9.1.2 The proof

Theorem 9.1 (The Law of Quadratic reciprocity)
Let $p, q > 2$ be two distinct primes. Then

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod{4} \textbf{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

Proof. Let g_1 be the Gauss sum associated to 1 modulo p i.e.

$$g_1 = \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)e_p(n).$$

We will compute g_1^q in two different ways then combine the results.

PART I. Let $P = p(-1)^{\frac{p-1}{2}}$, by Euler's criterion we have

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

By Proposition 9.1 and Lemma 9.1 we have

$$\begin{aligned} g_1^{q-1} &= (g_1^2)^{\frac{q-1}{2}} \\ &= P^{\frac{q-1}{2}} \\ &\equiv \left(\frac{P}{q}\right) \pmod{q} \end{aligned}$$

therefore,

$$g_1^q \equiv g_1\left(\frac{P}{q}\right) \pmod{q}$$

where the congruence is taken in $\mathbb{Z}[e_p]$.

PART II. Recall that if q is prime and $\alpha, \beta \in \mathbb{Z}[e_p]$ then

$$(\alpha+\beta)^q \equiv \alpha^q + \beta^q \pmod{q}.$$

As such we have that

$$\begin{aligned} g_1^q &= \left(\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e_p(n)\right)^q \\ &= \sum_{n=1}^{p-1} \left(\frac{n}{p}\right)^q e_p(n)^q \pmod{q}. \end{aligned}$$

Since q is odd then $\left(\frac{n}{q}\right)^q = \left(\frac{n}{q}\right)$ we can write

$$\begin{aligned} g_1^q &= \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e_p(qn) \pmod{q} \\ &\equiv g_q \pmod{q}. \end{aligned}$$

Recall $g_b = \left(\frac{b}{p}\right) g_1$ so,

$$g_q = \left(\frac{q}{p}\right) g_1$$

which implies that

$$g_1^q \equiv g_q \equiv \left(\frac{q}{p}\right) g_1 \pmod{q}.$$

PART III. Now we combine the results from the previous parts,

$$g_1^q \equiv g_1 \left(\frac{P}{q}\right) \equiv \left(\frac{q}{p}\right) g_1 \pmod{q}$$

thus,

$$g_1 \left(\frac{P}{q}\right) \equiv \left(\frac{q}{p}\right) g_1 \pmod{q}.$$

Multiplying by g_1 on both sides we get

$$g_1^2 \left(\frac{P}{q}\right) \equiv g_1^2 \left(\frac{q}{p}\right) \pmod{q}.$$

Since $\gcd(q, P) = 1$ we can cancel $g_1^2 = P$ from both sides of the congruence to get

$$\left(\frac{P}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q}.$$

Finally, since $\left(\frac{P}{q}\right), \left(\frac{q}{p}\right) \in \{-1, 1\}$ we must have that $\left(\frac{q}{p}\right) = \left(\frac{P}{q}\right)$.

As $P = p(-1)^{\frac{p-1}{2}}$ we conclude that

$$\begin{aligned}
\left(\frac{q}{p}\right) &= \left(\frac{P}{q}\right) \\
&= \left(\frac{p(-1)^{\frac{p-1}{2}}}{q}\right) \\
&= \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) \\
&= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \\
&= \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \\
&= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),
\end{aligned}$$

as desired.

□

10 Sum of two squares

Definition 10.1. An integer $m \in \mathbb{N}$ is a **sum of two squares** if $m = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

> **Remark 10.1.** In this definition we allow for a and b to be zero. Thus, perfect squares are also sums of two squares.

Definition 10.2. The **Gaussian integers** is the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Theorem 10.1. The **units** in $\mathbb{Z}[i]$ are: ± 1 and $\pm i$.

Theorem 10.2. Let $\alpha, \beta \in \mathbb{Z}[i]$, we say α **divides** β and, we write $\alpha \mid \beta$ if there exists a $\gamma \in \mathbb{Z}[i]$ with $\beta = \alpha\gamma$.

Definition 10.3. A **Gaussian prime** is a Gaussian integer $\mathfrak{p} \in \mathbb{Z}[i]$ such that $\mathfrak{p} \neq 0, \pm 1, \pm i$ and if $\mathfrak{p} \mid \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[i]$ then $\mathfrak{p} \mid \alpha$ or $\mathfrak{p} \mid \beta$.

> **Remark 10.2.** Since $\mathbb{Z} \subset \mathbb{Z}[i]$ we can deduce whether primes in $\mathbb{Z}$ are Gaussian primes. If a prime, p, is a sum of two squares i.e. $p^2 = a^2 + b^2$ then we can factor $p = (a + ib)(a - ib)$ in $\mathbb{Z}[i]$. So, p will not be a Gaussian prime. Conversely, if $p \in \mathbb{Z}$ is not a sum of two squares then p is a Gaussian prime.

Proposition 10.1. A positive integer, m, is a square if and only if every exponent a_i in the prime factorisation $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ is even.

Lemma 10.1

Suppose $m \in \mathbb{Z}$ is a sum of two squares i.e. $m = a^2 + b^2$ with $a, b \in \mathbb{Z}$. Then $m \equiv 0, 1, \text{ or } 2 \pmod 4$.

Proof. If $x \in \mathbb{Z}$ then x^2 is either 0 or 1 modulo 4. □

Corollary 10.1

If $m \equiv 3 \pmod 4$ then m is not a sum of two squares.

Lemma 10.1. Let $m \in \mathbb{Z}$, then m is a sum of two squares if and only if $m = |\alpha|^2$ for some $\alpha \in \mathbb{Z}[i]$.

Proof.

- Proof of ($\Rightarrow$). Suppose $m = a^2 + b^2$ then $m = (a + ib)(a - ib) = |a + ib|^2$.
- Proof of ($\Leftarrow$). If $n = |\alpha|^2$ for $\alpha = a + ib \in \mathbb{Z}[i]$ then $n = a^2 + b^2$.

□

Theorem 10.1

Let $m, n \in \mathbb{Z}$. If m and n are sums of two squares so is mn. We can write $m = a^2 + b^2$ and $n = c^2 + d^2$ then $mn = (ac - bd)^2 + (ad + bc)^2$.

Proof. Write $m = |\alpha|^2$ and $n = |\beta|^2$ for $\alpha, \beta \in \mathbb{Z}[i]$. Then $mn = |\alpha|^2 |\beta|^2 = |\alpha\beta|^2 \in \mathbb{Z}[i]$. So, by the previous lemma mn is a sum of two squares. Furthermore, we can write $m = a^2 + b^2 = (a + ib)(a - ib)$ and $n = c^2 + d^2 = (c + id)(c - id)$ as such,

$$\begin{aligned} mn &= (a + ib)(a - ib)(c + id)(c - id) \\ &= (a + ib)(c + id)(a - ib)(c - id) \\ &= [(ac - bd) + i(ad + bc)][(ac - bd) - i(ad + bc)] \\ &= (ac - bd)^2 + (ad + bc)^2. \end{aligned}$$

□

Example 10.1

Write $1313 = 13 \cdot 101$ as a sum of two squares.
Solution: Notice that

- $13 = 2^2 + 3^2$;
- $101 = 10^2 + 1^2$.

Therefore, we can write

$$\begin{aligned} 1313 &= (2 \cdot 10 - 3 \cdot 1)^2 + (2 \cdot 1 + 3 \cdot 10)^2 \\ &= 17^2 + 32^2. \end{aligned}$$

10.1 The two squares theorem

Theorem 10.3 (Pigeon hole principle)**.** If m objects are distributed into n containers and $m > n$ then **at least** one container contains more than 2 objects.

Example 10.1. Let $n \in \mathbb{N}$ and $S \subseteq \mathbb{Z}$ with $|S| = m > n$. There exists $a, b \in S$ with $a \neq b$ and $a \equiv b \pmod{n}$.

Lemma 10.2. Let $a, n \in \mathbb{Z}$ with $n > 1$ and n is not equal to a square number. Then there exists $(c_1, d_1), (c_2, d_2) \in \mathbb{Z} \times \mathbb{Z}$ with $0 \leq c_i, d_i < \sqrt{n}$ for $i = 1, 2$ such that:

- $c_1 + d_1 a \neq c_2 + ad_2$;
- $c_1 + ad_1 \equiv c_2 + ad_2 \pmod{n}$.

Theorem 10.2

Let p be a prime. Then p is a sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Theorem 10.3 (The two squares theorem)

An integer $n \in \mathbb{N}$ is a sum of two squares if and only if the exponent of every prime number which is congruent to 3 modulo 4 in the prime factorisation of n is even.

11 Irrational numbers

Definition 11.1. We use $\mathbb{R}$ to denote the real numbers, $\mathbb{C}$ the complex numbers and $\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \right\}$.

Definition 11.2. An **irrational number** is a complex number $z \in \mathbb{C}$ such that $z \notin \mathbb{Q}$.

Theorem 11.1. A real number $x \in \mathbb{R}$ is rational if and only if its decimal expansion either terminates or repeats.

Proposition 11.1

Let $z \in \mathbb{C}$ be a root of a polynomial $x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$ with integer coefficients $c_i \in \mathbb{Z}$. Then z is an integer or z is irrational.

Remark 11.1. We need the polynomial $f(x)$ to be monic i.e. the leading coefficient is 1.

Theorem 11.2. The number e is irrational.

11.1 Algebraic and transcendental numbers

Definition 11.3. A complex number $z \in \mathbb{C}$ is called **algebraic** if z is a root of a non-zero polynomial with rational coefficients.

Definition 11.4. A complex number z is called **transcendental** if it is not algebraic.

Example 11.1.

- $\frac{a}{b} \in \mathbb{Q}$ is algebraic as it is root of $x - \frac{a}{b}$.
- $\sqrt{2}$, $\sqrt[3]{5}$ and $\sqrt[d]{p}$ are all algebraic for $d \geq 2$ and p is prime.
- π and e are transcendental.

Example 11.1

Let $\alpha = \sqrt{7} + \sqrt{5}$. Find integers c_0, c_1, c_2, c_3 such that α is a root of $f(x) = x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$.

Solution: We know $\alpha = \sqrt{7} + \sqrt{5}$ which can be rewritten as $\alpha - \sqrt{7} = \sqrt{5}$ so,

$$(\alpha - \sqrt{7})^2 = (\sqrt{5})^2$$
$$\alpha^2 - 2\alpha\sqrt{7} + 7 = 5.$$

Which can be rewritten as $\alpha^2 + 2 = 2\alpha\sqrt{7}$. By squaring both sides

$$(\alpha^2 + 2)^2 = (2\alpha\sqrt{7})^2$$
$$\alpha^4 - 4\alpha^2 + 4 = 28\alpha^2$$
$$\alpha^4 - 24\alpha^2 + 4 = 0.$$

Therefore, the coefficients are

$$c_0 = 4$$
$$c_1 = c_3 = 0$$
$$c_2 = -24.$$

Theorem 11.1 (Dirichlet's approximation theorem)

Let $\alpha \in \mathbb{R}$ and $n \geq 1$ be an integer. Then there exists $\frac{a}{b} \in \mathbb{Q}$ with $a \in \mathbb{Z}$ and $1 \leq b \leq n$ such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{bn}.$$

Corollary 11.1. Suppose $\alpha \in \mathbb{R}$ is irrational. Then there exists infinitely many (distinct) rational numbers $\frac{a}{b}$ such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

Definition 11.5. Notation: For $\alpha \in \mathbb{R}$ let

$$\alpha = N(\alpha) + F(\alpha)$$

where $N(\alpha)$ is an integer $0 \leq F(\alpha) < 1$, where $F(\alpha)$ is called the **fractional part** of α and $N(\alpha)$ the **integer part** of α.

Example 11.2. $\pi = N(\pi) + F(\pi)$ with $N(\pi) = 3$ and $F(\pi) = 0.14159\ldots$

12 Liouville's Theorem

Theorem 12.1 (Liouville's Theorem)
Let $\alpha \in \mathbb{R}$ be an irrational number which is a root of a polynomial

$$f(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$$

with $c_i \in \mathbb{Q}$ and $c_m \neq 0$. Then there exists a real number $C > 0$ such that for all $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ we have

$$\left|\alpha - \frac{a}{b}\right| > \frac{C}{b^m}.$$

Note 12.1. The degree of b in the inequality is the degree of the polynomial f.

Theorem 12.2
The number $\sqrt{2}$ is irrational. Especially, we have

$$\left|\sqrt{2} - \frac{a}{b}\right| > \frac{C}{b^2}.$$

Proof. The proof of Liouville's theorem for the case $\alpha = \sqrt{2}$.
We will prove that for all $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ we have

$$\left|\sqrt{2} - \frac{a}{b}\right| > \frac{1}{b^2}\underbrace{\frac{1}{1+2\sqrt{2}}}_{C}.$$

- **Case 1.** If $\left|\sqrt{2} - \frac{a}{b}\right| < 1$ then we consider the polynomial $f(x) = x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2})$ to find bounds for $\left|f(\frac{a}{b})\right| = \left|\left(\frac{a}{b} - \sqrt{2}\right)\left(\frac{a}{b} + \sqrt{2}\right)\right|$.
  (We do this because we want to bound $\left|\frac{a}{b} - \sqrt{2}\right| = \left|\sqrt{2} - \frac{a}{b}\right|$).
  - **Upper bound** of $\left|f\left(\frac{a}{b}\right)\right|$. Note that by the triangle inequality we have

$$\begin{aligned}\left|\frac{a}{b} + \sqrt{2}\right| &= \left|\frac{a}{b} - \sqrt{2} + \sqrt{2} + \sqrt{2}\right| \\ &\leq \left|\frac{a}{b} - \sqrt{2}\right| + \left|\sqrt{2} + \sqrt{2}\right| \\ &\leq 1 + 2\sqrt{2}.\end{aligned}$$

    Therefore,

$$\left|f\left(\frac{a}{b}\right)\right| \leq \left|\frac{a}{b} - \sqrt{2}\right|\left(1 + 2\sqrt{2}\right).$$

  - **Lower bound** of $\left|f\left(\frac{a}{b}\right)\right|$. We have

$$\begin{aligned}\left|f\left(\frac{a}{b}\right)\right| &= \left|\left(\frac{a}{b}\right)^2 - 2\right| \\ &= \left|\frac{a^2 - 2b^2}{b^2}\right|.\end{aligned}$$

Since, $a^2 - 2b^2 \in \mathbb{Z}$ and $a^2 - 2b^2 \neq 0$ we have that $|a^2 - 2b^2| \geq 1$ hence,

$$\left| f\left(\frac{a}{b}\right) \right| \geq 1.$$

By combining the bounds we have

$$\frac{1}{b^2} \leq \left| f\left(\frac{a}{b}\right) \right| \leq \left| \frac{a}{b} - \sqrt{2} \right| \left(1 + 2\sqrt{2}\right),$$

which implies

$$\left| \sqrt{2} - \frac{a}{b} \right| > \frac{1}{(1 + 2\sqrt{2})\, b^2}.$$

- **Case 2.** If $\left|\sqrt{2} - \frac{a}{b}\right| \geq 1$ then we clearly have

$$\left| \sqrt{2} - \frac{a}{b} \right| > \frac{1}{(1 + 2\sqrt{2})\, b^2}$$

as well (since $b \geq 1$).

Therefore, we have

$$\left| \sqrt{2} - \frac{a}{b} \right| > \frac{1}{(1 + 2\sqrt{2})\, b^2}$$

in all cases. In this case we take $C = \frac{1}{1+2\sqrt{2}}$ in the statement of Liouville's theorem. $\square$

Note 12.2. By varying C the inequality can switch from $>$ to $\geq$ and vice versa.

Corollary 12.1

Let $\alpha \in \mathbb{R}$ be an irrational number as in Liouville's theorem. Suppose we have a real number $\varepsilon > 0$, then the inequality

$$\left| \alpha - \frac{a}{b} \right| < \frac{1}{b^{m+\varepsilon}}$$

holds for only finitely many $a \in \mathbb{Z}$ and $b \in \mathbb{N}$.

Example 12.1

The above corollary shows that thre exist pnly finite many a, b such that $\left|\sqrt{2} - \frac{a}{b}\right| \leq \frac{1}{b^3}$. We illustrate how to find them.
We have

$$\left|\sqrt{2} - \frac{a}{b}\right| > \frac{1}{(1 + 2\sqrt{2})b^2}$$

so if, $\left|\sqrt{2} - \frac{a}{b}\right| \leq \frac{1}{b^3}$ then, we have

$$\frac{1}{b^3} > \frac{1}{(1 + 2\sqrt{2})b^2}$$

which implies $b < 1 + 2\sqrt{2}$. Since, $b \in \mathbb{N}$, we deduce that $b = 1, 2, 3$.

- If $b = 3$, the inequality is $\left|\frac{a}{3} - \sqrt{2}\right| \leq \frac{1}{27}$ which implies that $\left|3\sqrt{2} - a\right| \leq \frac{1}{9}$. Since, $3\sqrt{2} \approx 4.24$, there are no integers within the range $\frac{1}{9}$ so, there are no a's satisfying the inequality.
- If $b = 2$ the inequality is $\left|\frac{a}{2} - \sqrt{2}\right| \leq \frac{1}{8}$ which implies that $\left|2\sqrt{2} - a\right| \leq \frac{1}{4}$. We get one solution, $a = 3$.
- If $b = 1$ we get $a = 1, 2$.

Proposition 12.1

The number $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.

Proof. Suppose for the sake of contradiction that α is a root of a polynomial of degree m with rational coefficients, i.e. α is algebraic. By Liouville's theorem we know there exists a real number $C > 0$ such that

$$\left|\alpha - \frac{a}{b}\right| > \frac{C}{b^m}$$

for all $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. To approximate α by rational number, consider the finite sum

$$\alpha_k = \sum_{n=1}^{k} \frac{1}{10^{n!}},$$

which has denominator of $10^{k!}$. Therefore, we have

$$|\alpha - \alpha_k| = \sum_{n=k+1}^{\infty} \frac{1}{10^{n!}}.$$

By considering the decimal expansion of

$$\begin{aligned}
\sum_{n=k+1}^{\infty} \frac{1}{10^{n!}} &= \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} + \dots \\
&= 0.01 + 0.000001 + 0.\underbrace{0\dots01}_{24} + \dots \\
&= 0.0\underset{2^{\text{th}}}{1}\,000\underset{6^{\text{th}}}{1}\,0\dots0\underset{24^{\text{th}}}{1}\ \dots
\end{aligned}$$

Generally, the decimal expansion of $\sum_{n=k+1}^{\infty} \frac{1}{10^{n!}}$ takes the form of

$$\begin{aligned}\sum_{n=k+1}^{\infty} \frac{1}{10^{n!}} &= 0.0\dots0 \underset{(k+1)!^{\text{th}}}{1} 0\dots0 \underset{(k+2)!^{\text{th}}}{1} \dots \\ &< 0.0\dots0 \underset{(k+1)!^{\text{th}}}{2} \\ &= \frac{2}{10^{(k+1)!}}.\end{aligned}$$

Therefore,

$$|\alpha - \alpha_k| = \sum_{n=k+1}^{\infty} \frac{1}{10^{n!}} < \frac{2}{10^{(k+1)!}}.$$

By taking k large enough, we can make $\frac{2}{10^{(k+1)!}} = \frac{2}{\left(10^{k!}\right)^{k+1}}$ less than $\frac{C}{\left(10^{k!}\right)^{m}}$, which contradicts Liouville's theorem. Hence, α is transcendental. $\square$

13 Pythagorean triples

Definition 13.1. We say $(x, y, z) \in \mathbb{N}$ is a **Pythagorean triple** if $x^2 + y^2 = z^2$.

Definition 13.2. A Pythagorean triple,(x, y, z), is called **primitive** if $\gcd(x, y, z) = 1$.

Lemma 13.1. Suppose (x, y, z) is a primitive Pythagorean triple. Then any two of three integers (x, y, z) are coprime.

Lemma 13.2. If (x, y, z) is a primitive Pythagorean triple the one of x, y is even and the other is odd.

Theorem 13.1. Let $n \in \mathbb{N}$ then n is a square (i.e. $n = c^2$ for $c \in \mathbb{N}$) if and only if in its prime factorisation each prime appears to an even power.

Lemma 13.3. Suppose $\gcd(a, b) = 1$ for $a, b \in \mathbb{N}$ and $ab = c^2$ for some $c \in \mathbb{N}$. Then a and b are both squares.

Theorem 13.1 (Pythagorean triples theorem)
All primitive Pythagorean triples, (x, y, z), with x even, are given by the formulas:

$$\begin{aligned} x &= 2st \\ y &= s^2 - t^2 \\ z &= s^2 + t^2 \end{aligned}$$

for integers

(i) $s > t > 0$;

(ii) $\gcd(s, t) = 1$;

(iii) $s \not\equiv t \pmod 2$.

To get all Pythagorean triples (up to swapping x and y) we take integers s and t as above and d another positive integer and consider

$$\begin{aligned} x &= 2dst \\ y &= d(s^2 - t^2) \\ z &= d(s^2 + t^2). \end{aligned}$$

Remark 13.1. The theorem implies that there is a bijection between primitive Pythagorean triples, (x, y, z) and $(s, t) \in \mathbb{N}$ which satisfy (i), (ii) and (iii).

Example 13.1. Find all primitive Pythagorean triples, (x, y, z) with $z = x + 3$.
Solution: Write $x = 2st$ and $z = s^2 + t^2$. So,

$$\begin{aligned} s^2 + t^2 = 2st + 3 \iff & s^2 - 2st + t^3 = 3 \\ \Rightarrow & (s - t)^2 = 3. \end{aligned}$$

Which has no solutions as 3 is not a perfect square. Therefore, there are no primitive Pythagorean triples with $z = x + 3$ and x being even.

Example 13.2. Find all primitive Pythagorean triples, (x, y, z) with x being even and $z = y + 2$.
Solution: Write $x = 2st, y = s^2 - t^2$ and $z = s^2 + t^2$.

$$\begin{aligned} s^2 + t^2 = s^2 - t^2 + 2 \Rightarrow & \, 2t^2 = 2 \\ \Rightarrow & \, t = 1. \end{aligned}$$

Since $s \not\equiv t \pmod 2, s > t, \gcd(s, t) = 1$ and $t = 1$, we have that s can be any positive even number.
Write, $s = 2k$ for $k \in \mathbb{N}$ and $t = 1$.

$$\begin{aligned} (x, y, z) &= (4k, (2k)^2 - 1, (2k^2) + 1) \\ &= (4k, 4k^2 - 1, 4k^2 + 1), \end{aligned}$$

with $b \in \mathbb{N}$ which satisfy $z = y + 2$.

Example 13.1 (Exam 2022)
Find all primitive Pythagorean triples with $x = 88$.
Solution: By the Pythagorean triples theorem we can write

$$x = 88 = 2st$$
$$\Rightarrow st = 44$$

for $s, t \in \mathbb{N}$. Since $s > t$ by property (i) we have

- $s = 44, t = 1$;
- $s = 22, t = 2$;
- $s = 11, t = 4$.

Now we need to check the remaining properties:

(s,t)	$\gcd(s,t)$	$s \not\equiv t \pmod 2$
$(44,1)$	1	✓
$(22,2)$	2	×
$(11,4)$	1	✓

Therefore, for $(s,t) = (44,1)$ we have

$$x = 88, y = 1935, z = 1937,$$

and for $(s,t) = (11,4)$ we have

$$x = 88, y = 105, z = 137.$$

14 Fermat's Last Theorem

Definition 14.1. Given $n \in \mathbb{N}$, the n^{th} **Fermat equation** is given

$$x^n + y^n = z^n.$$

Theorem 14.1
If $n \geq 3$ there are no positive integer solutions (x, y, z) to the equation

$$x^n + y^n = z^n.$$

Theorem 14.1. There are no positive integer solution, (x, y, z), to the equation

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

Remark 14.1. If (x_0, y_0, z_0) satisfy $x_0^4 + y_0^4 = z_0^2 = (z_0^2)^2$. Then (x_0, y_0, z_0^2) is a solution to the 4^{th} Fermat equation.
Similarly, if $n = 4k$ for $k \in \mathbb{N}$ then $4k^{\text{th}}$ Fermat equation has no solution by the theorem,

$$x^{4k} + y^{4k} = z^{4k} \iff (x^k)^4 + (y^k)^4 = (z^{2k})^2.$$

Note 14.1. We will use Fermat's method of "descent": given a solution (x, y, z) we produce another solution (x', y', z') with $z' < z$. This will be a contradiction if we start the solution by minimising z.

Proof. Let $(x, y, z) \in \mathbb{N}$ be a solution with minimum possible z.

- If $\gcd(x, y) > 1$ then $p \mid x$ and $p \mid y$ for some prime p. Then $p^4 \mid (x^4 + y^4)$ that is $p^4 \mid z^2$. Hence, $p^2 \mid z$. Then $(x', y', z') = \left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2}\right)$ is a solution in $\mathbb{N}$ with $z' < z$. This is a contradiction.

- If $\gcd(x, y) = 1$ then $\gcd(x^2, y^2) = 1$ and so (x^2, y^2, z) is a primitive Pythagorean triple. Without loss of generality, assume that x^2 is even and y^2 is odd, that is x is even and y is odd. Hence, there exists $s, t \in \mathbb{N}$ with $\gcd(s, t) = 1, s > t > 0$ and $s \not\equiv t \pmod 2$ such that
$$\begin{aligned} x &= 2st \\ y &= s^2 - t^2 \\ z &= s^2 + t^2. \end{aligned}$$
We can write
$$t^2 + y^2 = s^2$$
therefore, (t, y, s) is a primitive Pythagorean triple with t even since y is odd. Applying the Pythagorean Triple theorem again we can write
$$\begin{aligned} t &= 2uv \\ y &= u^2 - v^2 \\ s &= u^2 + v^2 \end{aligned}$$
with $\gcd(u, v) = 1, u > v > 0$ and $u \not\equiv v \pmod 2$. Observe that
  - $\gcd(u, u^2 + v^2) = \gcd(u, v^2) = 1$;
  - $\gcd(v, u^2 + v^2) = \gcd(v, u^2) = 1$.

  Recall
$$\begin{aligned} x^2 &= 2st \\ &= 4uv(u^2 + v^2) \\ \left(\frac{x}{2}\right)^2 &= uv(u^2 + v^2). \end{aligned}$$
Hence, $uv(u^2 + v^2)$ is a square which implies $u, v, u^2 + v^2$ are also squares. Since $\gcd(u, v) = \gcd(u, u^2 + v^2) = \gcd(v, u^2 + v^2) = 1$ then there exists $x', y', z' \in \mathbb{N}$ with
$$u = (x')^2, \quad v = (y')^2 \quad \text{and} \quad u^2 + v^2 = (z')^2$$

so,

$$\begin{aligned} u^2 + v^2 &= (x')^4 + (y')^4 \\ &= (z')^2. \end{aligned}$$

This implies (x', y', z') is a solution to Fermat's 4^{th} equation. Recall,

$$z = s^2 + t^2 \quad \text{and} \quad s = u^2 + v^2 = (z')^2$$

hence, $z > s^2 > z'$ which is a contradiction to minimality.

□

15 General Diophantine equation

Definition 15.1. Given integers $c_1, c_2, \ldots, c_n \in \mathbb{Z}$ a **Diophantine equation** is an equation of the form

Proposition 15.1. Let $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots c_1 x + c_0$ where $c_0, \ldots, c_n \in \mathbb{Z}$ with $c_n \neq 0$. If $a \in \mathbb{Z}$ is a root of $f(x)$ then

$$f(x) = (x - a)g(x),$$

where $g(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ where $b_0, \ldots, b_{n-1} \in \mathbb{Z}$.

Proposition 15.2. For each $k \in \mathbb{N}$ we have

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}).$$

15.1 Solving Diophantine equations

There is no general (known) method to solve Diophantine equations, but there are some special cases where there is a method.

Proposition 15.1

Suppose $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots c_1 x + c_0$ with $c_i \in \mathbb{Z}$, if $f(a) = 0$ with $a \in \mathbb{Z}$ then $a \mid c_0$.

Note 15.1. Strategy: To solve $f(x) = 0$ with $x \in \mathbb{Z}$ check $f(d)$ for each $d \mid c_0$.

Example 15.1. Find all integer solutions to $f(x) = 0$ for $f(x) = 2x^4 - 14x^3 + 3x^2 + 20x - 7$.

Solution. We have $c_0 = -7$ therefore, we must check if $f(d) = 0$ for $d \mid -7$ i.e. $d = \pm 1$ or $d = \pm 7$. Only $f(7) = 0$ hence, $x = 7$ is the only solution to $f(x)$ in $\mathbb{Z}$.

Example 15.2. Find all integer solutions to

$$x^4 + 4x^2 - 12xy + 9y^2 - 2 = 0.$$

Solution: Notice that $4x^2 - 12xy + 9y^2 = (2x - 3y)^2$. So, we have

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

Since, $x, y \in \mathbb{Z}$ we have that $x = \pm 1$ as the RHS is 2.

- If $x = 1$ then $(2-3y)^2 = 1 \Rightarrow y = 1$.
- If $x = -1$ then $(-2-3^2) = 1 \Rightarrow y = -1$.

The solutions (x, y) are $(1, 1)$ or $(-1, -1)$.

Example 15.3. Find all integer solutions to

$$x^2 - 3y^4 = 0.$$

Solutions: We can rewrite

$$x^2 = 3y^4$$
$$\left(\frac{x}{y^2}\right)^2 = 3 \text{ for } y \neq 0.$$

Therefore, the only solution is $(x, y) = (0, 0)$.

15.2 Diophantine and congruence equations

Consider a Diophantine equation $x^7 + 7y^5 = 610$. For each $m \in \mathbb{N}$ we get a corresponding congruence equation modulo m. Consider

$$x^7 + 7y^5 \equiv 610 \pmod{m}.$$

In the Diophantine equation we seek solutions in $\mathbb{Z}$ and in the congruence equation we seek solutions in $\mathbb{Z}_m$.

Proposition 15.3. If a Diophantine equation has a solution in $\mathbb{Z}$ then the corresponding congruence equation has a solution for each $m \geq 1$ in $\mathbb{Z}_m$.

> **Note 15.2.** Therefore, if the congruence equation has no solution in $\mathbb{Z}_m$ for some $m \geq 1$ then its associated Diophantine equation has no solution in $\mathbb{Z}$.

Example 15.4. Solve

$$x^7 + 7y^5 \equiv 610 \pmod{2}.$$

Solution. We note that $610 \equiv 0 \pmod{2}$ and for all $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ we have the following relation in modulo 2.

$$a^n \equiv a \pmod{2}.$$

Therefore, $x^7 \equiv x \pmod{2}$ and $7y^5 \equiv 7y \equiv y \pmod{2}$, since $7 \equiv 1 \pmod{2}$. So, we are left to solve

$$x + y \equiv 0 \pmod{2}.$$

The solutions are $(x, y) = ([0]_2, [0]_2)$ or $([1]_2, [1]_2)$.

Example 15.5. Solve the Diophantine equation

$$x^{12} + 13y^5 = z^{12} + 2.$$

Strategy for choosing m:
Want $x^{12}, 13y^5$ and z^{12} to take on few values modulo m.

Recall: By the Euler-Fermat theorem $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$.
Solution: With this in mind consider

$$x^{12} + 13y^5 \equiv z^{12} + 2 \pmod{13}.$$

So, $x^{12} \equiv 1$ or 0 modulo 13 if $13 \nmid x$ and $13 \mid x$ respectively. The next term $13y^5 \equiv 0 \pmod{13}$. Thus, we are left with

$$x^{12} \equiv z^{12} + 2 \pmod{13}.$$

LHS $\equiv 0$ or 1 modulo 13.
RHS $\equiv 2$ or 3 modulo 13. Hence, LHS $\neq$ RHS. This, congruence equation has no solution in $\mathbb{Z}_{13}$ which implies that the associated Diophantine equation has no solutions

> **Remark 15.1.** This method is not always possible i.e. some equation could have solutions for all $m \geq 1$ in modulo m but no integer solutions.

Example 15.6. Find all integer solutions to

$$x^4 + y^4 = z^4 + w^6 + 3.$$

Solution. We note that

$$x^4 \equiv 0, 1 \pmod{8}$$
$$w^6 \equiv 0, 1 \pmod{8}.$$

Therefore,

$$\text{LHS} \equiv 0, 1, 2 \pmod{8}$$
$$\text{RHS} \equiv 3, 4, 5 \pmod{8}$$

Hence, LHS $\not\equiv$ RHS $\pmod{8}$. This congruence equation has no solutions in $\mathbb{Z}_8$ thus, it will not have solutions in $\mathbb{Z}$.

15.3 Week 12 lectures

Diophantine Equations, additional examples

Ex Show that

$D: \quad x^2 = y^5 + 7$

has no solutions in integers.

Strategy Find an $m \in \mathbb{N}$ so that

$C_m: \quad x^2 \equiv y^5 + 7 \pmod{m}$

has no solutions in $\mathbb{Z}_m$.

How to choose m? We want x^2, y^5 to take on few values.

Euler's Criterion For $a \in \mathbb{Z}$

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

Let's $p = 3$.

$C_3: \quad x^2 \equiv y^5 + 7 \bmod 3$

$x^2 \equiv 0$ or $1 \bmod 3$

$x^2 \equiv y + 1 \bmod 3$

$\Updownarrow$

$y^4 \equiv 0$ or $1 \bmod 3$

$x \equiv 0$, $x \equiv \pm 1$

$y^5 \equiv y \bmod 3$

$y \equiv 2$ $\quad$ $y \equiv 0$

$p = 11$, $y^5 = y^{\frac{11-1}{2}} \equiv -1, 0, \text{ or } 1 \pmod{11}$

x	$x^2 \bmod 11$
± 1	1
± 2	4
± 3	9
± 4	$16 \equiv 5$
± 5	$25 \equiv 3$

$x^2 \equiv 0, 1, 3, 4, 5 \text{ or } 9 \pmod{11}$

$C_{11}: \quad x^2 \equiv y^5 + 7 \pmod{11}$

$\text{LHS} \equiv 0, 1, 3, 4, 5 \text{ or } 9 \pmod{11}$

$\text{RHS} \equiv 6, 7 \text{ or } 8 \bmod 11$

$\text{LHS} \not\equiv \text{RHS} \pmod{11} \Rightarrow C_{11}$ has no sol'ns in $\mathbb{Z}_{11} \Rightarrow D$ has no sol'ns in $\mathbb{Z}$.

(d) Show that the Diophantine equation $x^4 - 4y^4 = z^2$ has no solutions in positive integers x, y, z with $\gcd(x, z) = 1$. Precisely state any results you use from the lectures.
(Hint: Express the equation as $(x^2)^2 = (2y^2)^2 + z^2$ and use the Pythagorean Triples Theorem.)

$\ast$ $(2y^2, z, x^2)$

is a PPT since $\gcd(x,z)=1$

$\Rightarrow \gcd(2y^2, z, x^2) = 1$

Apply the PT Thm

$2y^2 = 2st$, $z = s^2 - t^2$, $x^2 = s^2 + t^2$

with $s > t > 0$, $\gcd(s,t) = 1$, $s \not\equiv t \pmod 2$

$\Rightarrow y^2 = st$. $\Rightarrow s,t$ are squares

So $\exists u, v \in \mathbb{N}$ with $s = u^2$, $t = v^2$

$\Rightarrow x^2 = u^4 + v^4$ $\Leftarrow$ has no sol'ns in positive integers by Thm 11.2 in the lectures.

$\Rightarrow x^4 - 4y^4 = z^2$ has no sol'ns in positive integers with $\gcd(x,z) = 1$.

(10) $x^{16} \equiv 7 \pmod 9$

$\boxed{-2 \text{ is a PR } \pmod 9.}$

$2^4 \equiv 7 \pmod 9$

& write $x = 2^j$ Solve $j \bmod \phi(9)$

$2^{16j} \equiv 2^4 \bmod 9$

Apply <u>Lemma 5.1</u> $\phi(9) = 6$

$\Rightarrow$ $16j \equiv 4 \bmod 6$

$\Leftrightarrow$ $8j \equiv 2 \bmod 3$

$\Leftrightarrow$ $j \equiv 1 \bmod 3$

$\Rightarrow$ $j \equiv 1$ or $4 \bmod 6$

2 sol'ns, $x \equiv 2^1, 2^4 \bmod 9$

$x \equiv 2, 7 \bmod 9$

May 2021

(c) Let p be a prime such that $p \equiv 1 \pmod 4$. For each integer $n \geq 1$, determine the number of solutions in $\mathbb{Z}_{p^n}^{\times}$ to the congruence equation

$$\boxed{x^p + x^{\frac{(p-1)}{2}} + px \equiv 0 \pmod{p^n}.}$$

1^{st} Solve:

$$f(x) = x^p + x^{\frac{p-1}{2}} + \overbrace{p\,x}^{\equiv 0 \bmod p} \equiv 0 \bmod p$$

in $\mathbb{Z}_p^{\times}$. For $\gcd(x,p)=1$

- $x^p \equiv x \pmod p$ $\longleftrightarrow$ Fermat's little Thm
- $x^{\frac{p-1}{2}} \equiv \left(\frac{x}{p}\right) \pmod p$ $\longleftrightarrow$ Euler's Criterion

$$f(x) \equiv x + \left(\frac{x}{p}\right) \bmod p$$

$$f(x) \equiv 0 \bmod p \iff \boxed{x \equiv -\left(\frac{x}{p}\right) \bmod p}$$

Recall $p \equiv 1 \bmod 4$

- $x = 1$

$$1 \cancel{\equiv} -\underbrace{\left(\frac{1}{p}\right)}_{=1} \bmod p$$

- Check $x=-1$

$$-1 \equiv -\left(\frac{-1}{p}\right) \bmod p \quad ✓$$

$\left(\frac{-1}{p}\right) = 1$ for $p \equiv 1 \bmod 4$

Hence, the only sol'n to

$$f(x) \equiv 0 \mod p$$

in $\mathbb{Z}_p^\times$ is $x \equiv -1 \mod p$.

We now check to see if
we can apply Hensel's Lemma.
to lift ~~to~~ our solution to
a solution in $\mathbb{Z}_{p^2}^\times$.

$$f'(-1) \overset{?}{\equiv} 0 \mod p$$

$$f'(x) = p x^{p-1} + \frac{p-1}{2} \cdot x^{\frac{p-1}{2}-1} + p$$

$$f'(-1) \equiv \underbrace{\frac{p-1}{2} (-1)^{\frac{p-3}{2}}}_{\not\equiv 0 \mod p} \mod p$$

$\not\equiv 0 \mod p$ (since p is prime)

Hensel applies

The solution $x_1 = -1$ will
lift to a unique solution x_n in $\mathbb{Z}_{p^n}^\times$
for each $n \geq 1$, with $x_n \equiv x_1 \mod p$

Note: $\gcd(x_n, p) = 1$ $\qquad \equiv 1$

$\Rightarrow \gcd(x_n, p^n) = 1$

$[x_n] \in \mathbb{Z}_{p^n}^{\times}$.

What if $f'(x_1) \equiv 0 \mod p$?

<u>Check</u> $p^2 \mid f(x_1)$

- If yes, p sol'ns, x_2
  $x_2 \equiv x_1 \mod p$ & $f(x_2) \equiv 0 \mod p^2$

- If no, <u>no sol'ns</u> x_2 with
  $f(x_2) \equiv 0 \mod p^2$ <u>&</u> $x_1 \equiv x_2 \mod p$.

(Lemma 3.7)

Review lecture

(d) For which odd primes p do we have

$$\left(\frac{-14}{p}\right) = -1?$$

(Your answer should be given in terms of a description of the possible congruence classes for p modulo some positive integer.)
[12 marks]

<u>Strategy</u> Set

multiplicctivity

$$-1 = \left(\frac{-14}{p}\right) \overset{R1}{=} \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{7}{p}\right)$$

Now compute the Legendre symbol

Rule for 2

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

$$\boxed{\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}} \quad \longleftrightarrow \text{ rule for } -1$$

$$\left(\frac{7}{p}\right) \overset{R4}{=} \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}\cdot\frac{7-1}{2}} = \left(\frac{p}{7}\right)(-1)^{\frac{p-1}{2}}$$

Quadratic reciprocity

$(-1)^3 = -1$

$$\to \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = \underbrace{(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}}}_{= (-1)^{p-1} = 1}\left(\frac{p}{7}\right)$$

$$= \underline{\left(\frac{p}{7}\right)}$$

we want

$$\boxed{-1 = \left(\frac{2}{p}\right)\left(\frac{p}{7}\right)}$$

~~choices~~ __Cases__; i) $\left(\frac{2}{p}\right) = -1$, $\left(\frac{p}{7}\right) = 1$

ii) $\left(\frac{2}{p}\right) = 1$, $\left(\frac{p}{7}\right) = -1$

x	x^2 mod 7
± 1	1
± 2	4
± 3	2 mod 7

$\longleftrightarrow$ QR mod 7

, 3, 5, 6 QNR mod 7

__case i)__ $\left(\frac{2}{p}\right) = -1$, $\left(\frac{p}{7}\right) = 1$

6 possibilities

$p \equiv \pm 3 \mod 8$ $\qquad$ $p \equiv 1, 2, 4 \mod 7$

case ii) $\left(\frac{2}{p}\right) = +1$ & $\left(\frac{p}{7}\right) = -1$

6 possibilities

$p \equiv \pm 1 \mod 8$ & $p \equiv 3, 5, 6 \mod 7$

CRT

$\Rightarrow$ $\boxed{p \equiv 11, 17, 29, 31, 33, 37, 41, 43, 47, 51, 53, \text{ or } 55 \pmod{56}}$

Answer

Revision

- Check your understanding questions
- Homework questions
- Revision questions
- Past exam questions

Do a past exam in exam conditions!

Mark your exam

Ex (lecture notes) Show the equation

$$x^3 + 2y^3 + 4z^3 = 9w^3 \quad (*)$$

has no solutions in positive integers.

Homogeneous eq'n i.e. each "variable" occurs to the same power

If $(*)$ has a solution

(x, y, z, w) then

for $d = \gcd(x, y, z, w)$

$\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}, \frac{w}{d}\right)$ is also a

sol'n to Ⓐ & $\gcd\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}, \frac{w}{d}\right) = 1$

Consider

C_9: $\quad x^3 + 2y^3 + 4z^3 \equiv \cancel{9w^3}$ $\equiv 0 \bmod 9$ $\pmod 9$

For $a \in \mathbb{Z}$, $\quad a^3 \equiv 0, \pm 1 \pmod 9$ — exercise

0 if $3 | a$, $\quad \pm 1$ if $\gcd(a, 3) = 1$

$\Rightarrow$ RHS $\equiv 0 \bmod 9$

LHS $\not\equiv 0 \bmod 9$ unless $3|x$, $3|y$ & $3|z$

check case by case

LHS $\equiv 0 \bmod 9$ if $\cancel{x} \equiv y \equiv z \equiv 0 \bmod 3$

If Ⓐ has a solution in $\mathbb{N}$

it has a primitive sol'n $\Leftrightarrow \gcd(x, y, z, w) = 1$

$\Rightarrow$ ~~If~~ C_9, has a sol'n x, y, z

are multiples of 3.

$$\underbrace{x^3 + 2y^3 + 4z^3}_{} = 9w^3$$

$\Rightarrow 3^3 | 9w^3 \Rightarrow 3 | w$

$\Rightarrow 3 | \gcd(x, y, z, w)$.

Hence ⊛ has no primitive sol'ns in $\mathbb{N}$ $\Rightarrow$ ⊛ has no sol'ns in $\mathbb{N}$.

Exam problem: Evaluate

$$\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right)$$

(b) Show that the number of solutions in $\mathbb{Z}_p \times \mathbb{Z}_p$ to the congruence equation

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

equals

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right).$$

Recall The # of sol'ns to $x^2 \equiv b \pmod{p}$ in $\mathbb{Z}_p$ equals $1 + \left(\frac{b}{p}\right)$, for $p > 2$, $b \in \mathbb{Z}$.

For each $y \pmod{p}$ the equation $x^2 \equiv y^2 + a \pmod{p}$ has $1 + \left(\frac{y^2+a}{p}\right)$ sol'ns in $\mathbb{Z}_p$.

(take $b = y^2+a$). Now sum over $y \pmod{p}$ to get the number of sol'ns in $\mathbb{Z}_p \times \mathbb{Z}_p$ is

$$= \sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right).$$

(c)

(i) Prove that the map $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$ given by $(x, y) \to (x + y, x - y)$ is a bijection.

(ii) For a such that $\gcd(a, p) = 1$, use part (i) to show that there are $p - 1$ solutions in $\mathbb{Z}_p \times \mathbb{Z}_p$ to the congruence equation

$$x^2 - y^2 \equiv a \pmod{p}.$$

(Hint: Make the change of variables $u = x + y, v = x - y$.)

i) It suffices to show the map is a surjection. $(p \neq 2)$

Let $([u]_p, [v]_p) \in \mathbb{Z}_p \times \mathbb{Z}_p$, we need to find $x, y \in \mathbb{Z}_p$

① $x + y = [u]_p$

② $x - y = [v]_p \quad \rightarrow \quad x = [v]_p + y$

$\Rightarrow \quad [v]_p + 2y = [u]_p$

$\Rightarrow \quad y = [2]_p^{-1}[u - v]_p$

Similarly $\quad x = [2]_p^{-1}[u + v]_p$

Hence the map is a surjection

$\Rightarrow$ bijection

ii) Use i) to show

(★) $x^2 - y^2 \equiv a \mod p$

has $p-1$ sol'ns in $\mathbb{Z}_p \times \mathbb{Z}_p$.

Let $u = x+y$ & $v = x-y$ then (★)

gives $x^2 - y^2 = (x-y)(x+y) = \boxed{vu \equiv a \mod p}$

Note: $p \nmid a$, For each $v \pmod p$

~~the~~ with $p \nmid v$ there is exactly 1

sol'n $\boxed{u \equiv a v^{-1} \mod p}$ & for $p \mid v$

there are no sol'ns.

There are $p-1$ $v \pmod p$, $v \not\equiv 0 \mod p$

$\boxed{\Rightarrow x^2 - y^2 \equiv a \pmod p \text{ has } p-1 \text{ sol'ns in } \mathbb{Z}_p \times \mathbb{Z}_p.}$

(d) Use parts (b) and (c) to show that if $\gcd(a, p) = 1$ then

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right) = -1.$$

What is the value of this sum if $p|a$?

By b) & c)

$$\cancel{p}-1 = \sum_{y=0}^{p-1}\left(1 + \left(\frac{y^2+a}{p}\right)\right)$$

$$= \cancel{p} + \sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right)$$

If $p|a$, $\left(\frac{y^2+a}{p}\right) \overset{R0}{=} \left(\frac{y^2}{p}\right) \overset{R1}{=} \left(\frac{y}{p}\right)^2$

$$= \begin{cases} 1 & \text{if } p \nmid y \\ 0 & \text{if } p | y \end{cases}$$

$$\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right) = p-1$$

(c) Let p be a prime number. Prove that the congruence equation

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

has exactly one solution in $\mathbb{Z}_p$ for each odd integer n if and only if p is of the form $2^k + 1$.

Let g be a PR mod p

write $x \equiv g^i \pmod{p}$, $1 \equiv g^0 \bmod p$

Lemma 5.1

$\boxed{g^{in} \equiv 1 \bmod p} \longrightarrow$ ~~old~~ $in \equiv 0 \pmod{p-1}$

exercise

Claim $in \equiv 0 \bmod p-1 \iff \boxed{i \equiv 0 \bmod \left(\frac{p-1}{\gcd(n, p-1)}\right)}$

~~we~~ $\Rightarrow$ $x^n \equiv 1 \bmod p$

has 1 sol'n each odd n

iff $\gcd(n, p-1) = 1$

for each odd n

iff $p-1 = 2^k$

iff $p = 2^k + 1$

Appendix

A Equivalence relations

Definition A.1. A binary operation on a set X is said to be an **equivalence relation**, if and only if it is reflexive, symmetric and transitive. That is for all $a, b, c \in X$:

- Reflexivity: $a \sim a$;
- Symmetry: $a \sim b$ if and only if $b \sim a$;
- Transitivity: if $a \sim b$ and $b \sim c$ then $a \sim c$.

A.1 Equivalence classes

Theorem A.1. If $\sim$ is an equivalence relation on a set X and $x, y \in X$ then, these statements are equivalent:

- $x \sim y$;
- $[x] = [y]$;
- $[x] \cap [y] = \emptyset$

B Solving linear congruences

Proposition B.1. Let $a, b \in \mathbb{Z}$ and let m be a positive integer. Set $g = \gcd(a, m)$. The congruence relation

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

has integer solutions for x if and only if $g \mid b$. If $d \mid b$, the solutions are given by the integers x such that

$$[x]_{\frac{m}{g}} = \left[\frac{a}{g}\right]^{-1}_{\frac{m}{d}} \left[\frac{b}{d}\right]_{\frac{m}{d}}.$$

Proof. If $ax \equiv b \pmod{m}$ then $b = ax + km$ for some $k \in \mathbb{Z}$. So $\gcd(a, m)$ (which divided a and m) must divide b. Conversely, if $d \mid b$ then

$$\frac{a}{g}x \equiv \frac{b}{g} \left(\mathrm{mod}\ \frac{m}{g}\right)$$

if and only if $ax \equiv b \pmod{m}$. Multiplying by an inverse of $\frac{a}{d}$ modulo $\frac{m}{d}$ we get that

$$\frac{a}{g}x \equiv \frac{b}{g} \left(\mathrm{mod}\ \frac{m}{g}\right)$$

if and only if

$$[x]_{\frac{m}{g}} = \left[\frac{a}{g}\right]^{-1}_{\frac{m}{d}} \left[\frac{b}{d}\right]_{\frac{m}{d}}.$$

□