INTRODUCTION TO NUMBER THEORY
LECTURE NOTES

Contents

Date: September 13, 2024.

1. GCD & Euclidean algorithm, Bezout's Lemma, LCM & Linear Diopantine Equations

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 $b|a$.

Here are some basic properties of divisibility: let a, b, c, be three integers

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

Theorem 1.2. *Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that*

$$a = qb + r$$

and $0 \leq r < b$.

Proof. Let $S = \{a - nb : n \in \mathbb{Z}\}$. Then we let $r = a - qb$ be the smallest non-negative element of S. Since S contains positive elements (take n to be the negative of a very large integer) this smallest element exists by the well-ordering principle. We have $0 \leq r < b$, otherwise $r - b$ is a smaller non-negative element of S.

If $a = qb + r = q'b + r'$ then $b|(r - r')$, and $-b < r - r' < b$ so this implies that $r = r'$ and therefore $q = q'$. This shows uniqueness of q and r. □

Greatest common divisors.

Definition 1.3. Let a and b be integers. If d is another integer with $d|a$ and $d|b$ we say that d is a *common divisor* of a and b.

If at least one of a and b are non-zero, 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. We write $\gcd(a, b)$ for the greatest common divisor of a and b.

The Euclidean algorithm. The most obvious way to find the gcd of two integers is to write down all the divisors of each number and compare them to find the greatest common divisor. Of course this method will be very slow in practice! A more efficient way of calculating the gcd is based on the following:

Lemma 1.4. *If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Suppose d is a common divisor of a and b. Since $r = a - qb$ we also have $d|r$ so d is a common divisor of b and r. In the other direction, if d is a common divisor of b and r, then we also have $d|a$, since $a = qb + r$. So d is a common divisor of a and b. We therefore see that the two sets of integers {common divisors of a and b}, and {common divisors of b and r} are the same, so they have the same largest element and we have $\gcd(a, b) = \gcd(b, r)$. □

Suppose we start off with integers a, b and we want to work out $\gcd(a, b)$. First we do some easy simplifications: we can assume that a and b are both non-zero, since the gcd is easy to work out if one of them is zero. Also, since $\gcd(a, b) = \gcd(|a|, |b|)$ we can assume that a and b are both positive. If $a = b$ then $\gcd(a, b) = |a|$, so we can assume $a \neq b$. Finally, since $\gcd(a, b) = \gcd(b, a)$ we can assume $a > b > 0$.

The above Lemma tells us that we can work out $\gcd(a, b)$ by first dividing a by b and then working out the gcd of b and r, where $b > r \geq 0$. Since r is smaller than b we have reduced the problem to working out the gcd of smaller integers. Let's write this out more formally.

First we write

$$a = q_1 b + r_1 \text{ with } 0 \leq r_1 < b.$$

If $r_1 = 0$ then $b|a$ and $\gcd(a, b) = b$. If $r_1 \neq 0$ we divide again and write:

$$b = q_2 r_1 + r_2 \text{ with } 0 \leq r_2 < r_1.$$

We have $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2)$. If $r_2 = 0$ then $\gcd(a, b) = r_1$. If $r_2 \neq 0$ we divide again:

$$r_1 = q_3 r_2 + r_3 \text{ with } 0 \leq r_3 < r_2$$

and we continue on in this way. Since $b > r_1 > r_2 > \cdots \geq 0$ we eventually get a remainder $r_n = 0$ (with $r_{n-1} > 0$). So $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_{n-1}, 0) = r_{n-1}$. Let's do an example:

Example. Let $a = 1492$ and $b = 1066$. We have

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

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

1.2. **Bezout's Lemma.** This algorithm gives us a practical way to work out the gcd of two integers. It also gives us an important theoretical result:

Theorem 1.5 (Bezout's lemma)**.** *Let a and b be integers (not both 0). Then there exist integers u and v such that*

$$\gcd(a, b) = au + bv$$

Proof. As before, we can reduce to the case that $a > b > 0$. The last two steps in the Euclidean algorithm to compute $\gcd(a, b)$ have

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$$

and

$$r_{n-2} = q_n r_{n-1} + 0$$

with $r_{n-1} = \gcd(a, b)$. So we have an equation

$$\gcd(a, b) = r_{n-3} - q_{n-1}r_{n-2}.$$

From the previous equation in the Euclidean algorithm, we get $r_{n-2} = r_{n-4} - q_{n-2}r_{n-3}$, so we can substitute this in to eliminate r_{n-2} and write $\gcd(a, b)$ as a linear combination of r_{n-3} and r_{n-4}. Repeating this process, we eventually write $\gcd(a, b)$ as a linear combination of a and b. □

Note that the above proof gives us a practical algorithm to compute integers u, v with $\gcd(a, b) = au + bv$:

Example. We again set $a = 1492$ and $b = 1066$. We have

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

Bezout's lemma is very useful for establishing theoretical properties of the greatest common divisor.

Another proof of Bezout's lemma. Here is a different proof.

Proposition 1.6. *Let a, b be integers, not both zero, and consider the set*

$$S = \{au + bv : u, v \in \mathbb{Z}\}.$$

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

Proof. We have $d = au + bv$. Dividing a by d we get

$$a = qd + r$$

with $0 \leq r < d$. Since $r = a - qd = a(1 - qu) - b(qv) \in S$ and d is the smallest positive element of S we must have $r = 0$. So $d|a$. By the same argument, we have $d|b$, so d is a common divisor of a and b. Since $\gcd(a, b)$ divides a and b, it divides $d = au + bv$. In particular, we have $\gcd(a, b) \leq d$. Since d is a common divisor of a and b we also have $d \leq \gcd(a, b)$ and we conclude that $d = \gcd(a, b)$. □

Remark. Here are two consequences of this Proposition:

(1) We have integers u, v such that $\gcd(a, b) = au + bv$ (in other words, the Proposition gives a new proof of Bezout's lemma)
(2) $\gcd(a, b) = 1$ if and only if there are integers u, v such that

$$1 = au + bv.$$

Corollary 1.7. *Let a, b be integers, not both zero, and again consider the set*

$$S = \{au + bv : u, v \in \mathbb{Z}\}.$$

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.

Proof. We let $S' = \{n \gcd(a, b) : n \in \mathbb{Z}\}$. We are going to show that $S \subset S'$ and $S' \subset S$ and deduce that $S = S'$. For the first inclusion, if $x = au + bv \in S$ then, since $\gcd(a, b)$ divides a and b, it divides $au + bv = x$. So x is a multiple of $\gcd(a, b)$ which means that $x \in S'$. This proves that $S \subset S'$.

Conversely, we now prove that $S' \subset S$. So let $y \in S'$. We have $y = n \gcd(a, b)$. By Bezout's lemma, we have $\gcd(a, b) = au + bv$ for some integers u, v. Multiplying by n we get $y = a(nu) + b(nv)$. So $y \in S$. This shows that $S' \subset S$, and we have completed the proof. □

Corollary 1.8. *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 $c | \gcd(a, b)$.*

Proof. If $c | \gcd(a, b)$ then $c|a$ and $c|b$, so c is a common divisor of a and b.

Conversely, suppose c is a common divisor of a and b. By Bezout's lemma we have integers u, v such that

$$\gcd(a, b) = au + bv.$$

Since $c|a$ and $c|b$ we $c|(au + bv) = \gcd(a, b)$. □

Coprimality.

Definition 1.9. We say that two integers a, b are *coprime* or *relatively prime* if

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

Lemma 1.10. *Suppose a, b are coprime.*

1. *If $a|c$ and $b|c$ then $(ab)|c$.*
2. *If $a|(bc)$ then $a|c$.*
3. *If a and c are also coprime, then a and bc are coprime.*

Proof. (1) We have $1 = au + bv$ for some integers u, v. We can also write $c = ae$ and $c = bf$, since $a|c$ and $b|c$. Multiplying the first equation by c we get

$$c = cau + cbv = (bf)au + (ae)bv = ab(fu + ev)$$

so $(ab)|c$.

(2) Again we have $c = cau + cbv$. Since $a|(bc)$ and $a|a$, we get that $a|a(cu) + (bc)v = c$.

(3) We have $1 = au + bv$ and $1 = ax + cy$. Multiplying the equations together gives

$$1 = (au + bv)(ax + cy) = a(uax + ucy + bvx) + bc(vy).$$

It follows from Proposition 1.6 that $\gcd(a, bc) = 1$.

□

1.3. LCM & Linear Diophantine Equations.

Definition 1.11. If a, b are integers, then a *common multiple* of a and b is an integer c such that $a|c$ and $b|c$. If a and b are both non-zero, the *least common multiple* of a and b is defined to be the smallest positive integer $\mathrm{lcm}(a, b)$ which is a common multiple of a and b.

Proposition 1.12. *Let a, b be non-zero integers. Then*

$$\gcd(a, b)\mathrm{lcm}(a, b) = |ab|.$$

Proof. Set $a' = \frac{a}{\gcd(a,b)}$ and $b' = \frac{b}{\gcd(a,b)}$. We want to show that $\frac{|ab|}{\gcd(a,b)} = \mathrm{lcm}(a, b)$. First we need to check that $\frac{|ab|}{\gcd(a,b)}$ is a (positive) common multiple of a and b. Since $\gcd(a, b)$ is a common divisor of a and b, this follows from the fact that

$$\frac{|ab|}{\gcd(a, b)} = |a|\frac{|b|}{\gcd(a, b)} = |b|\frac{|a|}{\gcd(a, b)}$$

Now we need to show that $\frac{|ab|}{\gcd(a,b)}$ is the *least* common multiple. Suppose c is an arbitrary positive common multiple of a and b. We have $a|c$ and $b|c$. Dividing by $\gcd(a, b)$, we get that a' and b' divide $\frac{c}{\gcd(a,b)}$. Since a' and b' are coprime (by Homework Sheet 1), Lemma 1.10 implies that $a'b'$ divides $\frac{c}{\gcd(a,b)}$. Multiplying by $\gcd(a, b)$, we deduce that $\frac{|ab|}{\gcd(a,b)} = \gcd(a, b)|a'b'|$ divides c, so in particular $c \geq \frac{|ab|}{\gcd(a,b)}$.

This shows that $\frac{|ab|}{\gcd(a,b)} = \mathrm{lcm}(a, b)$. □

Remark. We showed in the above proof that any common multiple of a and b is a multiple of $\mathrm{lcm}(a, b)$.

Diophantine equations are equations in one or more variables, for which we seek integer-valued solutions. Corollary 1.7 allows us to describe the solutions to the simplest family of Diophantine equations: *linear Diophantine equations* where we have integers a, b, c and look for integer solutions (x, y) to

$$ax + by = c.$$

Theorem 1.13. *Let a, b, c be integers, with a and b not both 0, and let $d = \gcd(a, b)$. The equation*

$$ax + by = c$$

has an integer solution (x, y) if and only if c is a multiple of d.

Now we assume c is a multiple of d. Fix integers u, v with $au + bv = d$. Then the solutions to

$$ax + by = c$$

are given by $(x_n, y_n)_{n\in\mathbb{Z}}$, where

$$x_n = \frac{c}{d}u + \frac{b}{d}n, \quad y_n = \frac{c}{d}v - \frac{a}{d}n$$

Proof. The first part of the theorem follows immediately from Corollary 1.7. For the second part, we can check by substituting in that the pairs (x_n, y_n) are solutions to the equation. It remains to check that these are *all* the solutions. Suppose that (x, y) is a solution. We can assume that $b \neq 0$ (otherwise we swap a and b). We have $ax+by = c$ and $ax_0+by_0 = c$, so subtracting one equation from the other gives

$$a(x - x_0) + b(y - y_0) = 0$$

Dividing by d and rearranging gives

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0).$$

Again we use the fact that $\frac{a}{d}$ and $\frac{b}{d}$ are coprime (Homework Sheet 1). Since $\frac{b}{d}$ divides $\frac{a}{d}(x - x_0)$ it follows from Lemma 1.10 that $\frac{b}{d}$ divides $x - x_0$. So we have $n \in \mathbb{Z}$ such that $x - x_0 = \frac{b}{d}n$. This shows that $x = x_n$ and we then have $y = \frac{c-ax_n}{b} = y_n$. □

Check your understanding.

(1) Why did we not define $\gcd(0, 0)$?
(2) Show that $\gcd(a, b) = \gcd(|a|, |b|)$
(3) For a a non-zero integer, show that $\gcd(a, 0) = |a|$.
(4) Prove the basic properties of divisibility:
   (a) If $a|b$ and $b|c$, then $a|c$.
   (b) If $a|b$ and $a|c$ then $a|(bx + cy)$ for all $x, y \in \mathbb{Z}$.
   (c) If $a|1$ then $a = \pm 1$.
   (d) If $a|b$ and $b|a$ then $a = \pm b$.
   (e) Suppose $c \neq 0$. Then $a|b$ if and only if $ac|bc$.
(5) Explain why the Euclidean algorithm will always terminate.
(6) Explain step-by-step how the Euclidean algorithm works. Can you write a computer program to implement the Euclidean algorithm?
(7) Explain how to use the Euclidean algorithm so it also outputs integers u, v with $\gcd(a, b) = au + bv$. Can you write a computer program to implement this algorithm?
(8) If d is not a mutliple of $\gcd(a, b)$ explain how you know that the equation

$$ax + by = d$$

will not have any solutions $x, y \in \mathbb{Z}$.

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 that 1 and p. An integer $n > 1$ is called *composite* if it is not prime.

Remark. By convention, the number 1 is neither prime nor composite, it is a *unit* i.e. a number with a multiplicative inverse.

Lemma 2.2. *Euclid's Lemma*

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

Proof. (1) If p does not divide a, then $\gcd(a, p) = 1$. So it follows from Lemma 1.10 that $p|b$.
(2) We repeatedly apply the first part. If p does not divide a_1 then $p|(a_2 a_3 \cdots a_n)$. If p does not divide a_2 either, then $p|(a_3 a_4 \cdots a_n)$. We see that p eventually has to divide one of the a_i.

□

Theorem 2.3 (Fundamental theorem of arithmetic)**.** *Every integer $n > 1$ can be expressed uniquely (up to reordering) as a product of primes.*

Proof. First we prove existence of a prime factorisation, by induction on n. Since 2 is prime, it has a prime factorisation. For the inductive step, we suppose that all integers less than n can be expressed as a product of primes. If n is prime, then it is its own prime factorisation and we are done. If n is not prime, then we have $n = md$ with $1 < m < n$ and $1 < d < n$. By our inductive hypothesis, both m and d have prime factorisations, so n does. Uniqueness follows from Lemma 2.2: suppose

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

are two prime factorisations. Since $p_1|n$ we have $p_1|q_i$ for some i. Up to reordering we can assume $p_1|q_1$, and since q_1 is prime we must have $p_1 = q_1$. Now we dividing through by p_1 we get

$$p_2 \cdots p_r = q_2 \cdots q_s$$

Repeatedly applying the same argument, we can show that $r = s$ and $p_i = q_i$ for all i's (after reordering the q_i). □

If $n > 1$ is an integer, we often write its prime factorisation as

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

with the p_i distinct primes and the a_i positive integers. Sometimes we will allow some of the a_i to be equal to 0 as well (in this case prime p_i is not a factor of n).

We can read off information about the divisibility properties of integers from their prime factorisations.

Lemma 2.4. *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.

(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 $\prod_{i=1}^{r}(a_i + 1)$.*

Proof. Exercise (see Homework sheet 2). □

Lemma 2.5. *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 are integers which are ≥ 0.

(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* $f_i = \max(a_i, b_i)$

Proof. Exercise (use the previous lemma to work out what the common divisors of m and n are, and use Proposition 1.12 to work out the lcm once you know the gcd). □

Theorem 2.6 (Euclid)**.** *There are infinitely many primes.*

Proof. We give a proof by contradiction. Suppose there are only finitely many primes, which we enumerate by $p_1, p_2, \ldots, p_n$. Define

$$N = p_1 p_2 \cdots p_n + 1$$

By the fundamental theorem of arithmetic, there is a prime p with $p|N$. Also, $p|p_1 p_2 \cdots p_n$ since $p = p_j$ for some $j = 1, \ldots, n$. But $1 = N - p_1 p_2 \cdots p_n$ so this implies that $p|1$ which is impossible. □

Modifying Euclid's argument it is possible to show that the sequence of integers of the form $4n - 1$, i.e. $\{3, 7, 11, 15, \ldots\}$, also contains infinitely many primes.

Proposition 2.7. *There are infinitely many primes of the form $4k - 1$, with k a positive integer.*

Proof. We give a proof by contradiction. Suppose that there are only finitely many primes of the form $4k - 1$ with k a positive integer, say $p_1, \ldots, p_n$. Consider the number

$$N = 4p_1 \cdots p_n - 1.$$

We know there exists a prime p such that $p|N$ by the fundamental theorem of arithmetic. Since N is odd $p \neq 2$. Also we cannot have that $p|p_1 \cdots p_n$ since this would imply p divides $N - 4p_1 \cdots p_n = 1$. As we have assumed $p_1, \ldots, p_n$ are all the primes of the form $4k-1$ all the prime factors of N must be of the form $4k+1$ for $k \in \mathbb{N}$. However, the product of numbers of the form $4k + 1$ are of the form $4m + 1$ [since, for example, $(4k + 1)(4l + 1) = 4m + 1$,

where $m = 4kl + k + l]$; so N is congruent of the form $4k+1$. This is a contradiction, since by construction N is of the form $4k - 1$.

□

In 1841 Dirichlet generalised this result to arbitrary linear sequences, and showed that given $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ the sequence $qk + a$ contains infinitely many primes provided that $\gcd(q, a) = 1$.

Theorem (Dirichlet (1841)). *Let $a \in \mathbb{Z}$ and $q \in \mathbb{N}$. Suppose $\gcd(a, q) = 1$. Then there are infinitely many primes of the form $qk + a$ with k a positive integer.*

The proof of this result is beyond the scope of the course and involves substantial new innovations, in particular *Dirichlet characters*, which have had an enormous impact in the development of number theory.

Detecting primes over values of quadratic polynomials (and polynomials of higher degree), is much harder and remains a challenging open problem!

Conjecture. *There are infinitely many primes of the form $n^2 + 1$.*

This conjecture has been generalised to higher degree polynomials and is known as the *Bateman-Horn Conjecture*. A breakthrough towards the quadratic case is due to Iwaniec (1978).

Theorem (Iwaniec (1978)). *The sequence $\{n^2 + 1\}_{n\in\mathbb{N}}$ contains infinitely many primes or infinitely many numbers with exactly two prime factors.*

2.2. **Congruences.**

Definition 2.8. 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 $m|(a - b)$.

If a is congruent to b modulo m, we write

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

Here are some basic 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) if $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$.
(5) if $a \equiv b \pmod{m}$ and $c \neq 0$, then $ac \equiv bc \pmod{mc}$.

Definition 2.9. Let m be a positive integer. A set $\{x_1, x_2, \ldots, x_r\}$ is called a *complete residue system modulo m* if for every integer y there is exactly one x_i such that

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

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

There are other possibilities too: for example, if $m = 5$ then $\{-2, -1, 0, 1, 2\}$ is a complete residue system modulo 5.

Definition 2.10. Let m be a non-zero integer and $a \in \mathbb{Z}$. The *residue class* or *congruence class* of a is the set

$$[a]_m = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\}$$

We might just write $[a]$ if we don't need to specify the modulus m.

Lemma 2.11.

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

Proof. This follows from the definitions, it's an exercise to write down the proof. □

If follows from the above Lemma that if $\{x_1, x_2, \ldots, x_m\}$ is a complete residue system modulo m then for every integer a there is a unique x_i such that $[a]_m = [x_i]_m$. The collection of all congruence classes modulo m is therefore a finite set of cardinality m.

Definition 2.12. For a positive integer m, we let $\mathbb{Z}_m$ denote the set of congruence classes modulo m.

Remark. We can write

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

In fact, if $\{x_1, x_2, \ldots, x_m\}$ is *any* complete residue system modulo m then we have

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

Now we are going to recall the fact that the congruence classes modulo m naturally form a *commutative ring*. In other words, we can add and multiply congruence classes.

Definition 2.13. For $m \neq 0$ and $a, b \in \mathbb{Z}$ we define addition and multiplication operations on $\mathbb{Z}_m$ by:

$$[a]_m + [b]_m = [a+b]_m$$

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

Using the properties of congruences, you can check that these binary operations are well-defined: in other words, if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then $[a]_m + [b]_m = [a']_m + [b']_m$ and $[a]_m \cdot [b]_m = [a']_m \cdot [b']_m$.

2.3. **Solving equations in $\mathbb{Z}_m$ and the Chinese Remainder Theorem.** We already saw the example of linear Diophantine equations. Suppose we want to find integer solutions x to a polynomial equation in one variable like

$$x^7 + 2x + 2 = 0.$$

This might be difficult in general, but in the next few lectures we will study the easier problem of solving these equations modulo m for positive integers m.

Problem. Given a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_i \in \mathbb{Z}$ and a positive integer m, find all integers $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \pmod{m}$.

Lemma 2.14. *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial with integer coefficients $a_i \in \mathbb{Z}$. If $a \equiv b \pmod{m}$ then $f(a) \equiv f(b) \pmod{m}$.*

Proof. Since $a \equiv b \pmod{m}$ we have $a^i \equiv b^i \pmod{m}$ for all $i \geq 0$. So $a_ia^i \equiv a_ib^i \pmod{m}$ for all $i \geq 0$. Adding together these congruences we get $f(a) \equiv f(b) \pmod{m}$. □

This lemma means that to find all the integers $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \pmod{m}$ we just need to check if $f(a) \equiv 0 \pmod{m}$ or not for one a in each congruence class. Moreover, we can view the set of solutions to the congruence equation $f(x) \equiv 0 \pmod{m}$ as a subset of $\mathbb{Z}_m$.

Another way of seeing this is that we can consider the *reduction modulo m* of $f(x)$:

$$[f]_m(x) = [a_0]_m + [a_1]_m x + \cdots + [a_n]_m x^n$$

this is a polynomial with coefficients in $\mathbb{Z}_m$. If $[a]_m \in \mathbb{Z}_m$ we can evaluate $[f]_m(x)$ at $[a]_m$ to and the *Problem* is to solve the equation

$$[f]_m(x) = [0]_m$$

in $\mathbb{Z}_m$. Again we see that the solutions to this equation are a subset of $\mathbb{Z}_m$.

Example. Let $f(x) = x^2 + 1$ and consider $m = 3$. Then there are *no* solutions to $f(x) \equiv 0 \pmod{3}$ (since none of $0^2 + 1$, $1^2 + 1$ and $2^2 + 1$ are divisible by 3)/

Consider $m = 5$. Then the solutions to $f(x) \equiv 0 \pmod{5}$ are given by $x \equiv \pm 2 \pmod{5}$.

Remark. If we replace $f(x)$ with a polynomial $g(x)$ whose coefficients are all congruent to those of f modulo m, then the solutions to $f(x) \equiv 0 \pmod{m}$ and $g(x) \equiv 0 \pmod{m}$ are exactly the same.

Here are some examples I didn't do in the lecture:

Example. Let $m = 5$ and $f(x) = x^2 + 2x + 2$. We check which elements in the complete residue system $\{-2, -1, 0, 1, 2\}$ satisfy $f(x) \equiv 0 \pmod{5}$:

$$\begin{aligned} f(-2) &= 2 \\ f(-1) &= 1 \\ f(0) &= 2 \\ f(1) &= 5 \equiv 0 \pmod{5} \\ f(2) &= 10 \equiv 0 \pmod{5} \end{aligned}$$

So the solutions to $f(x) \equiv 0 \pmod{5}$ are given by $x \equiv 1, 2 \pmod{5}$.

Example. Let $m = 4$ and $f(x) = x^5 - x^2 + x - 3$. We check which elements in the complete residue system $\{-1, 0, 1, 2\}$ satisfy $f(x) \equiv 0 \pmod{4}$:

$$\begin{aligned} f(-1) &= -6 \\ f(0) &= -3 \\ f(1) &= -2 \\ f(2) &= 27 \end{aligned}$$

So there are no solutions to $f(x) \equiv 0 \pmod 4$. As an immediate consequence, there are no integer solutions to $f(x) = 0$, as a solution to this equation would give a solution $\pmod 4$.

If m is very large this method would take a long time! We are going to develop some tools that will enable us to solve this problem more efficiently.

Theorem 2.15 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_r$ be positive integers, with $\gcd(m_i, m_j) = 1$ for all $i \neq j$. Let $a_1, \ldots, a_r$ 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 integers x lying in a single congruence class $\pmod{m_1 m_2 \cdots m_r}$.

Proof. We start by doing the case $r = 2$. By Bezout's lemma we have integers u, v such that $m_1 u + m_2 v = 1$. In particular, we have $m_1 u \equiv 1 \pmod{m_2}$ and $m_2 v \equiv 1 \pmod{m_1}$.

Suppose $x \equiv m_1 u a_2 + m_2 v a_1 \pmod{m_1 m_2}$. Then we have $x \equiv m_2 v a_1 \equiv a_1 \pmod{m_1}$ and $x \equiv m_1 u a_2 \equiv a_2 \pmod{m_2}$. This gives us some solutions, and now we check that *all* the solutions are given by $x \equiv m_1 u a_2 + m_2 v a_1 \pmod{m_1 m_2}$.

Suppose x' is another solution. Then $x - x' \equiv a_1 - a_1 \equiv 0 \pmod{m_1}$, and similarly $x - x' \equiv 0 \pmod{m_2}$. So $m_1 | (x - x')$ and $m_2 | (x - x')$. Since m_1 and m_2 are coprime this implies that $m_1 m_2$ divides $(x - x')$. We deduce that $x' \equiv x \pmod{m_1 m_2}$.

This finishes the case of $r = 2$. For the general case $r > 2$ we just repeatedly apply the case $r = 2$. Let's explain the case $r = 3$: we have three simultaneous equations and we begin by considering the first two:

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

The case $r = 2$ tells us that these two equations are equivalent to the equation $x \equiv a_{12} \pmod{m_1 m_2}$ where a_{12} is some integer (it's $m_1 u a_2 + m_2 v a_1$, using the notation from earlier). Now we just have two simultaneous equations to solve:

$$x \equiv a_{12} \pmod{m_1 m_2}$$
$$x \equiv a_3 \pmod{m_3}$$

and applying the case $r = 2$ again tells us that these are equivalent to $x \equiv a \pmod{m_1 m_2 m_3}$ for some integer a. □

Note that the above proof gives a procedure for finding the solutions x.

Check your understanding.

(1) Let $a \in N$ and $q \in \mathbb{N}$. Suppose $\gcd(a, q) > 1$. Explain why that there are no primes of the form $qn + a$, $(n > 0)$.
(2) Prove Lemma 2.5.
(3) Prove that if p is a prime of the form $3k + 1$ then it is also of the form $6k + 1$.
(4) Prove the properties (1)-(5) of modular arithmetic listed after Definition 2.8. Here is the first part of (3) to get you started: if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $m|(a-b)$ and $m|(c-d)$. We have $ac - bd = a(c-d) + d(a-b)$ so $m|(ac-bd)$.
(5) Given an example to show that $a^2 \equiv b^2 \pmod{m}$ need not imply that $a \equiv b \mod m$.
(6) Solve the following system of simultaneous congruences: $x \equiv 1 \pmod 3, x \equiv 2 \pmod 5, x \equiv 3 \pmod 7$.
(7) Find all the solutions to $x^2 - 1 \equiv 0 \pmod{35}$.

3. The Chinese Remainder Theorem and Hensel's Lemma

3.1. **The Chinese Remainder Theorem revisited.** Recall that $\mathbb{Z}_m$ is a ring. If we think a bit about the statement of the Chinese remainder theorem, it is not hard to deduce the following ring-theoretic formulation of this theorem:

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

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

given by

$$[a]_m \mapsto ([a]_{m_i})_{i=1,\dots,r}$$

is a bijection (in fact it is a ring isomorphism).

Example. Let's find all the solutions to

$$x^2 + 1 \equiv 0 \pmod{10}.$$

We begin by finding solutions to

$$x^2 + 1 \equiv 0 \pmod{m_i}$$

where $m_1 = 2, m_2 = 5$. The solutions are given by $x \equiv 1 \pmod 2$, $x \equiv -2, 2 \pmod 5$. Now we apply the proof of the CRT: the integers u, v in Bezout's lemma can be taken to be $u = -2, v = 1$ since $1 = 2(-2) + 5(1)$. Our solutions are given by $x \equiv m_1 u a_2 + m_2 v a_1 \pmod{m_1 m_2}$ where $m_1 = 2, m_2 = 5, a_1 = 1$ and $a_2 = \pm 2$.

So we get

$$x \equiv 2 \cdot (-2) \cdot (\pm 2) + 5 \cdot (1) \cdot (1) \equiv \mp 8 + 5 \equiv \pm 3 \pmod{10}$$

Subsituting back in you see that these do give solutions, since $(\pm 3)^2 + 1 = 10 \equiv 0 \pmod{10}$.

Now we move on to discussing inverses modulo an integer, which appeared implicitly in the proof of the Chinese Remainder Theorem (where we find u and v such that $m_1 u \equiv 1 \pmod{m_2}$ and $m_2 v \equiv 1 \pmod{m_1}$.)

Lemma 3.1. *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 a b an inverse of a modulo m*, and denote the residue class $[b]_m$ (which depends only on the residue class $[a]_m$) by $[a]_m^{-1}$.*

Proof. We know by Bezout's lemma that we have $au + mv = 1$ for some integers u, v. This says that $au \equiv 1 \pmod m$ so u is an inverse to a modulo m.

If $a' \equiv a \pmod m$ then $a'u \equiv au \equiv 1 \pmod m$ so u is also an inverse to $a' \pmod m$. Finally if b, b' are two inverses to a modulo m then $ab \equiv ab' \pmod m$ which implies that $m | a(b - b')$. Since m, a are coprime this implies that $m | b - b'$ and so $[b]_m = [b']_m$. This shows that the residue class $[b]_m$ depends only on $[a]_m$ (in particular, it is independent of the choice of b). □

Remark. We showed that if a, m are coprime then there is an inverse to a modulo m. In fact, if there exists b such that $ab \equiv 1 \pmod{m}$ then a must be coprime to m, since we know that there are integers u, v with $au + mv = 1$ *if and only if* a, m are coprime.

Definition 3.2. Given a commutative ring R with identity element 1_R we say that $a \in R$ is a *unit* provided there exists $b \in R$ such that $a \cdot b = 1_{\mathbb{R}}$.

Example. Consider the ring $R = \mathbb{Z}_p$. If p is a prime number, then the congruence classes $[1]_p, \ldots, [p-1]_p$ are units in $\mathbb{Z}_p$. The remaining congruence class $[0]_p$ does not have an inverse modulo p, so it is not a unit in $\mathbb{Z}_p$.

The set of units in a ring R form a group under multiplication. It follows from Lemma 3.1 that $\mathbb{Z}_m^\times$ with the multiplication operation is a (commutative) group, with identity element $[1]_m$. In particular, for every $g \in \mathbb{Z}_m^\times$ there is an inverse $g^{-1} \in \mathbb{Z}_m^\times$ with $g \cdot g^{-1} = g^{-1} \cdot g = [1]_m$.

Definition 3.3. 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

$$\mathbb{Z}_m^\times = \{[a]_m \in \mathbb{Z}_m : a, m \text{ are coprime}\}$$

We will now begin to investigate the structure of the group of units $\mathbb{Z}_m^\times$.

Proposition 3.4. *Suppose* $\gcd(m, n) = 1$. *The image of the map* $\mathbb{Z}_{mn}^\times \to \mathbb{Z}_m \times \mathbb{Z}_n$ *given by*

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

equals $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$. *Moreover, this gives a bijection between* $\mathbb{Z}_{mn}^\times$ *and* $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, *(in fact it is a group isomorphism).*

Proof. Recall that the CRT gives a bijection

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

where the maps is $[a]_{mn} \mapsto ([a]_m, [a]_n)$. We will show that this gives a bijection

$$\mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times.$$

In fact this bijection is an isomorphism of groups.

Here are two arguments the first of which appeals to general ring theory:

(1) Firstly, if I have an isomorphism $R \cong S$ of rings, then it induces an isomorphism $R^\times \cong S^\times$ of their multiplicative groups. Secondly, if I have a product $R \times S$ of rings, the multiplicative group of the product $(R \times S)^\times$ is isomorphic to the product of the multiplicative groups $R^\times \times S^\times$. This completes the proof.

(2) Here is a more direct argument:

More directly, we need to show that $\gcd(a, mn) = 1$ if and only if $\gcd(a, m) = \gcd(a, n) = 1$. A common divisor of a and m is a common divisor of a and mn, so if $\gcd(a, mn) = 1$ we must have $\gcd(a, m) = 1$; applying the same argument to n as well shows that if $\gcd(a, mn) = 1$ we have $\gcd(a, m) = \gcd(a, n) = 1$.

Conversely, suppose that $\gcd(a, m) = \gcd(a, n) = 1$. Then $\gcd(a, mn) = 1$ by Lemma 1.10. This completes the proof of the claim.

□

Here is some terminology which is sometimes used to describe the analogue of a complete residue system, but just representing congruence classes in $\mathbb{Z}_m^\times$.

Definition 3.5. 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

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

3.2. **Hensel's Lemma.** We go back to find roots of polynomials modulo m. Suppose we have a prime factorisation $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. The Chinese Remainder Theorem tells us that to solve an equation modulo m it suffices to solve the equation modulo $p_i^{a_i}$ for each i. A very powerful tool for finding roots of polynomials modulo a prime power (like $p_i^{a_i}$) is provided by Hensel's Lemma:

Theorem 3.6 (Hensel's Lemma)**.** *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ 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 $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. 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

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

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

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

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

Remark. The formula $x_{r+1} = x_r - f(x_r)u$ is similar to the formula $x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$ which appears in the Newton–Raphson method for finding zeroes of a function f.

Remark. If $f'(x_r) \equiv 0 \pmod{p}$ then Hensel's lemma doesn't tell us anything — we have to find roots of the polynomial another way.

We will prove Hensel's Lemma using the following key result:

Lemma 3.7. *For $t \in \mathbb{Z}$ and a positive integer r, we have*

$$f(x + p^r t) \equiv f(x) + f'(x) p^r t \pmod{p^{r+1}}$$

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

Proof. It suffices to prove the Lemma for $f(x) = x^n$ (multiply by the coefficients a_i and add together to get the general case). We have

$$(x + p^r t)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} (p^r t)^i$$

For $i \geq 2$, $(p^r t)^i \equiv 0 \pmod{p^{r+1}}$, so we have

$$(x + p^r t)^n \equiv \sum_{i=0}^{1} \binom{n}{i} x^{n-i} (p^r t)^i = x^n + n x^{n-1} (p^r t) \pmod{p^{r+1}}$$

□

Proof of Hensel's Lemma. We are looking for a solution to $f(x) \equiv 0 \pmod{p^{r+1}}$ of the form $x = x_r + p^r t$. Applying the previous lemma, we see that we get a solution if and only if

$$f(x_r) + f'(x_r) p^r t \equiv 0 \pmod{p^{r+1}}$$

This equation is equivalent to

$$p^r t \equiv -f(x_r) u \pmod{p^{r+1}}$$

where u is an inverse to $f'(x_r)$ modulo p. The solutions to this equation are given by $t \equiv -\frac{f(x_r)}{p^r} u \pmod{p}$. Note that we are using the assumption that $f(x_r) \equiv 0 \pmod{p^r}$ to see that $\frac{f(x_r)}{p^r}$ is an integer.

We deduce that all solutions to $f(x) \equiv 0 \pmod{p^{r+1}}$ with $x \equiv x_r \pmod{p^r}$ are given by $x \equiv x_r - f(x_r) u \pmod{p^{r+1}}$. □

Example. Let's consider the equation

$$f(x) = x^2 + 1 \equiv 0 \pmod{65^e}$$

We are going to show that for each $e \geq 1$ this equation has exactly 4 solutions in $\mathbb{Z}_{65^e}$.

It suffices to show that there are two solutions x_1, x_2 modulo 5^e and two solutions y_1, y_2 modulo 13^e for each e (then we apply the Chinese Remainder theorem to get four solutions, for example one congruent to $x_1 \pmod{5^e}$ and one congruent to $y_2 \pmod{13^e}$).

First we consider the equation mod 5: there are two solutions $x \equiv -2, 2 \pmod{5}$. Now $f'(x) = 2x$, so $f'(-2)$ and $f'(2)$ are both non-zero mod 5. It follows that we can apply Hensel's Lemma to show that there are exactly two solutions mod 5^2, one congruent to 2 (mod 5), the other to -2. Repeatedly applying Hensel's Lemma we get exactly two solutions mod 5^e for each $e \geq 1$. The same argument works mod 13 (the two solutions mod 13 are $x \equiv \pm 5$). So we conclude there are also exactly two solutions mod 13^e.

The conclusion of this section is that, using the CRT and Hensel's Lemma, we can, in good situations (when the conditions of Hensel's Lemma are met) reduce solving congruence equations modulo m to the problem of solving congruence equations modulo p, for prime factors p of m. The next theorem gives some control on the number of possible solutions.

Theorem 3.8. *Let p be a prime, and let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial of 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 $\mathbb{Z}_p$.

Proof. (Non-examinable) The proof is by induction on n. If $n = 0$, and $a_0 \not\equiv 0 \pmod{p}$ then there are no solutions to $a_0 = f(x) \equiv 0 \pmod{p}$, as required. Now we do the inductive step. So we assume that $n \geq 1$ and that all polynomials $g(x)$ of degree $\leq n-1$ with some coefficient not divisible by p have at most $n-1$ solutions.

If $f(x) \equiv 0$ has no solutions, then there is nothing left to prove, so suppose $[a]_p$ is a solution. So $p|f(a)$. We have

$$f(x) - f(a) = \sum_{i=1}^{n} a_i(x^i - a^i)$$

and for each i we have

$$x^i - a^i = (x-a)(x^{i-1} + ax^{i-2} + \cdots + a^{i-2}x + a^{i-1})$$

Taking out the common factor of $(x-a)$ we can write

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

where $g(x)$ is a polynomial with integer coefficients of degree $\leq n-1$. If p divided all the coefficients of $g(x)$ it would divide all the coefficients of $f(x) - f(a)$. Since $p|f(a)$ this implies that p divides all the coefficients of $f(x)$, which is a contradiction. So there is a coefficient of $g(x)$ which is not divisible by p and by our inductive hypothesis we conclude that the equation $g(x) \equiv 0$ has at most $n-1$ roots in $\mathbb{Z}_p$. Now suppose we have $f(b) \equiv 0 \pmod{p}$. Then we have $(b-a)g(b) \equiv 0 \pmod{p}$. If $p|(b-a)g(b)$ then either $p|(b-a)$ or $p|g(b)$. So there are at most n possibilities for $b \pmod{p}$ — either $b \equiv a \pmod{p}$ or the congruence class of b is one of the roots of $g(b)$ in $\mathbb{Z}_p$. □

In fact the above Theorem is a special case of a general fact about roots of polynomials with coefficients in a field. Note that the statement of the Theorem doesn't hold without the assumption that p is prime: for example, let's consider the equation

$$x^2 \equiv 1 \pmod{8}$$

You can check that the solutions are given by $x \equiv 1, 3, 5, 7 \pmod{8}$ so there are > 2 solutions in $\mathbb{Z}_8$.

Check your understanding.

(1) Find all solutions to $x^2 + 4 \equiv 0 \mod 10$.
(2) Find an integer b such that $[52]_{71}^{-1} = [b]_{71}$.
(3) What are the units in $\mathbb{Z}$? Consider the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. (*Hint: It suffices to find $a, b \in \mathbb{Z}$ such that $(1+\sqrt{2})(a+b\sqrt{2}) = -1$.*)

(4) Given a solution x_r to $f(x) \equiv 0 \pmod{p^r}$ Hensel's Lemma provides a formula for a solution to $f(x) \equiv 0 \pmod{p^{r+1}}$ provided that $f'(x_r) \not\equiv 0 \pmod{p}$. Suppose $f'(x_r) \equiv 0 \pmod{p}$ and $f(x_r) \not\equiv 0 \pmod{p^{r+1}}$. How many solutions are there to $f(x) \equiv 0 \mod p^{r+1}$ with $x \equiv x_r \mod p^r$? (*Hint: Use Lemma 3.7).*)
(5) Find all solutions to $x^2 + 2 \equiv 0 \pmod{27}$. How do you know you have found all solutions?
(6) Find all solutions to $x^3 + 2 \equiv 0 \pmod{27}$.

4. Euler's ϕ-function, The Fermat-Euler theorem, and Primitive Roots

In this week we will explore the structure of the multiplicative group of units $\mathbb{Z}_m^\times$. In particular we will determine the order of $\mathbb{Z}_m^\times$ as well as gain insight into the case where $m = p$ is prime.

4.1. Euler's ϕ function.

Definition 4.1. Let m be a positive integer. We define $\phi(m)$ to be the number of integers a such that $1 \leq a \leq m$ and $\gcd(a, m) = 1$. Equivalently $\phi(m) = |\mathbb{Z}_m^\times|$, the cardinality of the multiplicative group $\mathbb{Z}_m^\times$.

Example. If p is prime then $\phi(p) = p - 1$.

Lemma 4.2. *Let p be prime and i a positive integer. Then*

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

Proof. An integer a with $1 \leq a \leq p^i$ is coprime to p^i if and only if a is not divisible by p. So the number of such integers is equal to p^i minus the number of multiples of p in $\{1, \ldots, p^i\}$. There are p^{i-1} multiples of p in this range, namely $\{p, 2p, \ldots, p^{i-1}p\}$, so we get $\phi(p^i) = p^i - p^{i-1} = p^{i-1}(p-1)$. □

Lemma 4.3. *Let m, n be coprime positive integers. Then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. This follows immediately from Proposition 3.4. Here is another proof, which is from a less group theoretic viewpoint.

We want to count integers $1 \leq a \leq mn$ with $\gcd(a, mn) = 1$. First we note that a is coprime to mn if and only if it is coprime to m and n (see the previous paragraph for a proof of this). So we need to count integers $1 \leq a \leq mn$ with $\gcd(a, m) = \gcd(a, n) = 1$. Since m, n are coprime the Chinese Remainder Theorem says that for each pair of integers $1 \leq a_1 \leq m$, $1 \leq a_2 \leq n$ there is an integer a, unique modulo mn with $a \equiv a_1 \pmod{m}$ and $a \equiv a_2 \pmod{n}$. Since the integers between 1 and mn are a complete residue system mod mn this says that there is a unique integer a with $1 \leq a \leq mn$ with $a \equiv a_1 \pmod{m}$ and $a \equiv a_2 \pmod{n}$. As we let a_1 run over the $\phi(m)$ possibilities which are coprime to m and a_2 run over the $\phi(n)$ possibilities which are coprime to mn, we get $\phi(m)\phi(n)$ integers a with $1 \leq a \leq mn$ and a coprime to mn, and we get all such integers this way. So $\phi(mn) = \phi(m)\phi(n)$.

□

This Lemma says that ϕ is a *multiplicative function*. If m and n are not coprime, we usually don't have $\phi(mn) = \phi(m)\phi(n)$. For example $\phi(4) = 2 \neq \phi(2)\phi(2) = 1$.

Example. $\phi(1000) = \phi(2^3 5^3) = \phi(2^3)\phi(5^3) = 4 \cdot 25 \cdot 4 = 400$

4.2. **The Fermat-Euler theorem.** First we will establish the following result concerning Euler's ϕ function which we will use later.

Proposition 4.4. *Let m be a positive integer. Then*

$$\sum_{0<d|m} \phi(d) = m.$$

Proof. For each positive divisor d of m we let $S_d = \{1 \leq a \leq d : \gcd(a,d) = 1\}$. We have $|S_d| = \phi(d)$. For every integer a with $1 \leq a \leq m$ we have a positive divisor $\frac{m}{\gcd(a,m)}$ of m and an element $\frac{a}{\gcd(a,m)}$ of $S_{\frac{m}{\gcd(a,m)}}$. Conversely, for $a \in S_d$ we get an integer $a\frac{m}{d}$ with $1 \leq a\frac{m}{d} \leq m$, and $\gcd(a\frac{m}{d}, m) = \frac{m}{d}$. This shows that we have a bijection

$$\{1, 2, \ldots, m\} \leftrightarrow \{\text{pairs } (d,a) : 0 < d|m \text{ and } a \in S_d\}$$

The cardinality of the left hand side is m, whilst the cardinality of the right hand side is $\sum_{0<d|m} \phi(d)$. □

Theorem 4.5 (The Fermat–Euler Theorem)**.** *Let $a \in \mathbb{Z}$ and let m be a positive integer. Suppose* $\gcd(a,m) = 1$. *Then*

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

Proof. Since $\mathbb{Z}_m^\times$ is a group of order $\phi(m)$, and $[a]_m \in \mathbb{Z}_m^\times$, it is an immediate consequence of Lagrange's theorem in group theory that $[a]_m^{\phi(m)} = [1]_m$, because the order of the cyclic group generated by $[a]_m$ is a divisor of $\phi(m)$. In other words,

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

Here is an alternative proof, without using group theory: let $x_1, x_2, \ldots, x_{\phi(m)}$ be the list of integers between 1 and m which are coprime to m. You can check that the integers $ax_1, ax_2, \ldots, ax_{\phi(m)}$ are all distinct modulo m and coprime to m, so this gives another list (possibly reordered) of integers whose congruence classes give all the units in $\mathbb{Z}_m$. In other words we have

$$\mathbb{Z}_m^\times = \{[x_1]_m, [x_2]_m, \ldots, [x_{\phi(m)}]_m\} = \{[ax_1]_m, [ax_2]_m, \ldots, [ax_{\phi(m)}]_m\}$$

Taking the product of all the elements in each list, we get

$$[x_1]_m[x_2]_m \cdots [x_{\phi(m)}]_m = [ax_1]_m[ax_2]_m \cdots [ax_{\phi(m)}]_m = [a^{\phi(m)}]_m[x_1]_m[x_2]_m \cdots [x_{\phi(m)}]_m.$$

Dividing through by the unit $[x_1]_m[x_2]_m \cdots [x_{\phi(m)}]_m$ gives $[a^{\phi(m)}]_m = 1$. □

Corollary 4.6 (Fermat's Little Theorem)**.** *Let p be a prime and let $a \in \mathbb{Z}$ be an integer which is coprime to p. Then*

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

If a is an arbitrary integer, we have $a^p \equiv a \pmod{p}$.

Proof. The first part is a special case of the Fermat–Euler Theorem. The second part follows from the first, unless $p|a$, in which case $a^p \equiv a \equiv 0 \pmod{p}$, so the statement also holds in this case. □

4.3. **Primitive roots.**

Definition 4.7. Let m be a positive integer and let $[a] \in \mathbb{Z}_m^\times$. The *order* of $[a]$ (also called the order of a modulo m) is defined to be the smallest positive integer i such that $[a]^i = [1]$. In other words, it is the order of the cyclic subgroup of $\mathbb{Z}_m^\times$ generated by $[a]$.

As noted in the proof of the Fermat–Euler Theorem, the order of $[a]$ is a divisor of $\phi(m)$.

This section is about trying to understand the structure of $\mathbb{Z}_m^\times$ as a group. We will briefly recall some basic facts from group theory.

Let G be a finite group, with group multiplication $\cdot$ and identity e. The order of G is the number of elements of G. If $g \in G$ then the order of g, denoted $o(g)$ is the smallest positive integer i such that $g^i = e$. The order $o(g)$ is also the order of the cyclic group

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{o(g)-1}\}$$

generated by g.

If i is an integer, we have $g^i = e \iff o(g)|i$.

Problem. For which positive integers m is $\mathbb{Z}_m^\times$ a cyclic group?

In other words, for which m is there an integer a (coprime to m) such that the order of a modulo m is $\phi(m)$. If such an a exists, then $\mathbb{Z}_m^\times$ is cyclic, generated by $[a]_m$, and we say that a is a *primitive root modulo* m.

Definition 4.8. Let m be a positive integer. If a is an integer co-prime to m, such that the order of a modulo m is $\phi(m)$, we say that a is a *primitive root* mod m.

If a is a primitive root modulo m, then $\mathbb{Z}_m^\times$ is a cyclic group generated by $[a]_m$. If $\mathbb{Z}_m^\times$ is cyclic and $g \in \mathbb{Z}_m^\times$ is a generator, we will also refer to (the congruence class) g as a primitive root.

Lemma 4.9 (The Primitive Root Test)**.** *Let m be a positive integer, and let a be coprime to m. Then a is a primitive root modulo m if and only if*

$$a^{\phi(m)/p} \not\equiv 1 \pmod{m}$$

for all prime divisors p of $\phi(m)$.

Proof. The order of a modulo m is a divisor of $\phi(m)$. There are two possibilities: either the order is equal to $\phi(m)$, or the order is less than $\phi(m)$, in which case it divides $\phi(m)/p$ for some prime factor p of $\phi(m)$. Exercise to finish from here. □

Example. Let $m = 5$. Then $\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$ and $o([2]) = 4 = \phi(5)$, by the previous Lemma since $[2]^2 \neq [1]$. So $\mathbb{Z}_5^\times$ is cyclic.

Example. Let $m = 8$. Then $\mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$. You can check that $o([3]) = o([5]) = o([7]) = 2$, so no element has order $4 = \phi(8)$ and the group is not cyclic.

Lemma 4.10. *Let p be a prime number. For each $d|p-1$ 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 $d|p-1$.

Proof. If W_d is empty then we obviously have $0 = w_d \leq \phi(d)$. So suppose W_d contains an element $[a]$. The powers $a, a^2, \ldots, a^d$ are all distinct modulo p, since a has order d modulo p, they are all roots of the polynomial $f(x) = x^d - 1$ in $\mathbb{Z}_p$. It follows from Theorem 3.8. that these are *all* the roots of this polynomial, since it has at most d. Now let $[b]$ be any element of W_d. Since $[b]$ is a root of $x^d - 1$ we have $[b] = [a^i]$ for some $i = 1, 2, \ldots, d$. Since $o([b]) = d$, we must have $\gcd(i, d) = 1$, as we have $[b]^{d/\gcd(d,i)} = ([a]^d)^{i/\gcd(d,i)} = [1]$ (see Exercise 4 on Homework 4), so we must have $d/\gcd(d, i) = d$. It follows that there are at most $\phi(d)$ possibilities for $[b]$ — it is equal to $[a^i]$ for one of the $\phi(d)$ integers i with $1 \leq i \leq d$ and $\gcd(a, d) = 1$. So we have shown that $w_d \leq \phi(d)$, which completes the proof. □

Theorem 4.11. *Let p be a prime number. Then $\mathbb{Z}_p^\times$ has $\phi(d)$ elements of order d, for each $0 < d|(p-1)$. In particular, $\mathbb{Z}_p^\times$ is cyclic, as there are $\phi(p-1)$ elements of order $p-1$ (which are the primitive roots).*

Proof. Let $d|(p-1)$ be a positive divisor of $p-1$. We define $W_d = \{[a] \in \mathbb{Z}_p^\times : [a] \text{ has order } d\}$ and let $w_d = |W_d|$. We want to show that $w_d = \phi(d)$ for each d. We know that every element of $\mathbb{Z}_p^\times$ is an element of W_d for exactly one d (the order of the element, which is necessarily a divisor of $p-1$). So we have

$$\sum_{0<d|p-1} w_d = p - 1.$$

We also have (Proposition 4.4)

$$\sum_{0<d|p-1} \phi(d) = p - 1$$

so

$$\sum_{0<d|p-1} (\phi(d) - w_d) = 0.$$

By Lemma 4.10 we know $w_d \leq \phi(d)$ for all $d|p-1$. This means that the above sum is a sum of non-negative integers with value 0, so all the summands must be 0, and we are done. □

Example. We know that for every prime p there is a primitive root modulo p, but how can we actually find one? For example, let's find a primitive root modulo 19. First we try 2, by the primitive root test (Lemma 4.9) need to compute $[2]^{\phi(19)/p}$ for each $p|\phi(19)$ since $\phi(19) = 18$ we only need to check $p = 2, 3$. Since $[2]^{18/3} = [8]$ and $[2]^{18/3} = [18]$, it follows that 2 is a primitive root.

Check your understanding.

(1) Compute $\phi(100)$, $\phi(1001)$, and $\phi(36000)$.
(2) Use Lemmas 4.2 and 4.3 to show that for any integer $n > 1$

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the $\prod_{p|n}$ denotes a product ranging over prime divisor of n. E.g.

$$\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40.$$

(3) Prove each of the following:
   (a) If n is an odd integer then $\phi(2n) = \phi(n)$
   (b) If n is even then $\phi(2n) = 2\phi(n)$.
   (c) $\phi(n) = n/2$ if and only if $n = 2^k$ for some $k \geq 1$.
(4) Use Fermat's little theorem to verify that 17 divides $11^{104} + 1$.
(5) Find the last two digit of 7^{2003} using the Fermat-Euler Theorem.
(6) Show that there is no primitive root modulo 15.
(7) Determine all primitive roots modulo 11.
(8) Find an integer n with $n^5 \equiv 1 \pmod{11}$ and $n^4 \not\equiv 1 \pmod{11}$. Show that the integer you have found has the required properties.

5. Applications of primitive roots, primitive roots to prime powers and Quadratic residues

5.1. **Applications of primitive roots.** In the last section we proved that there exists a primitive root for any prime number. In this section we will explore some consequences of this. First let us prove the following lemma which will be quite useful.

Lemma 5.1. *Let G be a finite group with identity element e. Then for $g \in \mathbb{G}$ we have that $g^n = e$ if and only if $o(g)$ divides n.*

Remark. In practice we will use this lemma with $G = \mathbb{Z}_m^\times$, in which case the lemma states for an integer a with $\gcd(a, m) = 1$ that

$$[a]_m^n = [1]$$

if and only if the order of a modulo m divides n.

Proof. If $o(g)|n$ then clearly $g^n = e$. If $g^n = e$ we can write $n = q \cdot o(g) + r$ where $0 \leq r < o(g)$ and $q \in \mathbb{Z}$. Hence, $g^n = (g^{o(g)})^q g^r = e$ so that $g^r = e$. Since $0 \leq r < o(g)$ we must have $r = 0$. Therefore $o(g)|n$. □

Example.

(1) We check that 2 is a primitive root modulo 11: Since $\phi(11) = 10$, we just need to check that 2^5 and 2^2 are not 1 mod 11, which is easy.

(2) We find all solutions to

$$7x^3 \equiv 3 \pmod{11}$$

We have $[7]_{11}^{-1} = [-3]_{11}$ so we have to solve

$$x^3 \equiv -3 \cdot 3 \equiv 2 \pmod{11}$$

Since 2 is a primitive root mod 11, we have

$$\mathbb{Z}_{11}^\times = \{[2]_{11}^i : i = 0, 1, \ldots, 10\}$$

so to solve the equation we need to find the i such that $([2]_{11}^i)^3 = [2]_{11}^{3i} = [2]_{11}$. This is equivalent to

$$3i \equiv 1 \pmod{10}.$$

We have $[3]_{10}^{-1} = 7$, so we get

$$i \equiv 7 \pmod{10}.$$

So finally, the solution is given by $[x]_{11} = [2]_{11}^7$, or equivalently

$$x \equiv 2^7 = 128 \equiv 7 \pmod{11}$$

(3) We find all positive integers y such that

$$4^y \equiv 5 \pmod{11}$$

Since $5 \equiv 2^4 \pmod{11}$ we have to solve $2^{2y} \equiv 2^4 \pmod{11}$. Equivalently, we have $2y \equiv 4 \pmod{10}$. This is equivalent to $y \equiv 2 \pmod{5}$.

(4) Here's an additional example where we will find there are no solutions: consider the equation

$$x^8 \equiv 10 \pmod{11}$$

We have $10 \equiv -1 \equiv 2^5 \pmod{11}$. So we need to find i such that $([2]_{11}^i)^8 = [2]_{11}^{8i} = [2]_{11}^5$. This is equivalent to

$$8i \equiv 5 \pmod{10}.$$

This equation has no solutions, since $\gcd(8, 10) = 2 \nmid 5$. So there are no solutions to the original equation (see the Appendix).

5.2. **Primitive roots of prime powers.** Now we are going to study the case of prime powers $m = p^i$.

Proposition 5.2. *Let p be a prime number. Suppose a is a primitive root modulo p. Then a or $a + p$ is a primitive root modulo p^2.*

Proof. We have $\phi(p^2) = p(p-1)$. Since $o([a]_p) = o([a+p]_p) = p-1$ we know that $o([a]_{p^2})$ and $o([a+p]_{p^2})$ are divisors of $p(p-1)$ which are divisible by $p-1$ (see the below remark for more on this). So these orders are equal to either $p-1$ or $p(p-1)$. If $o([a]_{p^2}) = p(p-1)$ then a is a primitive root modulo p^2 and we are done. So suppose $o([a]_{p^2}) = p-1$. Then

$$(a+p)^{p-1} \equiv a^{p-1} + p(p-1)a^{p-2} \equiv 1 - pa^{p-2} \pmod{p^2}$$

(the first congruence is by Lemma 3.7, or directly by considering the binomial expansion) which is not congruent to 1, so we must have $o([a+p]_{p^2}) = p(p-1)$ and $a+p$ is a primitive root modulo p^2. □

Remark. A bit more explanation of one of the steps in the above proof: we claimed that $o([a]_{p^2})$ and $o([a+p]_{p^2})$ are divisors of $p(p-1)$ which are divisible by $p-1$. The fact that these orders divide $p(p-1)$ is because of Lagrange's theorem: the order of an element divides the order of $\mathbb{Z}_{p^2}^\times$ which is $\phi(p^2) = p(p-1)$. The fact that the orders are divisible by $p-1$ is because of the following (the same argument works for a and $a+p$): by definition we have $a^{o([a]_{p^2})} \equiv 1 \pmod{p^2}$. If an integer is divisible by p^2 it is divisible by p, so we get $a^{o([a]_{p^2})} \equiv 1 \pmod{p}$. But now we use Lemma 5.1: if $g^i = e$ then $o(g)$ divides i. In this case this means that $o([a]_p)$ divides $o([a]_{p^2})$. Since a is a primitive root modulo p, we get that $p-1$ divides $o([a]_{p^2})$.

The Proposition immediately implies that $\mathbb{Z}_{p^2}^\times$ is cyclic, and gives a procedure to find a primitive root if we already know a primitive root mod p.

Proposition 5.3. *Let p be an odd prime and suppose a is a primitive root modulo p^2. Then a is a primitive root modulo p^i for all $i \geq 2$.*

Proof. The proof is by induction. Let $i \geq 2$ and suppose a is a primitive root modulo p^i. We want to show that a is a primitive root modulo p^{i+1}. By the same proof as described in the above remark, we know that $o([a]_{p^{i+1}})$ is divisible by $o([a]_{p^i}) = p^{i-1}(p-1)$, so it suffices to show that

$$a^{p^{i-1}(p-1)} \not\equiv 1 \pmod{p^{i+1}}.$$

We have $a^{p^{i-1}(p-1)} = (a^{p^{i-2}(p-1)})^p$. Since a is a primitive root modulo p^i we know that

$$a^{p^{i-2}(p-1)} \equiv 1 \pmod{p^{i-1}}$$

but

$$a^{p^{i-2}(p-1)} \not\equiv 1 \pmod{p^i}$$

So there is an integer x such that $a^{p^{i-2}(p-1)} = 1 + p^{i-1}x$ and p does not divide x.

Now we have

$$a^{p^{i-1}(p-1)} = (a^{p^{i-2}(p-1)})^p = (1 + p^{i-1}x)^p \equiv 1 + p^i x + \binom{p}{2} p^{2i-2}x^2 \pmod{p^{i+1}}$$

and since p is an odd prime we have $p|\binom{p}{2}$, so $p^{i+1}|\binom{p}{2}p^{2i-2}$ (here we use $i \geq 2$). So we get

$$a^{p^{i-1}(p-1)} \equiv 1 + p^i x \not\equiv 1 \pmod{p^{i+1}}$$

since p does not divide x. This completes the proof. □

We already say that $\mathbb{Z}_8^\times$ is not cyclic, so we cannot expect this Proposition to work for $p = 2$.

Fact 5.4. Let m be a positive integer. Then $\mathbb{Z}_m^\times$ is cyclic if and only if $m = 1, 2, 4, p^i$ or $2p^i$ for some odd prime p and positive integer i.

Here is a useful additional Proposition, generalising Theorem 4.11:

Proposition 5.5. *Suppose $m > 0$ is a positive integer, and suppose that $\mathbb{Z}_m^\times$ has a primitive root. (For example, we could have $m = p^n$ with p an odd prime). Then the number of primitive roots in $\mathbb{Z}_m^\times$ is $\phi(\phi(m))$.*

Proof. Let g be a primitive root modulo m. Then the elements of $\mathbb{Z}_m^\times$ are $\{[g]^i : 1 \leq i \leq \phi(m)\}$. We claim that $[g]^i$ is a primitive root if and only if i is coprime to $\phi(m)$. In particular there are $\phi(\phi(m))$ primitive roots. The claim follows from Exercise 4 on Homework 4. □

5.3. **Quadratic residues.**

Problem. Given a prime p and an integer a, decide whether

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

has a solution or not.

If $a \equiv 0 \pmod{p}$ then the equation is solved by $x \equiv 0 \pmod{p}$. If $p = 2$, then the only other possibility is $a \equiv 1 \pmod{2}$, in which case the equation is solved by $x \equiv 1 \pmod{2}$. So from now on we assume that p is odd and a is coprime to p.

Definition 5.6. Let p be an odd prime and a an integer coprime to p. We say that a is a *quadratic residue modulo p* if the equation

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

has a solution, and we say that a is a *quadratic non-residue modulo p* otherwise.

Note that whether a is a quadratic residue or not depends only on the congruence class $[a]_p$. So it makes sense to ask if a congruence class $[a] \in \mathbb{Z}_p^\times$ is a quadratic residue or not.

Example. The quadratic residues modulo 11 are the congruence classes of $1, 3, 4, 5, 9$.

Proposition 5.7. *Let $g \in \mathbb{Z}$ be a primitive root modulo p. Then $[g^i]_p$ is a quadratic residue if and only if i is even.*

Proof. If $i = 2k$ is even, then $(g^k)^2 \equiv g^i \pmod{p}$, so $[g^i]$ is a quadratic residue.

Conversely, if $x^2 \equiv g^i \pmod{p}$ then we have $[x] = [g^k]$ for some integer k, so we have $g^{2k} \equiv g^i \pmod{p}$. Equivalently, we have $2k \equiv i \pmod{p-1}$. Since $2k$ and $p-1$ are even, i must also be even. □

Corollary 5.8. *There are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues in $\mathbb{Z}_p^\times$.*

Proof. Let g be a primitive root modulo p. We have $\mathbb{Z}_p^\times = \{[1], [g], \ldots, [g^{p-2}]\}$. By the previous Proposition, the quadratic residues are $\{[1], [g^2], [g^4], \ldots [g^{p-3}]\}$ and the quadratic non-residues are $\{[g], [g^3], \ldots, [g^{p-2}]\}$. □

Theorem 5.9. *-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 $x = g^{(p-1)/2}$. 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 $(p-1)/2$ is even, which gives the statement of the Theorem. □

Appendix: Solving linear congruences.

Proposition 5.10. *Let $a, b \in \mathbb{Z}$ and let m be a positive integer. Set $d = \gcd(a, m)$. The congruence equation*

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

has an integer solution for x if and only if $d|b$.

If $d|b$, the solutions are given by integers x such that

$$[x]_{\frac{m}{d}} = \left[\frac{a}{d}\right]_{\frac{m}{d}}^{-1} \left[\frac{b}{d}\right]_{\frac{m}{d}}$$

Proof. If $ax \equiv b \pmod{m}$ then $b = ax + km$ for some integer k. So $\gcd(a, m)$ (which divides a and m) must divide b. Conversely, if $d|b$ then

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

if and only if $ax \equiv b \pmod{m}$. Multiplying by an inverse of $\frac{a}{d}$ modulo $\frac{m}{d}$ (which exists since $\frac{a}{d}$ and $\frac{m}{d}$ are coprime) we get that

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

if and only if

$$[x]_{\frac{m}{d}} = \left[\frac{a}{d}\right]_{\frac{m}{d}}^{-1} \left[\frac{b}{d}\right]_{\frac{m}{d}}$$

□

Check your understanding.

(1) Find the two solutions to $x^4 \equiv 4 \pmod{11}$ in $\mathbb{Z}_{11}$.
(2) Explain why $x^5 \equiv 4 \pmod{11}$ has no solutions in $\mathbb{Z}_{11}$.
(3) Find all integer solutions y to $8^y \equiv 7 \pmod{11}$.
(4) Find the two primitive roots $\pmod{3^2}$. Explain how to find all the primitive roots $\pmod{3^3}$ (there are 6 of them in total).
(5) Determine the total number of primitive roots in $\mathbb{Z}_{11^2}$.
(6) Verify that the quadratic residues $\pmod{17}$ are $1, 2, 4, 8, 9, 13, 15, 16$.
(7) Suppose a is a quadratic residue $\pmod{p}$. Explain why a is not a primitive root $\pmod{p}$.

6. Euler's Criterion, the Legendre Symbol, the Law of Quadratic Reciprocity

In this section we further explore quadratic residues and in particular we will be able to quickly determine whether a given integer is a quadratic residue $\pmod p$.

6.1. **The Legendre Symbol.** First we begin with the following result on primes congruent to 1 (mod 4).

Corollary 6.1. *There are infinitely many primes p with $p \equiv 1 \pmod 4$.*

Proof. For sake of contradiction suppose that $p_1, \ldots, p_r$ are all the primes congruent to 1 modulo 4. Now let

$$x = 2p_1p_2 \cdots p_r, \qquad N = x^2 + 1.$$

Let q be a prime divisor of N. Then q is odd. We have $x^2 + 1 \equiv 0 \pmod q$, hence by Theorem 5.9, $q \equiv 1 \pmod 4$. By assumption, q must be one of the primes $p_1, \ldots, p_r$ so that $q|x$. But this is a contradiction, since q does not divide $1 = N - x^2$. □

This result is a special case of *Dirichlet's Theorem* whose proof is beyond the scope of this course:

Theorem 6.2 (Dirichlet's Theorem)**.** *Let a, q be coprime positive integers. Then there exist infinitely many prime numbers p with*

$$p \equiv a \pmod q$$

Theorem 6.3 (Euler's criterion)**.** *Let $[a] \in \mathbb{Z}_p^\times$. Then $[a]$ is a quadratic residue if and only if*

$$[a]^{(p-1)/2} \equiv 1 \pmod p$$

and $[a]$ is a quadratic non-residue if and only if

$$[a]^{(p-1)/2} \equiv -1 \pmod p$$

Proof. We let g be a primitive root and suppose $[a] = [g]^i$. Then $[a]^{(p-1)/2} = [g]^{i(p-1)/2}$. If i is even we have $i(p-1)/2 \equiv 0 \pmod{p-1}$, so $[g]^{i(p-1)/2} = [1]$. If i is odd we have $i(p-1)/2 \equiv (p-1)/2 \pmod{p-1}$, so $[g]^{i(p-1)/2} = [g]^{(p-1)/2} = [-1]$, as we saw in the proof of Theorem 5.9. □

We finish this section with an application to solving the equation $x^2 \equiv a \pmod p$ for primes $p \equiv 3 \pmod 4$.

Lemma 6.4. *Let p be a prime which is congruent to 3 (mod 4). Suppose a is a quadratic residue modulo p. Then $x = a^{(p+1)/4}$ is a solution to*

$$x^2 \equiv a \pmod p.$$

Proof. By Euler's Criterion

$$[x^2] = [a]^{(p+1)/2} = [a]^{(p-1)/2}[a] = [a].$$

□

Example. Given that 3 is a quadratic residue (mod 131), find a solution to

$$x^2 \equiv 3 \pmod{131}.$$

By the lemma above we know

$$x = 3^{(131+1)/4} = 3^{33}$$

is a solution to $x^2 \equiv 3 \pmod{131}$. We now need to compute $3^{33} \pmod{131}$. Using the method of repeated squaring we have that in $\mathbb{Z}_{131}$:

$$\begin{aligned} [3]^2 &= [9], \quad [3]^4 = [81], \quad [3]^8 = [81]^2 = [11] \\ [3]^{16} &= [11]^2 = [-10], \quad [3]^{32} = [-10]^2 = [100], \end{aligned}$$

We conclude that

$$[3]^{33} = [100] \cdot [3] = [38]$$

is a solution to $x^2 \equiv 3 \pmod{131}$.

6.2. **The Legendre symbol.** We now give some new notation which will us to keep track of whether something is a quadratic residue.

Definition 6.5. Let a be an integer. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ by,

$$\left(\frac{a}{p}\right) = +1 \text{ if } a \text{ is a quadratic residue modulo } p$$
$$\left(\frac{a}{p}\right) = -1 \text{ if } a \text{ is a quadratic non-residue modulo } p$$

If $p|a$ we define $\left(\frac{a}{p}\right) = 0$.

The definition of the Legendre symbol depends only on the congruence class of a, so we can also view it as being defined on elements $[a] \in \mathbb{Z}_p$. Hence, if $a \equiv b \pmod{p}$ then

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

Lemma 6.6. *The number of solutions in $\mathbb{Z}_p$ to*

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

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

Proof. If $p|a$ the only solution is $x = [0]$, and $1 = 1 + 0 = 1 + \left(\frac{a}{p}\right)$.

If a is a quadratic non-residue mod p then there are no solutions (by definition of a non-residue), and $0 = 1 - 1 = 1 + \left(\frac{a}{p}\right)$.

If a is a quadratic residue mod p we have one solution x_1, and $-x_1$ gives a second solution (since $p > 2$ and $x_1 \neq [0]$ we have $-x_1 \neq x_1$). Since the polynomial $x^2 - a$ has degree 2, there are at most two solutions, so we have two solutions in this case, and $2 = 1 + 1 = 1 + \left(\frac{a}{p}\right)$. □

Remark. Let's reformulate Euler's criterion (Corollary 6.3) in terms of the Legendre symbol. It says that if $[a] \in \mathbb{Z}_p^\times$ then we have

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

In fact, if $p|a$ we also have

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

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

Lemma 6.7 (Multiplicativity of the Legendre symbol)**.** *Let a, b be two integers. Then*

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

Proof. By Euler's criterion, as reformulated in the above remark, we have

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

Since $p > 2$, the only way we can have a congruence

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

between two numbers, which are one of $-1, 0, +1$, is if

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

□

Lemma 6.8 (The Rule for -1)**.** *Let $p > 2$ be prime. We have that*

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

Proof. Using the above remark with $a = -1$ we conclude that

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

The implies $(-1)^{(p-1)/2} = \left(\frac{a}{p}\right) + bp$ for some $b \in \mathbb{Z}$. Clearly, we must have $b = 0$. □

Proposition 6.9 (The Rule for 2)**.** *Let p be an odd prime. Then*

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

Proof. The proof is non-examinable, and is sketched in Exercise 8 in Homework 6. □

6.3. **Quadratic Reciprocity.**

Theorem 6.10 (the Law of Quadratic reciprocity)**.** *Let p and q be two distinct odd primes. Then*

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

We will give a proof of quadratic reciprocity in the next section. As well as being a beautiful theorem, the quadratic reciprocity law is useful for calculating Legendre symbols.

Example. Compute $\left(\frac{43}{83}\right)$:

First we check that 43 and 83 are prime. They are also both congruent to 3 mod 4 so we have

$$\begin{aligned} \left(\frac{43}{83}\right) &= -\left(\frac{83}{43}\right) \\ &= -\left(\frac{40}{43}\right) \text{ since } 83 \equiv 40 \pmod{43} \\ &= -\left(\frac{2^3 \cdot 5}{43}\right) = -\left(\frac{2}{43}\right)^3\left(\frac{5}{43}\right) = -\left(\frac{2}{43}\right)\left(\frac{5}{43}\right) \\ &= \left(\frac{5}{43}\right) \text{ since } 43 \equiv 3 \pmod 8 \\ &= \left(\frac{43}{5}\right) = \left(\frac{3}{5}\right) \text{ apply quadratic reciprocity and reduce mod 5} \\ &= \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) \text{ quadratic reciprocity and reduce mod 3} \end{aligned}$$

Finally, we can check that $\left(\frac{2}{3}\right) = -1$. So we get

$$\left(\frac{43}{83}\right) = -1$$

Example. How many solutions does the equation

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

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

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

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

We have $[8] = [3]^{-1}$, so we have to solve

$$(x+1)^2 \equiv 8.$$

Now we compute

$$\left(\frac{8}{23}\right) = \left(\frac{2}{23}\right)^3 = \left(\frac{2}{23}\right) = +1$$

since $23 \equiv 7 \pmod 8$. So there are two solutions to this equation in $\mathbb{Z}_{23}$.

Example. We are going to describe all of the odd primes p with

$$\left(\frac{3}{p}\right) = +1.$$

We may assume that $p \neq 3$. The quadratic reciprocity law says that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ if $p \equiv 1 \pmod 4$ and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ if $p \equiv 3 \pmod 4$. So we get $\left(\frac{3}{p}\right) = +1$ if $\left(\frac{p}{3}\right) = +1$ and $p \equiv 1 \pmod 4$ or if $\left(\frac{p}{3}\right) = -1$ and $p \equiv 3 \pmod 4$.

We have $\left(\frac{p}{3}\right) = +1$ if $p \equiv 1 \pmod 3$ and $\left(\frac{p}{3}\right) = -1$ if $p \equiv 2 \pmod 3$. So we conclude that $\left(\frac{3}{p}\right) = +1$ if $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$ or if $p \equiv -1 \pmod 4$ and $p \equiv -1 \pmod 3$. Using the Chinese remainder theorem, we see that these conditions are equivalent to

$$p \equiv \pm 1 \pmod{12},$$

and this is our final description of the odd primes with $\left(\frac{3}{p}\right) = +1$.

Check your understanding.

(1) Given that 3 is a quadratic residue $\pmod{59}$ find all solutions to

$$x^2 \equiv 3 \pmod{59}.$$

(2) Prove that if a is a quadratic non-residue and $p \equiv 1 \pmod 4$ then $x = a^{(p-1)/4}$ is a solution to

$$x^2 + 1 \equiv 0 \pmod p.$$

(3) Let $p > 2$ and $p \nmid a$. Show that for $k \geq 1$ that
- $\left(\frac{a}{p}\right)^{2k} = 1$.
- $\left(\frac{a}{p}\right)^{2k+1} = \left(\frac{a}{p}\right)$.
- Conclude that for $n = p_1^{a_1} \cdots p_r^{a_r}$, where p_j are distinct, and $p \nmid n$ that

$$\left(\frac{n}{p}\right) = \prod_{p_j : a_j \text{ is odd}} \left(\frac{p_j}{p}\right)$$

where the product ranges over p_j such that a_j is odd.

(4) Show that

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

(5) Show that $\left(\frac{35}{59}\right) = 1$.

(6) Show that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 3$.

7. Gauss sums, the Proof of Quadratic Reciprocity, and Integers which are sums of two squares

Gauss found the first proof of the Law of Quadratic Reciprocity, which he referred to as the "golden theorem". Throughout his lifetime he found many more proofs and today there are several hundred known proofs. One of my favourite proofs is via the theory of Gauss sums, which is due originally to Gauss.

7.1. **Gauss Sums.** In this section we will establish some basic properties of Gauss sums which will be needed for the proof of Quadratic Reciprocity. We first introduce some notation. Given a prime p and integer a, let

$$e_p(a) = e^{2\pi i a/p} = \cos(2\pi a/p) + i\sin(2\pi a/p),$$

where i is a solution to $x^2 + 1 = 0$. We also write $e_p = e_p(1)$, for short. The complex number e_p satisfies $e_p^p = 1$. Also, $e_p(a) = e_p(1)^a$, so if $p|a$ we have $e_p(a) = 1$.

Using properties of geometric sums we have the following result.

Lemma 7.1. *Let $m, n \in \mathbb{Z}$. Then*

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

Proof. If $p|(m-n)$ then $p|a(m-n)$ and we have $e_p(a(m-n)) = 1$ by the comments preceding the lemma for each $0 \le a < p$.

If $m \not\equiv n \pmod p$ then $e_p(m-n) \neq 1$. Recall Recall that for any $z \in \mathbb{C}$ with $z \neq 1$ the geometric sum

$$\sum_{j=0}^{n-1} z^j = \frac{1-z^n}{1-z}.$$

Hence, using this with $z = e_p(m-n)$ we have that

$$\sum_{a=0}^{p-1} e_p(m-n)^a = \frac{1-e_p(m-n)^p}{1-e_p(m-n)} = \frac{1-(e_p^p)^{m-n}}{1-e_p(m-n)} = 0,$$

where we again used the comments preceding the lemma. □

Definition 7.2. Let $p > 2$ be prime and $a \in \mathbb{Z}$. The *Gauss sum* associated to a modulo p is

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

Lemma 7.3. *Let $a \in \mathbb{Z}$ and $p > 2$ be prime. Then*

$$g_a = \left(\frac{a}{p}\right) g_1.$$

Proof. If $p|a$ then $e_p(an) = 1$ for every $n \in \mathbb{Z}$ and $g_a = 0$ (Exercise 7 on Homework sheet 6), so the result holds in this case.

If $p \nmid a$, recall that $\{an : 1 \leq n < p\}$ is a complete reduced residue system modulo p. Hence, also using that $\left(\frac{a}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{an}{p}\right)$ we have

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

Multiplying the above equation by $\left(\frac{a}{p}\right)$ concludes the proof. □

Proposition 7.4. *For a prime $p > 2$ and integer a which is co-prime to p we have that*

$$g_a^2 = (-1)^{(p-1)/2} p.$$

Proof. We compute $\sum_{a=0}^{p-1} g_a^2$ in *two different ways.* Then combine results.

1st approach. Applying Lemma 7.1 we have that

$$\begin{aligned}\sum_{a=0}^{p-1} g_a^2 &= \sum_{n_1=1}^{p-1} \sum_{n_2=1}^{p-1} \left(\frac{n_1 n_2}{p}\right) \sum_{a=0}^{p-1} e_p((n_1+n_2)a) \\ &= p \sum_{n_1=1}^{p-1} \sum_{\substack{1 \leq n_2 < p \\ n_2 \equiv -n_1 \pmod p}} \left(\frac{n_1 n_2}{p}\right).\end{aligned}$$

Since $1 \leq n_1, n_2 < p$ we know $2 \leq n_1 + n_2 < 2p$. Also, $n_1 + n_2 \equiv 0 \pmod p$ so we must have $n_1 + n_2 = p$ that is $n_2 = -n_1 + p$. Recalling $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ we conclude that

$$\sum_{a=0}^{p-1} g_a^2 = p \sum_{n_1=1}^{p-1} \left(\frac{n_1(-n_1+p)}{p}\right) = \left(\frac{-1}{p}\right) p \sum_{n_1=1}^{p-1} \left(\frac{n_1}{p}\right)^2 = (-1)^{(p-1)/2} p(p-1).$$

2nd approach. We evaluate $\sum_{a=0}^{p-1} g_a^2$ using Lemma 7.3 to get that

$$\sum_{a=0}^{p-1} g_a^2 = g_1^2 \sum_{a=0}^{p-1} \left(\frac{a}{p}\right)^2 = g_1^2 (p-1).$$

Combining the two equations above we get $g_1^2 = (-1)^{(p-1)/2} p$. Using Lemma 7.3 we know $g_a^2 = g_1^2$ for $p \nmid a$, which completes the proof. □

7.2. **Proof of Quadratic Reciprocity.** Recall that the Law of Quadratic Reciprocity states that for any odd primes p, q that

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

To complete the proof of quadratic reciprocity we will need to use some basic facts about arithmetic over the ring

$$\mathbb{Z}[e_p] = \{f(e_p) : f(X) \in \mathbb{Z}[X]\}$$

where recall $\mathbb{Z}[X]$ is the ring of polynomials with integer coefficients.

Definition 7.5. Given $\alpha, \beta, \gamma \in \mathbb{Z}[e_p]$ we say α is *congruent to* β *modulo* γ and write $\alpha \equiv \beta \pmod{\gamma}$ if there exists $\delta \in \mathbb{Z}[e_p]$ such that $\gamma\delta = \beta - \alpha$.

Remark. Using properties of binomial coefficients it is not difficult to see that for any $\alpha, \beta \in \mathbb{Z}[e_p]$ and any prime $p \in \mathbb{Z}$ that

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

Proof of Quadratic Reciprocity. Let g denote the Gauss sum associated to 1 modulo p. We will now compute g^q in two different ways then combine our results.

1st approach. Let $P = (-1)^{(p-1)/2}p$. By Euler's Criterion

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

By Proposition 7.4 and Lemma 7.3 $g^{q-1} = (g^2)^{(q-1)/2} = P^{(q-1)/2}$ so that

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

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

2nd approach. Using the remark preceding the proof we have that

$$g^q \equiv \sum_{n=1}^{p-1} \left(\frac{n}{p}\right)^q e_p(qn) \pmod{q}$$

Since q is odd $\left(\frac{n}{q}\right)^q = \left(\frac{n}{q}\right)$. Multiplying by $\left(\frac{q}{p}\right)^2$ we have

$$g^q \equiv \left(\frac{q}{p}\right) \sum_{n=1}^{p-1} \left(\frac{qn}{p}\right) e_p(qn) \equiv \left(\frac{q}{p}\right) g \pmod{q}.$$

Combining our two expressions for $g^q \pmod{q}$ we get that $g\left(\frac{P}{q}\right) \equiv g\left(\frac{q}{p}\right) \pmod{q}$. Multiplying this by g we have that

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

Since $\gcd(q, P) = 1$ so we can cancel $g^2 = P$ from both sides of the congruence to get $\left(\frac{P}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q}$. Finally, since $\left(\frac{P}{q}\right), \left(\frac{q}{p}\right) \in \{\pm 1\}$ we must have that $\left(\frac{q}{p}\right) = \left(\frac{P}{p}\right)$. We conclude that

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

as desired. □

7.3. **Integers which can be represented as a sum of two squares.** In the section we study integers which are the sums of two integers which are square numbers. For example, 5 is a sum of two square since

$$1^2 + 2^2 = 5$$

however 7 is not since the equation $x^2 + y^2 = 7$ has no solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

To motivate this problem consider the *Gaussian integers* $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$. The Gaussian integers have a rich and beautiful structure not unlike the integers themselves. The notions of divisibility and congruences extend naturally to the setting of Gaussian integers. Given $\alpha, \beta \in \mathbb{Z}[i]$ we say α divides β if there exists $\gamma \in \mathbb{Z}[i]$ such that $\alpha\gamma = \beta$. Be aware that are notable differences between $\mathbb{Z}$ and $\mathbb{Z}[i]$, for example there are four units in $\mathbb{Z}[i]$: $1, -1, i, -i$.

Definition 7.6. Let $a, b \in \mathbb{Z}$. Then $p = a + ib \in \mathbb{Z}[i]$ is a *Gaussian prime* if $p \neq 0, \pm 1, \pm i$ and for $\alpha, \beta \in \mathbb{Z}[i]$ if $p|\alpha\beta$ then $p|\alpha$ or $p|\beta$.

Since $\mathbb{Z} \subset \mathbb{Z}[i]$ it is natural to wonder whether primes in $\mathbb{Z}$ are Gaussian primes. If we can write a prime p as a sum of two squares $p = a^2+b^2$ then we can factor $p = (a+ib)(a-ib)$ in $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ so p will not be prime in $\mathbb{Z}[i]$. Conversely, it turns out that if $p \in \mathbb{Z}$ is not a sum of two squares then p is a Gaussian prime.

Proposition 7.7. *A positive integer n is a square if and only if every exponent a_i in the prime factorisation $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ is even.*

Proof. If $n = m^2$ is a square then by considering the prime factorisation of m we see that the exponents in the prime factorisation of n are even.

Conversely, if every exponent a_i is even, then

$$n = (p_1^{a_1/2} p_2^{a_2/2} \cdots p_r^{a_r/2})^2$$

□

Question. Which positive integers are sums of two squares?

If you look at the first few integers, you can check that $1, 2, 4, 5, 8, 9, 10, 13$ are sums of two squares and $3, 6, 7, 11, 12$ are not.

Lemma 7.8. *Suppose $n = a^2 + b^2$ with $a, b \in \mathbb{Z}$. Then $n \equiv 0, 1$ or $2 \pmod 4$.*

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

Corollary 7.9. *If $n \equiv 3 \pmod 4$ then n is not a sum of two squares.*

Lemma 7.10. *Let n be a positive integer. Then n is a sum of two squares if and only if $n = |\alpha|^2$ for some $\alpha \in \mathbb{Z}[i]$.*

Proof. If we have $n = a^2 + b^2$ then $n = (a + ib)(a - ib) = |a + ib|^2$. Conversely if $n = |\alpha|^2$ for $\alpha = a + ib \in \mathbb{Z}[i]$ then $n = a^2 + b^2$. □

Lemma 7.11. *Let m, n be positive integers. If m and n are sums of two squares, so is mn.*

Proof. We can write $m = |\alpha|^2$ and $n = |\beta|^2$, with $\alpha, \beta \in \mathbb{Z}[i]$. So $mn = |\alpha\beta|^2$ is also a sum of two squares by the preceding lemma. □

Check your understanding.

(1) Explain why $e_p(an) = 1$ for any integer n if $p|a$.

(2) Show that
$$\sum_{a=0}^{p-1} g_a = 0.$$

(3) For any positive integer a show that $g_a \in \mathbb{Z}[e_p]$.

(4) Explain why
$$\mathbb{Z}[e_p] = \left\{ \sum_{j=0}^{p-1} a_j e_p(j) : a_j \in \mathbb{Z} \right\}.$$
(*Hint:* Use that $e_p^n = 1$ if $p|n$ and $e_p^a = e_p^b$ if $a \equiv b \pmod{p}$.)

(5) If $m = a^2 + b^2$ and $n = c^2 + d^2$ show that
$$mn = (ac - bd)^2 + (ad + bc)^2.$$
(*Hint:* Write $m = (a + ib)(a - ib)$.)

(6) Using (5) find a, b such that
$$485 = a^2 + b^2.$$
(*Hint:* $485 = 5 \cdot 97$ and $97 = 4^2 + 9^2$).

8. The two squares theorem, irrational, algebraic and transcendental numbers

This week we will continue our study on integers which are sums of two squares as well as begin our investigation into Diophantine approximation. The latter of which is an area of number theory which studies how accurately a given real number can be approximated by rationals.

8.1. **The two squares theorem.**

Theorem 8.1. *Let p be a prime. p is a sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

Proof. We know that if $p \equiv 3 \pmod 4$ then p is not a sum of two squares, and $2 = 1^2 + 1^2$. So it remains to show that if $p \equiv 1 \pmod 4$ then p is a sum of two squares.

Since $p \equiv 1 \pmod 4$ we have $\left(\frac{-1}{p}\right) = +1$. So we can let $a \in \mathbb{Z}$ be a solution to the equation $a^2 + 1 \equiv 0 \pmod p$. Let $k = \lfloor \sqrt{p} \rfloor$, so $k^2 < p < (k+1)^2$. For each of the $(k+1)^2 > p$ different pairs of integers (c, d) with $0 \leq c \leq k$ and $0 \leq d \leq k$ consider the integer $c + ad$. Since there are only p distinct residue classes mod p, we must have $c_1 + ad_1 \equiv c_2 + ad_2 \pmod p$ for two different pairs $(c_1, d_1), (c_2, d_2)$ (this is an example of the *pigeonhole principle*). So we have

$$c_1 - c_2 \equiv a(d_2 - d_1) \pmod p$$

and squaring both sides gives

$$(c_1 - c_2)^2 \equiv -(d_2 - d_1)^2 \pmod p$$

We deduce that p divides $(c_1 - c_2)^2 + (d_2 - d_1)^2$. Moreover, we have

$$0 < (c_1 - c_2)^2 + (d_2 - d_1)^2 \leq k^2 + k^2 < 2p$$

but the only multiple of p between 0 and $2p$ is p itself, so we are forced to have $p = (c_1 - c_2)^2 + (d_2 - d_1)^2$ and we have shown that p is a sum of two squares. □

The theorem shows that for a prime $p \equiv 1 \pmod 4$ we can factor $p = (a + ib)(a - ib)$ in $\mathbb{Z}[i]$ and this shows that p is not a Gaussian prime (see the Week 8 notes), whereas if $p \equiv 3 \pmod 4$ no such factorisation is possible and it turns out such primes are Gaussian primes.

Fact 8.2. Let $a + bi \in \mathbb{Z}[i]$ be a Gaussian prime with $a, b \in \mathbb{Z}$. Then either:

- a or b is zero and the other is a prime $\equiv 3 \pmod 4$;
- both a, b are non-zero and $a^2 + b^2$ is a prime $\not\equiv 3 \pmod 4$.

Theorem 8.3 (Two squares theorem)**.** *A positive integer n is a sum of two squares if and only if the exponent of every prime number which is congruent to* 3 (mod 4) *in the prime factorisation of n is even.*

Proof. First suppose that $n = p_1 p_2 \cdots p_k m^2$ with each prime p_i equal to either 2 or $\equiv 1 \pmod 4$. Then n is a sum of two squares, since it is a product of integers which are sums of two squares. Conversely, suppose $n = a^2 + b^2$ be a sum of two squares. Let $d = \gcd(a, b)$. Then we have $n = d^2((\frac{a}{d})^2 + (\frac{b}{d})^2)$ and $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Suppose $p|n$ and $p \equiv 3 \pmod 4$. If $p|((\frac{a}{d})^2 + (\frac{b}{d})^2)$ then we can solve the equation $x^2 + y^2 \equiv 0 \pmod p$, with x, y coprime. In particular p does not divide x or y (otherwise the equation would force p to divide both, in which case $p|\gcd(x.y)$). So we have $([x]_p[y]_p^{-1})^2 = [-1]_p$ and -1 is a quadratic residue modulo p. This contradicts the assumption that $p \equiv 3 \pmod 4$. So if $p|n$ and $p \equiv 3 \pmod 4$ we must have $p|d$ and $p \nmid ((\frac{a}{d})^2 + (\frac{b}{d})^2)$. This implies that the exponent of p in the prime factorisation of n is even. □

Fact 8.4. A positive integer is a sum of three squares if and only if it is not of the form $4^a(8k + 7)$ with a, k non-negative integers.

Fact 8.5. Every positive integer is a sum of four squares.

8.2. **Irrational numbers.** Recall that $\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\}$ is the set of rational numbers, and we use $\mathbb{R}$ to denote the real numbers and $\mathbb{C}$ to denote the complex numbers.

Definition 8.6. A complex number $x \in \mathbb{C}$ is called *irrational* if $x \notin \mathbb{Q}$.

Theorem 8.7. *A real number $x \in \mathbb{R}$ is rational if and only if its decimal expansion either terminates or repeats.*

Proof. We analyse what it means for a real number to have a repeating decimal expansion. We suppose that $0 < x < 1$ and that we can write $x = 0.a\overline{b} = 0.a_1a_2a_3 \cdots a_n\overline{b_1b_2 \cdots b_k}$.

Then we have $y := 10^n x - a = 0.\overline{b}$ and $10^k y = b + y$, so $y = \frac{b}{10^k - 1}$. So we have

$$x = \frac{a + y}{10^n} = \frac{(10^k - 1)a + b}{10^n(10^k - 1)}$$

Conversely if $x = \frac{c}{10^n(10^k-1)}$ with $0 < c < 10^n(10^k-1)$ then we can write $c = (10^k-1)a+b$ with $0 \le b < (10^k-1)$ and $0 \le a < 10^n$. So to show that a rational number has a repeating (or terminating) decimal expansion, it suffices to show that it can be written as a fraction with denominator $10^n(10^k - 1)$. Suppose $x = \frac{r}{s}$ with $r \in \mathbb{Z}$ and $s \in \mathbb{N}$. Multiplying top and bottom of the fraction by a multiple of 2 or 5 if necessary, we can write $x = \frac{r'}{10^n s'}$ where s' is coprime to 10. Since 10 is coprime to s' there is an integer k such that $10^k \equiv 1 \pmod{s'}$. For example, we can take $k = \phi(s')$. In other words, we have $s'|(10^k - 1)$, so multiplying top and bottom of the fraction by $(10^k - 1)/s'$ we can write x as a fraction with denominator $10^n(10^k - 1)$ as desired. □

Example. The number

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

is irrational.

Proposition 8.8. *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 either z is an integer or z is irrational.*

Proof. Suppose z is rational. We must show that z is actually an integer. Write $z = \frac{a}{b}$ with $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and $\gcd(a, b) = 1$. We have

$$\left(\frac{a}{b}\right)^m + c_{m-1}\left(\frac{a}{b}\right)^{m-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0$$

and multiplying by b^m we get

$$a^m + c_{m-1}a^{m-1}b + \cdots + c_1 ab^{m-1} + c_0 b^m = 0$$

and in particular we have $b|a^m$. Since $\gcd(a, b) = 1$ we also have $\gcd(a^m, b) = 1$. Combining this with the fact that $b|a^m$ means we must have $b = 1$ so $z \in \mathbb{Z}$. □

Remark. Note that in the above Proposition it is crucial that the leading coefficient of the polynomial is 1. For example, if you consider the polynomial $2x + 1$ you see that polynomials which are not monic (whose leading coefficient is not 1) can have rational, but non-integral, roots.

Example. $\sqrt[3]{2}$ is irrational: since it is a root of $x^3 - 2$ the preceding proposition implies that either $\sqrt[3]{2}$ is irrational, or there is an integer n with $n^3 = 2$. But there is no such integer (if $n > 1$ then $n^3 > 2$).

Recall the number $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$

Theorem 8.9 (Euler, 1737)**.** *e is irrational*

Proof. This proof is due to Fourier. Euler's original proof uses *continued fractions* which is a very nice topic in elementary number theory which we don't have time to cover in this course. They are discussed in some of the books on the reading list.

Suppose $e = \frac{a}{b}$ is rational. Then for $n \geq b$ the number

$$N = n!\left(e - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}\right)\right) = n!\left(\frac{a}{b} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}\right)\right)$$

is a positive integer, since multiplying by $n!$ clears all the denominators. On the other hand, we have

$$N = n!\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\right) = \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots$$

and the right hand side is strictly less than

$$\frac{1}{n+1} + \frac{1}{(n+1)^2} + \cdots = \frac{1}{n}$$

So, taking $n > 1$ we get a contradiction to the claim that N is a positive integer. So we deduce that e must be irrational after all. □

A harder fact to prove (proven by Lambert in 1761) is that π is also irrational.

8.3. **Algebraic and transcendental numbers.**

Definition 8.10. A complex number $z \in \mathbb{C}$ is called *algebraic* if z is a root of a non-zero polynomial with rational coefficients.

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

Example. If $z \in \mathbb{Q}$ then z is a root of the polynomial $x - z$, and is therefore algebraic.

So every transcendental number is irrational

Example. $\sqrt[3]{2}$ and $\sqrt[3]{2} + 1$ are algebraic numbers.

Fact 8.11. e is transcendental (Hermite, 1873) π is transcendental (Lindemann, 1882)

Conjecture (A special case of *Schanuel's conjecture*)**.** *$e + \pi$ is transcendental*

At the moment, it is not even known whether or not $e + \pi$ is irrational!

The proofs of the above facts are quite complicated. An easier result is that $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental. We will prove this by considering the problem of approximating irrational numbers by rational numbers. Since the rational numbers are dense in the real numbers, any irrational number $\alpha \in \mathbb{R}$ can be approximated arbitrarily closely by a rational number — for example, consider the rational numbers obtained by cutting off the decimal expansion of α further and further along. However, the denominators of these rational numbers get large as we approximate α closer and closer. So, more precisely, we want to say something about the difference $|\alpha - \frac{a}{b}|$ in terms of the denominator b. Let's think about how good our naive way of producing rational approximations using the decimal expansion does: if $\alpha = 0.a_1a_2a_3 \cdots a_n a_{n+1}a_{n+2} \cdots$ and we consider the rational approximation $\alpha_n = 0.a_1a_2 \cdots a_n$ then we have

$$|\alpha - \alpha_n| = 0.00 \cdots 0a_{n+1}a_{n+2} \cdots < \frac{1}{10^n}$$

and the denominator of α_n is 10^n, so our approximation α_n is, in general, within distance $\frac{1}{b}$ of α, where b is the denominator of α_n.

Theorem 8.12 (Dirichlet's approximation theorem)**.** *Let $\alpha \in \mathbb{R}$ be a real number. Let $n > 0$ be a positive integer. Then there exist integers $a \in \mathbb{Z}, b \in \mathbb{N}$, with $b \leq n$, such that*

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

Proof. We begin by rewriting the inequality in the statement of the theorem as

$$|a - b\alpha| < \frac{1}{n}.$$

So we want to find a natural number $b \leq n$ such that $b\alpha$ is close to an integer a. Consider the multiples $0\alpha, 1\alpha, \ldots, n\alpha$ of α. For each integer i with $0 \leq i \leq n$ we write $i\alpha = N_i + F_i$ where N_i is an integer and $0 \leq F_i < 1$ (so F_i is the *fractional part* of $i\alpha$). We have $n + 1$ numbers $F_0, F_1, \ldots, F_n$ all in the interval $[0, 1)$. We divide $[0, 1)$ into the n smaller intervals $[0, 1/n), [1/n, 2/n), \ldots, [(n-1)/n, 1)$. By the pigeonhole principle one of these intervals

must contain at least 2 of the numbers F_i. So we have two integers $i < j$ (with $j \leq n$) such that $|F_i - F_j| < \frac{1}{n}$. We can rewrite this inequality as

$$|(i\alpha - N_i) - (j\alpha - N_j)| < \frac{1}{n}$$

and finally we get

$$|(N_j - N_i) - (j - i)\alpha| < \frac{1}{n}.$$

So we can take $a = N_j - N_i$ and $b = j - i$. □

Corollary 8.13. *Suppose $\alpha \in \mathbb{R}$ is irrational. Then there exist infinitely many (distinct) rational numbers $\frac{a}{b}$ such that*

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

Proof. The preceding theorem tells us that for each n we can find a_n, b_n such that

$$|\alpha - \frac{a_n}{b_n}| < \frac{1}{b_n n}$$

and $b_n \leq n$. So we also have

$$|\alpha - \frac{a_n}{b_n}| < \frac{1}{b_n^2}.$$

We claim that this must give us infinitely many distinct rational numbers $\frac{a_n}{b_n}$: if not, we must have a single rational number $\frac{a}{b}$ with

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

for infinitely many n. But taking the limit as $n \to \infty$ shows that this implies that $\alpha = \frac{a}{b}$ and we assumed that α was irrational. So we have shown the claim. □

Remark. Note that the rational approximations a/b which are guaranteed to exist by the above corollary are much better than the approximations we got in general using the decimal expansion — the error is $< 1/b^2$ whereas for the decimal approximations we got error $< 1/b$.

Continued fractions give a systematic way to compute numbers a/b with $|\alpha - \frac{a}{b}| < \frac{1}{b^2}$.

Check your understanding.

(1) Suppose $\gcd(a, b) = 1$ and $p|(a^2 + b^2)$. Explain why $\gcd(p, a) = \gcd(p, b) = 1$.
(2) Determine which of the following integers are sums of two squares:
   - $2646 = 3^3 \cdot 7^2 \cdot 2$;
   - $2250 = 2 \cdot 3^2 \cdot 5^3$.
(3) Show that $\sqrt{e}$ is an irrational number.
(4) Let $\left(\frac{n}{7}\right)$ denote the legendre symbol. Explain why

$$\alpha = \sum_{n=1}^{\infty} \frac{\left(\frac{n}{7}\right) + 3}{10^{n!}}$$

is irrational.

(5) Find a non-zero polynomial with rational coefficients and $\sqrt[3]{2}+1$ as a root.

(6) Given a real number x, we can write $x = N(x) + F(x)$ where $N(x) \in \mathbb{Z}$ and $0 \leq F(x) < 1$ is the fractional part of x.
   - Explain why $F(x+1) = F(x)$ i.e. $F(x)$ is a periodic function.
   - Plot $F(x)$.

9. Liouville's Theorem, Pythagorean triples, the Pythagorean triples theorem

9.1. **Liouville's Theorem.** Dirichlet's approximation theorem tells us that we can find rational numbers which approximate α quite closely (relative to the denominator of the rational number). Now we can ask whether it is possible to do even better than the result in Dirichlet's theorem: for example, for an irrational number $\alpha \in \mathbb{R}$ is it possible to find infinitely many rational numbers $\frac{a}{b}$ with

$$|\alpha - \frac{a}{b}| < \frac{1}{b^3}?$$

Theorem 9.1 (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 is a real number $C > 0$ such that that

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

for all $a \in \mathbb{Z}, b \in \mathbb{N}$.

In particular, if $m = 2$ this theorem implies that we *cannot* find infinitely many rational numbers $\frac{a}{b}$ with $|\alpha - \frac{a}{b}| < \frac{1}{b^3}$, as for b large enough we have $\frac{1}{b^3} < \frac{C}{b^2}$.

Proof. (non-examinable) By dividing out factors $x - \beta$ with β rational, we can assume that all the roots of $f(x)$ are irrational. Multiplying by an integer to clear denominators, we can also assume that the coefficients c_i are all integers. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ be the complex roots of $f(x)$, so $f(x) = c_m(x - \alpha_1)\cdots(x - \alpha_m)$. Suppose $a \in \mathbb{Z}, b \in \mathbb{N}$ with $|\alpha - \frac{a}{b}| < 1$. We have

$$\begin{aligned}\left|f\left(\frac{a}{b}\right)\right| &= |c_m||a/b - \alpha_1|\cdots|a/b - \alpha_m| \\ &< |c_m||\alpha - a/b|(1 + |\alpha| + |\alpha_2|)\cdots(1 + |\alpha| + |\alpha_m|) = c|\alpha - a/b|\end{aligned}$$

where we use the inequality $|a/b| < 1 + |\alpha|$, and $c > 1$ is a real number.

On the other hand,

$$f\left(\frac{a}{b}\right) = \frac{c_m a^m + c_{m-1}a^{m-1}b + \cdots + c_1 a b^{m-1} + c_0 b^m}{b^m}$$

and the numerator of this fraction is a non-zero integer (non-zero because $f(x)$ has no rational roots). So we have $|f\left(\frac{a}{b}\right)| \geq \frac{1}{b^m}$.

We deduce that

$$\frac{1}{b^m} \leq \left|f\left(\frac{a}{b}\right)\right| < c|\alpha - a/b|$$

Now we take $C = c^{-1}$ and claim that this satisfies the statement of the theorem. Since $c > 1$ we have $C < 1$, so if

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

we certainly have $|\alpha - \frac{a}{b}| < 1$. Now we know that $|\alpha - a/b| > c^{-1}\frac{1}{b^m} = \frac{C}{b^m}$ which is a contradiction. So we have proven that

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

for all a, b. □

Example. The proof of the above theorem is a bit tricky. Let's go through the proof in the special case $\alpha = \sqrt{2}$. In this case, our polynomial is $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. We have $\alpha = \alpha_1 = \sqrt{2}$ and $\alpha_2 = -\sqrt{2}$.

We assume that $\frac{a}{b}$ is a rational number with $|\sqrt{2} - \frac{a}{b}| < 1$. Then we have $|sqrt2 + \frac{a}{b}| \leq |\frac{a}{b} - \sqrt{2}| + 2\sqrt{2}$ by the triangle inequality, so $|\sqrt{2} + \frac{a}{b}| < 1 + 2\sqrt{2}$.

On the other hand we have $(\frac{a}{b}) = \frac{a^2 - 2b^2}{b^2}$ so $|f(\frac{a}{b})| \geq \frac{1}{b^2}$.

Combining everything, we get

$$|\frac{a}{b} - \sqrt{2}|(1 + 2\sqrt{2}) > |\frac{a}{b} - \sqrt{2}||\sqrt{2} + \frac{a}{b}| = |f(\frac{a}{b})| \geq \frac{1}{b^2}$$

and so

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

This was all assuming $|\sqrt{2} - \frac{a}{b}| < 1$ but if $|\sqrt{2} - \frac{a}{b}| \geq 1$ we clearly have $|\sqrt{2} - \frac{a}{b}| > \frac{1}{(1+2\sqrt{2})b^2}$ as well (since $b \geq 1$). So we deduce that we have

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

in all cases.

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

Corollary 9.2. *The number $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.*

Proof. Suppose for a contradiction α is a root of a polynomial of degree m with rational coefficients. So there is a real number $C > 0$ such that

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

for all $a \in \mathbb{Z}, b \in \mathbb{N}$.

To approximate α by rational numbers, we just consider the finite sums $\alpha_k = \sum_{n=1}^{k} \frac{1}{10^{n!}}$, which have denominator $10^{k!}$. We have

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

(to check the inequality, just compare the two decimal expansions). By taking k large enough, we can make $\frac{2}{10^{(k+1)!}} = \frac{2}{(10^{k!})^{k+1}}$ less than $\frac{C}{(10^{k!})^m}$, which contradicts Liouville's theorem. So α is transcendental. □

Here is a nice consequence of Liouville's theorem:

Corollary 9.3. *Let $\alpha \in \mathbb{R}$ be an irrational number which is a root of a non-zero polynomial with rational coefficients and degree m, as in Liouville's theorem. Suppose we have a real number $\epsilon > 0$. Then the inequality*

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

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

Proof. Suppose we have $\left|\alpha - \frac{a}{b}\right| \leq \frac{1}{b^{m+\epsilon}}$. Combining this inequality with Liouville's theorem gives us $\frac{C}{b^m} < \frac{1}{b^{m+\epsilon}}$, so we have $b^\epsilon < \frac{1}{C}$ or equivalently $b < \frac{1}{C^{1/\epsilon}}$. So there are only finitely many possibilities for b. For each value of b, there are only finitely many possibilities for a such that $\left|\alpha - \frac{a}{b}\right| \leq \frac{1}{b^{m+\epsilon}}$ holds (it's an exercise to convince yourself of this). So there are only finitely many possibilities for a and b. □

Remark. We deduced the corollary fairly easily from Liouville's theorem. It is a very similar statement, but the statement of the Corollary doesn't imply Liouville's theorem. If you think about the following, you should be able to see why this is: the function $\frac{1}{b^m \log b}$ satisfies:

- $\frac{1}{b^m \log b} \leq \frac{1}{b^{m+\epsilon}}$ for only finitely many positive integers b
- There is no real number $C > 0$ such that $\frac{1}{b^m \log b} > \frac{C}{b^m}$ for all positive integers b.

Example. The above corollary shows that there exist only finite many a, b such that $\left|\sqrt{2} - \frac{a}{b}\right| \leq \frac{1}{b^3}$. Let's find all of 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 is a positive integer, we deduce $b = 1, 2, 3$. Now let's decide what the possible values of a are for each of these values of b.

If $b = 3$ the inequality is $|\frac{a}{3} - \sqrt{2}| \leq \frac{1}{27}$ which implies that $|3\sqrt{2} - a| \leq \frac{1}{9}$. Since $3\sqrt{2}$ is 4.24 to two decimal places, there are no integers within the range $\frac{1}{9}$, so there are no a's satisfying this inequality.

If $b = 2$ the inequality is $|\frac{a}{2} - \sqrt{2}| \leq \frac{1}{8}$ which implies that $|2\sqrt{2} - a| \leq \frac{1}{4}$. We get one solution, $a = 3$.

Finally, if $b = 1$ we get $a = 1$ or 2.

9.2. **Pythagorean triples.** Let's consider the equation $x^2 + y^2 = z^2$ and try to describe all integer solutions (x, y, z).

Definition 9.4. A *Pythagorean triple* is a set of three positive integers (x, y, z) such that $x^2 + y^2 = z^2$. We say that the triple is *primitive* if the only positive common divisor of x, y and z is 1 (i.e. $\gcd(x, y, z) = 1$).

We call a right-angled triangle with integer length sides a *Pythagorean triangle*. Its side lengths form a Pythagorean triple.

Example. $(3, 4, 5)$ and $(5, 12, 13)$ are primitive Pythagorean triples.

Lemma 9.5. *Supppose (x, y, z) is a primitive Pythagorean triple. Then any two of the three integers (x, y, z) are coprime.*

Proof. Suppose p is a prime number with $p|x, p|z$. Then $y^2 = z^2 - x^2$ so $p|y^2$ which implies that $p|y$. This contradicts the primitivity of (x, y, z). So x, z are coprime. A similar argument applies to the other pairs x, y, y, z. □

To find all Pythagorean triples, it suffices to find all primitive Pythagorean triples — any Pythagorean triple (x, y, z) is equal to (dx', dy', dz') where $d = \gcd(x, y, z)$ and (x', y', z') is a primitive Pythagorean triple.

Lemma 9.6. *If (x, y, z) is a primitive Pythagorean triple then one of x, y is even and the other is odd.*

Proof. If x, y are both even, then $z^2 = x^2 + y^2$ is also even, so z is even. This is impossible, because (x, y, z) is assumed to be primitive. If x, y are both odd, then $z^2 \equiv 2 \pmod 4$ which is impossible (the square of any integer is either 0 or 1 mod 4). □

From now on, we can assume (by swapping x and y if necessary) that a primitive Pythagorean triple (x, y, z) has x even and y odd.

Here is a trick which we will use a couple of times:

Lemma 9.7. *Suppose a, b are coprime positive integers and $ab = c^2$ is the square of an integer c. Then a and b are themselves squares.*

Proof. Consider the prime factorisations $a = p_1^{a_1} \cdots p_r^{a_r}$, $b = q_1^{b_1} \cdots q_s^{b_s}$, with the a_i and b_i positive integers. Since a and b are coprime, the primes p_i, q_i are all distinct, so the prime factorisation of ab is

$$ab = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$$

and ab is a square if and only if all the numbers a_i, b_i are even, which happens if and only if both a and b are squares. □

9.3. **The Pythagorean triples theorem.**

Theorem 9.8. *All primitive Pythagorean triples, with x even, are given by the formulas:*

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

for integers $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$.

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

$$x = 2dst, y = d(s^2 - t^2), z = d(s^2 + t^2).$$

Proof. Let (x, y, z) be a primitive Pythagorean triple. Since y and z are both odd we have integers u, v such that $z - y = 2u$ and $z + y = 2v$. The equation $x^2 + y^2 = z^2$ can be rewritten as

$$x^2 = z^2 - y^2 = (z - y)(z + y) = 4uv$$

so $\left(\frac{x}{2}\right)^2 = uv$.

Now we claim that $\gcd(u,v)=1$. Indeed, if $d|u$ and $d|v$ then d divides $u+v=y$ and $u-v=z$. Since y and z are coprime, we must have $d=1$. Since uv is a square and u,v are coprime, we see that both u and v are squares, so we write $u=t^2$ and $v=s^2$ with s,t positive integers.

Now we have $z=s^2+t^2$, $y=s^2-t^2$ and $x^2=4s^2t^2$, so $x=2st$. Since $\gcd(y,z)=1$, we have $\gcd(s,t)=1$, and since y is odd we have $s\not\equiv t \pmod 2$.

To check that the formulas give a primitive Pythagorean triple is left as an exercise.

To get all Pythagorean triples, we just use the observation above that if (x,y,z) is a Pythagorean triple then $(x,y,z)=(dx',dy',dz')$ where (x',y',z') is a primitive Pythagorean triple. □

Example application.

(1) We are going to find all primitive Pythagorean triples (a,b,c) with $c=b+3$.

Since c is always odd (for a primitive triple), if $c=b+3$ then b is even. So we deduce from Theorem 9.8 that we have integers s,t with $b=2st$, $a=s^2-t^2$ and $c=s^2+t^2$.

If $c=b+3$ then we have $s^2+t^2=2st+3$. Rearranging this equation gives $(s-t)^2=3$, which has no integer solutions. So there are no primitive Pythagorean triples with $c=b+3$.

(2) We are going to find all primitive Pythagorean triples (a,b,c) with $c=b+2$. This time b is odd, so we have integers s,t with $a=2st$, $b=s^2-t^2$ and $c=s^2+t^2$.

If $c=b+2$ we get $s^2+t^2=s^2-t^2+2$ which is equivalent to $t=1$.

So the primitive Pythagorean triples with $c=b+2$ are given by $(2s,s^2-1,s^2+1)$, where s is any even positive integer.

Check your understanding.

(1) Find all rational numbers a/b with $\gcd(a,b)=1$ such that

$$\left|\sqrt{3}-\frac{a}{b}\right|<\frac{1}{b^3}.$$

Hint: There are only two such numbers.

(2) Without using decimal expansions, show that

$$\sum_{m=n+1}^{\infty}\frac{1}{10^{m!}}\le\frac{1}{10^{(n+1)!}}\sum_{j=0}^{\infty}\frac{1}{10^j}.$$

By summing the geometric series conclude that

$$\sum_{m=n+1}^{\infty}\frac{1}{10^{m!}}\le\frac{(10/9)}{10^{(n+1)!}}.$$

Hint: Write $\dfrac{1}{10^{m!}}=\dfrac{1}{10^{(n+1)!}}\cdot\dfrac{1}{10^{m!-(n+1)!}}$. For $m\ge n+1$ and $n\ge 1$ show that $m!-(n+1)!\ge m-(n+1)$ and conlcude $\dfrac{1}{10^{m!-(n+1)!}}\le\dfrac{1}{10^{m-(n+1)}}$. Now use this inequality and re-index the sum by taking $j=m-(n+1)$.

(3) The greatest common divisor of a, b, c, $\gcd(a, b, c)$ is the largest integer d such that $d|a$, $d|b$ and $d|c$. Explain why $\gcd(a, b, c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$. Use the Euclidean algorithm to find $\gcd(1764, 819, 1162)$. (**Solution:** The answer is $\gcd(1764, 819, 1162) = 7$.)

(4) Show that a positive integer n is a square (i.e.$n = c^2$ for some $c \in \mathbb{Z}$) if and only if in the prime factorisation of n the power of every prime factor is even.

(5) Obtain all primitive Pythagorean triples (x, y, z) in which $x = 40$; do the same for $x = 60$.

(6) If (x, y, z) is a primitive Pythagorean triple prove that $x+y$ and $x-y$ are congruent modulo 8 to either 1 or 7.

10. Fermat's Last Theorem, General Diophantine equations

10.1. **Fermat's Last Theorem.**

Theorem 10.1 (Wiles, Taylor, 1994)**.** *If $n \geq 3$ there are no positive integer solutions (x, y, z) to the equation*

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

The simplest case of Fermat's Last Theorem is when $n = 4$ — for this case (and perhaps only this case) Fermat is likely to have found a proof himself. In fact we can prove something a bit stronger:

Theorem 10.2. *There are no positive integer solutions (x, y, z) to the equation*

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

Proof. For a contradiction, we suppose (x_0, y_0, z_0) is a positive integer solution. We can assume that $\gcd(x_0, y_0) = 1$, as if d divides x_0 and y_0 then d^2 divides z_0 and $(x_0/d, y_0/d, z_0/d^2)$ is another solution. Now (x_0^2, y_0^2, z_0) is a primitive Pythagorean triple. We can assume x_0 is even (otherwise we swap x_0 and y_0), and then we have

$$x_0^2 = 2st, y_0^2 = s^2 - t^2, z_0 = s^2 + t^2$$

for integers $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$.

So we get another primitive Pythagorean triple (t, y_0, s), with y_0 odd, and therefore t even. So we have

$$t = 2uv, y_0 = u^2 - v^2, s = u^2 + v^2$$

with u, v coprime, and we have $x_0^2 = 4uv(u^2 + v^2)$. Since u, v are coprime, we also have $u, u^2 + v^2$ and $v, u^2 + v^2$ coprime. Considering the prime factorisations of u, v and $(u^2 + v^2)$ we deduce from the equation $x_0^2 = 4uv(u^2+v^2)$ that all three of u, v and u^2+v^2 are squares.

Letting $u^2 + v^2 = z_1^2, u = x_1^2$ and $v = y_1^2$, we get

$$z_1^2 = x_1^4 + y_1^4$$

so we have produced another positive integer solution (x_1, y_1, z_1) to the equation $x^4 + y^4 = z^2$. Moreover, we have $z_1 \leq s < s^2 + t^2 = z_0$. So z_1 is strictly less than z_0. But now we can repeat this procedure and produce an infinite sequence of *positive* integers $z_0 > z_1 > z_2 > \cdots$. This is impossible, so we get the desired contradiction. This method of proof is called 'Fermat descent'. I explained a slightly different version of the proof in lectures, where you start out assuming that z_0 is minimal and then get a contradiction by finding a solution (x_1, y_1, z_1) with z-value $z_1 < z_0$ (contradicting the minimality of z_0). □

10.2. **General Diophantine equations.**

We met the notion of Diophantine equations, and the special case of linear Diophantine equations, earlier in the course.

The general form of a Diophantine equation is a multivariable polynomial equation:

$$f(x_1, x_2, \ldots, x_r) = c_1 x_1^{a_{11}} x_2^{a_{12}} \cdots x_r^{a_{1r}} + \cdots + c_m x_1^{a_{m1}} x_2^{a_{m2}} \cdots x_r^{a_{mn}} = 0$$

where the coefficients c_i are all integers, and we seek integer solutions $(x_1, x_2, \ldots, x_r)$ to this equation.

Example.

$$x^4 + 2x^2 - 4xy + 2y^2 - 1 = 0$$

Given a Diophantine equation we can ask how many (if any) solutions the equation has, and whether there is an algorithm or formula to find the solutions. There is no general theory to answer these questions (in fact there is a theorem in mathematical logic which says that there cannot be such a general theory — try reading about 'Hilbert's tenth problem'). We will discuss a collection of examples which illustrate some of the methods you can use. We should emphasise that these examples are all carefully chosen — if you pick a completely random Diophantine equation you are very unlikely to be able to find its solutions.

However, in the case where there is only one variable the situation is much simpler.

Proposition 10.3. *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 $b_0, \ldots, b_{n-1} \in \mathbb{Z}$.

For a root a of $f(x)$ follows that $c_0 = -a \cdot b_0$. In particular, if $f(a) = 0$ with $a \in \mathbb{Z}$ then $a|c_0$ and consequently to find all integer roots of $f(x)$ it suffices to check $f(d)$ for all divisors (positive and negative) of c_0.

Proof. Observe that

$$\begin{aligned} f(x) - f(a) &= \sum_{j=1}^{n} c_j(x^j - a^j) \\ &= \sum_{j=1}^{n} c_j(x-a)(x^{j-1} + ax^{j-2} + \cdots + a^{j-2}x + a^{j-1}) = (x-a)g(x) \end{aligned}$$

where $g(x)$ is a polynomial with integer coefficients. □

Example. Here are some simple examples of equations which we can solve completely:

(1) $x^3 - 2x = 0$ — the only integer solution is $x = 0$.
(2) $x^4 + 2x^2 - 4xy + 2y^2 - 1 = 0$ — we can rewrite this equation as $x^4 + 2(x-y)^2 = 1$. If x, y are integers then $x^4 + 2(x-y)^2 = 1$ is only possible if we have $x^4 = 1, (x-y)^2 = 0$, so the solutions are given by $x = \pm 1$ and $y = x$.
(3) $x^3 = 5y^6$ — we get one obvious solution $x = y = 0$. If $y \neq 0$ then $x \neq 0$. Let a be the power of 5 in the prime factorisation of x and let b be the power of 5 in the prime factorisation of y. Then the equation implies that $3a = 6b + 1$ so we get $1 = 3(a - 2b)$ which is impossible. So there is no solution with $y \neq 0$.

Suppose we have a Diophantine equation $f(x_1, x_2, \ldots, x_r) = 0$. We observe that if this equation has an integer solution then the congruence equation

$$f(x_1, x_2, \ldots, x_r) \equiv 0 \pmod{m}$$

has a solution for every positive integer m. So one way to show that a Diophantine equation has *no* solutions is to find a positive integer m such that the equation

$$f(x_1, x_2, \ldots, x_r) \equiv 0 \pmod{m}$$

has no solutions.

Example. (1) Consider the equation $x^2 = y^5 + 7$. We are going to show it has no integer solutions. We can consider the equation mod 11. Euler's criterion implies that $y^5 \equiv 0, 1$ or $-1 \pmod{11}$ for every integer y. So the right hand side of the equation can take the values $6, 7$ or $8 \pmod{11}$. On the other hand x^2 can take the values $0, 1, 3, 4, 5, 9 \pmod{11}$. Since there are no common values in these lists, there are no solutions to the equation

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

and hence no integer solutions to the equation $x^2 = y^5 + 7$.

(2) The equation $x^{12} + y^{12} = z^{12} + w^{12} + 3$ has no integer solutions: we consider the equation mod 13. Fermat's little theorem says that $x^{12} + y^{12} \equiv 0, 1$ or $2 \pmod{13}$, and similarly $z^{12} + w^{12} + 3 \equiv 3, 4$ or $5 \pmod{13}$. As in the previous example, there are no common values so the equation $x^{12} + y^{12} = z^{12} + w^{12} + 3$ has no integer solutions.

(3) Consider the equation $15x^2 - 7y^2 = 9$. Suppose we have an integer solution (x, y). We get $3|(7y^2)$, so $3|y$. Let $y = 3y'$. Then we have $15x^2 - 63(y')^2 = 9$ or equivalently $5x^2 - 21(y')^2 = 3$. This now implies that $3|x$ so we let $x = 3x'$. Then we get the equation $15(x')^2 - 7(y')^2 = 1$. Finally, we observe that this equation has no solutions mod 3: reducing mod 3 we get an equation $2(y')^2 \equiv 1 \pmod{3}$, which has no solutions. So the original equation $15x^2 - 7y^2 = 9$ has no integer solutions.

The first two of these examples could be described as finding a prime p such that the congruence classes of terms in the equation only have a few possible values, in order to rule out solutions. The last one works by identifying prime divisors of possible solutions (x, y) and dividing out by these to simplify the equation.

We already considered the example of $y^2 = x^5 + 7$. Now we will consider a very similar equation which is rather trickier to analyse:

Example. Consider the equation $y^2 = x^3 + 7$. First we note that if (x, y) is a solution then x must be odd: if x is even then $y^2 \equiv 3 \pmod{4}$ which is impossible.

So we deduce that x is odd and y is even. Let's rewrite the equation as

$$y^2 + 1 = x^3 + 8 = (x + 2)((x - 1)^2 + 3)$$

Since $(x - 1)$ is even, the second factor on the right hand side is a positive integer which is $\equiv 3 \pmod{4}$. This implies that the right hand side of the above equation is divisible by a prime p with $p \equiv 3 \pmod{4}$. So $y^2 \equiv -1 \pmod{p}$. But this is impossible since -1 is not a square modulo a prime which is $3 \pmod{4}$. We deduce that the original equation $y^2 = x^3 + 7$ has no integer solutions.

Here are two more examples which I didn't do in lectures:

Example. Find all integer solutions of $x^3 + 2y^3 + 4z^3 = 9w^3$. There is one obvious solution: $(0, 0, 0, 0)$. Now suppose that not all of x, y, z, w are 0. Then we let d be the greatest common divisor of x, y, z, w. Dividing through by d we get another solutions $(x/d, y/d, z/d, w/d)$, so we can assume that x, y, z, w have greatest common divisor 1.

For any integer a, $a^3 \equiv 0$ or $\pm 1 \pmod 9$. Since $x^3 + 2y^3 + 4z^3 \equiv 0 \pmod 9$, you can check that we must have $x^3 \equiv 2y^3 \equiv 4z^3 \equiv 0 \pmod 9$. So we have $x \equiv y \equiv z \equiv 0 \pmod 3$ and therefore $x^3 \equiv y^3 \equiv z^3 \equiv 0 \pmod{27}$. We deduce that $3|w$. But this contradicts the assumption that x, y, z, w have gcd 1 since we have shown that 3 divides all of them.

In this example, we used the fact that the equation was *homogeneous* (each term has the same degree) to divide through by common divisors and reduce to the case where a solution has no common factors.

Finally, we give another tricky example:

Example. Consider the equation $x^4 + x^3 + x^2 + x + 1 = y^2$.

We consider $f(x) = 4(x^4 + x^3 + x^2 + x + 1)$. Then

$$f(x) = (2x^2 + x)^2 + 3x^2 + 4x + 4 = (2x^2 + x)^2 + 3(x + 2/3)^2 + 8/3 > (2x^2 + x)^2$$

On the other hand,

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

Since we also have $f(x) = (2y)^2$, $f(x)$ cannot lie between the squares of consecutive integers, $2x^2 + x$ and $2x^2 + x + 1$. So we must have $(x + 1)(x - 3) < 0$. This means that we only get solutions with $x \in [-1, 3]$. By considering each possible value for x in turn and solving for y we get solutions $(-1, \pm 1), (0, \pm 1), (3, \pm 11)$.

Check your understanding.

(1) Explain why Theorem 10.2 implies $x^4 + y^4 = z^4$ has no solutions, and more generally why $x^{4k} + y^{4k} = z^{4k}$ has no solutions.

(2) Show that the equation $x^2 + y^2 = z^3$ has infinitely many solutions for x, y, z positive integers.

(*Hint:* For any $n > 3$, let $x = n(n^2 - 3)$ and $y = 3n^2 - 1$.)

(3) Find all integer solutions to

$$x^4 - 2x^3 - 9x^2 + 11x - 28 = 0.$$

(There is only one integer solution.)

(4) By considering the prime factorisations of x, y show that

$$x^3 = 5y^6$$

has no integer solutions.

(5) Find all integer solutions to

$$x^4 + 2x^2 + 4xy + 2y^2 - 1 = 0.$$

(*Hint:* Rewrite this as $(x^2)^2 + 2(x+y)^2 = 1$. For $x, y \in \mathbb{Z}$ notice that this implies $x + y = 0$.)

(6) Show that

$$x^6 + y^6 + 14z = 3$$

has no integer solutions.

(*Hint:* Use Fermat's little theorem.)