M3P14 Number Theory

Lectured by Prof Toby Gee
Typeset by David Kurniadi Angdinata

Autumn 2018

Contents

Lecture 1
Friday
05/10/18

0 Introduction

Roughly speaking number theory is the study of the integers. More specifically, problems in number theory often have a lot to do with primes and divisibility, congruences, and include problems about the rational numbers. For example, solving equations in integers or in the rationals, such as $x^2 - 2y^2 = 1$, etc. We will be looking at problems that can be tackled by elementary means, but this does not mean easy. Also the statements of problems can be elementary without the solution being elementary, such as Fermat's Last Theorem, or even known, such as the twin prime conjecture. Sometimes we will state interesting things, like the prime number theorem, without proving them. Typically these will be things that we could prove if the course was much longer. We will start the course with a look at prime numbers and factorisation, a review of Euclid's algorithm and consequences, congruences, the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$, RSA algorithm, and quadratic reciprocity. We will return to primes at the end, too. Typical questions here include the following.

1. How do you tell if a number is prime?
2. How many primes are there congruent to a modulo b for given a, b?
3. How many primes are there less than n?

A warning is that we will be using plenty of things from previous algebra courses, about groups, rings, ideals, fields, Lagrange's theorem, the first isomorphism theorem, and so on. You may want to revise this material if you are not comfortable with it. The course is not based on any particular book, although some material, such as continued fractions, was drawn from the following.

1. A Baker, A concise introduction to the theory of numbers, 1984

Not everything we will do is in that book, though.

1 Euclid's algorithm and unique factorisation

1.1 Divisibility

Definition 1. Let $a, b \in \mathbb{Z}$. We say that a **divides** b, written $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$. If a does not divide b, write $a \nmid b$.

Note. If $a, b, c \in \mathbb{Z}$ such that $a \mid b$ and $a \mid c$, then $a \mid (rb + sc)$ for any $r, s \in \mathbb{Z}$.

Definition 2. Let $a, b \in \mathbb{Z}$, not both zero. The **greatest common divisor** (gcd) or **highest common factor** (hcf) of a and b, written (a, b), is the largest positive integer dividing both a and b.

Such an integer always exists since if $a \neq 0$ and $c \mid a$, then $-a \leq c \leq a$.

Example. $(-10, 15) = 5$.

Note. This notation is consistent with notation from ring theory. The ring $\mathbb{Z}$ is a principal ideal domain (PID), that is it is an integral domain, and every ideal can be generated by one element. The ideal generated by $f_1, \ldots, f_n \in R$ for some ring R is usually written $(f_1, \ldots, f_n)$, and indeed the ideal (a, b) is generated by the highest common factor of a and b, by Theorem 6 below.

Definition 3. $n \in \mathbb{Z}$ is **prime** if n has exactly two positive divisors, namely 1 and n.

Note. By definition, primes can be both positive and negative. In spite of this, frequently when people talk about prime numbers they restrict to the positive case. In this course when we say 'Let p be a prime number' we will generally mean $p > 0$. Also 1 is not prime.

1.2 Euclid's algorithm

Proposition 4. Let $a, b \in \mathbb{Z}$, not both zero. Then for any $n \in \mathbb{Z}$, we have $(a, b) = (a, b - na)$.

Proof. By definition of (a, b), it suffices to show that any $r \in \mathbb{Z}$ divides both a and b if and only if it divides both a and $b - na$. But if r divides a and b, it clearly divides $b - na$, and if it divides a and $b - na$, it clearly divides b. □

This suggests an approach to computing (a, b) by replacing (a, b) by a pair $(a, b - na)$, and repeat until the numbers involved are small enough that it is easy to compute the greatest common divisor. The key to being able to do this is the following innocuous looking result.

Theorem 5. Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.

Proof. Let $q = \lfloor a/b \rfloor$ be the largest integer less than a/b. Then by definition $0 \leq a/b - q < 1$. Thus $0 \leq a - qb < b$, so we can take $r = a - bq$. Uniqueness is easy. □

This gives us **Euclid's algorithm** for finding (a, b) for any $a, b \in \mathbb{Z}$ not both zero. Without loss of generality, assume $0 \leq b \leq a$ and $a > 0$.

1. Check if $b = 0$. If so then $(a, b) = a$.
2. Otherwise, replace (a, b) with (b, r) as in Theorem 5. Then return to step 1.

Since at every stage $|a| + |b|$ is decreasing, this algorithm terminates. We have shown that $(a, b) = (b, r)$ so the output is always equal to (a, b).

Example. Let us make this explicit.

$$\begin{aligned} (120, 87) &= (87, 33) & 120 &= 87 + 33 \\ &= (33, 21) & 87 &= 2\,(33) + 21 \\ &= (21, 12) & 33 &= 21 + 12 \\ &= (12, 9) & 21 &= 12 + 9 \\ &= (9, 3) & 12 &= 9 + 3 \\ &= (3, 0) & 9 &= 3\,(3) + 10 \end{aligned}$$

Now run this backwards, writing out the equations.

$$\begin{aligned} 3 &= 12 - 9 \\ &= 12 - (21 - 12) \\ &= 2\,(12) - 21 \\ &= 2\,(33 - 21) - 21 \\ &= 2\,(33) - 3\,(21) \\ &= 2\,(33) - 3\,(87 - 2\,(33)) \\ &= 8\,(33) - 3\,(87) \\ &= 8\,(120 - 87) - 3\,(87) \\ &= 8\,(120) - 11\,(87)\,. \end{aligned}$$

The same works in general, that is the algorithm gives us more than just a way to compute (a, b). It also allows us to express (a, b) in terms of a and b.

Theorem 6. Let $a, b \in \mathbb{Z}$, not both zero. Then there exist $r, s \in \mathbb{Z}$ such that $(a, b) = ra + sb$.

Proof. Let $a_0 = a$ and $b_0 = b$, and for each i let (a_i, b_i) be the result after running i steps of Euclid's algorithm on the pair (a, b). For some r we have $a_r = (a, b)$ and $b_r = 0$. We will show, by downwards induction on i, that there exist $n_i, m_i \in \mathbb{Z}$ such that $(a, b) = n_i a_i + m_i b_i$. For $i = r$ this is clear. On the other hand, for any i we have $a_i = b_{i-1}$ and $b_i = a_{i-1} - q_i b_{i-1}$ for some $q_i \in \mathbb{Z}$. Thus if $(a, b) = n_i a_i + m_i b_i$, we have

$$(a, b) = n_i b_{i-1} + m_i\,(a_{i-1} - q_i b_{i-1}) = (n_i - m_i q_i)\,b_{i-1} + m_i a_{i-1},$$

and the claim follows. □

1.3 Unique factorisation

The fact that (a, b) is an integer linear combination of a and b has strong consequences for factorisation and divisibility. First note the following.

Proposition 7. Let $n, a, b \in \mathbb{Z}$, and suppose that $n \mid ab$ and $(n, a) = 1$. Then $n \mid b$.

Proof. Since $(n, a) = 1$, there exists $r, s \in \mathbb{Z}$ such that $rn + sa = 1$. Thus $rnb + sab = b$. But n clearly divides rnb and sab, so $n \mid b$. □

By definition, if n is prime, then either $n \mid a$ or $(n, a) = 1$. If $(n, a) = 1$, we say that n, a are **coprime**.

Lecture 2
Tuesday
09/10/18

Corollary 8. If p is prime, and $a, b \in \mathbb{Z}$ are such that $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof. If $p \nmid a$ then $(p, a) = 1$, so 7 implies $p \mid b$. □

Proposition 9. If $(a, b) = 1$, and $a \mid n$ and $b \mid n$, then $ab \mid n$.

Proof. By 6, we can write $n = n\,(a, b) = nra + nsb$ with $r, s \in \mathbb{Z}$. Each term is divisible by ab, so $ab \mid n$. □

We say that $m_1, \ldots, m_n \in \mathbb{Z}$ are **pairwise coprime** if $(m_i, m_j) = 1$ for all $i \neq j$.

Corollary 10. Suppose that $m_1, \ldots, m_n$ are pairwise coprime. If $m_i \mid N$ for all i, then $m_1 \ldots m_n \mid N$.

Proof. Induction on n. $n = 2$ is Proposition 9. (TODO Exercise) □

We can now prove the existence and uniqueness of prime factorisations.

Proposition 11. Every $n \in \mathbb{Z}^\times$ can be written as $\pm p_1 \ldots p_r$ for some $r \geq 0$ and some primes $p_1, \ldots, p_r$.

Proof. Use induction on $|n|$. The case $|n|$ is trivial, so suppose $|n| > 1$. Then either $|n|$ is prime, or $|n| = ab$ with $1 < a, b < |n|$, and by induction each of a, b is a product of primes. □

Theorem 12. Let $n \in \mathbb{Z}_{>0}$. Then n can be written as $p_1 \ldots p_r$ where the p_i are prime, and are uniquely determined up to reordering.

Proof. Existence is Proposition 11. For uniqueness, suppose that

$$n = p_1 \ldots p_r = q_1 \ldots q_s,$$

with p_i, q_i prime. Then without loss of generality suppose $r, s \geq 1$. Then $p_1 \mid p_1 \ldots p_r$, so $p_1 \mid q_1 \ldots q_s$. By Corollary 8, either $p_1 \mid q_1$ or $p_1 \mid q_2 \ldots q_s$. Proceeding inductively, eventually $p_1 \mid q_i$ for some i. Since q_i is prime this means $p_1 = q_i$. We then have

$$p_2 \ldots p_r = q_1 \ldots q_i \ldots q_s.$$

Since this product is smaller than n, by the inductive hypothesis we must have $r - 1 = s - 1$ and the p_i except p_1 are a rearrangement of the q_i except q_i. □

Put together, these are the fundamental theorem of arithmetic.

1.4 Linear diophantine equations

Suppose now that we are given $a, b, c \in \mathbb{Z}^\times$ and we want to solve $ax + by = c$ for $x, y \in \mathbb{Z}$. We first note that (a, b) divides both a and b, so for there to be any solutions, we must have $(a, b) \mid c$.

Example. $2x + 6y = 3$ has no solutions.

From now on, suppose this is true. Let $a' = a/(a,b)$, $b' = b/(a,b)$, and $c' = c/(a,b)$. Then $ax + by = c$ if and only if $a'x + b'y = c'$. By Theorem 6, since $(a', b') = 1$, we can find $r, s \in \mathbb{Z}$ with $a'r + b's = 1$, so $a'rc' + b'sc' = c'$. So $x = rc'$, $y = sc'$ is a solution. X, Y is another solution if and only if $a'X + b'Y = a'x + b'y$, if and only if $a'(X - x) = b'(y - Y)$. For this to hold, we need $a' \mid (y - Y)$, $b' \mid (X - x)$. Putting this all together, we find that if x, y is one solution to $ax + by = c$, then the other solutions are exactly of the form

$$X = x + n\frac{b}{(a,b)}, \qquad Y = y - n\frac{a}{(a,b)}$$

for all $n \in \mathbb{Z}$.

Example. Using the example above where we have $8(120) - 11(87) = 3$, we can solve $120x + 87y = 9$. One solution is $x = 24$ and $y = -33$. The general solution is $x = 24 + 29n$ and $y = -33 - 40n$. Taking $n = -1$, we have for example, $x = -5$ and $y = 7$.

2 Congruences and modular arithmetic

2.1 Congruences

Definition 13. Let $n \in \mathbb{Z}^\times$, and let $a, b \in \mathbb{Z}$. We say a is **congruent to** b **modulo** n, written $a \equiv b \mod n$, if $n \mid (a - b)$.

For n fixed, it is easy to verify that congruence modulo n is an equivalence relation, and therefore partitions $\mathbb{Z}$ into equivalence classes. The set of equivalence classes modulo n is denoted $\mathbb{Z}/n\mathbb{Z}$.

Example. If $a \equiv b \mod n$, $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.

In fact $\mathbb{Z}/n\mathbb{Z}$ is a ring, with the obvious addition and multiplication. Indeed $n\mathbb{Z} = \{nr \mid r \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ is just the quotient ring. For any $a \in \mathbb{Z}$, we sometimes write $\overline{a}$ for the image of a in $\mathbb{Z}/n\mathbb{Z}$. We can write $a = qn + r$ with $0 \leq r < n$. Then $a \equiv r \mod n$, so $\overline{a} = \overline{r}$.

Example. If $n = 12$, then $\overline{25} = \overline{1}$.

It follows that $0, \ldots, n - 1$ are representatives for the elements of $\mathbb{Z}/n\mathbb{Z}$, so every element of $\mathbb{Z}/n\mathbb{Z}$ is equal to $\overline{r}$ for some unique $r \in \{0, \ldots, n - 1\}$. It will also be convenient to write $\mathbb{Z}/n\mathbb{Z} = \{0, \ldots, n - 1\}$.

Example. If $n = 6$, we could write $3 + 4 = 1$ and $3 \times 4 = 0$.

Recall that if R is a commutative ring, a **unit** of R is an element with a multiplicative inverse, that is x such that there exists $y \in R$ with $xy = 1$. Write $R^\times$ for the set of units in R. This is a group under multiplication.

Example. $\mathbb{Z}^\times = \{\pm 1\}$ and $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\} = \{x \in \mathbb{Q} \mid x \neq 0\}$.

We want to understand $(\mathbb{Z}/n\mathbb{Z})^\times$. Which elements of $\{0, \ldots, n - 1\}$ are in $(\mathbb{Z}/n\mathbb{Z})^\times$? If $r \in \mathbb{Z}$ and $\overline{r} \in (\mathbb{Z}/n\mathbb{Z})^\times$ then there exists $s \in \mathbb{Z}$ such that $rs \equiv 1 \mod n$. This implies that $(r, n) = 1$. Conversely, if $(r, n) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $rx + ny = 1$, so $\overline{rx} = 1$, so $\overline{r}$ is a unit. Thus we have $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{i} \mid (i, n) = 1\}$.

Note. If p is a prime, then either $a \equiv 0 \mod p$ or $(a, p) = 1$, so $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \ldots, p - 1\}$. Thus every non-zero congruence class modulo p is a unit, that is $\mathbb{Z}/p\mathbb{Z}$ is a ring with the property that every non-zero element has a multiplicative inverse, so it is a field. Another equivalent way to see this is to check that $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

Lecture 3
Wednesday
10/10/18

2.2 Linear congruence equations

Fix $a, b \in \mathbb{Z}$ and $c \in \mathbb{Z}^\times$. Suppose we want to solve $ax \equiv b \mod c$. This is equivalent to finding x, y such that $ax + cy = b$. In particular, by our analysis of linear diophantine equations, there is a solution precisely when $(a, c) \mid b$. Furthermore, there is a unique solution modulo $c' = c/(a, c)$, because all the solutions are obtained by adding multiples of c' to our given x, and subtracting the corresponding multiple of $a/(a, c)$ from y. This implies that there are a total of (a, c) solutions to the original congruence modulo c. If x is a solution, the other solutions are of the form $X = x + c'j$ for $0 \leq j < (a, c)$. In particular, if $(a, c) = 1$, then there is a unique solution to $ax \equiv b \mod c$. Indeed $a \in (\mathbb{Z}/c\mathbb{Z})^\times$, so it has an inverse a^{-1}, and $x \equiv a^{-1}b \mod c$ is the unique solution.

Example. $2x \equiv 3 \mod 6$ has no solutions as $(2, 6) = 2 \nmid 3$. $2x \equiv 4 \mod 6$, which is equivalent to $x \equiv 2 \mod 3$, has solutions $x \equiv 2 \mod 6$ and $x \equiv 5 \mod 6$.

2.3 Chinese remainder theorem

Theorem 14 (Chinese remainder theorem)**.** Let $m_1, \ldots, m_n \in \mathbb{Z}_{\geq 0}$ be pairwise coprime. Then the natural map

$$\mathbb{Z}/m_1 \ldots m_n\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$$

is an isomorphism of rings, and the induced map

$$(\mathbb{Z}/m_1 \ldots m_n\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})^\times$$

is an isomorphism of abelian groups.

Remark. This is false without the assumption that m_i pairwise coprime, for example $m_1 = m_2 = 2$.

Proof. Note firstly that the map exists and is a ring homomorphism. This follows from the fact that if $x \equiv y \mod m_1 \ldots m_n$ then certainly $x \equiv y \mod m_i$ for each i. The source and target of the ring homomorphism both have order $m_1 \ldots m_n$, so it suffices to show that the map is injective to show that it is an isomorphism. So we only need to check that the kernel is zero. So we need to know that if $m_i \mid N$ for all i, that is $\overline{N} = 0$ in $\mathbb{Z}/m_i\mathbb{Z}$, then $m_1 \ldots m_n \mid N$, that is $\overline{N} = 0$ in $\mathbb{Z}/m_1 \ldots m_n\mathbb{Z}$. This is just Corollary 10. The statement about unit groups follows by noting that if R, S are rings, then $(R \times S)^\times = R^\times \times S^\times$. □

Note. This can be reformulated more concretely as a statement about congruences. It says that for any a_i, there is a unique $x \mod m_1 \ldots m_n$ such that $x \equiv a_i \mod m_i$. The proof does not tell us how to find x, but it is actually quite easy in practice. Here is one way to do it. Write $M = m_1 \ldots m_n$ and $M_i = M/m_i$. Choose q_i such that $q_i M_i \equiv 1 \mod m_i$, using Euclid's algorithm and $(M_i, m_i) = 1$ because $(m_j, m_i) = 1$ for all $j \neq i$. Then set

$$x = a_1 q_1 M_1 + \cdots + a_n q_n M_n.$$

For each i we have $M_j \equiv 0 \mod m_i$ if $i \neq j$, so $x \equiv a_i q_i M_i \equiv a_i \mod m_i$ for each i.

3 The structure of $(\mathbb{Z}/n\mathbb{Z})^\times$

For the next few lecture we will study the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$.

3.1 The Euler Φ function

We define a function $\Phi(n)$ on $\mathbb{Z}_{>0}$ by letting $\Phi(n)$ denote the order of $(\mathbb{Z}/n\mathbb{Z})^\times$. Explicitly we have $\Phi(n) = \#\{1 \leq i < n \mid (i, n) = 1\}$, that is $\Phi(n)$ is the number of integers between 0 and $n - 1$ coprime to n.

Example. If p is prime, $\Phi(p) = p - 1$.

Φ is called **Euler's Φ function**.

Definition 15. A function f on $\mathbb{Z}_{>0}$ is **multiplicative** if for all $m, n \in \mathbb{Z}$ such that $(m, n) = 1$, we have $f(mn) = f(m) f(n)$. We say f is **strongly multiplicative** if for any pair of $m, n \in \mathbb{Z}_{>0}$ we have $f(mn) = f(m) f(n)$.

Note. By the Chinese remainder theorem, Φ is multiplicative, because if $(m, n) = 1$ then $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, but not strongly multiplicative, since $\Phi(4) = 2 \neq 1 = \Phi(2)\Phi(2)$.

It is clear that a multiplicative function is determined by its values on prime powers. For p prime we have $(i, p^a) = 1$ if and only if p does not divide i, so $\Phi(p^a)$ is the number of integers between 0 and $p^a - 1$ that are not divisible by p. There are p^{a-1} numbers in this range divisible by p, so we have

$$\Phi(p^a) = \#\{1 \leq i < p^a \mid (i, p^a) = 1\} = \#\{1 \leq i < p^a \mid p \nmid i\} = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right).$$

Write $n = \prod_i p_i^{a_i}$ where p_i are distinct primes. From this and multiplicativity of Φ one has that

$$\Phi(n) = \prod_i \Phi(p_i^{a_i}) = \prod_i p_i^{a_i}\left(1 - \frac{1}{p_i}\right) = n\prod_i\left(1 - \frac{1}{p_i}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right),$$

where p runs over the primes dividing n.

3.2 Euler's theorem

The units $(\mathbb{Z}/n\mathbb{Z})^\times$ form a group under multiplication. By definition, $\phi(n)$ is the order of this group. Recall that for any group G of finite order d, Lagrange's theorem states that for all $g \in G$, g^d is the identity in G. For the group $(\mathbb{Z}/n\mathbb{Z})^\times$, this means the following.

Theorem 16 (Euler's theorem)**.** Let $a \in \mathbb{Z}$ with $(a, n) = 1$. Then $a^{\Phi(n)} \equiv 1 \mod n$.

Proof. This is equivalent to saying that $\overline{a}^{\Phi(n)} = 1$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. This is a group of order $\Phi(n)$, so this is immediate from Lagrange's theorem. □

Corollary 17 (Fermat's little theorem)**.** If p is a prime and $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$.

Proof. Theorem 16 with $n = p$, so $\Phi(n) = p - 1$. □

Of course knowing the order of an abelian group does not tell you its structure.

Example. Let $n = 5$. $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$. This has order 4. There are two isomorphism classes of abelian groups of order 4, namely $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. So it is either cyclic of order 4 or a product of two cyclic groups of order 2. $2^2 = 4$, $2^3 = 3$, $2^4 = 1$ in $(\mathbb{Z}/5\mathbb{Z})^\times$. So $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclic of order 4.

By the Chinese remainder theorem, to understand the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$, it is enough to understand the structure of $\mathbb{Z}/p^m\mathbb{Z}$ where p is prime and $m \geq 1$. We will do this next, beginning with the case $m = 1$.

Lecture 4
Friday
12/10/18

Definition 18. If G is a group and $g \in G$ is an element, the **order** of g is the least $a \geq 1$ such that $g^a = 1$. In particular, if $(g, n) = 1$, then we write $ord_n(g)$ for the order of g in $(\mathbb{Z}/n\mathbb{Z})^\times$, or the order of g modulo n.

Equivalently, let $n \in \mathbb{Z}_{>0}$ and $g \in \mathbb{Z}$ with $(g, n) = 1$, then the order of g modulo n is the smallest $a \in \mathbb{Z}_{\geq 0}$ such that $g^a \equiv 1 \mod n$.

Proposition 19. If G is a group and g is an element of order a, then $g^n = 1$ if and only if $a \mid n$.

Equivalently, let $g \in \mathbb{Z}$ with $(g, n) = 1$, then if $g^n \equiv \mod n$ then $ord_n(g) \mid n$.

Proof. If $n = ab$ then $g^n = (g^a)^b = 1^b = 1$. Conversely write $n = ab + r$ with $b, r \in \mathbb{Z}$ and $0 \leq r < a$. Then since $g^a = 1$ it follows that $g^r = 1$. Since $r < a$, r cannot be positive by the definition by order, so $r = 0$ and $n = ab$. □

In particular, if $(g,n)=1$, then $g^{\Phi(n)}=1$ by Euler's theorem, so Proposition 19 gives the order of g modulo n divides $\Phi(n)$. We are going to prove that if p is prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Equivalently, we need to show that there exists g such that $ord_p(g)=\Phi(p)=p-1$. We will do this by counting the number of elements of each order. Key point is that $\mathbb{Z}/p\mathbb{Z}$ is a field. For any $d\geq 1$, the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order dividing d are exactly the roots of the equation X^d-1 in $\mathbb{Z}/p\mathbb{Z}$ by Proposition 19.

Example. The equation $X^2=1$ has exactly two solutions modulo p for any prime p, namely ± 1, but it can have more modulo n if n is composite. If $n=15$, then $4,11$ are also solutions. $X^2-1\equiv 0 \mod n$ if and only if $n\mid (X+1)(X-1)$, so $15\mid (4+1)(4-1)$.

Definition 20. $g\in\mathbb{Z}$ with $(g,p)=1$ is a **primitive root modulo** p if the order of g modulo p is exactly $p-1$, equivalently, if $\overline{g}$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.

To prove that primitive roots exist, we require some results about roots of polynomials modulo p. Over the rational numbers we all know that a polynomial of degree d has at most d roots. This can fail over other rings.

Example. The polynomial x^2-x has the roots $0,1,3,4$ modulo 6. The issue here is that $\mathbb{Z}/6\mathbb{Z}$ is not a field.

Lemma 21. Let R be a commutative ring, and let $P(X)$ be a polynomial in X with coefficients in R. If $\alpha\in R$ has $P(\alpha)=0$, then there exists a polynomial $Q(X)$ with coefficients in R such that $P(X)=(X-\alpha)Q(X)$.

Example. If $R=\mathbb{Z}/15\mathbb{Z}$, $X^2-1=(X+1)(X-1)=(X+4)(X-4)$.

Proof. We proceed by induction on the degree of P, the degree zero case being clear. Suppose the result is true for polynomials of degree less than $d-1$, and let $P(X)$ have degree d. If the leading term of $P(X)$ is cX^d, so $P(X)=cX^d+\ldots$, let $S(X)=P(X)-cX^{d-1}(X-\alpha)$. We have $S(\alpha)=0$, and $S(X)$ has degree less than $d-1$. By induction, there exists $R(X)$ with coefficients in R such that we can write $S(X)=(X-\alpha)R(X)$. Set $Q(X)=cX^{d-1}+R(X)$. Then

$$(X-\alpha)Q(X)=(X-\alpha)\left(cX^{d-1}+R(X)\right)=cX^{d-1}(X-\alpha)+S(X)=P(X).$$

□

Theorem 22. Let F be a field, and $P(X)$ a polynomial of degree d with coefficients in F. Then $P(X)$ has at most d distinct roots in F.

Proof. We again proceed by induction on $d=\deg(P)$. The case $d=0$ is clear. If P has no roots, then we are done. Otherwise, $P(X)$ has degree d and let α be a root. By Lemma 21, we can write $P(X)=(X-\alpha)Q(X)$. Now if $P(\beta)=0$, then $(\beta-\alpha)Q(\beta)=0$, so since F is a field either $\beta=\alpha$ or β is a root of $Q(X)$. By the inductive hypothesis $Q(X)$ has degree $d-1$, so P has at most d roots and we are done by induction. □

As a corollary, we deduce the following.

Corollary 23. Let p be a prime, and let d be any divisor of $p-1$. Then there are exactly d elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order dividing d.

Equivalently, we have to show that the polynomial X^d-1 has exactly d roots modulo p.

Proof. Note that by Fermat's little theorem, $1,\ldots,p-1$ are all roots of $x^{p-1}-1$ modulo p. Thus $X^{p-1}-1$ has exactly $p-1$ roots. Now fix d dividing $p-1$ and write

$$X^{p-1}-1=\left(X^d-1\right)\left(\left(X^d\right)^{\frac{p-1}{d}-1}+\cdots+1\right)=\left(X^d-1\right)Q(X),\qquad \deg(Q)=p-1-d,$$

for a polynomial $Q(X)$. $Q(X)$ has integer coefficients so we can view it as a polynomial modulo p. Now $X^{p-1}-1$ has exactly $p-1$ roots, X^d-1 has at most d roots, and $Q(X)$ has at most $p-1-d$ roots by Theorem 22. We must therefore have equality in these inequalities, that is X^d-1 has exactly d roots modulo p. □

Another way of stating the corollary is to say that for any d dividing $p-1$, there are exactly d elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ whose order divides d.

Example. Let $p=7$. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ has

1. 1 element of order 1,
2. 2 elements of order dividing 2, so 1 element of order 2,
3. 3 elements of order dividing 3, so 2 elements of order 3, and
4. 6 elements of order dividing 6, so 2 elements of order 6.

Lemma 24. For any $n \geq 1$, we have $\sum_{d|n,\ d>0} \Phi(d) = n$.

Proof. For each $d \mid n$, the elements $i \in \{1,\dots,n\}$ with $(i,n) = n/d$ are precisely those of the form $i = (n/d)\,j$ with $1 \leq j \leq d$ and $(j,d) = 1$. There are exactly $\Phi(d)$ possibilities for j, so there are exactly $\Phi(d)$ such elements. Summing over all d, since the n/d run over all the divisors of n, we are done with the result. □

Theorem 25. Let p be a prime. Then for any d dividing $p-1$, there are exactly $\Phi(d)$ elements of order d in $(\mathbb{Z}/p\mathbb{Z})^\times$. In particular there are $\Phi(p-1)$ primitive roots modulo p, and $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Proof. We prove this by strong induction on d. The case $d=1$ is clear. Fix d. The inductive hypothesis tells us that for any d' dividing d and strictly less than d there are $\Phi(d')$ elements of exact order d'. On the other hand by Corollary 23 there are a total of d elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order dividing d. Thus the number of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order exactly d is

$$\Phi(d) = d - \sum_{d'|d,\ d'\neq d} \Phi(d').$$

precisely by Lemma 24. Now use inductive hypothesis. □

Lecture 5
Tuesday
16/10/18

We can now go on to the case of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for $n \geq 2$. Firstly we do the case $p > 2$.

Proposition 26. Let p be an odd prime and let $n \geq 1$. Then $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic.

Proof. Consider three cases.

$n=1$ Theorem 25.

$n=2$ Let g be a primitive root modulo p. Claim that either $g^{p-1} \not\equiv 1 \mod p^2$, and g is a generator for $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$, or $g^{p-1} \equiv 1 \mod p^2$, and $g+p$ is a generator for $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$. Either way, $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ is cyclic. Suppose firstly that $g^{p-1} \not\equiv 1 \mod p^2$. $g^{ord_{p^2}(g)} \equiv 1 \mod p^2$ gives $g^{ord_{p^2}(g)} \equiv 1 \mod p$, so we have by assumption

$$p-1 = ord_p(g) \mid ord_{p^2}(g) \mid \#\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times = \Phi\left(p^2\right) = p(p-1).$$

But $ord_{p^2}(g) \neq p-1$, as $g^{p-1} \not\equiv 1 \mod p^2$. So $ord_{p^2}(g) = p(p-1)$ as required. Now suppose that $g^{p-1} \equiv 1 \mod p^2$, and set $h = g+p$. It suffices to show that $h^{p-1} \not\equiv 1 \mod p^2$, as we can then apply the analysis above with h in place of g to show that $ord_{p^2}(h) = p(p-1)$ and $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ is cyclic. To see the claim, observe that if we expand with the binomial theorem, then we get

$$h^{p-1} = (g+p)^{p-1} \equiv g^{p-1} + (p-1)\,pg^{p-2} \equiv 1 + p(p-1)\,g^{p-2} \mod p^2,$$

and since $p \nmid (p-1)\,g^{p-2}$, $(g+p)^{p-1} \not\equiv 1 \mod p^2$, as required.

$n \geq 2$ We claim that if $ord_{p^2}(g) = p(p-1)$ then in fact $ord_{p^n}(g) = p^{n-1}(p-1)$ for all $n \geq 2$, so that in particular $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic. We do this by induction on n. So assume that $ord_{p^n}(g) = p^{n-1}(p-1)$. Then

$$p^{n-1}(p-1) = ord_{p^n}(g) \mid ord_{p^{n+1}}(g) \mid \Phi\left(p^{n+1}\right) = p^n(p-1).$$

So either $ord_{p^{n+1}}(g) = p^n(p-1)$, or $ord_{p^{n+1}}(g) = p^{n-1}(p-1)$. The statement that $ord_{p^{n+1}}(g) = p^n(p-1)$ is equivalent to showing that $g^{p^{n-1}(p-1)} \not\equiv 1 \mod p^{n+1}$. To do this, consider $g^{p^{n-2}(p-1)} \mod p^{n-1}$ and $g^{p^{n-2}(p-1)} \mod p^n$. Since $\Phi\left(p^{n-1}\right) = p^{n-2}(p-1)$, $g^{p^{n-2}(p-1)} \equiv 1 \mod p^{n-1}$ by Euler's theorem, so we may write

$$g^{p^{n-2}(p-1)} = 1 + p^{n-1}t.$$

Since $ord_{p^n}(g) = p^{n-1}(p-1)$ by assumption, $g^{p^{n-2}(p-1)} \not\equiv 1 \mod p^n$, that is $p \nmid t$. Then the binomial theorem shows that

$$g^{p^{n-1}(p-1)} = \left(g^{p^{n-2}(p-1)}\right)^p = \left(1 + p^{n-1}t\right)^p \equiv 1 + p^n t + \binom{p}{2} p^{2(n-1)}t^2 + \cdots + p^{p(n-1)}t^p \mod p^{n+1},$$

Now $r(n-1) \geq n+1$ if and only if $(r-1)n \geq r+1$. Since $p > 2$,

$$p \,\Big|\, \binom{p}{2} \qquad \Longrightarrow \qquad p^{n+1} \,\Big|\, p^{2n-1} = p^{2(n-1)+1} \,\Big|\, \binom{p}{2} p^{2(n-1)}.$$

So $g^{p^{n-1}(p-1)} \equiv 1 + p^n t \not\equiv 1 \mod p^{n+1}$, because $p \nmid t$. So the statement holds for $n+1$, and we are done by induction

□

Note. We used the hypothesis that $p \neq 2$ right at the end here. If $p = 2$ then we cannot ignore the higher order terms.

If $n = 1, 2$ then the proof of Proposition 26 did not use $p > 2$, and indeed

1. $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ is cyclic,
2. $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$ is cyclic of order 2, with 3 as a generator, but
3. this fails for higher powers, say $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ is not cyclic since $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod 8$, so every element has order two.

The key is the following lemma.

Lemma 27. For $n \geq 0$ we have $5^{2^n} \equiv 1 + 2^{n+2} \mod 2^{n+3}$.

Proof. Induction on n. The case $n = 0$ follows from $5 = 1 + 4$. Suppose that $5^{2^n} = 1 + 2^{n+2}t$ with t odd. Then

$$5^{2^{n+1}} = \left(1 + 2^{n+1}t\right)^2 = 1 + 2^{n+3}t + 2^{2(n+2)}t^2 = 1 + 2^{n+3}\left(t + 2^{n+1}t^2\right),$$

and since $n + 1 \geq 1$ and $t + 2^{n+1}t^2$ is odd we are done by induction. □

Proposition 28. If $n \geq 2$ then we have an isomorphism $(\mathbb{Z}/2^n\mathbb{Z})^\times \to (\mathbb{Z}/2\mathbb{Z}) \times \left(\mathbb{Z}/2^{n-2}\mathbb{Z}\right)$, so that in particular if $n \geq 3$ then $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic.

Proof. Consider the natural map

$$\langle -1 \rangle \times \langle 5 \rangle \to (\mathbb{Z}/2^n\mathbb{Z})^\times,$$

where if G is a group and $g \in G$ we write $\langle g \rangle$ for the cyclic subgroup $\left\{1, \ldots, g^{ord(g)-1}\right\}$ of G generated by g. We claim that this map is an isomorphism. To see this, note that it is injective, because if $(-1)^r(5)^s \equiv 1 \mod 2^n$ then in particular $(-1)^r(5)^s \equiv 1 \mod 4$ so $(-1)^r \equiv 1 \mod 4$, so we must have $r = 1$ and $5^s \equiv 1 \mod 2^n$, that is $5^s = 1$ in $\langle 5 \rangle$. $\langle -1 \rangle \cong \mathbb{Z}/2\mathbb{Z}$ has order 2 and $\langle 5 \rangle \cong \mathbb{Z}/2^{n-2}\mathbb{Z}$ has order $ord_{2^n}(5) = 2^{n-2}$ by Lemma 27. So $\langle -1 \rangle \times \langle 5 \rangle$ has order $2\left(2^{n-2}\right) = 2^{n-1} = \Phi(2^n) = \#(\mathbb{Z}/2^n\mathbb{Z})^\times$. So the map $\langle -1 \rangle \times \langle 5 \rangle \to (\mathbb{Z}/2^n\mathbb{Z})^\times$ is an injection of groups of the same order, so it is a bijection. □

Using what we have shown so far, one can conclude the following. See the first example sheet.

Theorem 29. Let $n \in \mathbb{Z}_{>0}$. The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if either

1. $n = 1, 2, 4$,
2. $n = p^r$ where p is an odd prime and $r \geq 1$, or
3. $n = 2p^r$ where p is an odd prime and $r \geq 1$.

Lecture 6
Wednesday
17/10/18

Note that while the existence of primitive roots is very useful both theoretically and computationally, there is no simple procedure for finding them in practice, beyond trial and error by guessing small values of g, and see if g is a generator. If p is prime then there are $\Phi(p-1)$ primitive roots modulo p, so they are plentiful, which means that you have a high probability of success, and so trying $2, 3, 5, 6, \ldots$ is a reasonable strategy, but note that trying 4 would not be a good idea. We could work out $1, \ldots, g^{p-2}$ and check these are distinct, but this would be inefficient. Better is to check that if q is any prime factor of $p-1$, then $g^{(p-1)/q} \neq 1$. This works, because if g is not a primitive root, then the order of g modulo p is a proper factor of $p-1$, so divides some $(p-1)/q$, so $g^{(p-1)/q} = 1$, while if $g^{(p-1)/q} \neq 1$ then $ord_p(g) \mid (p-1)$ and $ord_p(g) \nmid (p-1)/q$. If this holds for all $q \mid (p-1)$, then $ord_p(g) = p-1$, because otherwise it would be a proper divisor, and so would divide $(p-1)/q$ for some prime $q \mid (p-1)$.

Note. This does rely on being able to factor $p-1$, which is a hard problem in general. See the next section.

The work of computing powers of a^k modulo p can be done efficiently by repeated squaring followed by multiplication according to the binary expansion of k.

Example. Let us find a primitive root modulo $p = 31$. $p - 1 = 30 = (2)(3)(5)$. g is a primitive root if and only if $g^{15} \neq 1$, $g^{10} \neq 1$, $g^6 \neq 1$. It is easy to see that 2 does not work because $2^2 = 4$, $2^4 = 16$, $2^6 = 2$, but $2^10 = 2^15 = 1$ because $2^5 = 32 = 1$, so 2 is not a primitive root. We claim that 3 is a primitive root. We need to show that none of 3^6, 3^{10}, 3^{15} are 1.

$$3^2 = 9, \quad 3^4 = -12, \quad 3^8 = 20 \quad \Longrightarrow \quad 3^6 = 9(-12) = 16, \quad 3^{10} = 9(20) = 25, \quad 3^{15} = 3(25)(-12) = -1.$$

So 3 is a primitive root modulo 31, as required.

4 Primality testing and factorisation

The basic idea of this section, which will be exploited in the next brief section on cryptography, is that checking whether $n \in \mathbb{Z}$ is prime or not is easy, but factorising n is expected to be hard, even if we know that it is not prime. Actually, there is no proof that factorisation is hard, merely an expectation. We will not make the notions of easy and hard precise, but the difficulty should be measured in terms of $\log n$, that is in terms of the number of digits of n in some base. Easy here means that there is an algorithm to check whether n is prime or not which runs in time polynomial in $\log n$. Then it is known that there exists a deterministic algorithm, the Agrawal-Kayal-Saxena (AKS) algorithm in 2005, to check whether or not n is prime which runs in time which is polynomial in $\log n$. We will not describe this algorithm, although it is fairly elementary. We will discuss another algorithm which is more effective than this in practice. In contrast it is unknown whether or not there is an algorithm for factorising n that runs in time polynomial in $\log n$, but it is suspected that no such algorithm should exist. There are algorithms better than exponential in $\log n$, but nothing close to polynomial time.

4.1 Factorisation

One way to check if n is prime or not is to try dividing by all primes up to $\sqrt{n}$, because if d is a proper divisor of n, then either $d \leq \sqrt{n}$ or $n/d \leq \sqrt{n}$. This is fine if you are factoring a small integer in your head, but hopeless if you want to factor numbers which are hundreds of digits long on a computer.

Note. If you want to check primality or factorise relatively small numbers, there are tricks. In particular, if you want to check divisibility by 2, 3, 5, 7, or 11 there are the following tests.

1. Checking by divisibility by 2 or 5 is easy, just a matter of looking at the last decimal digit.

2. For 3 and 11, we have $10 \equiv 1 \mod 3$ and $10 \equiv -1 \mod 11$, so

$$\sum_{i=0}^{\log n} a_i 10^i \equiv \sum_{i=0}^{\log n} a_i \mod 3, \qquad \sum_{i=0}^{\log n} a_i 10^i \equiv \sum_{i=0}^{\log n} a_i (-1)^i \mod 11,$$

   so we can check divisibility by taking the sum of the decimal digits for 3 or 9, and taking the alternating sum for 11.

3. For 7 things are slightly more awkward, but there is the following observation. $10x + y \equiv 0 \mod 7$ if and only if $-2(10x + y) \equiv 0 \mod 7$ if and only if $x - 2y \equiv 0 \mod 7$. So we can repeatedly subtract off twice the last digit from the number formed by removing the last digit.

If we wanted to factor three digit numbers, or small four digit numbers, say $n \leq 400$ is composite, with paper or calculator, then n has a prime factor $d \leq \sqrt{400} = 20$. Then we only have to worry about checking divisibility by primes up to 19. If n is not divisible by $2, 3, 5, 7, 11$, then the smallest prime factor of n is at least 13. So with these tests we only have difficulties if the only prime factors are 13, 17, 19, where there are no good tests. Since $13^3 > 400$, it can have at most 2 prime factors. If you can recognise the squares 169, 289, 361, then you only have to remember a short list $13 \times 17 = 221$, $13 \times 19 = 247$, $13 \times 23 = 299$, $13 \times 29 = 377$, $17 \times 19 = 323$, $17 \times 23 = 391$.

Example. $143 \equiv 1 - 4 + 3 \equiv 0 \mod 11$, $144 \equiv 1 + 4 + 4 \equiv 0 \mod 9$, and $154 \equiv 15 - 2(4) = 7 \equiv 0 \mod 7$.

Lecture 7
Friday
19/10/18

In fact, there is a method due to Fermat which allows you to factor even four digit numbers by hand, if you really have to. Idea is to first eliminate small prime factors by hand, up to say $p = 2, \ldots, 19$. If n is composite and does not have any small factors, the remaining possibility is that if n has prime factors, they are close together to $\sqrt{n}$, as in the exceptional cases we considered in the last paragraph. Now, if $n = ab$ with $a \leq b$ both odd, then we can write

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

If you know $(a+b)/2$ and $(b-a)/2$, you can recover a, b. This suggests the following procedure. If n is a square, we are done. If not, let m be the least integer with $m^2 \leq n < (m+1)^2$, and check if $(m+1)^2 - n$ is a square. If it is not, try $(m+2)^2 - n$, and so on. Once you can write $y^2 - n = x^2$ then $n = y^2 - x^2 = (y+x)(y-x)$ and we have a factorisation.

Example. If $n = 6077$, then you find that $77^2 < 6077 < 78^2$, and

$$\begin{aligned} 78^2 - 6077 &= 7, \\ 79^2 - 6077 &= 164, \\ 80^2 - 6077 &= 323, \\ 81^2 - 6077 &= 484 = 22^2, \end{aligned}$$

so $6077 = 81^2 - 22^2 = 103 \times 59$.

In the worst case even the combination of trial division and the Fermat method run in time which is exponential in $\log n$. The fastest algorithms known for factoring n run in better than exponential time in $\log n$ are subexponential. They are the quadratic sieve, Lenstra elliptic curve factorisation, and the general number field sieve. They are all significantly more complicated, although at least the **quadratic sieve** could be described in this course if we wanted to. Rather than go through it in detail, we just give a sense of the idea using an example.

Example. Imagine trying to factor $n = 1649$ using the Fermat method. Since $40^2 < 1649 < 41^2$, we compute

$$41^2 - 1649 = 32 = 2^5,$$
$$42^2 - 1649 = 115 = 5 \times 23,$$
$$43^2 - 1649 = 200 = 2^3 \times 5^2.$$

We certainly have not factored it yet, as none of these is a square, and indeed we would have to do another fourteen steps to find a factor. However, $32 \times 200 = 2^8 \times 5^2 = 80^2$. This means that we have a congruence

$$\left(2^5 \times 2^3 \times 5^2\right)^2 = (41 \times 43)^2 \equiv 80^2 \mod 1649.$$

Since $41 \times 43 = 1763 \equiv 114 \mod 1649$, this means that $1649 \mid (114 + 80)(114 - 80) = 194 \times 34 = 2^2 \times 17 \times 97$ and indeed $1649 = 17 \times 97$.

This is the basic idea of the quadratic sieve. In order to factor n, rather than trying to find numbers a, b with $a^2 - b^2 = n$, you try to find them with $a^2 \equiv b^2 \mod n$. Then you can hope that one of $a \pm b$ has a common factor with n.

Note. For illustration we factored $a \pm b$ above, but in general a better idea for the last step would be to compute the gcd $(a \pm b, n)$, $(194, 1649) = 97$ and $(34, 1649) = 17$, quickly using Euclid's algorithm.

How do we find congruences like this? To make this into an efficient algorithm, the idea is that it is easy to spot relations like the one we found if the numbers have only small prime factors. In fact, we can turn it into a linear algebra problem over the field with two elements $\mathbb{Z}/2\mathbb{Z}$, in the following way. Suppose that we have a set $x_1, \ldots, x_r \in \mathbb{Z}$ and we want to find a product of a subset of them which is a square. If we know the prime factorisation for the x_i, we can write $x_i = p_1^{a_{i1}} \ldots p_k^{a_{ik}}$, then we are trying to find $\epsilon_i \in \{0, 1\}$ such that $\prod_{i=1}^r x_i^{\epsilon_i}$ is a square. Equivalently, for each $1 \leq j \leq k$, want the exponent of p_j to be even, that is we have $\sum_{i=1}^r \epsilon_i a_{ij} = \epsilon_1 a_{1j} + \cdots + \epsilon_r a_{rj} \equiv 0 \mod 2$. This is just a linear algebra question.

Example. Let $x_1 = 2^5$, $x_2 = 5 \times 23$, $x_3 = 2^3 \times 5^2$. If we just look at the numbers above which only had small primes less than or equal to 5 in their factorisations, then we are looking at x_1 and x_3. Taking $p_1 = 2$ and $p_2 = 5$, we need to solve

$$\begin{pmatrix}\epsilon_1 & \epsilon_2\end{pmatrix}\begin{pmatrix}5 & 0\\ 3 & 2\end{pmatrix} \equiv \begin{pmatrix}0 & 0\end{pmatrix} \mod 2 \qquad \Longleftrightarrow \qquad \begin{pmatrix}\epsilon_1 & \epsilon_2\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix}$$

in the field $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$, that is $\epsilon_1 + \epsilon_2 = 0$, which has the non-trivial solution $\epsilon_1 = \epsilon_2 = 1$.

This step, solving linear equations in $\mathbb{Z}/2\mathbb{Z}$, can be done efficiently. In order to make this into a practical algorithm to factor n, the remaining difficulty is to find a good supply of $m \in \mathbb{Z}$ such that $m^2 - n$ is smooth, in the sense that it only has small prime factors.

Note. This is something that you could try to do by trial division. Once we had decided above that we only wanted prime factors up to 5, we could just keep dividing $a^2 - n$ by 2, 3, 5, and if we did not get to 1 then we could throw the number away. In practice, there are faster ways to proceed, which is where the sieve in quadratic sieve comes from.

The basic idea is if we fix a list of small primes to start with, we use congruence conditions on m, because for each prime $2 < p \nmid n$, there will be zero or two possible values for m in $m^2 \equiv n \mod p$. It turns out that there is a straightforward algorithm for solving $m^2 \equiv n \mod p$, which is part of the theory of quadratic residues, which we will get to shortly. If you do this for lots of primes p, you get a supply of congruence conditions for m, so you can eliminate ever considering m such that $m^2 - n$ has large prime factors.

Example. It is easy to check that $m^2 \equiv 1649 \mod 3$ has no solutions, so there would have been no point in looking for 3, and if we want 5 to be a factor of $m^2 - 1649$ then we need $x \equiv \pm 2 \mod 5$, and so on.

Lecture 8
Tuesday
23/10/18

4.2 Testing primality

By Euler's theorem if $(a,n)=1$ then $a^{\Phi(n)} \equiv 1 \mod n$. In particular, if p is prime then $a^{p-1} \equiv 1 \mod p$ for all $1 \leq a \leq p-1$. Conversely, if we can find an $1 \leq a < n$ with $a^{n-1} \not\equiv 1 \mod n$, then n is not prime. Even just taking $a=2$ in $2^{n-1} \not\equiv 1 \mod n$ is often enough to show that n is not prime, and using repeated squaring this can be checked quickly.

Example. To check if 9 is prime, we can compute $2^8 \equiv 2^{2^{2^2}} \equiv 4^{2^2} \equiv 7^2 \equiv 4 \mod 9$.

However it does not always work. $341 = 11 \times 31$ has $2^{340} \equiv 1 \mod 341$. In general even varying a is not enough. A **Carmichael number** is a composite number such that for all $(a,n)=1$ then $a^{n-1} \equiv 1 \mod n$. It is known that infinitely many of them exist, a hard theorem, although they are rare. See the example sheet for an example of a few of them. A variant on this idea gives an efficient primality test, the **Miller-Rabin test**, a test for whether $n \in \mathbb{Z}$ is prime or not. We restrict ourselves to considering the case that $n \equiv 3 \mod 4$, as the essential idea is already clear in this case, but the analysis is more complicated in the case $n \equiv 1 \mod 4$, in an example sheet. Of course if n is even we do not need a primality test. The key point is the following.

Lemma 30. If $n \equiv 3 \mod 4$, then n is prime if and only if for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have $a^{(n-1)/2} \equiv \pm 1 \mod n$.

Proof. Suppose firstly that n is prime. Then $a^{n-1} \equiv 1 \mod n$ by Fermat's little theorem, so $\left(a^{(n-1)/2}\right)^2 \equiv 1 \mod n$, so $a^{(n-1)/2} \equiv \pm 1 \mod n$, because n is prime, the equation $x^2=1$ has just the roots ± 1 in $\mathbb{Z}/n\mathbb{Z}$. Suppose next that $n=p^k$ for p prime is a prime power with $k \geq 2$, and take $a = 1+p$. Then

$$(1+p)^{\frac{n-1}{2}} \equiv 1 + \left(\tfrac{n-1}{2}\right) p \mod p^2,$$

by the binomial theorem. If $(1+p)^{(n-1)/2} \equiv \pm 1 \mod p^k = n$, then $(1+p)^{(n-1)/2} \equiv \pm 1 \mod p, p^2$ gives

$$\pm 1 \equiv (1+p)^{\frac{n-1}{2}} \equiv 1 + \left(\frac{n-1}{2}\right) p \equiv 1 \mod p \qquad \Longrightarrow \qquad 1 \equiv (1+p)^{\frac{n-1}{2}} \equiv 1 + \left(\frac{n-1}{2}\right) p \mod p^2,$$

then $p \mid ((n-1)/2)$, so $p \mid (n-1)$. But $p \mid n$, a contradiction. Finally for the remaining case suppose that n is composite but not a power of a prime, and write $n = rs$ for $r, s > 1$ and odd, and $(r,s)=1$. By the Chinese remainder theorem, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$. We can choose a with $(a,n)=1$ such that $a \equiv -1 \mod r$ and $a \equiv 1 \mod s$. Then $(a,r) = (a,s) = 1$, so $(a,n)=1$. Since $n \equiv 3 \mod 4$ by assumption, $(n-1)/2$ is odd, so $a^{(n-1)/2} \equiv -1 \mod r$ and $a^{(n-1)/2} \equiv 1 \mod s$. So $a^{(n-1)/2} \not\equiv \pm 1 \mod n$. □

So we know that if n is composite, there will exist values of a with $a^{(n-1)/2} \not\equiv \pm 1 \mod n$. To understand how efficient the algorithm is, we need to know how many such a there are.

Lemma 31. Suppose that $n \equiv 3 \mod 4$ and that n is composite. Then the set of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ satisfying $a^{(n-1)/2} \equiv \pm 1 \mod n$ is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. That it is a subgroup follows easily from the definition. Just check that it is closed under products and inverses. Certainly $1^{(n-1)/2} \equiv 1 \mod n$. If $a^{(n-1)/2} \equiv \pm 1 \mod n$ and $b^{(n-1)/2} \equiv \pm 1 \mod n$,

$$(ab)^{(n-1)/2} \equiv a^{(n-1)/2} b^{(n-1)/2} \equiv (\pm 1)(\pm 1) \equiv \pm 1, \quad \left(a^{-1}\right)^{(n-1)/2} \equiv \left(a^{(n-1)/2}\right)^{-1} \equiv (\pm 1)^{-1} \equiv \pm 1 \mod n.$$

So this set is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. That it is a proper subgroup is then immediate from Lemma 30. □

We immediately get the following bound.

Corollary 32. Suppose that $n \equiv 3 \mod 4$ and that n is composite. Then at most half of the values of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ satisfy $a^{(n-1)/2} \equiv \pm 1 \mod n$.

Proof. The set of such elements is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ by Lemma 31, and any proper subgroup has index at least two. □

In fact we can do better than this. It can be shown with some more work that you can improve this to show that at least 3/4 of the integers $1 \leq a \leq n-1$ satisfy $a^{(n-1)/2} \not\equiv \pm 1 \mod n$. It follows that if $n \equiv 3 \mod 4$ and you choose x integers $1 \leq a \leq n-1$ at random, and n is composite, then the probability that you find such an a with $a^{(n-1)/2} \not\equiv \pm 1 \mod n$ is at least $1 - 1/4^x$, so this gives an efficient polynomial time probabilistic random algorithm for testing if n is prime. If you want it to be deterministic, if you assume the generalised Riemann hypothesis (GRH), then it is known that you can find a counterexample $a \in \mathbb{Z}$ with

$$1 \leq a \leq \left\lceil 2 (\log n)^2 \right\rceil, \qquad a^{(n-1)/2} \not\equiv \pm 1 \mod n,$$

and again we have a polynomial time algorithm. In practice it is even better than this.

Example. If $n < 341550071728321$, it is enough to test $a = 2, 3, 5, 7, 11, 13, 17$.

5 Public-key cryptography

5.1 Messages as sequences of classes modulo n

How do we turn messages into numbers in $\mathbb{Z}/n\mathbb{Z}$? Since the advent of computers, the idea of representing a message by a string of numbers is a familiar one. In practice, to do this one typically chooses a way of encoding individual characters as binary numbers of a fixed length d, usually eight or sixteen bits, that is binary digits. If we then cut a message up into blocks or strings of at most k characters and concatenate the binary representations of each character in the block together, we obtain a dk bit binary number that represents an k character block as an integer between 0 and 2^{dk}. If we choose some very large modulus $n > 2^{dk}$, then we can alternatively represent a block as a class in $Z/n\mathbb{Z}$. Thus we will be mainly concerned with the problem of communicating a congruence class c modulo n, for some large n, between a sender A and a recipient B. The goal is to do this in such a way that any eavesdroppers on the communication cannot deduce what c is, but B can.

5.2 The Rivest-Shamir-Adleman (RSA) algorithm

Most traditional forms of cryptography rely on a shared secret known to both A and B. This shared secret is effectively some invertible function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. The idea is that rather than sending c to B directly, A applies f to c and computes $f(c)$, sends that to B, and then B applies some other function $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and computes $g(f(c))$, where $g = f^{-1}$, to get back the number A started with. Since eavesdroppers do not know f, they, at least in principle, cannot recover c from $f(c)$. In practice, for A and B to agree on a function f poses problems. In particular, they have to communicate to do so, and if eavesdroppers listen to that communication they can learn f. Want to be able to make f public without making g public. The algorithm we describe today avoids this problem completely. It is what is known as a public-key algorithm. Instead of secrets being shared between A and B, our recipient B creates a secret known only to B, his **private key**, and then releases additional information, his **public key**, to anyone who wants to communicate with him. For anyone to send B a message, only the public key is required, but decoding the message requires the private key. Here is how the algorithm works.

1. B first chooses two large prime numbers p and q and sets $n = pq$. In practice, each of these is around 2^{1024} or so. An integer modulo n thus allows B to represent 2048 bits of information, or 256 eight bit characters.

2. B also chooses a number e such that $(e, \Phi(n)) = 1$, and lets d be a multiplicative inverse of e modulo $\Phi(n)$ such that $de = 1 \mod \Phi(n) = (p-1)(q-1) = n - (p+q) + 1$.

3. The public key, that B publishes and shares with everyone, consists of the numbers n and e.

4. The private key, that B must keep secret, consists of the numbers p, q, $\Phi(n)$, and d.

5. To encode a message x, a sender A computes $f(x) \equiv x^e \mod n$, and sends it to B.

6. Given an encoded message y, B decodes it by computing $g(y) \equiv y^d \mod n$.

The reason this works is that if $y \equiv x^e \mod n$, then one has $(x^e)^d \equiv x^{ed} \equiv x^{1+k\Phi(n)} \mod n$, since, by construction, $de \equiv 1 \mod \Phi(n)$. Thus $y^d \equiv x^{ed} \equiv x^1 \equiv x \mod n$ by Euler's theorem, $x^{\Phi(n)} \equiv 1 \mod n$.

Note. This works provided x is coprime to n, but the probability of this is extremely high. It is still ok even without that, since n is squarefree. (TODO Exercise using Fermat's little theorem plus Chinese remainder theorem)

The prevailing assumption is that with only the information n and e, it is hopeless to discover d. Any eavesdropper who knows x^e and wants to recover x from x^e then has to be able to compute an e^{th} root of x modulo n. As far as we know, this is quite difficult computationally. The best publicly known approaches all involve factoring n. For numbers around 2^{2048}, this is not feasible with today's computing equipment, and might well never be feasible. On the other hand, we have no formal proof that factoring is as computationally difficult as it seems to be. As far as I am aware, we do not even have a formal proof that breaking RSA is as computationally difficult as factoring. In spite of these uncertainties, our intuition and experience suggests that recovering x from x^e without knowing a factorisation of n is computationally infeasible. It is this infeasibility that allows the cryptosystem to work.

Lecture 9 Wednesday 24/10/18

Lecture 9 is a problem class.

5.3 Signing with RSA

Lecture 10 Friday 26/10/18

Public-key cryptography can also be used as verification of identity. Suppose B wants to make a declaration to the world, and prove beyond all doubt that it was B who made the declaration, and not an impostor. Perhaps this declaration is a will, or acceptance of a contract, for instance. Suppose B has functions $f, g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $f \circ g = g \circ f = id$. Again, make f public, and any time B publishes a message m, B also publishes $g(m)$. Then anyone can apply f to $g(m)$ to recover $m = f(g(m))$, but without g, no one can forge B's signature. With RSA, B first represents the message he wants to sign as a class m modulo n. To sign this class, B computes m^d modulo n using the private part of the key, and sends the world the pair (m, m^d). Suppose A wants to verify that a pair (m, s) was a message signed by B. Then A computes s^e modulo n, which requires only the public part of the key. If $s \equiv m^d \mod n$, then $s^e = m^{de} \equiv m \mod n$. So A just needs to check that $s^e \equiv m \mod n$ and if so the signature is verified. To fake a message signed by B, a forger needs to solve the problem of, given a message m, finding a signature s such that $s^e \equiv m \mod n$. This is precisely the same problem as deciphering a message sent by the algorithm above. Thus forging signatures is just as hard as breaking the encryption.

5.4 Discrete logarithms

If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, for example, if n is prime, and g is a generator for this group, that is a primitive root, then the map $\mathbb{Z}/\Phi(n)\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^\times$ taking a modulo $\Phi(n)$ to g^a is an isomorphism, from the additive group of $\mathbb{Z}/\Phi(n)\mathbb{Z}$ to $(\mathbb{Z}/n\mathbb{Z})^\times$. It thus has an inverse, which we call the **discrete logarithm to the base** g. Explicitly, if g is a primitive root modulo n, then the discrete logarithm to the base g, denoted $\log_g$, is defined for any $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ by $\log_g(a) \equiv m \mod \Phi(n)$, for some unique $m \in \mathbb{Z}$ such that $0 \leq m < \Phi(n)$ and $g^m \equiv a \mod n$.

Example. One use of the discrete logarithm is to solve exponential equations modulo n. By applying $\log_g$ to both sides of the equation $x^r \equiv a \mod n$, write $x = g^y$, we obtain that the congruence becomes equivalent to the linear congruence equation $yr \equiv \log_g(a) \mod \Phi(n)$, and we can solve those with techniques explained earlier.

Unfortunately, or fortunately for cryptography, it is expected that the discrete logarithm is hard to compute, much in the way that it is expected to be hard to crack RSA, but we do not know for sure. In particular, there is no known polynomial time algorithm.

Example. Here is a practical application of this. Imagine that you have a system where you need to safely store passwords for different users, but you do not want to store the actual passwords. One way to do this is to let p be a large prime, big enough so that all passwords can be thought of as residues mod $(p-1)$, and fix a primitive root g modulo p. Then if someone inputs their password to be x, you can compute and store

g^x modulo p. If they later want to login with input y, you compute g^y, and check if it matches what you stored. If it does then $y \equiv x \mod p-1$. Even if someone has access to what you have stored, and to g, they still cannot recover the password a without solving the discrete logarithm problem. Of course, nor can you, so it is not so good if you require people to be able to be reminded of their passwords.

6 Quadratic reciprocity

6.1 Quadratic residues

Definition 33. Let p be a prime number and $a \in \mathbb{Z}$ not divisible by p, that is $(a,p)=1$. We say that a is a **quadratic residue modulo** p (QR) if and only if there exists a solution $x \in \mathbb{Z}$ to $x^2 \equiv a \mod p$. If no such d exists, so a is not a QR, it is called a **quadratic non-residue modulo** p (QNR).

Note. By this convention, $a \in \mathbb{Z}$ divisible by p are neither QRs nor QNRs modulo p. Other conventions exist, so sometimes zero is a QR.

Example. If $p=2$, 1 is a QR. If $p=3$, 1 is a QR, -1 is a QNR, since $1^2 \equiv (-1)^2 \equiv 1 \mod 3$. If $p=5$, $1,4$ are QRs, $2,3$ are QNRs, since $1^2 \equiv (-1)^2 \equiv 1 \mod 5$ and $2^2 \equiv 3^2 \equiv 4 \mod 5$.

Lemma 34. If $p>2$ then there are exactly $(p-1)/2$ QRs modulo p, and $(p-1)/2$ QNRs modulo p.

Proof. The QRs are exactly the image of the group homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ by $x \mapsto x^2$. This has kernel $x = \pm 1$, so the image has order $(p-1)/2$. □

Proposition 35. Let $a, b \in \mathbb{Z}$ with $(a,p) = (b,p) = 1$. Then

1. if a and b are both QRs modulo p, then so is ab,
2. if a is a QR modulo p and b is a QNR modulo p, then ab is a QNR modulo p, and
3. if a and b are both QNRs modulo p, then ab is a QR modulo p.

Proof. Note that the set H of QRs in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a subgroup, because it is the image of the group homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ by $x \mapsto x^2$ by Lemma 34, and by the first isomorphism theorem we have $(\mathbb{Z}/p\mathbb{Z})^\times / H \cong \mathbb{Z}/2\mathbb{Z}$. The proposition is a restatement of this, since $(\mathbb{Z}/p\mathbb{Z})^\times = H \sqcup 1 + H$. □

Definition 36. The **Legendre symbol** $\left(\frac{a}{p}\right)$, for p a prime and $a \in \mathbb{Z}$, is defined by

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

Proposition 35 above then amounts to saying that the map $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ defined by $a \mapsto \left(\frac{a}{p}\right)$ is a group homomorphism, that is $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right)$. Even holds if we do not assume that $(a,p) = (b,p) = 1$. In fact, the existence of primitive roots gives us an easy description of the following map.

Lecture 11
Tuesday
30/10/18

Theorem 37 (Euler's criterion)**.** Let p be an odd prime, and $a \in \mathbb{Z}$ not divisible by p. Then

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

Proof. Let g be a primitive root modulo p, and write $a \equiv g^r \mod p$ for $0 \le r < p-1$. Then $\left(g^{(p-1)/2}\right)^2 = g^{p-1} \equiv 1 \mod p$. So $g^{(p-1)/2} \equiv \pm 1 \mod p$. Since g is a primitive root, $g^{(p-1)/2} \not\equiv 1 \mod p$, so $g^{(p-1)/2} \equiv -1 \mod p$. So $a^{(p-1)/2} \equiv (g^r)^{(p-1)/2} \equiv \left(g^{(p-1)/2}\right)^r = (-1)^2 \mod p$. But

$$\begin{aligned} \left(\frac{a}{p}\right) = 1 \quad &\iff \quad (g^s)^2 \equiv a \mod p \quad &&\iff \quad 2s \equiv r \mod p-1 \\ &\iff \quad 2 \mid r \quad &&\iff \quad (-1)^r \equiv 1 \mod p, \end{aligned}$$

and we are done. □

6.2 Computing Legendre symbols

Euler's criterion lets us determine, for fixed p, which a are QRs modulo p. What if we fix a, and ask for which odd primes p is a a QR? When $a = -1$, Euler's criterion gives an easy answer. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, so -1 is a QR modulo p if and only if $(p-1)/2$ is even. In other words, the following holds.

Proposition 38. $-1 \in \mathbb{Z}$ is a QR modulo p if and only if $p = 2$ or $p \equiv 1 \mod 4$.

Proof. $p = 2$ is trivial. If $p > 2$, then by Euler's criterion, $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \mod p$, so in fact $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Then

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}.$$

□

Example. If $p = 5$ then it is a square, and if $p = 7$ it is not, and in each case we can check directly.

When $a = 2$, the situation is more difficult, but still amenable to a direct approach.

Proposition 39 (A special case of Gauss' Lemma)**.**

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases},$$

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

Example. $\left(\frac{2}{7}\right) = 1$ since $2 \equiv 3^3 \mod 7$. $\left(\frac{2}{11}\right) = -1$ since squares modulo 11 are $1, 4, 9, 5, 3$. $\left(\frac{-1}{11}\right) = -1$, so $\left(\frac{-2}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{-1}{11}\right) = (-1)^2 = 1$ and $-2 \equiv 3^2 \mod 11$.

Proof. $\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \mod p$ by Euler's criterion. Let $q = (p-1)/2$, and set

$$Q = (2)(4)\ldots(p-3)(p-1) = (2\times 1)(2\times 2)\ldots(2\times(q-1))(2\times q) = 2^q q! = 2^{\frac{p-1}{2}} q!.$$

Reduce all the factors in the product defining Q modulo p so that they lie between $-q$ and q, that is subtract p from every factor which is greater than q. Let Q' be the resulting product $(2)(4)\ldots(-3)(-1)$. We have $Q' \equiv Q \mod p$. On the other hand, the factors in the product defining Q' are the even integers from 1 to q and the negatives of the odd integers from 1 to q. Thus $Q' = (-1)^r q!$, where r is the number of odd integers between 1 and q. We thus have $2^q q! \equiv (-1)^r q! \mod p$, and since $p \nmid q!$, we have $2^{(p-1)/2} \equiv (-1)^r \mod p$. The result follows by noting that

$$(-1)^r = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases},$$

and invoking Euler's criterion. □

Example. If $p \equiv 1 \mod 8$, say $p = 1 + 8n$, so $q = 4n$. Odd integers in $1, \ldots, 4n$ are $1, \ldots, 4n-1$, so $r = 2n$.

Since we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, to answer this question in full generality it suffices to answer it for $a = -1$, for $a = 2$, and for a an odd prime. In the latter case we have the following.

Theorem 40 (Law of quadratic reciprocity)**.** Let p and q be odd primes. Then

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & p \equiv q \equiv 3 \mod 4 \\ \left(\frac{q}{p}\right) & \text{otherwise} \end{cases}.$$

One can rephrase this a bit more tersely as the equivalent statement

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

Note that this implies that for each odd prime q, the question of whether q is a QR modulo p has an answer in terms of congruence conditions modulo q and modulo 4. From this and the Chinese remainder theorem, we can deduce that the question, for which primes p is a a QR modulo p, has an answer in terms of congruence conditions on p.

Example. If $p \neq 5$ is an odd prime, then we see that 5 is QR modulo p if and only if p is a QR modulo 5, so $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, that is if and only if $p \equiv \pm 1 \mod 5$. So

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 5 \\ -1 & p \equiv \pm 2 \mod 5 \end{cases}.$$

Example. Slightly more complicated example, let $p \neq 3$ be an odd prime. When is 3 a QR modulo p, that is what is $\left(\frac{3}{p}\right)$? Well, if $p \equiv 1 \mod 4$ then this is if and only if p is a QR modulo 3, so if and only if $p \equiv 1 \mod 3$, so

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1 \mod 3 \\ -1 & p \equiv -1 \mod 3 \end{cases}.$$

If $p \equiv -1 \mod 4$ then if and only if $p \equiv -1 \mod 3$, so

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv -1 \mod 3 \\ -1 & p \equiv 1 \mod 3 \end{cases}.$$

Putting this together with the Chinese remainder theorem,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 12 \\ -1 & p \equiv \pm 5 \mod 12 \end{cases}.$$

If $p = 7$, QRs are $1, 2, 4$, so $\left(\frac{3}{p}\right) = -1$. If $p = 11$, $5^2 \equiv 3 \mod 11$, so $\left(\frac{3}{p}\right) = 1$.

In general to compute $\left(\frac{a}{p}\right)$, we could do the following. Use that if $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. So without loss of generality $|a| < p$. Then write $a = \pm \prod_i q_i^{s_i}$ for q_i prime. Then $\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \prod_i \left(\frac{q_i}{p}\right)^{s_i}$. If s_i is even, then $\left(\frac{q_i}{p}\right)^{s_i} = 1$. If s_i is odd, then $\left(\frac{q_i}{p}\right)^{s_i} = \left(\frac{q_i}{p}\right)$. We have formulas for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$. If q is an odd prime, $q < p$, then use quadratic reciprocity to relate $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$. Then repeat modulo q.

Example. $\left(\frac{6}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{3}{19}\right) = (-1)(-1) = 1$. $\left(\frac{2}{19}\right) = -1$ because $19 \equiv 3 \mod 8$. $\left(\frac{3}{19}\right) \equiv -1 \mod 12$ by the above.

More generally, one can ask, given a monic polynomial f with integer coefficients, for which primes p does f have a root? The above case is the case of the polynomial $X^2 - a$. This is a very deep question in number theory. Indeed, we are still extremely far from having a complete answer. One question it is natural to ask is, for which f does the above question have an answer given in terms of congruence conditions on p. A deep branch of algebraic number theory called class field theory tells us that this will happen precisely when the field extension determined by f has abelian Galois group. Beyond this we know very little, but there are connections to the theory of modular forms.

Lecture 12
Wednesday
31/10/18

6.3 Proof of quadratic reciprocity

Quadratic reciprocity was one of the deepest results of the 18^{th} century, and there are many approaches to proving it, none of which are particularly simple. The more motivated ones require algebraic number theory, and even then the motivation is really coming from class field theory, which is a long way beyond the boundaries of this course. The proof that we give is due to Rousseau, from 1991. It has the merits of

being elementary and relatively easy to remember, and of resembling the proof of Gauss' Lemma that we gave above, that $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Let p, q be distinct odd primes, and consider the group

$$(\mathbb{Z}/pq\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times .$$

What are we going to do is to compare the products of different sets of coset representatives for the subgroup $\{\pm 1\}$. That is, we will look at different ways of choosing exactly one element of each pair $\{x, -x\}$ for each $x \in (\mathbb{Z}/pq\mathbb{Z})^\times$. We will always write everything as a pair $(\alpha, \beta) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. Firstly we recall from the first example sheet.

Theorem 41 (Wilson's theorem)**.** If p is prime then $(p-1)! \equiv -1 \mod p$.

Write $P = (p-1)/2$, $Q = (q-1)/2$, and $R = (pq-1)/2 = pQ + P$. As out first set of coset representatives, consider the product of all the pairs

$$\left\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \mid 1 \le x \le P,\ 1 \le y \le q-1\right\}.$$

Let A be the product of these coset representatives. Then the product of the y-coordinates is $(q-1)!^P \equiv (-1)^P \mod q$. The product of the x-coordinates is $P!^{q-1}$ in the same way, so

$$A = \prod_{1\le x\le P,\ 1\le y\le q-1} (x, y) = \left(P!^{q-1}, (-1)^P\right).$$

Similarly we let the second set of representatives be all the pairs

$$\left\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \mid 1 \le x \le p-1,\ 1 \le y \le Q\right\}.$$

Let B be the product of these representatives. In the same way by symmetry, we get

$$B = \prod_{1\le x\le p-1,\ 1\le y\le Q} (x, y) = \left((-1)^Q, Q!^{p-1}\right).$$

For the third set of representatives, select the pairs in $\mathbb{Z}/pq\mathbb{Z}$ which correspond via the Chinese remainder theorem to the set

$$\{1 \le i \le R \mid (i, pq) = 1\}.$$

Let C be the product of these coset representatives. Let us figure out the product of the x-coordinates. It is

$$\prod_{i=1,\ (i,pq)=1}^{R} i.$$

Since

$$\prod_{i=1,\ (i,pq)=1}^{R} i = \left(\prod_{i=1,\ (i,pq)=1}^{pQ} i\right)\left(\prod_{i=pQ+1,\ (i,p)=1}^{pQ+P} i\right), \tag{1}$$

$$\prod_{i=1,\ (i,pq)=1}^{R} i = \left(\prod_{i=1,\ (i,p)=1}^{R} i\right) \Bigg/ \left(\prod_{i=1,\ (i,p)=1,\ q|i}^{R} i\right), \tag{2}$$

$$\prod_{i=1,\ (i,p)=1,\ q|i}^{R} i = \prod_{j=1,\ (j,p)=1}^{P} qj = q^P P!, \tag{3}$$

combining (1), (2), (3), get that the x-coordinate of the product is

$$\prod_{i=1,\ (i,pq)=1}^{R} i = \frac{(p-1)!^Q P!}{q^P P!} = \frac{(-1)^Q}{q^P}.$$

So by symmetry we have the product of these representatives

$$C = \left(\frac{(-1)^Q}{q^P}, \frac{(-1)^P}{p^Q} \right) = \left((-1)^Q \left(\tfrac{q}{p}\right), (-1)^P \left(\tfrac{p}{q}\right) \right),$$

by Euler's criterion. Now, we can compare A, B, C. We know that they all agree up to sign, that is up to possibly multiplication by ± 1, that is up to multiplication by the pair $(-1,-1) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. Comparing the y-coordinates, we have $C = \left(\frac{p}{q}\right) A$ and comparing the x-coordinates, similarly $C = \left(\frac{q}{p}\right) B$. So

$$B = \left(\tfrac{q}{p}\right)\left(\tfrac{p}{q}\right) A.$$

But we can compare A and B more directly. To go between A and B we need to swap the signs of all the PQ elements of the form (x,y) with $1 \le x \le P$ and $Q \le y \le q-1$. So $B = (-1)^{PQ} A$. So $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{PQ}$, that is $\left(\frac{q}{p}\right) = (-1)^{PQ}\left(\frac{p}{q}\right)$.

6.4 Jacobi symbols

While it is often quite straightforward to compute Legendre symbols using quadratic reciprocity, there is one serious difficulty, which is that in order to compute $\left(\frac{a}{p}\right)$, we need to factor a, and we do not know a polynomial time algorithm for factorisation. However it is possible to make computations for Legendre symbols in polynomial time, with the key being the following generalisation due to Jacobi.

Definition 42. Let $b \in \mathbb{Z}_{>0}$ be odd, and $a \in \mathbb{Z}$. Then the **Jacobi symbol** $\left(\frac{a}{b}\right)$ is defined to be $\prod_{i=1}^s \left(\frac{a}{p_i}\right)^{r_i}$, where $b = \prod_{i=1}^s p_i^{r_i}$ for p_i distinct primes is the prime factorisation of b.

Note. In the special case that b is prime this agrees with the Legendre symbol. Warning that it is no longer the case that $\left(\frac{a}{b}\right) = 1$ implies that a is a square modulo b. On the other hand, of course $\left(\frac{a}{b}\right) = -1$ implies that a is not a square modulo b.

Lecture 13
Friday
02/11/18

The key properties of the Jacobi symbol are deduced from those of the Legendre symbol in the following lemma.

Lemma 43.

1. We have $\left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right) = \left(\frac{a_1 a_2}{b}\right)$ and $\left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right) = \left(\frac{a}{b_1 b_2}\right)$.
2. $\left(\frac{a}{b}\right)$ depends only on a modulo b.
3. $\left(\frac{a^2}{b}\right) = 1$.
4. $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$.
5. $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$.
6. If $a, b > 0$ are both odd then $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{((a-1)/2)((b-1)/2)}$.

Proof. All of these statements are true for Legendre symbols, that is for b prime, and a prime in 6. The first three parts are immediate from the definition and the corresponding results for the Legendre symbol. The same is true of the last three from 1 and the corresponding statements for Legendre symbols. We give the details for $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$. It is enough to show that if it holds for b_1, b_2, then it holds for $b_1 b_2$. Since $\left(\frac{2}{b_1 b_2}\right) = \left(\frac{2}{b_1}\right)\left(\frac{2}{b_2}\right)$, we need to show that $(-1)^{(b_1^2-1)/8}(-1)^{(b_2^2-1)/8} = (-1)^{((b_1 b_2)^2-1)/8}$, or equivalently that

$$(b_1^2 - 1) + (b_2^2 - 1) \equiv (b_1 b_2)^2 - 1 \mod 16,$$

which is equivalent to $(b_1^2-1)(b_2^2-1) \equiv 0 \mod 4$, which is true because $b_1^2 \equiv b_2^2 \equiv 1 \mod 4$. □

The last quadratic reciprocity property means that we can compute Jacobi symbols, and thus Legendre symbols, in a similar way to computing (a, b) with Euclid's algorithm, although we also have to take care of powers of two in the numerator.

Example. 9283 is prime, and we can compute $\left(\frac{7411}{9283}\right)$ as follows.

$$\begin{aligned}\left(\tfrac{7411}{9283}\right) &= -\left(\tfrac{9283}{7411}\right) = -\left(\tfrac{1872}{7411}\right) = -\left(\tfrac{16}{7411}\right)\left(\tfrac{117}{7411}\right) = -\left(\tfrac{117}{7411}\right) = -\left(\tfrac{7411}{117}\right) = -\left(\tfrac{40}{117}\right) \\ &= -\left(\tfrac{8}{117}\right)\left(\tfrac{5}{117}\right) = -\left(\tfrac{2}{117}\right)\left(\tfrac{5}{117}\right) = \left(\tfrac{5}{117}\right) = \left(\tfrac{117}{5}\right) = \left(\tfrac{2}{5}\right) = -1.\end{aligned}$$

So 7411 is not a square modulo 9283.

7 Sum of squares

Which integers are the sum of two squares or four squares?

7.1 Sums of two squares

Definition 44. We say that $n \in \mathbb{Z}$ is a **sum of two squares** if $n = x^2 + y^2$ for $x, y \in Z$.

Example. If $n = x^2 + y^2$, then since $x^2, y^2 \equiv 0, 1 \mod 4$, we cannot have $n \equiv 3 \mod 4$.

Example. $21 \equiv 1 \mod 4$, but 21 is not a sum of two squares. On the other hand, we will see that all primes which are 1 modulo 4 are sums of two squares.

Definition 45. The **Gaussian integers** $\mathbb{Z}[i]$ are the subring of $\mathbb{C}$ consisting of $a + bi$ for $a, b \in \mathbb{Z}$. $N : \mathbb{Z}[i] \to \mathbb{Z}_{>0}$ is a **norm** defined by $N(a + bi) = a^2 + b^2$, that is $N(z) = z\overline{z}$.

$N(zw) = (zw)(\overline{zw}) = (z\overline{z})(w\overline{w}) = N(z)N(w)$. If $z = a + bi$, $w = c + di$, then $zw = (ac - bd) + (ad + bc)i$, so $\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac - bd)^2 + (ad + bc)^2$.

Lemma 46. If m, n are each a sum of two squares, then so is mn.

Theorem 47 (Fermat's two square theorem)**.** If $p \equiv 1 \mod 4$ is prime, then p is a sum of two squares.

Lemma 46 and Theorem 47 together allow you to give a complete classification of the integers which are sums of two squares, in terms of their prime factorisations.

Definition 48. A ring R is a **Euclidean domain** if it is an integral domain, that is $ab = 0$ gives $a = 0$ or $b = 0$, and there exists a function $N : R \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that $a = qb + r$, and $r = 0$ or $N(r) < N(b)$.

If R is a Euclidean domain, then you can carry out Euclid's algorithm. In particular, irreducible elements are the same as prime elements, and every element can be factored as a product of primes, uniquely up to reordering and multiplication by units. $\mathbb{Z}[i]$ together with N is a Euclidean domain. By definition, $n \in \mathbb{Z}$ is a sum of two squares if and only if there exists $z \in \mathbb{Z}[i]$ with $N(z) = n$. Since $N(zw) = N(z)N(w)$, all we have to do is to figure out what the primes in $\mathbb{Z}[i]$ are, and what their norms are. (TODO Exercise: Show that the units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$)

Lecture 14 Tuesday 06/11/18

Two elements of $\mathbb{Z}[i]$ are **associates** if their ratio is a unit, that is z, w are associates if $z = uw$ for $u \in \{\pm 1, \pm i\}$. $\mathbb{Z}[i]$ is a Euclidean domain, so in particular we have unique factorisation into primes.

Lemma 49. Let p be a prime in $\mathbb{Z}[i]$. Then there is a prime q of $\mathbb{Z}$ such that either $N(p) = q$ or $N(p) = q^2$. In the latter case, p is an associate of q. Given q a prime in $\mathbb{Z}$, there exists p such that $N(p) = q$ if and only if q is a sum of two squares.

Proof. Write $n = N(p)$, and let $n = q_1^{s_1} \dots q_r^{s_r}$ be the prime factorisation of n in $\mathbb{Z}$. By definition, $n = p\overline{p}$, so $p \mid n$ in $\mathbb{Z}[i]$, and so since p is prime, $p \mid q_i$ for some i. Write $q = q_i$. Then $p \mid q$ gives $q = pv$ for some v, so $N(p)N(v) = N(pv) = N(q) = q^2$. If $N(p) = 1$, then p is a unit, a contradiction. So $N(p) \mid q^2$ gives $N(p) = q$ or $N(p) = q^2$, as claimed. If $N(p) = q^2$, then $N(v) = 1$, so v is a unit, and since $q = pv$, p is an associate of q, by definition. If $N(p) = q$, then writing $p = a + bi$, we have $q = a^2 + b^2$. Conversely, if $q = a^2 + b^2 = (a + bi)(a - bi)$, then since $p \mid q$, we have either $p \mid (a + bi)$ or $p \mid (a - bi)$, so $N(p) \mid N(a + bi) = q$ or $N(p) \mid N(a - bi) = q$, and either way $N(p) = q$. □

Corollary 50. The primes in $\mathbb{Z}[i]$ are either of the form $a+bi$ with a^2+b^2 a prime in $\mathbb{Z}$, or are primes of $\mathbb{Z}$ which are not sums of two squares.

Theorem 51. If $p=2$ or $p\equiv 1 \mod 4$, then p is a sum of two squares.

Proof. By Corollary 50, we just have to show that p is not a prime in $\mathbb{Z}[i]$. There exists n such that $n^2\equiv -1 \mod p$. If $p=2$ obvious, and if $p\equiv 1 \mod 4$, $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}=1$ by Euler's criterion. That is, $p \mid \left(n^2+1\right)=(n+i)(n-i)$. If p were prime, then $p\mid(n+i)$ or $p\mid(n-i)$, that is there exist $c,d\in\mathbb{Z}$ such that $n\pm i=p(c+di)$, so $1=pd$, a contradiction. □

Remark. If $p\equiv 3 \mod 4$ then p is not a sum of two squares, even modulo 4.

Remark. In practice, to go from $n^2+1\equiv 0 \mod p$ to finding a,b with $a^2+b^2=p$, you just compute $(n+i,p)=a+bi$. You can do this computation with Euclid's algorithm in $\mathbb{Z}[i]$.

Theorem 52. $n\in\mathbb{Z}$ is a sum of two squares if and only if its prime factorisation only contains primes congruent to 3 modulo 4 to even powers, that is

$$n=2^a\prod_{p_i\equiv 1 \mod 4} p_i^{r_i}\prod_{q_i\equiv 3 \mod 4} q_i^{2s_i}.$$

Proof. Suppose n is of this form. Then 2, each p_i, and each q_i^2 are all sums of two squares, so n is a sum of two squares by Lemma 46. Conversely suppose that $n=a^2+b^2$, and write $a+bi$ as a product of primes in $\mathbb{Z}[i]$. Then $n=N(a+bi)$ is the product of the norms of these primes, and we already saw that the norms of primes in $\mathbb{Z}[i]$ are either 2, a prime which is 1 modulo 4, or the square of a prime which is 3 modulo 4. □

7.2 Sums of four squares

Lagrange's theorem states that every positive integer is a sum of four squares.

Definition 53. $\mathbb{H}$, the **ring of quaternions**, is the ring of sums $a+bi+cj+dk$ for $a,b,c,d\in\mathbb{R}$, such that

1. addition is $(a+bi+cj+dk)+(A+Bi+Cj+Dk)=(a+A)+(b+B)i+(c+C)j+(d+D)k$, and
2. multiplication is $ij=-ji=k$, $jk=-kj=i$, and $ki=-ik=j$.

If $z=a+bi+cj+dk$, we write $z^*=a-bi-cj-dk$, so $(zw)^*=w^*z^*$.

Define $N(z)=zz^*=a^2+b^2+c^2+d^2$. Then

$$N(zw)=zw(zw)^*=zww^*z^*=zN(w)z^*=zz^*N(w)=N(z)N(w),$$

because $N(w)\in\mathbb{R}$. So

$$\begin{aligned}\left(a^2+b^2+c^2+d^2\right)\left(x^2+y^2+z^2+w^2\right)&=N(a+bi+cj+dk)N(x+yi+zj+wk)\\&=N((a+bi+cj+dk)(x+yi+zj+wk))\\&=(ax-by-cz-dw)^2+(ay+bx+cw-dz)^2\\&+(az-bw+cx+dy)^2+(aw+bz-cy+dx)^2.\end{aligned}$$

In particular, if m,n are sums of four squares, then mn is a sum of four squares. So to prove Lagrange's theorem, it suffices to show that all primes are sums of four squares. We already saw that 2, and any prime congruent to 1 modulo 4, is a sum of two squares. It remains to show that any prime congruent to 3 modulo 4 is a sum of four squares.