M3P14 Number Theory

Lectured by Prof Toby Gee
Typeset by David Kurniadi Angdinata

Autumn 2018

Contents

0 Introduction **2**

1 Euclidean algorithm and unique factorisation **2**
1.1 Divisibility . . . 2
1.2 Euclid's algorithm . . . 3
1.3 Unique factorisation . . . 4
1.4 Linear diophantine equations . . . 4

2 Congruences and modular arithmetic **5**
2.1 Congruences . . . 5
2.2 Linear congruence equations . . . 6
2.3 Chinese remainder theorem . . . 6

3 The structure of $(\mathbb{Z}/n\mathbb{Z})^*$ **6**
3.1 The Euler Φ function . . . 6
3.2 Euler's theorem . . . 7

4 Primality testing and factorisation **11**
4.1 Factorisation . . . 11
4.2 Primality testing . . . 13

5 Public key cryptography **13**
5.1 Rivest-Shamir-Adleman (RSA) algorithm . . . 14
5.2 Discrete logarithms . . . 14

6 Quadratic residues and quadratic reciprocity **14**

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 $(\mathbb{Z}/n\mathbb{Z})^*$, 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 Euclidean 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 $n \in \mathbb{Z}^*$ 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 $a, b, c \in \mathbb{Z}^*$ 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 $n \in \mathbb{Z}^*$, 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^* for the set of units in R. This is a group under multiplication.

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

We want to understand $(\mathbb{Z}/n\mathbb{Z})^*$. Which elements of $\{0, \ldots, n - 1\}$ are in $(\mathbb{Z}/n\mathbb{Z})^*$? If $r \in \mathbb{Z}$ and $\overline{r} \in (\mathbb{Z}/n\mathbb{Z})^*$ 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 $(\mathbb{Z}/n\mathbb{Z})^* = \left\{\overline{i} \mid (i, n) = 1\right\}$.

Note. If p is a prime, then either $a \equiv 0 \mod p$ or $(a, p) = 1$, so $(\mathbb{Z}/p\mathbb{Z})^* = \{1, \ldots, p - 1\}$. 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 $c \in \mathbb{Z}^*$. 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 $a \in (\mathbb{Z}/c\mathbb{Z})^*$, 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

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

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 $(R \times S)^* = R^* \times S^*$. □

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 $(\mathbb{Z}/n\mathbb{Z})^*$

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

3.1 The Euler Φ function

We define a function $\Phi(n)$ on $\mathbb{Z}_{>0}$ by letting $\Phi(n)$ denote the order of $(\mathbb{Z}/n\mathbb{Z})^*$. 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 $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, 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 $(\mathbb{Z}/n\mathbb{Z})^*$ 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 $(\mathbb{Z}/n\mathbb{Z})^*$, 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 $(\mathbb{Z}/n\mathbb{Z})^*$. 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 $n = 5$. $(\mathbb{Z}/5\mathbb{Z})^* = \{1, 2, 3, 4\}$. 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 $(\mathbb{Z}/5\mathbb{Z})^*$. So $(\mathbb{Z}/5\mathbb{Z})^*$ is cyclic of order 4.

By the Chinese Remainder Theorem, to understand the structure of $(\mathbb{Z}/n\mathbb{Z})^*$, 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 $(\mathbb{Z}/n\mathbb{Z})^*$, 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 $(\mathbb{Z}/p\mathbb{Z})^*$ 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 $(\mathbb{Z}/p\mathbb{Z})^*$ 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 $(\mathbb{Z}/p\mathbb{Z})^*$.

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 $(\mathbb{Z}/p\mathbb{Z})^*$ 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 $(\mathbb{Z}/p\mathbb{Z})^*$ whose order divides d.

Example. Let $p=7$. Then $(\mathbb{Z}/p\mathbb{Z})^*$ 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 $i \in \{1, \ldots, n\}$ 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 $(\mathbb{Z}/p\mathbb{Z})^*$. In particular there are $\Phi(p-1)$ primitive roots modulo p, and $(\mathbb{Z}/p\mathbb{Z})^*$ 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 $(\mathbb{Z}/p\mathbb{Z})^*$ of order dividing d. Thus the number of elements of $(\mathbb{Z}/p\mathbb{Z})^*$ 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 $(\mathbb{Z}/p^n\mathbb{Z})^*$ 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 $(\mathbb{Z}/p^n\mathbb{Z})^*$ 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 $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$, or $g^{p-1} \equiv 1 \mod p^2$, and $g+p$ is a generator for $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$. Either way, $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$ 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

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

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 $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$ 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 $(\mathbb{Z}/p^n\mathbb{Z})^*$ 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. $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$ is cyclic,
2. $(\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\}$ is cyclic of order 2, with 3 as a generator, but
3. this fails for higher powers, say $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ 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 $(\mathbb{Z}/2^n\mathbb{Z})^* \to (\mathbb{Z}/2\mathbb{Z}) \times \left(\mathbb{Z}/2^{n-2}\mathbb{Z}\right)$, so that in particular if $n \geq 3$ then $(\mathbb{Z}/2^n\mathbb{Z})^*$ is not cyclic.

Proof. Consider the natural map

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

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 $2\left(2^{n-2}\right) = 2^{n-1} = \Phi(2^n) = \#(\mathbb{Z}/2^n\mathbb{Z})^*$. So the map $\langle -1 \rangle \times \langle 5 \rangle \to (\mathbb{Z}/2^n\mathbb{Z})^*$ 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 $(\mathbb{Z}/n\mathbb{Z})^*$ 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

Idea is testing whether $n \in \mathbb{Z}$ is prime is easy. Factoring n is expected to be hard. Easy here means that there is an algorithm to check whether n is prime or not which runs in time polynomial in $\log n$. It is known that a deterministic algorithm exists to do this, the Agrawal-Kayal-Saxena (AKS) algorithm in 2005. We will see an algorithm that runs faster than this in practice. On the other hand, for factoring there are algorithms which are better than exponential in $\log n$, but there is nothing close to polynomial time, and the general expectation is that no such algorithm should exist.

4.1 Factorisation

How do we factor three digit numbers, or small four digit numbers, say $n \leq 400$, if we wanted to factor with paper or calculator? If $n \leq 400$ and n is composite, then n has a prime factor $d \leq \sqrt{400} = 20$. If $d \mid n$ then $d(n/d) = n$, so either $d \leq \sqrt{n}$ or $n/d \leq \sqrt{n}$. So you only have to be able to check for divisibility $2, 3, 5, 7, 11, 13, 17, 19$.

1. Checking by divisibility by 2 or 5 is easy. Just look at the last digit.
2. For 3, 11, use that $10 \equiv 1 \mod 3$ and $10 \equiv -1 \mod 3$. 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 you can check divisibility by 3 or 9 by checking for the sum of the digits, and 11 by taking the alternating sum.

3. For 7, $10x + y \equiv 0 \mod 7$ if and only if $-2(10x + y) \equiv 0 \mod 7$, if and only if $x - 2y \equiv 0 \mod 7$.

4. For 13, 17, 19, there are no good tests. If $n \leq 400$ and n is not divisible by $2, 3, 5, 7, 11$, then the smallest prime factor of n is at least 13. Since $13^3 > 400$, it can have at most 2 prime factors. So if you want to factor numbers ≤ 400, you only have to remember a short list

$$13^2, \quad 13\,(17), \quad 13\,(19), \quad 13\,(23), \quad 13\,(29), \quad 17^2, \quad 17\,(19), \quad 17\,(23), \quad 19^2.$$

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

Factor four digit numbers by an algorithm due to Fermat. Idea is to first check for small prime factors by hand, say $p = 2, \ldots 19$. If n is composite and does not have any small factors, then the prime factors of n should be close to $\sqrt{n}$. If $n = ab$ for a, b odd and $a \leq b$, then

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

If you know $(a+b)/2$ and $(b-a)/2$, you can recover a, b. So take m such that $m^2 \leq n < (m+1)^2$. If $n = m^2$, done, otherwise check if $(m+i)^2 - n$ is a square for increasing i.

Example. Let $n = 6077$. $77^2 < 6077 < 78^2$, so

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

Thus $6077 = 81^2 - 22^2 = (103)\,(59)$.

There exist algorithms for factoring n which run in better than exponential time in $\log n$, such as the quadratic sieve and the general number field sieve. The following is the **quadratic sieve**.

Example. Let $n = 1649$. $40^2 < 1649 < 41^2$, so

$$\begin{aligned} 41^2 - 1649 &= 32 = 2^5, \\ 42^2 - 1649 &= 115, \\ 43^2 - 1649 &= 200 = (2)^3\,(5)^2. \end{aligned}$$

$41^2 \equiv 2^5 \mod 1649$ and $43^2 \equiv (2)^3\,(5)^2 \mod 1649$, so $80^2 \equiv (41)^2\,(43)^2 = 1763^2 \equiv 114^2 \mod 1649$. Then $0 \equiv 114^2 - 80^2 = (194)\,(34) = (2)^2\,(17)\,(97) \mod 1649$. In fact, $1649 = (17)\,(97)$. Better for this last step would be to have computed $(194, 1649) = 97$ and $(34, 1649) = 17$. Can do this quickly using Euclid's algorithm.

To make this into an efficient algorithm, need to have a way given $x_1, \ldots, x_r$ to find a subset whose product is a square. If we know the prime factorisation for the x_i, we can write $x_i = p_1^{a_{i1}} \ldots p_k^{a_{ik}}$. Want to choose $\epsilon_i \in \{0, 1\}$ such that $\prod_{i=1}^r x_i^{\epsilon_i}$ is a square. Equivalently, for each j, want the exponent of p_j to be even, that is $\sum_{i=1}^r \epsilon_i a_{ij} \equiv 0 \mod 2$.

Example. $x_1 = 2^5$, $x_2 = (5)\,(23)$, $x_3 = (2)^3\,(5)^2$. $p_1 = 2$, $p_2 = 5$, $p_3 = 23$. Ignore all numbers with a large prime factor, here ignore 23. Left with $x_1 = 2^5$ and $x_3 = (2)^3\,(5)^2$.

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

in the field $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$, that is $\epsilon_1 + \epsilon_2 = 0$, so choose $\epsilon_1 = \epsilon_2 = 1$.

This step, solving linear equations in $\mathbb{Z}/2\mathbb{Z}$, can be done efficiently. The remaining difficulty is to find a supply of $m \in \mathbb{Z}$ such that $m^2 - n$ has only small prime factors. Idea is if we fix a list of small primes to start with, we get congruence conditions on m. It turns out that there is a straightforward algorithm for solving $m^2 \equiv n \mod p$. This gives two possible values for m modulo p. 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. $m^2 = 1649 \equiv 2 \mod 3$ has no solutions.

Lecture 8
Tuesday
23/10/18

4.2 Primality testing

Euler's theorem states that if $(a,n)=1$ then $a^{\Phi(n)} \equiv 1 \mod n$. In particular if p is prime then a^{p-1} then $a^{p-1} \equiv 1 \mod p$ for all $1 \leq a \leq p-1$. In particular if $2^{n-1} \equiv 1 \mod n$, then n cannot be prime. Problem is that there exists n composite such that $a^{n-1} \equiv 1 \mod n$ for all $(a,n)=1$. These numbers are called **Carmichael numbers**. It is known that infinitely many of these exist. Miller-Rabin test is a test for whether $n \in \mathbb{Z}$ is prime or not. Today let $n \equiv 3 \mod 4$. Example sheet is $n \equiv 1 \mod 4$.

Lemma 30. Let $n > 1$ be congruent to 3 modulo 4. Then n is prime if and only if for all $(a,n)=1$, $a^{(n-1)/2} \equiv \pm 1 \mod n$.

Proof. If 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 $a^{(n-1)/2} \equiv \pm 1 \mod n$. Suppose firstly that $n = p^k$ with p prime, and $k \geq 2$. Try $a = 1+p$. Then $(1+p)^{(n-1)/2} \equiv 1 + ((n-1)/2)\, p \mod p^2$, 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. The remaining case is that n is composite but not a power of a prime. Write $n = rs$, for $r, s > 1$ and odd, and $(r,s)=1$. By the Chinese remainder theorem, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$. Choose a such that $a \equiv -1 \mod r$ and $a \equiv 1 \mod s$. Then $(a,r) = (a,s) = 1$, so $(a,n)=1$. Since $n \equiv 3 \mod 4$, $(n-1)/2$ is odd, so $a^{(n-1)/2} \equiv -1 \mod r$ and $a^{(n-1)/2} \equiv 1 \mod s$. So $a^{(n-1)/2} \not\equiv \pm 1 \mod n$. □

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

Proof. 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 $(\mathbb{Z}/n\mathbb{Z})^*$. It is a proper subgroup by Lemma 30. □

Corollary 32. At most half the elements of $(\mathbb{Z}/n\mathbb{Z})^*$ satisfy $a^{(n-1)/2} \equiv \pm 1 \mod n$.

Proof. The set of such elements is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ by Lemma 31. □

In fact, with a bit more work, you can improve this to show that at least $3/4$ of the numbers $1 \leq a \leq n-1$ satisfy $a^{(n-1)/2} \not\equiv \pm 1 \mod n$. So if you randomly choose numbers $1 \leq a \leq n-1$ x times, and n is composite, the probability that you find some a with $a^{(n-1)/2} \not\equiv \pm 1 \mod n$ is at least $1 - (1/4)^x$. This gives a probabilistic algorithm to check if n is prime in polynomial time. If you assume generalised Riemann hypothesis (GRH) you can find some $a \in \mathbb{Z}$ with

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

In practice it is even better.

Example. If $n < 341550071728321$, then one of $a = 2, 3, 5, 7, 11, 13, 17$ will work.

5 Public key cryptography

How do we turn messages into numbers in $\mathbb{Z}/n\mathbb{Z}$? Idea is to choose n very large. Say $n > 2^{8k}$. Write down your message. Break it up into strings of at most k characters. Encode each character as an 8 bit binary number. String these integers together to get an $8k$ bit binary number. Regard that as an integer modulo n. Now apply some function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, and then tell whoever you are trying to communicate with the result of this computation. Then they should apply some other function $g : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, to get

back the number you started with. So want f to be injective. Want to be able to make f public without making g public. If you have functions $f, g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $f \circ g = g \circ f = id$, then you can also verify your identity, that is sign messages. Again, make f public, and any time you publish a message m, you also publish $g(m)$. Then anyone can apply f to $g(m)$ to recover $m = f(g(m))$, but without g, no one can forge your signature.

5.1 Rivest-Shamir-Adleman (RSA) algorithm

Idea is to choose two large prime numbers p, q and set $n = pq$. Choose $(e, \Phi(n)) = 1$. Find d such that $de = 1 \mod \Phi(n) = (p-1)(q-1) = n - (p+q) + 1$. Publish n and e, you keep $p, q, \Phi(n), d$ secret. $f(x) = x^e \mod n$ and $g(x) = x^d \mod n$. $x^{de} \equiv x^1 \equiv x \mod n$ because $de \equiv 1 \mod \Phi(n)$ and $x^{\Phi(n)} \equiv 1 \mod n$.

Lecture 9 Wednesday 24/10/18

Lecture 9 is a problem class.

So if someone wants to send you a message $c \in \mathbb{Z}/n\mathbb{Z}$, they compute $c^e \in \mathbb{Z}/n\mathbb{Z}$, and send it to you. To decode it, you compute $(c^e)^d = c^{de} \equiv c \mod n$. This assumes that $(c, n) = 1$, but the probability of this is extremely high. The prevailing assumption is that with only the information n and e, it is hopeless to discover d, or to find any other way of recovering c from c^e.

Lecture 10 Friday 26/10/18

5.2 Discrete logarithms

Suppose that n is prime, or more generally that $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic. Let g be a generator for this group, that is a primitive root. For any $a \in (\mathbb{Z}/n\mathbb{Z})^*$, we can write $a = g^m$ for some unique $0 \leq m < \Phi(n)$. We call m the **discrete logarithm** of a to base g, write $m = \log_g(a)$.

Example. If you want to solve $x^r \equiv a \mod n$, write $x = g^y$, and the congruence becomes equivalent to $yr \equiv \log_g(a) \mod \Phi(n)$.

Unfortunately, or fortunately for cryptography, computing $\log_g$ is believed to be a hard problem. In particular, there is no known polynomial time algorithm.

Example. Imagine that you have a system where you need to store passwords for different users, but you do not want to store the actual passwords. One way to do this is to choose a large prime p and a primitive root g, and if someone inputs x as their password, you store g^x modulo p. If they later input y, you compute g^y, and check it matches what you stored. If it does then $y \equiv x \mod p - 1$.

6 Quadratic residues and quadratic reciprocity

Let p be a prime number.

Definition 33. If $(a, p) = 1$, then a is a **quadratic residue** (QR) if and only if there is a solution to $x^2 \equiv a \mod p$. If $(a, p) = 1$ and is not a quadratic residue, it is called a **quadratic nonresidue** (QNR).

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, and $(p-1)/2$ QNRs modulo p.

Proof. The map $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ by $x \mapsto x^2$ is a group homomorphism with kernel is $\{\pm 1\}$. So the image has order $(p-1)/2$, and the image is exactly the QRs. □

Proposition 35. Suppose that $(a, p) = (b, p) = 1$. Then

1. if a, b are both QRs, then ab is a QR,
2. if one of a, b is a QR and one is a QNR, then ab is a QNR, and
3. if a, b are both QNRs, then ab is a QR.

Proof. Let H be the image of $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ by $x \mapsto x^2$, that is H is the QRs. Then $(\mathbb{Z}/p\mathbb{Z})^*/H$ is a group of order two by Lemma 34, so it is cyclic of order two. This statement is a restatement of the proposition, since $(\mathbb{Z}/p\mathbb{Z})^* = H \sqcup 1 + H$. □

Definition 36. Let a be an integer and p a prime. Then

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

Proposition 35 can be restated as saying that $(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ by $a \mapsto (a/p)$ is a group homomorphism, that is $(ab/p) = (a/p)\,(b/p)$. Even holds if we do not assume that $(a, p) = (b, p) = 1$.