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 $(\mathbb{Z}/n\mathbb{Z})^*$, RSA algorithm, and quadratic reciprocity. We will return to primes at the end, too. Typical questions here include:

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. $\square$

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. $\square$

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, to get:

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

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. $\square$

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 $n \mid b$. $\square$

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 $p \mid b$. $\square$

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 $ab \mid n$. $\square$

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) $\square$

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. $\square$

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. $\square$

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 $0 \le r < n$. Then $a \equiv r \mod n$, so $\overline{a} = \overline{r}$.

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

It follows that $0, \dots, n - 1$ 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 $r \in \{0, \dots, n - 1\}$. It will also be convenient to write $\mathbb{Z}/n\mathbb{Z} = \{0, \dots, n - 1\}$.

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 $\{0, \dots, n - 1\}$ 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 $(\mathbb{Z}/p\mathbb{Z})^* = \{1, \dots, p - 1\}$. 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 $m_1, \dots, m_n \in \mathbb{Z}_{\geq 0}$ be pairwise coprime. Then the natural map

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

is an isomorphism of rings, and the induced map

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

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 $x \equiv y \mod m_1 \dots m_n$ then certainly $x \equiv y \mod m_i$ for each i. The source and target of the ring homomorphism both have order $m_1 \dots m_n$, 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 $m_1 \dots m_n \mid N$, that is $\overline{N} = 0$ in $\mathbb{Z}/m_1 \dots m_n\mathbb{Z}$. This is just Corollary 10. The statement about unit groups follows by noting that if R, S are rings, then $(R \times S)^* = R^* \times S^*$. $\square$

Note. This can be reformulated more concretely as a statement about congruences. It says that for any a_i, there is a unique $x \mod m_1 \dots m_n$ 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 $M = m_1 \dots m_n$ 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 $q_j \equiv 0 \mod m_i$ 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

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

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 $g \mod n$.

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

Proof. If $n=ab$ then $g^n=(g^a)^b=1^b=1$. Conversely write $n=ab+r$ with $0\leq r<a$. Then $g^r=1$ and since $r<a$ we have $r=0$. ☐

In particular, if $(g,n)=1$, then $g^{\Phi(n)}=1$ by Euler's theorem, so Proposition 19 gives $ord_n(g)\mid\Phi(n)$. We want 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** if $ord_p(g) = p-1$, so $(\mathbb{Z}/p\mathbb{Z})^* = \langle g \rangle$.

Lemma 21. Let R be a commutative ring, and let $P(X) \in R[X]$. If $\alpha \in R$ has $P(\alpha) = 0$, then there exists $Q(X) \in R[X]$ 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. Induction on $d = \deg(P)$. $d = 0$ is obvious. Assume the result holds for degree less than $d-1$. Let $P(X) = cX^d + \dots$ and $S(X) = P(X) - cX^{d-1}(X - \alpha)$. Then $S(X)$ has degree less than $d-1$. Also $S(\alpha) = 0$. By induction, we can write $S(X) = (X-\alpha) R(X)$. Set $Q(X) = cX^{d-1} + R[X]$. Then

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

□

Theorem 22. Let F be a field. Let $P(X)$ be a polynomial in $F[X]$. Then $P(X)$ has at most d distinct roots in F.

Proof. Induction on $d = \deg(P)$. $d = 1$ is obvious. If P has no roots, then we are done. Otherwise, let α be a root. By Lemma 21, $P(X) = (X - \alpha) Q(X)$, $Q(X)$ has degree $d-1$, so we are done by induction. □

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

Proof. We have to show that $X^d - 1$ has exactly d roots in $\mathbb{Z}/p\mathbb{Z}$. $X^{p-1} - 1$ has exactly $p-1$ roots, by Fermat's little theorem. Since $d \mid (p-1)$, we can write

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

$X^{p-1} - 1$ 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. So $X^d - 1$ has exactly d roots. □

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 $\sum_{d \mid n} \Phi(d) = n$.

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

Theorem 25. Let p be prime, and let $d \mid (p-1)$. Then there are exactly $\Phi(d)$ elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order d. In particular, there are $\Phi(p-1)$ primitive roots, and $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

Proof. Induction on d. $d = 1$ is obvious. Assume the result holds for all $d' \mid d$, $d' \neq d$. Then by Lemma 24,

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

Now use inductive hypothesis and Corollary 23. □