Lecture 3 — Rings and Multiplication

Dr. D. Bernhard

In this lecture: rings — units and zero divisors — the group $\mathbb{Z}_n^\times$ — Euler's totient function — Euclid's algorithm — fields — exponent arithmetic

Learning outcomes. After this lecture and revision, you should be able to:

- Find the order of the multiplicative group modulo any n.
- Apply Euclid's algorithm to integers m, n to find a, b with $a \cdot n + b \cdot m = \gcd(m, n)$.
- Multiply and invert in $\mathbb{Z}_n^\times$.
- Tell if a structure is a ring.
- Classify ring elements as units, zero divisors or neither.
- Solve equations of the form $a \cdot x = b \pmod{n}$.
- Perform exponent arithmetic.

3 Rings and multiplication

The last two lectures, we have looked at groups which are a generalisation of addition. Today we look at multiplication.

3.1 Rings

We began this course by saying that a group is a bit like adding numbers. This is not quite true — a group is a bit like adding and subtracting numbers, since there must always be inverses. If we introduce multiplication as a group operation, this gives us division too but sometimes that is more than we need. In $\mathbb{Z}$ for example, you can multiply but you cannot always divide. A ring is a structure a bit like numbers with addition, subtraction and multiplication but you cannot necessarily divide (even when there is no 0 involved).

Definition 3.1. A structure $\mathcal{R} = (R, +, \cdot)$ where R is a set and $+, \cdot$ are two operations $R \times R \to R$ is a ring if the following hold.

additive group The structure $(R, +)$ is an Abelian group. We call its neutral element the zero of R and write it with the symbol 0 or sometimes 0_R.

multiplication The structure $(R, \cdot)$ is associative and has a neutral element, which we call the one of the ring and write as 1 or 1_R.

distributive law For any elements a, b, c in R we have $(a + b) \cdot c = a \cdot c + b \cdot c$ and $c \cdot (a + b) = c \cdot a + c \cdot b$.

The description of a ring requires the additive group to be commutative but not ncessarily the multiplication. We call a ring commutative if the multiplication is commutative too.

The standard example of a ring is $(\mathbb{Z}, +, \cdot)$. For any positive integer n, the space $(\mathbb{Z}_n, +_n, \cdot_n)$ is a ring too. If we take n-tuples of integers with componentwise addition and multiplication, this gives us yet another ring.

We state some basic facts about rings:

- There can only be one neutral element for multiplication.
- There is a ring with one element, which is the neutral element for both addition and multiplication ($0 = 1$!). As soon as a ring has at least two elements, the neutral elements 0 for addition and 1 for multiplication must be different however.
- Multiplying any element x in a ring with 0, the neutral element of addition, gives 0 (from both the left and the right, if the ring is not commutative).

3.2 Units and zero divisors

In a ring, things can happen that we might not expect from the usual integers. For example, the structure $(\mathbb{Z}_8, +_8, \cdot_8)$ is a ring in which $2 \cdot_8 4 = 0$, so a product of two nonzero elements can be zero even if neither of the factors are. If we take the ring of pairs of integers with component-wise addition and multiplication, $(0, 1) \cdot (1, 0) = (0, 0)$: another case where the product of two nonzero elements becomes zero.

We can classify all elements in a ring into the following classes.

Definition 3.2 (unit, zero divisor). In a ring $(R, +, \cdot)$:

- The neutral element of addition is called the zero of the ring and written with the symbol 0.

- An element a in the ring which has a multiplicative inverse b, i.e. $a \cdot b = 1$ and $b \cdot a = 1$, is called a unit of the ring. The neutral element of multiplication is always a unit.
- An element $a \neq 0$ for which there is some other $b \neq 0$ such that $a \cdot b = 0$ or $b \cdot a = 0$ is called a zero divisor.
- An element can also be neither of the above.

Most of the time, the classification zero/unit/zero divisor/none of the previous is unique, i.e. each element of the ring is in exactly one class. The only exception is that in the ring with one element, the element is both the zero and a unit; as soon as $1 \neq 0$ a unit can neither be zero nor a zero divisor.

3.3 The group $\mathbb{Z}_n^\times$

Let's try and build a structure where multiplication is a group operation. Start by looking at multiplication in $\mathbb{Z}$. Multiplication is associative and 1 is the neutral element. However, 0 causes problems if we try and find inverses: $0 \cdot x = 0$ for all x so there cannot be an x with $0 \cdot x = 1$. So let's get rid of 0 and look at $\mathbb{Z}^\times = \mathbb{Z} \setminus \{0\}$. We still don't have inverses: there is no integer z satisfying $3 \cdot z = 1$ for example. The usual way to carry on at this point is to introduce the fractions (without zero) $\mathbb{Q}^\times$ which form a group under multiplication.

Now let's look at the group $(\mathbb{Z}_{2^8}, +) = (\mathbb{Z}_{256}, +)$; this group is sometimes called `byte`, `uint8` or `unsigned char` in programming. What happens if we introduce multiplication on this group with the rule that if you exceed 255, you subtract 256 until you are back in range (equivalently, you ignore all "higher bits" of a number)?

Interestingly, we can solve the equation $3 \cdot_{256} z = 1$ where $\cdot_{256}$ is multiplication modulo 256. The solution is $z = 171$ since $3 \cdot 171 = 513 = 2 \cdot 256 + 1$ (division with remainder) so $3 \cdot_{256} 171 = 1$. So in some cases we can find inverses without resorting to fractions.

We quickly hit another problem though: $16 \cdot 16 = 256$, so $16 \cdot_{256} 16 = 0$ so 16 cannot have an inverse, fractions or no: if $16 \cdot_{256} x = 1$ had any solution for x, we could multiply both sides of the equation to get $0 = 16$ which is nonsense, even modulo 256.

Let's throw out all elements that cause problems from $\mathbb{Z}_n$. 0 is right out. Anything that gives 0 when multiplied with another number from $\mathbb{Z}_n$ except 0 is out too (that is, all zero divisors). This leaves us with a group:

Proposition 3.3 (the group $\mathbb{Z}_n^\times$). For a positive integer n, the set $\mathbb{Z}_n^\times$ is the subset of $\mathbb{Z}_n$ containing all elements x for which $x \cdot_n y \neq 0$ for all other elements $y \neq 0 \in \mathbb{Z}_n$. Together with multiplication modulo n, this forms a group $(\mathbb{Z}_n^\times, \cdot_n)$.

Let's check that this really is a group. Associativity follows from that of $\cdot$ on $\mathbb{Z}$, the same way we did it for $+_n$ in the first lecture. The neutral element is 1 since $1 \cdot_n y = y$ for any $y \neq 0 \in \mathbb{Z}_n$ and if $y \neq 0$ then $1 \cdot_n y = y$ is not 0 either, so we can't lose the element 1 in the definition of $\mathbb{Z}_n^\times$. To find inverses we have to invoke a bit more number theory.

Exercise. ($\star$) *Arithmetic modulo primes.* In this exercise, we choose the prime $p = 1009$ as our modulus and look at the ring $\mathcal{R} = (\mathbb{Z}_{1009}, +, \cdot)$.

1. Compute $824 + 3 \cdot 632$ in $\mathcal{R}$.
2. What is the order of 7 in $(\mathbb{Z}_{1009}, +)$?

Exercise. ($\star$) *Addition and multiplication tables.*

- Compute the addition and multiplication tables for $(\mathbb{Z}_5, +, \cdot)$.
- Do the same for $(\mathbb{Z}_4, +, \cdot)$.
- Write the group table for the group $(\mathbb{Z}_4^\times, \cdot)$.

Exercise. ($\star\star$) *Arithmetic modulo n.* Consider $n = 16$. Find all solutions modulo n of the equations

1. $5x = 1$
2. $6y = 1$
3. $8z = 0$

3.4 Euler's totient function

How many elements are left over in $\mathbb{Z}_n^\times$? We give this quantity a name.

Definition 3.4 (Euler totient function). Euler's totient function ϕ is the function $\phi(n) := |\mathbb{Z}_n^\times|$ for $n > 0 \in \mathbb{N}$ that maps a positive integer n to the number of elements in $\mathbb{Z}_n^\times$.

To compute this function, we can ask the related question, which elements have we got rid of? Let's take an element $x \neq 0$ that was in $\mathbb{Z}_n$ but not in $\mathbb{Z}_n^\times$, which means there is some $y \neq 0$ in $\mathbb{Z}_n$ such that $x \cdot_n y = 0$. The definition of $x \cdot_n y$ is the remainder when dividing $x \cdot y$ by n, so we must have $x \cdot y = c \cdot n + 0$, i.e. the remainder is 0 so $x \cdot y$ is a multiple of n. Since we assumed $x \neq 0$ and $y \neq 0$ then c cannot be 0 either: the product of two nonzero elements in $\mathbb{Z}$ is never zero. Further if y is not a multiple of n on its own, which it cannot be because $y \in \mathbb{Z}_n$ so $y < n$, then x and n must have a factor in common (that is higher than 1). Conversely, if x and n have the common factor k then we can write $x = ak$, $n = bk$ for some nonzero integers a, b and $b \cdot x = a \cdot b \cdot k = a \cdot n$ which is a multiple of n so $x \cdot_n b = 0$. So a number in $\mathbb{Z}_n$ is excluded from $\mathbb{Z}_n^\times$ if and only if it has a common factor (other than 1) with n.

This tells us $\phi(p)$ whenever p is a prime. Since primes are exactly those numbers that have no factors except 1 and themselves, the only element of $\mathbb{Z}_p$ that is excluded from $\mathbb{Z}_p^\times$ is 0 and we get $\phi(p) = p - 1$ and can say that $\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$.

If m and n are two positive integers that have no factors other than 1 in common (another way of saying this is that m, n are coprime) then the only elements of $\mathbb{Z}_{m \cdot n}$ that have a factor in common are those that already had a factor in common with m or with n. In other words,

> **Proposition 3.5.** Two integers m, n are coprime if their greatest common divisor is 1. For coprime positive integers m, n we have $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

In particular this holds when m, n are distinct primes. For primes, we can say even more: if we look at the numbers sharing a factor with p^k for p a prime and k a positive integer, these numbers must already share a factor with p since the factors of p^k are exactly $1, p, p^2, \ldots, p^k$. If we write the numbers from 1 to p^k in a p-column table, the table has $p^k/p = p^{k-1}$ rows and each row contains exactly one multiple of p in the last column, so there are $(p-1)$ columns with numbers that are coprime to p per row. This lets us find $\phi(p^k)$:

> **Proposition 3.6.** For a prime p and a positive integer k we have $\phi(p^k) = p^{k-1}(p-1)$.

The last two propositions allow us to find $\phi(n)$ for any n. We factor n as $p_1^{a_1} \cdot \ldots p_k^{a_k}$ where the $p_1, \ldots, p_k$ are distinct primes and a_i is the number of times the prime p_i appears. Then we have

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$$

This concludes our little excursion to investigate Euler's ϕ function and we return to showing that $(\mathbb{Z}_n^\times, \cdot_n)$, whose size we can now compute, is a group.

Exercise. ($\star$) *Euler's ϕ function.* How many elements are there in the group $(\mathbb{Z}_n^\times, \cdot)$ for

1. $n = 1009$ (this is a prime)
2. $n = 64$
3. $n = 60$

3.5 Euclid's algorithm

Our next step is a lemma by Euclid, a variation on division with remainder, that comes with an algorithm to find the numbers in question:

> **Lemma 3.7 (Euclidean algorithm).** If m, n are two nonzero integers then there are unique integers a, b such that
>
> $$a \cdot n + b \cdot m = \text{gcd}(m, n)$$

This gives us the inverses we want in $\mathbb{Z}_n^\times$. If m is coprime to n then the gcd is 1 (or m would not be in $\mathbb{Z}_n^\times$ at all) and we find a, b such that $a \cdot n + b \cdot m = 1$ which is equivalent to saying that $b \cdot m = (-a) \cdot n + 1$ so $b \cdot m$ leaves remainder 1 when dividing by n and $b \pmod{n}$ is the inverse we are looking for. (We take b modulo n again because Euclid's algorithm can return an b outside the range $\mathbb{Z}_n$ in some cases.) This concludes the proof that $(\mathbb{Z}_n^\times, \cdot_n)$ is a group.

Here's one way to compute the extended Euclidean algorithm. Suppose we want to invert 17 modulo 256. That is, we want to find b such that $17b = 1 \pmod{256}$, for which we find a, b with Euclid's algorithm such that $256a + 17b = 1$. Make a four-column table with headings **q** (quotient), **r** (remainder), **a** and **b**. Write the top two rows as in the table below with the numbers in the **r** column and the rest as shown.

q	r	a	b
0	256	1	0
0	17	0	1
15	1	1	-15
17	0	-17	256

For all further rows, calculate as follows. Let q', r', a', b' be the values from the last row and q'', r'', a'', b'' be the second-to-last row (so for the third row, $r' = 17$ and $r'' = 256$).

- Divide r'' by r' with remainder. Put the quotient and remainder as the new q, r values.
- Set $a := a'' - q \cdot a'$ and $b := b'' - q \cdot b'$.

For row 3, we get $256 = 15 \cdot 17 + 1$ so we start the third row with $q = 15, r = 1$. Then $a := 1 - 0 \cdot 15 = 1$ and $b := 0 - 1 \cdot 15 = -15$.

Repeat until the remainder becomes $r = 0$. When this happens, the last row with a nonzero remainder contains the important information: the r value in this row is the gcd of the two original numbers (in our case this is 1, without this we could not do modular inversion at all) and the a, b values in this row are the ones we are looking for. In our case $a = 1$ and $b = -15$ and indeed, $1 \cdot 256 - 15 \cdot 17 = 1$ so $-15 \mod 256 = 241$ is the inverse of 17 in $(\mathbb{Z}_{256}^{\times}, \cdot)$.

Exercise. ($\star\star$) *Euclid's algorithm.*

1. Find integers a, b such that $13a + 64b = 1$.
2. Find the inverse of 5 under multiplication modulo 1009.
3. Find all solutions of the equations $101 \cdot x = 1$ and $25 \cdot y + 6 = 98$ in $\mathbb{F} = (\mathbb{Z}_{1009}, +, \cdot)$.

Exercise. ($\star\star$) *Classification of ring elements.* Classify all elements of the rings $(\mathbb{Z}_n, +, \cdot)$ as zero, unit, zero divisor or neither for the following values of n.

1. $n = 1009$ (this is still a prime)
2. $n = 64$
3. $n = 60$
4. Do the same for $(\mathbb{Z}, +, \cdot)$.

3.6 Fields

A commutative ring in which every nonzero element is a unit is called a field. (Fields are therefore automatically integral domains.)

> **Definition 3.8 (field).** A structure $\mathbb{F} = (F, +, \cdot)$ is a field if it is a commutative ring and every element except the zero is a unit.

Another way of saying that $\mathbb{F}$ is a field is that $\mathbb{F} \setminus \{0\}$ forms a (commutative) group under multiplication — with the one exception of $(\{0\}, +, \cdot)$ which is also a field. We will return to fields and finite fields in particular in a later lecture. For now, we summarise the basic algebraic structures:

- A monoid[1] is a structure in which you can add.
- A group is a structure in which you can add and subtract.
- A ring is a structure in which you can add, subtract and multiply.
- A field is a structure in which you can add, subtract, multiply and divide[2].

Exercise. $(\star\star)$ *Fields modulo primes.* We know that $p = 1009$ is a prime. This means $(\mathbb{Z}_{1009}, +, \cdot)$ is a field (and the same holds for every other prime). Why?

The following section is for self-study.

3.7 Exponent arithmetic

We have learnt to add and multiply modulo n. Writing [ ] for reduction modulo n, we have $[a + b] = [[a] + [b]]$ and $[a \cdot b] = [[a] \cdot [b]]$. What about exponentiation? Since it is usually defined by repeated multiplication

$$a^n := \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ times}} \qquad (n \in \mathbb{N})$$

we obviously get $[a^n] = [[a]^n]$ and the usual rules such as $a^n \cdot b^n = (a \cdot b)^n, (a^n)^m = a^{n \cdot m}$ in any commutative ring. Note however that while a, b can be elements of any commutative ring, m, n are integers — exponentiation with exponents in any ring is not defined! Thus, in the last formula, the multiplication in the exponent is normal integer multiplication. In a field, we can define exponentiation with negative exponents the usual way $a^{-n} := (1/a)^n$ for any base except 0 (we leave 0^0 undefined).

In some cases, we can reduce exponents as well to calculate more efficiently. Let's try and calculate $3^{10} \pmod 5$. Since we expect a result in $\mathbb{Z}_5$, surely we can reduce that 10? The wrong way to do this is to note that $[10] = 0$ modulo 5, so $3^0 = 1$. Wrong, because $3^{10} = 59049 = 11809 \cdot 5 + 4$ so the correct answer is 4, not 1. What went wrong? The problem is that exponents, as we mentioned, are integers and not ring elements — even if ring elements are sometimes integers too. We summarise:

WARNING: you can reduce $\pmod n$ at any time in addition, subtraction, multiplication and (where defined) division in $\mathbb{Z}_n$. You cannot reduce exponents this way.

[1] We haven't formally covered monoids in this course but they are structures $(M, +)$ where $+$ is associative and has a neutral element, but not necessarily inverses. If $(R, +, \cdot)$ is a ring then $(R, \cdot)$ is a monoid.

[2] Except in the field with one element (the ring with one element is a field!), you cannot of course divide by zero.

There is a way to reduce the exponent correctly though. Recall that $(Z_n^\times, \cdot)$ is a group, so each element a of this group has an order k for which $a^k = 1$ in the group. And all these element orders must divide the group order by Lagrange's theorem; the group order is of course $\phi(n)$. So the correct way to reduce exponents is taking them modulo $\phi(n)$ instead of n. In our example $3^{10} \pmod 5$ we have $\phi(5) = 4$ so $3^{10} = 3^{10 \pmod{\phi(5)}} = 3^{10 \pmod 4} = 3^2 = 4 \pmod 5$. So the correct formula is

$$a^k = (a \mod n)^{(k \mod \phi(n))} \pmod n$$

using $[\,]_n$ to denote reduction modulo n we can also write this as

$$[a^k]_n = [\ ([a]_n)^{[k]_{\phi(n)}}\ ]_n$$

that is, you reduce group elements or bases modulo n and exponents modulo $\phi(n)$. In the special case where n is a prime, $\phi(n) = n - 1$.

For large values of n and its prime factors, computing $\phi(n)$ is much more time-consuming than simple computation modulo n: essentially, you have to perform a task similar to factoring n to get hold of $\phi(n)$. This forms the basis of the famous RSA cryptosystem and much of modern cryptography that has been developed since.

Exercise. ($\star\star$) *Exponentiation modulo n.* Compute the following value:

$$2^{128} - 1 \pmod{1009}$$

Hint: you definitely do not want to compute all the digits of 2^{128}! You know that $[a + b] = [[a] + [b]]$ and $[a \cdot b] = [[a] \cdot [b]]$ where $[\,]$ is reduction modulo 1009. You can also avoid doing 128 individual calculations and do 8 instead.

3.8 ◇ Cancellation and integral domains

◇ In a group, you can "cancel" in additions: $x+a = y+a$ implies $x = y$. This holds because group elements have inverses: given $x + a = y + a$ you can add the inverse of a on both sides to get $(x + a) + (-a) = (y + a) + (-a)$, swap the brackets round with the associative law to get $x + (a + (-a)) = y + (a + (-a))$, use the property of inverses to get $x + 0 = y + 0$ and the property of the neutral element to get $x = y$.

If an element in a ring is not zero or a zero-divisor, you can still cancel it — but the reason is a slightly different one. Suppose a is such an element and $a \cdot x = a \cdot y$. This implies that $a \cdot (x - y) = 0$ (subtract $a \cdot y$ on both sides and use the distributive law) but since a is not a zero divisor, this means that $x - y = 0$ and therefore $x = y$.

A ring in which there are no zero divisors and you can cancel multiplication with anything except 0 is called an integral domain. The standard example of an integral domain is $\mathbb{Z}$: $3 \cdot x = 3 \cdot y$ implies $x = y$ even without you having to extend to $\mathbb{Q}$ in order to invert 3.

Definition 3.9 (integral domain). A ring $\mathcal{R}$ in which there are no zero divisors is called an integral domain.