Chapter 1

Modular arithmetic and fields

We begin with some number theory, looking at divisibility properties of the natural numbers and the integers.

natural numbers: $\mathbb{N} = \{1, 2, 3, 4, \dots\}$
integers: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

We then introduce a fundamental concept in number theory: the idea of modular arithmetic due to Gauss. This provides examples of algebraic structures (groups and fields) that will be important throughout this subject. Modular arithmetic also plays a key role in cryptography, used daily to provide secure transmission of information over the internet.

1 Well-ordering and induction

An important property of the natural numbers that we will need is the following:

Well-ordering property: (WOP)

Every non-empty subset of $\mathbb{N}$ has a smallest element.

It is equivalent to the following:

Principle of mathematical induction: (PMI)

Suppose that we have a set of statements $\{S(n) \mid n \in \mathbb{N}\}$ satisfying:

1) $S(1)$ is true
2) $\forall n \in \mathbb{N} \quad S(n) \implies S(n+1)$

Then $S(n)$ is true for all $n \in \mathbb{N}$.

Which is equivalent to:

Strong form of induction: (SMI)

Suppose that we have a set of statements $\{S(n) \mid n \in \mathbb{N}\}$ satisfying:

1) $S(1)$ is true
2) $\forall n \in \mathbb{N} \quad (S(1) \wedge S(2) \wedge \cdots \wedge S(n)) \implies S(n+1)$

Then $S(n)$ is true for all $n \in \mathbb{N}$.

We will show that the above three properties of $\mathbb{N}$ are equivalent by showing that

$$\text{WOP} \implies \text{PMI} \implies \text{SMI} \implies \text{WOP}$$

WOP $\implies$ PMI: Suppose first that the well-ordering property holds. Assume that $S(n)$ are as in the statement of the principle of mathematical induction. We need to show that $S(n)$ is true for all $n \in \mathbb{N}$. Let $E = \{n \in \mathbb{N} \mid S(n) \text{ is false}\}$. Suppose, for a contradiction, that E is non-empty. By the WOP, E has a minimum element, call it $m \in E$. Since $S(1)$ is true, we have that $m \neq 1$. Therefore $m - 1 \in \mathbb{N}$ and $S(m-1)$ is true by the minimality of m. But $S(m-1)$ is true implies that $S(m)$ is true. From this contradiction we conclude that $E = \varnothing$.

PMI $\implies$ SMI: Exercise!

SMI $\implies$ WOP: Assume that SMI holds. Let $E \subseteq \mathbb{N}$ be such that E does not have a smallest element. We want to show that $E = \varnothing$. Let $S(n)$ be the statement $n \notin E$. Then $S(1)$ is true since otherwise $1 \in E$ would be minimal. Suppose that $S(1)$, S(2),$\ldots, S(n)$ are all true. Then $1 \notin E$,$\ldots, n \notin E$. If $n \in E$, then n would be minimal. Since E has no minimal element, we must have that $S(n)$ is true. From SMI we conclude that $S(n)$ is true for all $n \in \mathbb{N}$, that is, $E = \varnothing$.

Exercise 1. Show that WOP holds for every subset of $\mathbb{Z}$ that is bounded below. That is, if $E \subseteq \mathbb{Z}$ is bounded below, then every non-empty subset of E has a minimal element. What about subsets of $\mathbb{Q}$ (or $\mathbb{R}$) that are bounded below?

2 Integer division

Theorem 1.1

Let $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there exist $q, r \in \mathbb{Z}$ such that

$$a = qd + r \quad \text{and} \quad 0 \leqslant r < d$$

Moreover, q and r are uniquely determined by a and d.

The integers q and d are known as the **quotient** and **remainder** respectively.

Proof. Given $a \in \mathbb{Z}$ and $d \in \mathbb{N}$ define $E = \{k \in \mathbb{Z} \mid k \geqslant 0 \text{ and } k = a - qd \text{ for some } q \in \mathbb{Z}\}$. Note that $E \neq \varnothing$ since $a - (-|a|)d = a + d|a| \geqslant 0$. By WOP, E has a minimal element $r \in E$. Since $r \in E$, we have $r \geqslant 0$ and there is a $q \in \mathbb{Z}$ such that $r = a - qd$. Also, $r < d$ since

$$r \text{ is minimal in } E \implies r - d \notin E \implies r - d = a - (q+1)d \notin E \implies r - d < 0 \implies r < d$$

The uniqueness of q and r is left as an exercise. □

Remark. There are versions of this result that hold when $\mathbb{Z}$ is replaced by $\mathbb{R}[X]$ or $\mathbb{Z}[i]$ (and others). The proof is essentially the same.

Definition 1.2. Let $a, d \in \mathbb{Z}$. We say that d **divides** a if $\exists\, q \in \mathbb{Z}$ such that $a = qd$. It is often denoted by $d \mid a$. We also say that d is a **divisor** of a.

Lemma 1.3

Let $a, b, c \in \mathbb{Z}$. Then

1) $(a \mid b) \wedge (b \mid c) \implies a \mid c$
2) $(a \mid b) \wedge (a \mid c) \implies \forall x, y \in \mathbb{Z}, \quad a \mid (xb + yc)$
3) $(a \mid b) \wedge (b \mid a) \implies a = \pm b$
4) $a \mid 1 \implies a = \pm 1$

Proof. Left as an exercise. □

Definition 1.4. Let $a, b \in \mathbb{Z}$. A **greatest common divisor** (gcd) of a and b is an element $d \in \mathbb{Z}$ such that

1) $(d \mid a) \wedge (d \mid b)$

2) $\forall c \in \mathbb{Z}, \quad (c \mid a) \wedge (c \mid b) \implies c \mid d$

Lemma 1.5

Let $a, b \in \mathbb{Z}$ be such that at least one of a and b is non-zero. Then there is a unique $d \in \mathbb{N}$ such that d is a gcd of a and b. It will be denoted $d = \gcd(a, b)$.

Proof. We first show that there exists a greatest common divisor $d \in \mathbb{N}$. Let $E = \{k > 0 \mid \exists\, x, y \in \mathbb{Z}, \quad k = xa + yb\}$. Then $E \subseteq \mathbb{N}$ and $E \neq \varnothing$ (since $a^2 + b^2 \in E$). By the WOP, E has a minimal element $d \in S$. Fix $x, y \in \mathbb{Z}$ such that $d = xa + yb$. By Theorem 1.1 there exist $q, r \in \mathbb{Z}$ with $a = qd + r$ and $0 \leqslant r < d$. Then

$$r = a - qd = a - q(xa + yb) = (1 - qx)a + (-qy)b$$

We must, therefore, have $r = 0$ since otherwise $r \in E$ and $r < d$. Therefore $a = qd$, that is, $d \mid a$.

Similarly, $d \mid b$.

Now suppose that $c \mid a$ and $c \mid b$. Then $c \mid d = xa + yb$ (see Lemma 1.3).

Now for uniqueness. Suppose that d and d' are both satisfy the conditions for being a greatest common divisor of a and b. Then $d \mid d'$ and $d' \mid d$ which implies that $d' \pm d$. Since $d, d' \in \mathbb{N}$, we conclude that $d' = d$. □

Given the uniqueness pointed out in the above result we use the notation $\gcd(a, b)$ for *the* greatest common divisor of two integers a and b. In fact, the above proof establishes the following result.

Theorem 1.6: Bézout's Theorem

Let $a, b \in \mathbb{Z}$. Then there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$. □

Definition 1.7. We say that two integers $a, b \in \mathbb{Z}$ are **relatively prime** if $\gcd(a, b) = 1$.

2.1 Exercises

Exercise 2. Show that two integers $a, b \in \mathbb{Z}$ are relatively prime if and only if $\exists\, x, y \in \mathbb{Z}, \quad xa + yb = 1$.

Exercise 3. Find the quotient and remainder when:

(a) 25 is divided by 3 (b) 68 is divided by 7 (c) -33 is divided by 7

Exercise 4. Prove Lemma 1.3.

Exercise 5. Prove the uniqueness of q and d in Theorem 1.1. That is, show that if $qd + r = q'd + r'$ with $0 \leqslant r, r' < d$, then $q = q'$ and $r = r'$.

Exercise 6. Let $a, b, c \in \mathbb{Z}$ be integers with $\gcd(a, b) = 1$. Show that if $a \mid c$ and $b \mid c$, then $ab \mid c$.

Exercise 7. Let F_n be the n-th Fibonacci number, defined by $F_0 = 0$, $F_1 = 1$ and $F_{k+2} = F_k + F_{k+1}$.

(a) Use induction to show that $\gcd(F_n, F_{n+1}) = 1$ for all $n \in \mathbb{N}$.

(b) Find integers x_n, y_n such that $x_n F_n + y_n F_{n+1} = 1$.

3 Euclidean algorithm

The greatest common divisor of two integers can be computed by first finding the prime factorisations of the given integers. However, a mush more efficient method is given by the Euclidean algorithm. It is based on the following observations.

Lemma 1.8

Let $a, b, q, r \in \mathbb{Z}$.

1) $\gcd(a, b) = \gcd(b, a) = \gcd(-a, b)$
2) $\gcd(a, 0) = |a|$
3) If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$

Proof. We shall prove 3) and leave the rest as an exercise. Since $\gcd(a, b)$ divides both a and b, we have

$$\gcd(a, b) \mid b \quad \text{and} \quad \gcd(a, b) \mid r = (a - qb)$$

which implies that $\gcd(b, r) \mid \gcd(a, b)$. Similarly,

$$\gcd(b, r) \mid a = qb + r \quad \text{and} \quad \gcd(b, r) \mid b$$

which implies that $\gcd(a, b) \mid \gcd(b, r)$. Since both are positive, we have $\gcd(a, b) = \gcd(b, r)$. □

Given $a \geqslant b > 0$, define q_i and r_i as follows:

$$\begin{aligned} a &= q_1 b + r_1 & r_1 &< b \\ b &= q_2 r_1 + r_2 & r_2 &< r_1 \\ r_1 &= q_3 r_2 + r_3 & r_3 &< r_2 \\ &\vdots & &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n & r_n &< r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0 & 0 &< r_n \end{aligned}$$

Since the r_i are strictly decreasing, we must eventually arrive at a remainder of zero. By Lemma 1.8 we have

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, 0) = r_n$$

That is, the greatest common divisor of a and b is given by the last non-zero remainder obtained.

Example 1.9. We calculate the greatest common divisor of 4163 and 8869.

$$8869 = 2 \times 4163 + 543 \tag{1.1}$$
$$4163 = 7 \times 543 + 362 \tag{1.2}$$
$$543 = 1 \times 362 + 181 \tag{1.3}$$
$$362 = 2 \times 181 + 0 \tag{1.4}$$

Therefore $\gcd(4163, 8869) = 181$
Note that we can also express the greatest common divisor as a linear combination of a and b.
Working back through the above calculation, we get

$$\begin{aligned} 181 &= 543 - 362 && \text{(from 1.3)} \\ &= 543 - (4163 - 7 \times 543) && \text{(from 1.2)} \\ &= -4163 + 8 \times 543 \\ &= -4163 + 8(8869 - 2 \times 4163) && \text{(from 1.1)} \\ &= -17 \times 4163 + 8 \times 8869 \end{aligned}$$

3.1 Exercises

Exercise 8. Using the Euclidean Algorithm (by hand) find:

(a) $\gcd(14, 35)$
(b) $\gcd(105, 165)$
(c) $\gcd(1287, 1144)$
(d) $\gcd(1288, 1144)$
(e) $\gcd(1287, 1145)$

Exercise 9. Find the greatest common divisor $d = \gcd(a, b)$ for the following pairs of numbers (a, b), and find integers x and y so that $d = xa + yb$.

(a) $(27, 33)$ (b) $(27, 32)$ (c) $(312, 377)$

Exercise 10. Complete the proof of Lemma 1.8

4 Primes

Lemma 1.10

Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof. We have

$$xa + yb = 1 \qquad \text{for some } x, y \in \mathbb{Z}$$

and

$$bc = az \qquad \text{for some } z \in \mathbb{Z}$$

therefore

$$xac + ybc = c \implies xac + yaz = c \implies (xc + yz)a = c \implies a \mid c$$

□

Definition 1.11. A natural number $p \in \mathbb{N}$ is called **prime** if $p \neq 1$ and $\forall\, a, b \in \mathbb{Z}, \quad p \mid ab \implies (p \mid a) \vee (p \mid b)$

Lemma 1.12

A natural number $p \in \mathbb{N}$ is prime if and only if it has exactly two divisors in $\mathbb{N}$.

Proof. Assume that p is prime. Then $p \neq 1$ and both 1 and p are divisors of p. We need to show that these are the only positive divisors of p. Suppose that $p = ab$ for some $a, b \in \mathbb{N}$. Since $p \mid p = ab$ and p is prime, we have that $p \mid a$ or $p \mid b$. Note that

$$\begin{aligned} p \mid a &\implies a = pq && \text{(some } q \in \mathbb{N}) \\ &\implies p = pqb \\ &\implies qb = 1 && \text{(since } p \neq 0) \\ &\implies b = 1 && \text{(since } b, q \in \mathbb{N}) \\ &\implies a = p && \text{(since } p = ab) \end{aligned}$$

Similarly, if $p \mid b$, then $a = 1$ and $b = p$.

For the converse, assume that p has exactly two positive divisors. First note that $p \neq 1$ by Lemma 1.3. The two distinct positive divisors of p are therefore 1 and p. Let $a, b \in \mathbb{Z}$ be such that $p \mid ab$. We want to show that either $p \mid a$ or $p \mid b$, which is equivalent to showing that $p \nmid a \implies p \mid b$.

$$\begin{aligned} p \nmid a &\implies \gcd(a, p) = 1 && \text{(since } \gcd(a, p) \mid p) \\ &\implies p \mid b && \text{(by Lemma 1.10 since } p \mid ab) \end{aligned}$$

□

Theorem 1.13: The Fundamental Theorem of Arithmetic

Let $n \in \mathbb{N}$ with $n \geqslant 2$. Then there exist $k \in \mathbb{N}$, and $i_1, \ldots, i_k \in \mathbb{N}$, and primes $p_1 < p_2 < \cdots < p_k \in \mathbb{N}$ such that

$$m = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$$

Moreover, this expression is uniquely determined by m.

Proof. Left as an exercise. Hint: For existence use Strong Mathematical Induction. □

4.1 Exercises

Exercise 11. (a) Give an example of natural numbers a, b, c such that $a \mid c$ and $b \mid c$ but $ab \| c$.

(b) Let $a, b, c \in \mathbb{Z}$ be integers with $\gcd(a, b) = 1$. Prove that if $a \mid c$ and $b \mid c$ then $ab \mid c$.

Exercise 12. Prove Theorem 1.13.

5 Modular arithmetic

5.1 Congruence

Definition 1.14. Fix $m \in \mathbb{N}$. We say that $a, b \in \mathbb{Z}$ are **congruent modulo m** if $m \mid (a - b)$. It is denoted

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

Example 1.15.

$$42 \equiv 6 \pmod{4}$$
$$77 \equiv -4 \pmod{9}$$
$$15 \equiv 0 \pmod{5}$$

Remark. It follows from Theorem 1.1 that given $a \in \mathbb{Z}$ and $m \in \mathbb{N}$, there exists a unique $r \in \mathbb{Z}$ with $0 \leqslant r < m$ such that $a \equiv r \pmod{m}$.

The following are fundamental properties of the congruence relation. They say that, for a fixed m, being congruent modulo m is an "equivalence relation".

Lemma 1.16: congruence is an equivalence relation

Let $m \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then

1) $a \equiv a \pmod{m}$ (reflexive)
2) $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ (symmetric)
3) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$ (transitive)

Proof. For the first two, note that $m \mid 0$ and that $(a - b) \mid (b - a)$. For the third note that

$$(m \mid (a - b)) \wedge (m \mid (b - c)) \implies m \mid (a - b) + (b - c) = a - c$$

□

The next result is that congruence works well with the arithmetic operations on $\mathbb{Z}$.

Lemma 1.17

Let $m, n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$. Suppose that $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. Then

1) $a + b \equiv c + d \pmod{m}$
2) $a - b \equiv c - d \pmod{m}$
3) $ab \equiv cd \pmod{m}$
4) $a^n \equiv c^n \pmod{m}$

Proof. For the first note that

$$m \mid (a-c) \wedge m \mid (b-d) \implies m \mid ((a-c)+(b-d)) \implies m \mid ((a+b)-(c+d)) \implies a+b \equiv c+d \pmod{m}$$

For the third note that

$$\begin{aligned} m \mid (a-c) \wedge m \mid (b-d) &\implies (a-c=mk) \wedge (b-d=ml) && \text{(for some } k,l \in \mathbb{Z}\text{)} \\ &\implies (a=mk+c) \wedge (b=ml+d) \\ &\implies ab = cd + cml + mkd + m^2kl \\ &\implies ab - cd = m(cl+kd+mkl) \\ &\implies ab \equiv cd \pmod{m} \end{aligned}$$

The remaining cases are left as an exercise. □

Example 1.18. We find an r with $0 \leqslant r < 12$ such that $29^4 \equiv r \pmod{12}$. Rather than calculating 29^4, we will use Lemma 1.17. Noting first that $29 \equiv 5 \pmod{12}$, we have

$$\begin{aligned} & 29^4 \equiv 5^4 \pmod{12} && \text{(Lemma 1.17.4)} \\ \implies & 29^4 \equiv 25^2 \pmod{12} \\ \implies & 29^4 \equiv 1^2 \pmod{12} && \text{(since } 25 \equiv 1 \pmod{12}\text{)} \\ \implies & 29^4 \equiv 1 \pmod{12} \end{aligned}$$

Definition 1.19. Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$. The **congruence class** of a modulo m is the following subset of $\mathbb{Z}$ which is denoted $[a]_m$.

$$[a]_m = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

Example 1.20.

$$\begin{aligned} [0]_3 &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ [1]_3 &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ [2]_3 &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} \\ [3]_3 &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \end{aligned}$$

Exercise 13. Prove the following:

(a) $[a]_m = [b]_m$ if and only if $a \equiv b \pmod{m}$

(b) $[a]_m \cap [b]_m \neq \varnothing \implies [a]_m = [b]_m$

(c) $[0]_m \cup [1]_m \cup \cdots \cup [m-1]_m = \mathbb{Z}$

5.2 Integers modulo m

Definition 1.21. The set of congruence classes is denoted $\mathbb{Z}/m\mathbb{Z}$ and is called the **integers modulo** m. That is,

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

Remark. Notice that $|\mathbb{Z}/m\mathbb{Z}| = m$

Example 1.22. $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$

We define two binary operations on $\mathbb{Z}/m\mathbb{Z}$ in the following way:

$$\begin{aligned} [a]_m + [b]_m &= [a+b]_m \\ [a]_m \times [b]_m &= [a \times b]_m \end{aligned}$$

Remark.

1) It is important to realise that what is being defined here is what the symbols '+' and '×' mean when used as on the left. On the right of the above definitions the same symbols are used to represent the usual operations of addition and multiplication in $\mathbb{Z}$.

2) Each binary relation is a function $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

3) These operations are 'well-defined', meaning that if a, b, α, β are such that $[a]_m = [\alpha]_m$ and $[b]_m = [\beta]_m$, then $[a+b]_m = [\alpha+\beta]_m$ and $[a \times b]_m = [\alpha \times \beta]_m$.

4) As with $\mathbb{Z}$, we often omit the symbol '$\times$' and write $[a]_m[b]_m$ in place of $[a]_m \times [b]_m$.

5) $[a_m]_m[1]_m = [a]_m$ and $[a_m]_m + [0]_m = [a]_m$for all $[a]_m \in \mathbb{Z}/m\mathbb{Z}$.

6) Equipped with these operations, $\mathbb{Z}/m\mathbb{Z}$ forms what is called a 'commutative ring'.

Definition 1.23. We say that $[a]_m$ is the **multiplicative inverse** of $[b]_m$ if $[a]_m[b]_m = [1]_m$.

Exercise 14. Show that $[a]_m$ has at most one multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$.

Example 1.24. The multiplication table for $\mathbb{Z}/6\mathbb{Z}$ is shown. Note that in this table we have written a in place of $[a]_6$. The element $[5]_6$ is the multiplicative inverse of itself. The element $[2]_6$ has no multiplicative inverse.

$(\mathbb{Z}/6\mathbb{Z}, \times)$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Theorem 1.25

Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then $[a]_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$.

Proof. Suppose that $[a]_m$ has a multiplicative inverse. That is, there exists $b \in \mathbb{Z}$ such that $[a]_m[b]_m = [1]_m$. Then note that

$$\begin{aligned}
[a]_m[b]_m = [1]_m &\implies [ab]_m = [1]_m \\
&\implies ab \equiv 1 \pmod{m} \\
&\implies m \mid (ab-1) \\
&\implies ab - 1 = mk && \text{(for some } k \in \mathbb{Z}\text{)} \\
&\implies ab - mk = 1 \\
&\implies \gcd(a, m) = 1 && \text{(see Exercise 2)}
\end{aligned}$$

For the converse, we have

$$\begin{aligned}
\gcd(a, m) = 1 &\implies xa + my = 1 && \text{(for some } x, y \in \mathbb{Z}\text{, by Theorem 1.6)} \\
&\implies xa - 1 = -my \\
&\implies xa \equiv 1 \pmod{m} \\
&\implies [x]_m[a]_m = [1]_m
\end{aligned}$$

□

Corollary 1.26

If p is prime, then every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. □

5.3 Exercises

Exercise 15. Write down the multiplication tables for $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$.

Exercise 16. Decide whether the following congruences hold.

(a) $3 \equiv 42 \pmod{13}$

(b) $2 \equiv -20 \pmod{11}$

(c) $26 \equiv 482 \pmod{14}$

(d) $-2 \equiv 933 \pmod{5}$

(e) $-2 \equiv 933 \pmod{11}$

(f) $-2 \equiv 933 \pmod{55}$

Exercise 17. Simplify the following, writing your answers in the form $a \bmod m$ where $0 \leqslant a < m$.

(a) $482 \pmod{14}$

(b) $511 \pmod{9}$

(c) $-374 \pmod{11}$

(d) $933 \pmod{55}$

(e) $102725 \pmod{10}$

(f) $57102725 \pmod{9}$

Exercise 18. Calculate the following, giving answers in the form $a \bmod m$ where $0 \leqslant a < m$.
(Hint: it's easiest to reduce modulo m as soon as possible.)

(a) $24 \times 25 \pmod{21}$

(b) $84 \times 125 \pmod{210}$

(c) $25^2 + 24 \times 3 - 6 \pmod{9}$

(d) $36^3 - 3 \times 19 + 2 \pmod{11}$

(e) $1 \times 2 \times 3 \times 4 \times 5 \times 6 \pmod{7}$

(f) $1 \times 2 \times 3 \times \cdots \times 20 \times 21 \pmod{22}$

Exercise 19. Use congruences modulo 9 to show that the following multiplication is incorrect:

$$326 \times 4471 = 1357546.$$

Exercise 20. Show that if n is an integer with $n \equiv 7 \pmod{8}$, then the equation

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

has no solutions with x, y, z integers.

Exercise 21. In the following systems $\mathbb{Z}/m\mathbb{Z}$ write down the set of elements that have multiplicative inverses.

(a) $\mathbb{Z}/7\mathbb{Z}$

(b) $\mathbb{Z}/8\mathbb{Z}$

(c) $\mathbb{Z}/12\mathbb{Z}$

(d) $\mathbb{Z}/13\mathbb{Z}$

(e) $\mathbb{Z}/15\mathbb{Z}$

Exercise 22. Using the Euclidean algorithm, find the multiplicative inverses of the following (if they exist). Here we use a as an abbreviation for $[a]_m$.

(a) 32 in $\mathbb{Z}/27\mathbb{Z}$

(b) 32 in $\mathbb{Z}/39\mathbb{Z}$

(c) 17 in $\mathbb{Z}/41\mathbb{Z}$

(d) 18 in $\mathbb{Z}/33\mathbb{Z}$

(e) 200 in $\mathbb{Z}/911\mathbb{Z}$

Exercise 23. Find the smallest positive integer giving a remainder of 3 when divided by 7, and a remainder of 8 when divided by 11.

Exercise 24. (Harder!) Prove the **Chinese remainder theorem**:
Let m_1, m_2 be relatively prime integers, and let a_1, a_2 be any integers. Then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1} \qquad \text{and} \qquad x \equiv a_2 \pmod{m_2}$$

have a solution x and it is unique modulo $m_1 m_2$.
Generalise to an arbitrary number of congruences.

6 Fields

Definition 1.27. A **commutative ring** is a set R together with two binary operations '+' and '$\times$' satisfying

1) $\forall\, x, y, z \in R, \quad (x + y) + z = x + (y + z)$ (addition is associative)

2) $\forall\, x, y \in R, \quad x + y = y + x$ (addition is commutative)

3) $\exists\, 0 \in R\, \forall x \in R, \quad x + 0 = x$ (additive identity)

4) $\forall x \in R \, \exists y \in R, \quad x + y = 0$ (additive inverses)

5) $\forall\, x, y, z \in R, \quad (x \times y) \times z = x \times (y \times z)$ (multiplication is associative)

6) $\forall\, x, y \in R, \quad x \times y = y \times x$ (multiplication is commutative)

7) $\exists\, 1 \in R \, \forall x \in R, \quad 1 \times x = x$ (multiplicative identity)

8) $\forall\, x, y, z \in R, \quad x \times (y + z) = (x \times y) + (x \times z)$ (distriibutivity)

Example 1.28. 1. $\mathbb{Z}$ with the usual operations is a commutative ring

2. $\mathbb{N}$ with the usual operations is not a commutative ring (why not?)

3. $\mathbb{Z}/m\mathbb{Z}$ with the operations defined above is a commutative ring

4. $\mathbb{R}[X]$, the set of all polynomials equipped with the usual operations is a commutative ring

5. $\{*\}$ with operations given by $* + * = *$ and $* \times * = *$ is a commutative ring

Exercise 25. Show that the additive inverse of an element $x \in R$ (whose existence is given by axiom 4 above) is unique. It is denoted $-x$.

Exercise 26. Let R be a commutative ring, and $x \in R$ any two elements. Show that

a) $0x = 0$ b) $(-1)x = -x$

Exercise 27. Let R be a commutative ring. Show that if $1 = 0$ (i.e., the additive and multiplicative identities coincide), then R consists of a single element.

Definition 1.29. A **field** is a commutative ring having at least two elements and in which every non-zero element has a multiplicative inverse.

Example 1.30. 1. $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields

2. $\mathbb{Z}$ is not a field

3. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$ is a field

4. $\mathbb{Z}/p\mathbb{Z}$ for any prime p is a field. It will sometimes be denoted $\mathbb{F}_p$.

5. $\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\} \subset M_2(\mathbb{Z}/2\mathbb{Z})$ with the usual matrix operations is a field.

Definition 1.31. A field K is called **algebraically closed** if every non-constant polynomial over K has a root in K. That is,

$$\forall p(X) \in K[X], \quad \deg(p(X)) \geqslant 1 \implies (\exists\, k \in K, \quad p(k) = 0)$$

Example 1.32. 1. $\mathbb{Q}$ and $\mathbb{R}$ are not algebraically closed since $X^2 + 1$ has no root in $\mathbb{R}$

2. $\mathbb{F}_2$ is not algebraically closed since $X^2 + X + 1$ has no root in $\mathbb{F}_2$

We will need the following facts, we we state without proof.

Theorem 1.33: Fundamental Theorem of Algebra

The field $\mathbb{C}$ is algebraically closed.

Theorem 1.34: Algebraic closure

Any field can be embedded in an algebraically closed field.

6.1 Exercises

Exercise 28. Show that the set of all real numbers of the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ forms a field with the usual operations of addition and multiplication of the real numbers. (This is a *subfield* of $\mathbb{R}$.)

Exercise 29. Show that the set of all real numbers of the form $a + b\sqrt[3]{2}$ with $a, b \in \mathbb{Q}$ does not form a field with the usual operations of addition and multiplication of the real numbers. Is there a way to make a field, similar to the previous example of $\mathbb{Q}[\sqrt{2}]$, but which contains $\sqrt[3]{2}$ as well as the rational numbers?

Exercise 30. Find an element a of $\mathbb{F}_7$ so that every non-zero element of $\mathbb{F}_7$ is a power of a.

Exercise 31. Show that the set of all polynomials with real coefficients does not form a field (using the usual operations).

Exercise 32. (Harder) Let $\mathbb{C}(\!(t)\!)$ denote the set of all *formal Laurent series* of the form

$$c_{-k}t^{-k} + c_{-k+1}t^{-k+1} + \cdots + c_{-1}t^{-1} + c_0 + c_1 t + \cdots + c_s t^s + \ldots$$

with the usual operations of addition and multiplication of series. Show that $\mathbb{C}(\!(t)\!)$ forms a field. (You should ignore the question of whether the series are convergent.)

Exercise 33. Show that the field $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is not algebraically closed.

Exercise 34. Let K be a field having only finitely many elements. Show that K is not algebraically closed.

7 RSA cryptography

Cryptography is the study of keeping messages secret by coding the messages so only the intended recipient can read them.

In a **public key cryptosystem**, the key for encyrption can be made public, but decryption is not possible (in a reasonable amount of time) except by the intended recipient. In this section we outline the use of modular arithmetic in the **RSA cryptosystem**. It was developed in 1977 by Rivest, Shamir and Adleman and is a public key system very widely used today (for example, for transactions over the internet and in ATM machines). It relies on the difficulty of factoring large integers (typically more than 200 decimal digits) in a practical amount of time. (Currently, it takes many months of computing time to factor most numbers of 120-130 digits.) By contrast, large primes can be found efficiently using known primality tests.

7.1 Fermat's little theorem and Euler's theorem

We will need the following results.

Theorem 1.35: Fermat's Little Theorem

Let $p \in \mathbb{N}$ a prime number. If $a \in \mathbb{Z}$ is any integer which is not a multiple of p, then

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

Proof. Let $a \in \mathbb{Z}$ with $p \nmid a$. We will show that it must then be the case that p divides $a^{p-1} - 1$.

Since $p \nmid a$, we have that $[a]_p$ has a multiplicative inverse in $\mathbb{Z}/p\mathbb{Z}$ (Corollay 1.26). Let $[b]_p \in \mathbb{Z}/p\mathbb{Z}$ be such that $[b]_p[a]_p = [1]_p$. Consider the map $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ given by $[x]_p \mapsto [a]_p[x]_p$. This map is injective since

$$[a]_p[x]_p = [a]_p[y]_p \implies [b]_p[a]_p[x]_p = [b]_p[a]_p[y]_p \implies [x]_p = [y]_p$$

An injective map from a finite set to itself is necessarily also surjective. Therefore

$$\{[0]_p, [1]_p, \ldots, [p-1]_p\} = \{[0]_p, [a]_p, \ldots, [(p-1)a]_p\}$$

Multiplying together the non-zero elements, we obtain

$$\begin{aligned}
[a]_p \times [2a]_p \times \cdots \times [(p-1)a]_p &= [1]_p \times [2]_p \times \cdots \times [(p-1)]_p \\
[a^{p-1}(p-1)!]_p &= [(p-1)!]_p \\
\implies \quad & p \mid (a^{p-1}-1)(p-1)! \\
\implies \quad & p \mid (a^{p-1}-1) \text{ or } p \mid (p-1)! && (p \text{ is prime}) \\
\implies \quad & p \mid (a^{p-1}-1) && (\text{since } p \nmid (p-1)!)
\end{aligned}$$

□

Theorem 1.36: Euler

Let $p, q \in \mathbb{N}$ be primes with $p \neq q$. Suppose that $N \in \mathbb{N}$ satisfies $N \equiv 1 \pmod{(p-1)(q-1)}$.
Then

$$\forall a \in \mathbb{Z}, \qquad a^N \equiv a \pmod{pq}$$

Proof. Let $k \in \mathbb{Z}$ be such that $N = 1 + k(p-1)(q-1)$. By Fermat's Little Theorem, if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$. Thus

$$a^{k(p-1)(q-1)} \equiv (a^{p-1})^{k(q-1)} \equiv 1 \pmod{p}$$

and therefore

$$a^N \equiv a \pmod{p}$$

This equation also holds if $p \mid a$, since both sides are then 0. Therefore

$$\forall a \in \mathbb{Z} \qquad a^N \equiv a \pmod{p}$$

Similarly,

$$\forall a \in \mathbb{Z} \qquad a^N \equiv a \pmod{q}$$

Since $p \mid (a^N - a)$ and $q \mid (a^n - a)$ and $\gcd(p, q) = 1$, it follows that $pq \mid a^N - a$ (Exercise 11). Hence

$$\forall a \in \mathbb{Z} \qquad a^N \equiv a \pmod{pq}$$

□

7.2 RSA cryptosystem

Setting up an RSA cryptosystem

1. Choose two large primes $p \neq q$ (typically more than 150 decimal digits).
2. Compute $m = pq$.
3. Compute $n = (p-1)(q-1)$.
4. Choose an integer e with $1 < e < n$ such that $\gcd(e, n) = 1$.
5. Compute d such that $ed \equiv 1 \pmod{n}$ (using Euclid's algorithm).

We represent our message units by elements of $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$.

Then:

- the *public key* is: m, e. (These are made public and used to encrypt.)
- the *private key* is d. (This is kept secret and used to decrypt.)
- *encryption* of a message unit $X \in \mathbb{Z}/m\mathbb{Z}$ is given by

$$X \mapsto X^e \pmod{m}$$

- *decryption* is given by

$$Y \mapsto Y^d \pmod{m}$$

The original message is recovered since (by Euler's theorem)

$$(X^e)^d \equiv X^{ed} \equiv X \pmod{m}$$

Why is the RSA cryptosystem secure? To decrypt a message efficiently requires finding $n = (p-1)(q-1)$ or equivalently p and q. But factoring $m = pq$ is not computationally feasible with current algorithms and technology if m is large (e.g., 300-400 decimal digits).

Example 1.37. A very small example:

- Choose $p = 7, q = 13$
- Then $m = 7 \times 13 = 91$ and $n = 6 \times 72$
- Choose $e = 5$. (This is OK since $\gcd(5, 72) = 1$)
- Then $d = 29$ since $5 \times 29 = 145 \equiv 1 \pmod{72}$
- Public key is: $m = 91$, $e = 5$

If someone wants to send us the message:

$$23, \quad 85$$

they calculate

$$23^5 \equiv 4 \pmod{91}, \quad 85^5 \equiv 50 \pmod{91}$$

and send:

$$4, \quad 50$$

To decrypt, we calculate

$$4^{29} \equiv 23 \pmod{91}, \quad 50^{29} \equiv 85 \pmod{91}$$

and recover the original message:

$$23 \quad 85$$

7.3 Exercises

Exercise 35. We set up an RSA cryptosystem using primes $p = 3$ and $q = 19$.

(a) Write down $m = pq$ and $n = (p-1)(q-1)$.

(b) Show that $e = 5$ is a suitable choice of encrypting key.

(c) With this encrypting key, encrypt the message '2 3 6 18'.

(d) Calculate the decrypting key d (for $e = 5$).

(e) With this decrypting key, decrypt the message '7 50'.

Exercise 36. In this question we suppose that it has been agreed that the letters of the alphabet are encoded as

$$a = 1, b = 2, \ldots, z = 26 \quad \text{and} \quad \text{'space'} = 27$$

with no distinction made between upper and lower case. Messages are to be broken down into single letters which are then encrypted and sent in sequence.

Ada wants to be able to receive encrypted messages from her friends. She chooses two prime numbers: $p = 5$ and $q = 11$. The first part of her public key is then $m = 55$. She then calculates $n = (p-1)(q-1)$. Knowing that $e = 3$ satisfies $\gcd(e, n) = 1$, she tells all her friends to encrypt messages for her using the numbers 55 and 3.

(a) Calculate n. (Note that, in practice, m would be chosen large enough that calculating n without knowing the prime factorisation of m would be impractical.)

(b) Xav wants to send Ada the message: 'hi there'. What is the encrypted sequence Xav should send?

(c) Ada receives the encrypted message 2 20 39 15 8 21 9. By first calculating d such that $ed \equiv 1 \pmod{n}$, decrypt the message.