Mathematical preliminaries of crypto
Divisibility and Modular Arithmetic

Peeter Laud
(Minor changes by Dominique Unruh)

February 27, 2017

1 Integers. Divisibility

The cryptographic constructions we're going to see in further lectures and courses are built on top of various algebraic structures. All these structures, however, are ultimately built on top of integers. The set of *integers* is $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. On this set, we are given the binary operations "+" (addition) and "$\cdot$" (multiplication). The multiplication of elements can also be denoted by a simple juxtaposition of those elements, if that does not cause any confusion. The *algebraic structure*[1] $(\mathbb{Z}, +\cdot)$ is a *commutative ring*, meaning that

integers

- $(\mathbb{Z}, +)$ is an *Abelian group*, meaning that
  - $a + (b + c) = (a + b) + c$ and $a + b = b + a$ for all $a, b, c \in \mathbb{Z}$;
  - there exists a *zero element* $0 \in \mathbb{Z}$, such that $a + 0 = a$ for all $a \in \mathbb{Z}$;
  - for each $a \in \mathbb{Z}$, there exists its *negation*, denoted $-a$ and satisfying $a + (-a) = 0$.
- $(\mathbb{Z}, \cdot)$ is a *commutative monoid*, meaning that
  - $a(bc) = (ab)c$ and $ab = ba$ for all $a, b, c \in \mathbb{Z}$;
  - there exists a *unit element* $1 \in \mathbb{Z}$, such that $a \cdot 1 = a$ for all $a \in \mathbb{Z}$;
- Multiplication distributes over addition: $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{Z}$.

The multiplication operation in $\mathbb{Z}$ has further interesting properties that form the basis of most algorithms and constructions we're going to see in the future:

- Non-zero factors can be *canceled*: If $ac = bc$ and $c \neq 0$, then $a = b$.
- There are no *divisors of zero*: $ab = 0$ implies $a = 0$ or $b = 0$.

[1] A set with a number of operations given on it

- If $ab = 1$ then either $a = b = 1$ or $a = b = -1$. Hence the only *units* in $\mathbb{Z}$ are 1 and -1. An element x of some ring is a *unit* if there exists another element y of that ring, such that $xy = 1$. Such elements are also called *invertible* and y is called the *inverse* of x.

The set $\mathbb{Z}$ is also an ordered set. The order relation $\leq$ satisfies the following properties:

- It is reflexive ($a \leq a$), antisymmetric ($a \leq b$ and $b \leq a$ imply $a = b$) and transitive ($a \leq b$ and $b \leq c$ imply $a \leq c$).
- It is preserved by addition: $a \leq b$ implies $a + c \leq b + c$ for all $a, b, c \in \mathbb{Z}$.
- It is preserved by multiplication with non-negative integers: $a \leq b$ and $c \leq 0$ imply $ac \leq bc$ for all $a, b, c \in \mathbb{Z}$.

An important subset of $\mathbb{Z}$ is the set of *natural numbers* $\mathbb{N} = \{1, 2, \ldots\}$. For $\mathbb{N}$, certain divisibility-related properties are easier to state than for $\mathbb{Z}$, because $\mathbb{N}$ contains only a single unit element. **natural numbers**

We shall now study the concept of divisibility. This leads us to the notions of greatest common divisor (and least common multiple) and the equations they satisfy.

Definition 1. *Let $a, b \in \mathbb{Z}$. We say that a* divides *b (denoted $a \mid b$ or $b \vdots a$; the latter is read "b is divisible by a") if there exists $c \in \mathbb{Z}$, such that $b = ac$.* **divides**

For the same property we can also say that a is a *divisor* of b or that b is a *multiple* of a.

Exercise 1. *Among the following numbers, which are divisors of each other:*
$0, 1, -1, 2, 4, -5, 10, -10$*?*

Exercise 2. *Show that*

1. *units divide all integers;*
2. *only units divide units;*
3. *all integers divide* 0*;*
4. *the only integer dividing* 0 *is* 0*;*
5. *if $a \mid b$ and $b \mid a$ then exists a unit u, such that $a = ub$;*
6. *if $a \mid b$ and $a \mid c$ then $a \mid (b \pm c)$;*
7. *more generally: if $a \mid b_1, \ldots, a \mid b_n$ then $a \mid (b_1c_1 + \cdots + b_nc_n)$ for any $a, b_1, \ldots, b_n, c_1, \ldots, c_n \in \mathbb{Z}$;*
8. *if $a \mid b$ then $ac \mid bc$.*

Exercise 3. *Show that*

1. *$a \mid a$ for all $a \in \mathbb{Z}$;*

2. *If $a \mid b$ and $b \mid c$ then $a \mid c$ (for all $a, b, c \in \mathbb{Z}$).*

The previous exercise shows that the "divides" relation is a *pre-order* (a reflexive and transitive relation). As the set of natural numbers contains only a single unit, the property no. 5 in exercise 2 shows that "divides" relation is also antisymmetric on $\mathbb{N}$. Hence "divides" is a partial order on $\mathbb{N}$.

As the following results show, the partial order "divides" has a rich structure. Indeed, it satisfies the properties that are required from a *distributive lattice*.

2 Common divisors and multiples

Definition 2. *Let $a, b \in \mathbb{Z}$. An integer c is*

- common divisor *of a and b, if $c \mid a$ and $c \mid b$;* **common divisor**
- common multiple *of a and b, if $a \mid c$ and $b \mid c$;* **common multiple**
- greatest common divisor *of a and b if* **greatest common divisor**
  - *c is a common divisor of a and b, and*
  - *for all common divisors d of a and b the claim $d \mid c$ holds;*
- least common multiple *of a and b if* **least common multiple**
  - *c is a common multiple of a and b, and*
  - *for all common multiples d of a and b the claim $c \mid d$ holds.*

Exercise 4.

- *Find all common divisors of* 18 *and* 24.
- *Find all greatest common divisors of* 18 *and* 24.
- *Find all least common multiples of* 18 *and* 24.

Exercise 5. *Show that if c and d are both greatest common divisors [least common multiples] of a and b, then exists a unit u, such that $c = ud$.*

As there is only a single unit in $\mathbb{N}$, the greatest common divisor (if it exists; we haven't shown this yet) is uniquely determined among natural numbers. We let $\gcd(a, b) \in \mathbb{N}$ denote the greatest common divisor of $a, b \in \mathbb{Z}$ (if it exists). Similarly, we let $\operatorname{lcm}(a, b)$ denote the least common multiple of $a, b \in \mathbb{Z}$ (if it exists).

Exercise 6.

- *Show that if* $\gcd(a, b)$ *exists then* $\gcd(a, a + b)$ *also exists and equals* $\gcd(a, b)$.

- *Show that* $\gcd(a, b)$ *exists for all* a, b*. Hint: induction over* $|a| + |b|$*.*

The greatest common divisor also has the following properties.

Exercise 7. *Let* $a, b, c \in \mathbb{N} \cup \{0\}$*. Show that*

- $\gcd(a, b) = a$ *iff*[2] $a \mid b$*;*
- $\gcd(a, 0) = a$*;*
- $\gcd(a, b) = 0$ *iff* $a = b = 0$*;*
- $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.

The results analogous to the last few exercises also hold for the least common multiple. But they will be simpler to study after considering the unique-prime-factorization theorem.

3 Division with Remainder

Let a be an integer and b be a natural number. Then there exists a unique pair of integers (q, r), such that

$$a = qb + r \text{ and } 0 \leq r < b \ . \tag{1}$$

Here q is called the *quotient* and r the *remainder* of dividing a by b. Let us prove the claim of existence and uniqueness of (q, r). Consider the set

quotient
remainder

$$A = \{a - bx \,|\, x \in \mathbb{Z}, a - bx \geq 0\} \subseteq \mathbb{N} \cup \{0\} \ .$$

We show that the set A is not empty. Indeed, let $x = -a^2$. Then

$$a - bx = a - b(-a^2) = a + ba^2 \overset{(*)}{\geq} a + a^2 = a(a + 1) \overset{(**)}{\geq} 0 \ .$$

Here $(*)$ holds because $b \geq 1$ and $(**)$ holds because a and $a+1$ are either both positive, both negative (in both cases, their product is positive), or one of them is 0 (in this case, the product is also 0). Hence $a - b(-a^2)$ is an element of A.

Each non-empty subset of $\mathbb{N} \cup \{0\}$ has a minimal element (this claim is equivalent to the principle of mathematical induction). Let $r = \min A$. Let $q = (a - r)/b$. In other words, q is value of x that realizes $\min A$.

Let us show that $r < b$. If this were not the case then let $r' = r - b$ and $q' = q + 1$. We have $r > r'$ and $0 \leq r' = a - bq'$. Hence $r' \in A$ and $r \neq \min A$. We have shown that there exists a pair (q, r) that satisfies (1).

Let us show the uniqueness. Assume the opposite: there exist two pairs (q_1, r_1) and (q_2, r_2), both satisfying (1). We have $q_1 = (a - r_1)/b$ and $q_2 = (a - r_2)/b$. If $r_1 = r_2$ then also $q_1 = q_2$ and these two pairs would be equal. Assume thus that $r_1 \neq r_2$; w.l.o.g.[3] we

[2] "iff" is a contraction of "if and only if"

[3] without loss of generality

may assume that $r_1 > r_2$. From $a = qb_1 + r_1 = qb_2 + r_2$ we get $b(q_2 - q_1) = r_1 - r_2$, i.e. $r_1 - r_2$ is a multiple of b. But $b > r_1 - r_2 > 0$; there are no multiples of b between 1 and $b - 1$.

Exercise 8. *Find the quotient q and remainder r for the following for the following divisions a/b. Pay attention to the condition $0 \leq r < b$.*

- $6/3$*;*
- $7/3$*;*
- $(-6)/3$*;*
- $(-7)/3$.

We also introduce a notation for the remainder of the division. For $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ let $a \bmod b$ denote the number r in (1).

4 Euclid's algorithm for gcd

Exercise 9. *Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Show that* $\gcd(a, b) = \gcd(a \bmod b, b)$.

The previous exercise forms the basis of the general algorithm for finding the greatest common divisor of two integers $a, b \neq 0$. The algorithm works as follows

- Let $r_0 = |a|$ and $r_1 = |b|$. Assume w.l.o.g. that $r_0 \geq r_1$. Here $|x|$ denotes the *absolute value* of x.
- Compute $r_2 = r_0 \bmod r_1$, $r_3 = r_1 \bmod r_2$, $\ldots$, $r_i = r_{i-2} \bmod r_{i-1}$, $\ldots$
- Because of the properties of division with remainder, we have $r_i < r_{i-1}$ for all $i \geq 2$. Hence there exists an n, such that $r_n = 0$. We cannot continue the previous step beyond that point.
- $\gcd(a, b) = r_{n-1}$.

This algorithm is called the Euclid's algorithm.

Exercise 10. *Apply the previous algorithm to the following pairs of numbers (a, b) and see that it indeed computes* $\gcd(a, b)$ *for those numbers.*

- $(172, 20)$
- $(95, 39)$
- $(36, -108)$

Theorem 1. *Euclid's algorithm, when applied to $a, b \in \mathbb{N}$, computes* $\gcd(a, b)$.

The previous theorem easily generalizes to all non-zero integers.

Exercise 11. *How would one compute* $\gcd(a, b)$ *if* $a = 0$ *or* $b = 0$*?*

Let us prove theorem 1. It follows immediately from the following two lemmas. The first of them states that the algorithm outputs a common divisor of a and b, while the second states that it is the greatest one.

Lemma 1. *Euclid's algorithm outputs a common divisor of* a *and* b*.*

Proof. The output of Euclid's algorithm is the value r_{n-1}, where n is defined by the property $r_n = 0$. We show that r_{n-1} is a divisor of any r_i. The proof is by "downwards induction", where the base cases are $i = n - 1$ and $i = n$. Both cases are obvious: $r_{n-1} \mid r_{n-1}$ and $r_{n-1} \mid 0$.

Now let $i \leq n-2$. A step of the Euclid's algorithm defined $r_{i+2} = r_i \bmod r_{i+1}$. There exists an integer q_{i+2}, such that $r_i = q_{i+2}r_{i+1} + r_{i+2}$. By induction assumption, r_{n+1} divides r_{i-2} and r_{i-1}. Hence it also divides their integer linear combination r_i. □

Lemma 2. *If* c *is a common divisor of* a *and* b*, then it is also a divisor of* r_{n-1} *output by Euclid's algorithm.*

Proof. Let c be a common divisor of a and b. We show by induction that c is a common divisor of any r_i.

For $i = 0$ and $i = 1$ this is obvious. If $i \geq 2$ then $r_i = r_{i-2} \bmod r_{i-1}$. There exists an integer q_i, such that $r_{i-2} = q_i r_{i-1} + r_i$. By induction assumption, c divides r_{i-2} and r_{i-1}. Hence it also divides $q_i r_{i-1}$ and $r_i = r_{i-2} - q r_{i-1}$. □

There is an extremely important generalization of Euclid's algorithm which we can find in the proof of the following, equally important theorem.

Theorem 2 (Bézout's Identity)**.** *For all* $a, b \in \mathbb{Z}$ *there exist* $u, v \in \mathbb{Z}$*, such that* $au+bv = \gcd(a, b)$.

Proof. Consider Euclid's algorithm. We show by induction that for all $i \in \{0, \ldots, n-1\}$ there exist integers u_i, v_i, such that $au_i + bv_i = r_i$. Base cases: For $i = 0$ take $u_0 = \pm 1$ and $v_0 = 0$. For $i = 1$ take $u_1 = 0$ and $v_1 = \pm 1$ (here the signs depend on the signs of a or b).

For the induction step let $i \geq 2$ and assume we have the necessary integers $u_{i-2}, v_{i-2}, u_{i-1}, v_{i-1}$. Euclid's algorithm defines $r_i = r_{i-2} \bmod r_{i-1}$. Thus there exists $q_i = \lfloor r_{i-2}/r_{i-1} \rfloor$, such that $r_{i-2} = q_i r_{i-1} + r_i$ (here $\lfloor x \rfloor$ denotes the greatest integer not larger than x). Define now

$$u_i = u_{i-2} - q_i u_{i-1} \text{ and } v_i = v_{i-2} - q_i v_{i-1} \ .$$

Then

$$au_i+bv_i = au_{i-2}-aq_iu_{i-1}+bv_{i-2}-bq_iv_{i-1} = au_{i-2}+bv_{i-2}-q_i(au_{i-1}+bv_{i-1}) = r_{i-2}-qr_{i-1} = r_i \ .$$

□

The algorithm implicit in the proof of this theorem (finding $(u_0, v_0), (u_1, v_1), (u_2, v_2), \ldots, (u_{n-1}, v_{n-1})$ and outputting the last pair) is called the *extended Euclid's algorithm* (*EEA*).

extended Euclid's algorithm

Exercise 12. *Apply EEA to the pairs of integers in exercise 10.*

EEA

Exercise 13. *Show that* $a \mid bc$ *and* $\gcd(a, b) = 1$ *imply* $a \mid c$.

If $\gcd(a, b) = 1$ then we call the numbers a and b *mutually prime* and denote this situation by $a \perp b$.

mutually prime

5 Prime numbers

Definition 3. *A number* $n \in \mathbb{N}$ *is a* prime number *if it has exactly two divisors in* $\mathbb{N}$.

prime number

These two divisors are 1 (which divides all natural numbers) and the number n itself. Note that they must necessarily be different because the existence of two divisors has been required. The first primes are $2, 3, 5, 7, 11, 13, 17, \ldots$. Typically, we denote the set of all prime numbers by $\mathbb{P}$.

Definition 4. *A number* $n \in \mathbb{N}$ *is* composite *if it has more than two divisors in* $\mathbb{N}$.

composite

The first composite numbers are $4, 6, 8, 9, 10, 12, 14, 15, \ldots$. The number 1 is neither prime nor composite. All divisors (in $\mathbb{N}$) of n that are different from 1 and n are called *non-trivial divisors* of n.

Exercise 14. *Show that*

- *each* $n \in \mathbb{N} \backslash \{1\}$ *is divisible by some prime number;*
- *if* $p \in \mathbb{P}$ *and* $p \mid ab$ *then* $p \mid a$ *or* $p \mid b$.

The following results were already known at Euclid's time.

Theorem 3. *The set* $\mathbb{P}$ *is infinite.*

Proof. Assume the opposite: the set $\mathbb{P}$ is finite and $\mathbb{P} = \{p_1, \ldots, p_n\}$, where $p_1 < p_2 < \cdots < p_n$. Let $q = p_1 p_2 \cdots p_n + 1$. As $q > p_n$, the number q must be composite. By previous exercise, it must be divisible by some prime number — there exists i, such that $p_i \mid q$. But we also have $p_i \mid p_1 p_2 \cdots p_n = q - 1$ because this product contains p_i. Hence $p_i \mid q - (q - 1) = 1$ and $p_i = 1$, which is a contradiction because 1 is not a prime number. □

The prime numbers are the "building blocks" of all natural numbers if by "building" we mean multiplication.

Theorem 4 (Unique factorization theorem)**.** *Let* p_i *denote the* i*-th smallest prime number. Any natural number* n *can be expressed as*

$$n = \prod_{i \in \mathbb{N}} p_i^{e_i}, \tag{2}$$

where $e_i \in \mathbb{N} \cup \{0\}$ *and only a finite number of* e_i*-s are non-zero. Moreover, this representation is unique.*

Rushing ahead, the exponent e_i in (2) is called the *index* of p_i in n and denoted $\nu_{p_i}(n)$.

Proof. The existence of such factorization is easy to prove by induction over n. If $n = 1$ then take $e_1 = e_2 = \cdots = 0$. If n is a prime number p_i then take $e_i = 1$ and $e_j = 0$ for all $j \neq i$. If $n = m_1 m_2$ is a composite number and m_1, m_2 are its non-trivial divisors then by induction assumption, there exist factorizations of m_1 and m_2. The number n can be factorized by taking each e_i to be equal to the sum of corresponding exponents in the factorizations of m_1 and m_2. This summation also preserves the finiteness of the set of non-zero exponents.

Let us now show the uniqueness of such factorization. Assume the opposite: there exist two different lists $e_1, e_2, \ldots$ and $e'_1, e'_2, \ldots$, such that both lists have only a finite number of non-zero elements and

$$n = \prod_{i \in \mathbb{N}} p_i^{e_i} = \prod_{i \in \mathbb{N}} p_i^{e'_i} \ .$$

W.l.o.g. we may assume that n is the smallest number, such that these two different lists of exponents exist. In this case, for any i, $e_i \neq 0$ implies $e'_i = 0$ and vice versa, because otherwise we could divide both sides of the equation by p_i and obtain a smaller number n/p_i.

Now, if $e_i \neq 0$ then $p_i \mid \prod_{j \in \mathbb{N}} p_j^{e'_j}$. By the previous exercise, p_i divides a factor of the last product, i.e. some p_j where $e'_j \neq 0$. But $p_i \mid p_j$ is possible only if $i = j$. Hence $e'_i \neq 0$ which contradicts our choice of n as the smallest number for which two different prime factorizations exist. □

Exercise 15. *Find the prime factorizations of* 1, 4, 36, 720.

The prime factorizations are obviously very tightly related to the divisibility relation.

Exercise 16. *Let* $a = \prod_{i \in \mathbb{N}} p_i^{e_i}$ *and* $b = \prod_{i \in \mathbb{N}} p_i^{e'_i}$. *Show that*

- $a \mid b$ *iff* $e_i \leq e'_i$ *for all* i;
- $\gcd(a, b) = \prod_{i \in \mathbb{N}} p_i^{\min(e_i, e'_i)}$;
- $\operatorname{lcm}(a, b) = \prod_{i \in \mathbb{N}} p_i^{\max(e_i, e'_i)}$.

Exercise 17. *Prove the following properties of* gcd *and* lcm.

- $c \cdot \gcd(a, b) = \gcd(ac, bc)$ *and* $c \cdot \operatorname{lcm}(a, b) = \operatorname{lcm}(ac, bc)$;
- $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.
- *If* $a \perp c$ *and* $b \perp c$ *then* $ab \perp c$.

6 Modular arithmetic

If $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ then we let

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

denote that $a \bmod n = b \bmod n$ holds. As we immediately see, this "equivalence *modulo* n" behaves very nicely with respect to arithmetic operations.

Exercise 18. *Show that if* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$ *then* $a+c \equiv b+d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$.

Exercise 19. *Let* $k \in \mathbb{N}$. *Show that*

- $a \equiv b \pmod{n}$ *iff* $ak \equiv bk \pmod{nk}$.
- *If* $ka \equiv kb \pmod{n}$, *then* $a \equiv b \pmod{\frac{n}{\gcd(k,n)}}$.
  - *In particular: if* $k \perp n$ *then* $ka \equiv kb \pmod{n}$ *implies* $a \equiv b \pmod{n}$, *i.e.* k *cancels out. In a short while, we will see a deeper algebraic meaning of this cancelability.*

Exercise 20. *Show that* $a \equiv b \pmod{n}$ *iff* $n \mid (b - a)$.

When we say that an arithmetic expression *has to be computed modulo* n then we mean that we are interested in the remainder of the value of this expression when divided by n. For example, $(2 + 5) \cdot (8 + 6)$ is equal to 7 *modulo* 11, or

$$(2 + 5) \cdot (8 + 6) \equiv 10 \pmod{11} \ .$$

Exercise 18 allows us to perform computations *modulo* n, such that the intermediate values do not become much larger than n. Actually, when the operations that we're applying are only addition, subtraction and multiplication, then no intermediate value has to be larger than n^2. Namely, we can compute the remainder (by n) after each step of the computation. Thus, we could perform the previous computation by

$$\begin{aligned} 2 + 5 &= 7 \\ 8 + 6 = 14 &\equiv 3 \pmod{11} \\ 7 \cdot 3 = 21 &\equiv 10 \pmod{11} \ . \end{aligned}$$

Exercise 21. *Perform the following computations:*

- $(5 \cdot 8 - 3 \cdot 6) \cdot (8 + 4) \pmod{9}$;
- $\underbrace{7 \cdot 7 \cdots 7}_{15 \text{ times}} \pmod{11}$.
- $1 \cdot 2 \cdots 10 \pmod{25}$.

7 Residue classes

A *residue class modulo* n is a set of all integers that give the same remainder when divided by n. Formally, the residue class of $a \in \mathbb{Z}$ *modulo* $n \in \mathbb{N}$ is **residue class**

$$\overline{a} = \{b \in \mathbb{Z} \,|\, a \equiv b \pmod{n}\} = \{a + kn \,|\, k \in \mathbb{Z}\} \ .$$

In this notation, the modulus n is implicit. As the following exercises show, all residue classes *modulo* n partition the set $\mathbb{Z}$ into n parts.

Exercise 22. *Show that for all $a, b \in \mathbb{Z}$, the following three claims are equivalent:*

- $\overline{a} = \overline{b}$;
- $\overline{a} \cap \overline{b} \neq \emptyset$;
- $a \equiv b \pmod{n}$;
- *exists $k \in \mathbb{Z}$, such that $a = b + kn$.*

Exercise 23. *Show that $\overline{0}$, $\overline{1}$, ..., $\overline{n-1}$ are different residue classes.*

The first of those two exercises shows that there are at most n different residue classes *modulo* n, because there are n different remainders when dividing by n. The second exercise shows that the number of residue classes is at least n.

Denote $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. We can define addition and multiplication on $\mathbb{Z}_n$ as follows:

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a} \cdot \overline{b} &= \overline{a \cdot b} \ . \end{aligned}$$

Thanks to the properties of $\equiv$, as shown in exercise 18, these operations are *well-defined*. Namely, when we write $\overline{a+b}$, the integer a is only defined as an arbitrary element of the residue class $\overline{a}$. When we take an arbitrary element a of $\overline{a}$, and an arbitrary element b of $\overline{b}$, is it the case that the residue class $\overline{a+b}$ is always the same? In exercise 18 we showed that it indeed is. Similarly, the multiplication of residue classes is well-defined.

Exercise 24. *Show that $\mathbb{Z}_n$, together with the addition and multiplication operations we have defined, is a commutative ring.*

Because of the last exercises, we call $\mathbb{Z}_n$ the *residue class ring modulo* n.

Exercise 25. *Write down the addition and multiplication tables for $\mathbb{Z}_7$ and $\mathbb{Z}_8$.*

8 Units in residue class rings

Recall that an element x of a commutative ring R is called a unit if it is invertible — there exists y, such that $xy = 1$. We also denote such y by x^{-1}. We let R^* denote the set of all units of R.

Exercise 26. *Show that the inverse of a unit is unique and the inverse of the inverse is the element itself.*

Exercise 27. *Show that the product of two units of a ring is again a unit of that ring.*

The ring $\mathbb{Z}$ had just two units — 1 and (-1). As we saw in exercise 25, there may be more units in residue class rings. From the multiplication tables we constructed, we can also find the inverses of all elements of $\mathbb{Z}_7^*$ and $\mathbb{Z}_8^*$. Namely:

- In $\mathbb{Z}_7$: $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{4}$ (and vice versa), $\overline{3}^{-1} = \overline{5}$ (and vice versa), $\overline{6}^{-1} = \overline{6}$.
- In $\mathbb{Z}_8$: $\overline{a}^{-1} = \overline{a}$ for $a \in \{1, 3, 5, 7\}$.

When is an element invertible in $\mathbb{Z}_n$? We have the following result, the proof of which also explains how to find the inverse.

Theorem 5. *$\overline{a} \in \mathbb{Z}_n$ is invertible iff $a \perp n$.*

Proof. Let us first show the right-to-left direction. Assume $\gcd(a, n) = 1$. According to Theorem 2, there exist integers u and v (which can be found by using the extended Euclid's algorithm), such that $au + nv = 1$. This equality also holds *modulo* n, i.e. $au + nv \equiv 1 \pmod{n}$. Bu $n \mid nv$, hence $nv \equiv 0 \pmod{n}$ and $au \equiv 1 \pmod{n}$. In the residue class ring $\mathbb{Z}_n$, the last is equivalent to $\overline{a} \cdot \overline{u} = \overline{1}$, i.e. $\overline{a}^{-1} = \overline{u}$.

Let us now show the left-to-right direction. Assume $\overline{a}$ is invertible in $\mathbb{Z}_n$; let $\overline{b} = \overline{a}^{-1}$. The equality $\overline{a} \cdot \overline{b} = \overline{1}$ implies $ab \equiv 1 \pmod{n}$. The latter implies the existence of $k \in \mathbb{Z}$, such that $ab + kn = 1$. The properties of gcd now give us

$$\gcd(a, n) \leq \gcd(ab, n) = \gcd(ab + kn, n) = \gcd(1, n) = 1 \ .$$

Hence $\gcd(a, n) = 1$ because it cannot be smaller than that. □

Exercise 28. *Do the following residue classes have inverses in the following residue class rings? If yes, then find the inverse.*

- $\overline{6}$ *in* $\mathbb{Z}_9$*;*
- $\overline{13}$ *in* $\mathbb{Z}_{18}$*;*
- $\overline{21}$ *in* $\mathbb{Z}_{105}$*;*
- $\overline{100}$ *in* $\mathbb{Z}_{1001}$*.*

9 Solving linear congruences

Consider the following task. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Find $x \in \mathbb{Z}$ so, that

$$ax \equiv b \pmod{n} \ . \tag{3}$$

Obviously, if this congruence has any solutions, then it has an infinite number of solutions — the value of x is determined only *modulo* n. In effect, we are really considering (3) as a linear equation in the ring $\mathbb{Z}_n$ — find all $\overline{x} \in \mathbb{Z}_n$, such that $\overline{a} \cdot \overline{x} = \overline{b}$. We want to obtain a method for finding all suitable values of $\overline{x} \in \mathbb{Z}_n$.

If $\overline{a} \in \mathbb{Z}_n^*$, then it is easy to find such $\overline{x}$: multiply both sides of this equation by $\overline{a}^{-1}$. We obtain that in this case, $\overline{x} = \overline{b} \cdot \overline{a}^{-1}$. What if there were several $\overline{x}$-s satisfying the equation: $\overline{ax_1} = \overline{b}$ and $\overline{ax_2} = \overline{b}$. In this case we subtract the second equality from the first and obtain

$$\overline{a}(\overline{x_1} - \overline{x_2}) = \overline{0} \Rightarrow n \mid a(x_1 - x_2) \Rightarrow n \mid (x_1 - x_2) \Rightarrow x_1 \equiv x_2 \pmod{n} \Rightarrow \overline{x_1} = \overline{x_2} \ .$$

Here the second implication follows from our assumption that $a \perp n$, while other implications follow directly from the definitions of residue classes and congruences.

If $\overline{a}$ is not invertible in $\mathbb{Z}_n$, then let $d = \gcd(a, n)$; in this case $d > 1$. If $d \mid b$, then exercise 19 gives us

$$ax \equiv b \pmod{n} \Longleftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}} \ .$$

Let $a' = a/d$, $b' = b/d$, $n' = n/d$. We must solve the congruence $a'x \equiv b' \pmod{n'}$. We already know how to do it, because $a' \perp n'$. We obtain a single solution x_0 *modulo* n'. *Modulo* n, this corresponds to d different solutions — x_0, $x_0 + n'$, $x_0 + 2n'$, …, $x_0 + (d-1)n'$.

If $d = \gcd(a, n)$ is greater than 1 and b is not divisible by d, then the congruence (3) has no solutions. Indeed, if x were a solution then there would exist $k \in \mathbb{Z}$, such that $ax + kn = b$. Here ax and kn are both divisible by d, but b is not divisible by d.

Exercise 29. *Solve the following linear congruences*

- $6x \equiv 8 \pmod{11}$*;*
- $6x \equiv 8 \pmod{14}$*;*
- $6x \equiv 8 \pmod{15}$.

10 Elements of Group theory

We met the notion of *Abelian group* at the very beginning of this study unit, when we listed the properties of the ring of integers. Abelian groups are a subclass of groups, which we define next. **Abelian group**

A *group* is a set G together with a binary operation (denoted $\cdot$ or simply by juxtaposition) on it, such that **group**

- $\cdot$ is associative: for all $g_1, g_2, g_3 \in G$: $(g_1 g_2)g_3 = g_1(g_2 g_3)$;
- there is a unit element: exists $e \in G$, such that for all $g \in G$: $eg = g = ge$;
- each element has an inverse: for all $g \in G$ exists an element of G that we denote g^{-1}, such that $gg^{-1} = g^{-1}g = e$.

A group is *Abelian* if additionally, $\cdot$ is commutative: $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$.

If n is natural number and $g \in G$, then g^n denotes the element $\underbrace{g \cdot g \cdots g}_{n}$. Note that because of associativity, we do not have to indicate the order in which the multiplications have to be done. We extend this notation to all $n \in \mathbb{Z}$ by defining $g^0 = e$ and $g^{-n} = (g^{-1})^n$.

There are numerous examples of groups (mostly Abelian groups) among various sets of numbers. If we consider $+$ as the operation, then integers (the set $\mathbb{Z}$) is a group. Rational, real, or complex numbers are also groups. For each $n \in \mathbb{N}$, $\mathbb{Z}_n$ is also a group with respect to addition. All these groups are Abelian and 0 is the unit element in all of them.

With respect to the operation $\cdot$ (multiplication of numbers), the integers do not form a group. Neither do rationals, reals, or complex numbers form a group, because 0 has no inverse. But all non-zero rationals, reals, or complex numbers form a group.

For each ring R, the set R^* of all invertible elements of R forms a group with respect to multiplication in R. In particular, $\mathbb{Z}_n^*$ is a (multiplicative) group for each n.

For a different kind of an example, consider some set X and the set S_X of all *permutations* of X. I.e. the elements of S_X are functions φ from X to X, such that

1. for all $x_1, x_2 \in X$: if $\varphi(x_1) = \varphi(x_2)$ then $x_1 = x_2$;
2. for all $x \in X$ exists $y \in X$, such that $\varphi(y) = x$.

Note that because of the first property, the element y in the second property is uniquely determined by x.

The *composition* $(\varphi_1 \circ \varphi_2)$ of functions φ_1, φ_2 is defined by $(\varphi_1 \circ \varphi_2)(x) = \varphi_1(\varphi_2(x))$ for all $x \in X$. The set S_X is group with respect to the composition operation $\circ$. If X has at least 3 elements then this group is not commutative.

A *subgroup* of a group G is a subset H of G that **subgroup**

- is closed with respect to the group operation $\cdot$: if $h_1, h_2 \in H$ then also $h_1 h_2 \in H$;
- contains the inverses of all of its elements: if $h \in H$ then also $h^{-1} \in H$.

From these two properties follows trivially, that $e \in H$. We write $H \leq G$ if H is a subgroup of G.

Exercise 30. *Find all subgroups of* $\mathbb{Z}_{24}^*$, $\mathbb{Z}_{23}^*$, *and* $S_{\{1,2,3,4\}}$.

An important class of subgroups are those generated by a set of elements. Let $g_1, \ldots, g_k \in G$. The *group generated by* $g_1, \ldots, g_k$ is denoted by $\langle g_1, \ldots, g_k \rangle$ and it is the smallest subset of G that satisfies

- $g_1, \ldots, g_k \in \langle g_1, \ldots, g_k \rangle$;
- if $h_1, h_2 \in \langle g_1, \ldots, g_k \rangle$, then also $h_1 h_2 \in \langle g_1, \ldots, g_k \rangle$;
- if $h \in \langle g_1, \ldots, g_k \rangle$, then also $h^{-1} \in \langle g_1, \ldots, g_k \rangle$.

Comparing this definition with the definition of the subgroup, it is easy to see that $\langle g_1, \ldots, g_k \rangle \leq G$.

Exercise 31. *Enumerate the elements of the following subgroups generated by the following sets of elements:*

- $\langle 3 \rangle \leq \mathbb{Z}_{13}^*$;
- $\langle 3 \rangle \leq \mathbb{Z}_7^*$;
- $\langle 7, 15 \rangle \leq \mathbb{Z}_{16}^*$;
- $\langle \varphi_1, \varphi_2 \leq S_{\{1,2,3,4\}}$, *where*

$$\begin{aligned} \varphi_1(1) &= 2 & \qquad \varphi_2(1) &= 2 \\ \varphi_1(2) &= 3 & \qquad \varphi_2(2) &= 1 \\ \varphi_1(3) &= 1 & \qquad \varphi_2(3) &= 4 \\ \varphi_1(4) &= 4 & \qquad \varphi_2(4) &= 3 \ . \end{aligned}$$

Subgroups generated by a single element are called *cyclic* subgroups. A group G is a *cyclic group* if there exists $g \in G$, such that $\langle g \rangle = G$. Such g is called a *generator* of G. **cyclic group**

If we consider the addition of numbers as the group operation, then $\mathbb{Z}$, as well as all $\mathbb{Z}_n$ are cyclic — number 1 generates them all. For multiplicative groups, we state the following non-trivial number-theoretic result without a proof.

Theorem 6. *$\mathbb{Z}_n^*$ is cyclic iff $n = 2$ or $n = 4$ or $n = p^k$ or $n = 2p^k$ for some odd prime p and a natural number k.*

For a finite set X, we let $|X|$ denote its *cardinality* — the number of elements in X. For a finite group, "*order*" is a synonym of "cardinality". If G is a group and $g \in G$, then the *order of g* is the order of $\langle g \rangle$.

Exercise 32. *Find the orders of all elements of $\mathbb{Z}_7^*$ and $\mathbb{Z}_8^*$.*

Exercise 33. *Let G be a finite group and $g \in G$. Show that if n is the order of g, then $g^n = e$, and $g^m \neq e$ for all $m \in \{1, \ldots, n-1\}$.*

We finish this section with the following result that finds frequent applications in cryptography.

Theorem 7 (Lagrange)**.** *If G is a finite group and $H \leq G$ then the order of H divides the order of G.*

Proof. For any $a \in G$ define the set aH as follows:

$$aH = \{a \cdot h \,|\, h \in H\} \ .$$

The set aH is called a *(left) coset* of H (corresponding to the element $a \in G$). The following claims are trivial to prove.

- If $h \in H$ then $hH = H$. In particular, $eH = H$.
- If $a' \in aH$ and $h' \in H$, then $a'h' \in aH$.
- If $a_1, a_2 \in aH$ then there exists $h \in H$, such that $a_1 h = a_2$.
  - Indeed, if $a_1 = ah_1$ and $a_2 = ah_2$ for some $h_1, h_2 \in H$, then $a_2 = a_1 \cdot (h_1^{-1} h_2)$.

Obviously, each element $a \in G$ is an element of the coset aH. Hence the cosets of H cover the group G. We will show that they actually partition the group G. For this, it is sufficient to show that two different cosets do not intersect.

Let aH and bH be cosets of H and assume there exists some $g \in G$, such that $g \in aH \cap bH$. Let $h_a, h_b \in H$ be such that $g = ah_a = bh_b$. We will show that then $aH \subseteq bH$, a symmetric argument would then show $bH \subseteq aH$ and thus $aH = bH$. Let a' be an arbitrary element of aH. Let $h' \in H$ be such that $gh' = a'$; such h' exists according to the last claim above. Then $a' = gh' = b(h_b h')$, showing that a' is an element of bH.

As next we show that if aH and bH are two different cosets then they have the same cardinality. We do this by exhibiting a bijective mapping φ from aH to bH. The mapping is defined by $\varphi(g) = ba^{-1}g$ for all $g \in aH$. We have that:

- φ maps aH to bH. Indeed, if $g = ah \in aH$, then $\varphi(g) = ba^{-1}g = ba^{-1}ah = bh \in bH$.
- φ is onto. Indeed, if $g' = bh' \in bH$ then $\varphi(ah') = g'$.
- φ is injective. Indeed, if $\varphi(g_1) = \varphi(g_2)$ then $ba^{-1}g_1 = ba^{-1}g_2$. Multiplying the sides of this equality from the left with ab^{-1} gives us $g_1 = g_2$.

We have thus shown that G is partitioned into cosets of H and all cosets (including H itself) have the same cardinality. This is possible only if the cardinality of all cosets divides the cardinality of G. □

A simple corollary of this result is, that the order of each element $g \in G$ divides the order of G.