# Cryptography (Math 134)

UCSC, Fall 2018

Robert Boltje

# Contents

# 1 The Integers and the Euclidean Algorithm

**1.1 Notation** $\mathbb{N} := \{1, 2, 3, \ldots\}$, the natural numbers;
$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$;
$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the integers.

**1.2 Definition** Let $a, b \in \mathbb{Z}$. We say that $a$ is a *multiple* of $b$ (or also that $b$ *divides* $a$) if there exists $q \in \mathbb{Z}$ with $bq = a$. In this case we also write $b \mid a$. Note that if $a \neq 0$ then also $q \neq 0$ and then $|b| = b \cdot 1 \leqslant |b| \cdot |q| = |bq| = |a|$. Thus, any non-zero number $a$ has only finitely many divisors.

**1.3 Lemma (Division with remainder)** *Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$. There exist unique elements $r, q \in \mathbb{Z}$ satisfying*

$$a = qm + r \quad \textit{and} \quad r \in \{0, \ldots, m-1\}\,. \tag{1.3.a}$$

*The number $r$ is called the* remainder *of $a$ modulo $m$.*

**Proof** Existence: Let $q$ be the integer with the property $q \leqslant \frac{a}{m} < q+1$ and define $r := a - qm$. Then $q, r \in \mathbb{Z}$ and (1.3.a) holds.

Uniqueness: Assume also $q'$ and $r'$ are integers satisfying (1.3.a). Then $m > |r - r'| = |q - q'| \cdot m$. This implies that $m$ divides $|r - r'|$ and that $|r - r'| = 0$. Thus, $r = r'$ and then also $q = q'$. □

**1.4 Example** For $a = -8$ and $m = 3$ we have $a = (-3) \cdot m + 1$, so $q = -3$ and $r = 1$.

For $a = 8$ and $m = 3$ we have $a = 2 \cdot m + 2$, so $q = 2$ and $r = 2$.

**1.5 Remark** Let $a \in \mathbb{Z}$, $m \in \mathbb{N}$ and let $r$ be the remainder of $a$ modulo $m$. Then we have $m \mid a$ if and only if $r = 0$.

**1.6 Definition** Let $a, b \in \mathbb{Z}$, not both *zero*. The *greatest common divisor* of $a$ and $b$ is the largest number $d \in \mathbb{N}$ with $d \mid a$ and $d \mid b$. We write $\gcd(a, b) = d$.

**1.7 Remark** We immediately have the following rules for the greatest common divisor. Let $a, b \in \mathbb{Z}$, not both zero.

(a) $\gcd(a, b) = \gcd(b, a)$.

(b) If $a \neq 0$ then $\gcd(a, 0) = |a|$.

(c) If $a \mid b$ then $\gcd(a,b) = |a|$.
(d) If $m \in \mathbb{Z}$ is non-zero then $\gcd(am, bm) = \gcd(a,b) \cdot |m|$.
(e) $\gcd(a,b) = \gcd(|a|,|b|)$.
(f) If $a \neq 0 \neq b$ then $\gcd(a,b) \in \{1, \ldots, \min\{|a|,|b|\}\}$.

**1.8 Example** $\gcd(-9,15) = 3$.

The following algorithm gives a fast recipe to compute the greatest common divisor of any two integers $a$ and $b$ (not both 0). Note that by the rules in the above remark we can restrict ourselves to the case that $a, b \in \mathbb{N}$, $b < a$ and $b \nmid a$.

**1.9 Theorem (Euclidean Algorithm)** *Let $a, b \in \mathbb{N}$ with $b < a$ and $b \nmid a$. According to Lemma 1.3 there exist*

$$n \in \mathbb{N}, \quad q_1, \ldots, q_{n+1} \in \mathbb{N}, \quad r_1, \ldots, r_n \in \mathbb{N}$$

*such that*

$$\begin{aligned}
a &= q_1 b + r_1 && \text{with} \quad 0 < r_1 < b && (1)\\
b &= q_2 r_1 + r_2 && \text{with} \quad 0 < r_2 < r_1 && (2)\\
r_1 &= q_3 r_2 + r_3 && \text{with} \quad 0 < r_3 < r_2 && (3)\\
&\vdots && && \vdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} && \text{with} \quad 0 < r_{n-1} < r_{n-2} && (n-1)\\
r_{n-2} &= q_n r_{n-1} + r_n && \text{with} \quad 0 < r_n < r_{n-1} && (n)\\
r_{n-1} &= q_{n+1} r_n && && (n+1)
\end{aligned}$$

*One has $r_n = gcd(a,b)$.*

**Proof** Equation $(n+1)$ implies $r_n \mid r_{n-1}$.
This and equation $(n)$ implies $r_n \mid r_{n-2}$.
The above and equation $(n-1)$ imply $r_n \mid r_{n-3}$.
$\vdots$
The above and equation (4) imply $r_n \mid r_2$.
The above and equation (3) imply $r_n \mid r_1$.
The above and equation (2) imply $r_n \mid b$.
The above and equation (1) imply $r_n \mid a$.
Thus, $r_n$ is a common divisor of $a$ and $b$.

Now, assume that $d \in \mathbb{N}$ is a common divisor of $a$ and $b$.
Then, equation (1) implies $d \mid r_1$.
This and equation (2) implies $d \mid r_2$.
The above and equation (3) imply $d \mid r_3$.
$\vdots$
The above and equation $(n-1)$ imply $d \mid r_{n-1}$.
The above and equation $(n)$ imply $d \mid r_n$.
Thus, $d \leqslant r_n$. This shows that $r_n$ is the greatest common divisor of $a$ and $b$. □

**1.10 Example** We compute $\gcd(1001, 1339)$.
$1339 = 1 \cdot 1001 + 338$,
$1001 = 2 \cdot 338 + 325$,
$338 = 1 \cdot 325 + 13$,
$325 = 25 \cdot 13$.
Thus, $\gcd(1001, 1339) = 13$.

**1.11 Theorem** *Let $a, b \in \mathbb{N}$, $n$, $r_1, \ldots, r_n$, $q_1, \ldots, q_{n+1} \in \mathbb{N}$ be as in Theorem 1.9. Then, $r_n = \gcd(a, b)$ is an integral linear combination of $a$ and $b$, i.e., there exist $u, v \in \mathbb{Z}$ such that*

$$\gcd(a, b) = ua + vb\,.$$

*More precisely, if we set*

$$u_0 := 0,\ v_0 := 1,\ u_1 := 1,\ v_1 := -q_1,$$

*and define recursively*

$$u_i := u_{i-2} - q_i u_{i-1} \quad \text{and} \quad v_i := v_{i-2} - q_i v_{i-1}\,, \quad \text{for } i = 2, \ldots, n,$$

*then*

$$r_i = u_i a + v_i b \quad \text{for } i = 1, \ldots, n. \tag{1.11.a}$$

*In particular,*

$$\gcd(a, b) = r_n = u_n a + v_n b\,.$$

**Proof** It suffices to prove equation (1.11.a) for $i = 1, \ldots, n$. We do this by induction on $i$. Equation (1) from Theorem 1.9 implies $r_1 = a - q_1 b = u_1 a + v_1 b$. Equation (2) implies

$$\begin{aligned} r_2 &= b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - q_2 v_1)b \\ &= u_2 a + v_2 b\,. \end{aligned}$$

Thus, equation (1.11.a) is proved for $i = 1$ and $i = 2$. Now let $i \in \{3, \ldots, n\}$ and assume that equation (1.11.a) holds for $i-1$ and $i-2$. Then equation $(i)$ from Theorem 1.9 implies

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} = u_{i-2} a + v_{i-2} b - q_i(u_{i-1} a + v_{i-1} b) \\ &= (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b = u_i a + v_i b \end{aligned}$$

and the proof is complete. □

**1.12 Remark** Using Remark 1.7 we can easily see that, for arbitrary $a, b \in \mathbb{Z}$, not both zero, one can write $\gcd(a, b) = ua + vb$ for some $u, v \in \mathbb{Z}$.

**1.13 Example** Let $a = 1339$, $b = 1001$ as in Example 1.10.

| | | $q_i$ | $u_i$ | $v_i$ |
|---|---|---|---|---|
| $i = 0:$ | | | $0$ | $1$ |
| $i = 1:$ | $1339 = 1 \cdot 1001 + 338$ | $1$ | $1$ | $-1$ |
| $i = 2:$ | $1001 = 2 \cdot 338 + 325$ | $2$ | $-2$ | $3$ |
| $i = 3:$ | $338 = 1 \cdot 325 + 13$ | $1$ | $3$ | $-4$ |
| $i = 4:$ | $325 = 25 \cdot 13$ | | | |

It follows from the last theorem that $\gcd(1001, 1339) = 13 = 3 \cdot 1339 + (-4) \cdot 1001$.

**1.14 Definition** A natural number $p$ is called a *prime number* or short a *prime* if $p$ has precisely two different positive divisors, namely 1 and $p$. (So, 1 is not a prime. The primes are $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.)

**1.15 Theorem** *Every $2 \leqslant a \in \mathbb{N}$ can be written as a product of primes.*

**Proof** Induction on $a$. For $a = 2$ this is clear (we use one factor). So let $a > 2$ and assume that every natural number between 2 and $a - 1$ can be

written as a product of primes. If $a$ is prime then $a$ can be written as a product with one factor. If $a$ is not a prime then $a$ can be written as $a = bc$ with $b, c \in \{2, \ldots, a-1\}$. By induction, we know that $b$ and $c$ can be written as products of prime numbers. It follows that also $a = bc$ can be written as a product of primes. This completes the proof. □

**1.16 Theorem (Euclid)** *There exist infinitely many primes.*

**Proof** Assume that there exist only finitely many primes $p_1, \ldots, p_n$. Consider the natural number

$$a := p_1 \cdot p_2 \cdots p_n + 1\,.$$

By Theorem 1.15 we can write $a$ as a product of primes. So, $p_i \mid a$ for some $i = 1, \ldots, n$ and we can write $a = p_i b$. Now, $p_i b = a = p_1 \cdots p_n + 1$ implies that

$$1 = p_i(b - p_1 \cdots p_{i-1} p_{i+1} \cdots p_n)$$

But this is a contradiction, since $p_i > 1$. □

**1.17 Proposition** *Let $a, b \in \mathbb{Z}$ and let $p$ be a prime. If $p$ divides $ab$ then $p$ also divides $a$ or $b$.*

**Proof** If $a = b = 0$ then the statement is clearly true, since every integer divides 0. So assume that $a$ and $b$ are not both 0. If $p \mid a$ we are done. So assume that $p \nmid a$. Then $\gcd(p, a) = 1$ and by the Remark following Theorem 1.11 we can write $1 = up + va$ for some $u, v \in \mathbb{Z}$. Also, there exists $c \in \mathbb{Z}$ with $ab = pc$. Multiplying the equation $1 = up + va$ by $b$ we obtain $b = upb + vab = upb + vcp = (ub + vc)p$ and $p \mid b$. □

**1.18 Theorem (Unique prime factorization)** *Let $a \in \mathbb{N}$ with $a \geqslant 2$. Then $a$ can be written as*

$$a = p_1 \cdots p_r \tag{1.18.a}$$

*with unique primes $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$.*

**Proof** We already know from Theorem 1.15 that $a$ can be written as a product as in equation (1.18.a). We only have to show that if $a = p_1 \cdots p_r = q_1 \cdots q_s$ with primes $p_1 \leqslant \cdots \leqslant p_r$ and $q_1 \leqslant \cdots \leqslant q_s$ then $r = s$ and $p_i = q_i$

for $i = 1, \ldots, r$. We prove this by induction on $a$. If $a$ is a prime this is obviously true, so it is true for $a = 2$. Fix $a > 2$ and assume that the uniqueness statement holds for all integers in $\{2, \ldots, a-1\}$. If $a$ is a prime we are done. So, we can assume that $a$ is not a prime. Then we have $r \geqslant 2$ and $s \geqslant 2$. Let $p$ be the largest prime that divides $a$. Since also $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are primes that divide $a$, we have $p_r \leqslant p$ and $q_s \leqslant p$. By repeated application of Proposition 1.17 we obtain $p \mid p_i$ and $p \mid q_j$ for some $i \in \{1, \ldots, r\}$ and some $j \in \{1, \ldots, s\}$. This implies $p \leqslant p_i \leqslant p_r \leqslant p$ and $p \leqslant q_j \leqslant q_s \leqslant p$. It follows that $p_r = p$ and $q_s = p$. We can write $a = bp$ with $b \in \mathbb{N}$ and obtain $b = p_1 \cdots p_{r-1}$ and $b = q_1 \cdots q_{s-1}$. Since $2 \leqslant b < a$, induction yields $r - 1 = s - 1$ and $p_i = q_i$ for $i = 1, \ldots, r-1$. This concludes the proof. □

**1.19 Definition** (a) Two non-zero integers $a$ and $b$ are called *coprime* or *relatively prime* if $\gcd(a, b) = 1$.

(b) The *Euler $\phi$-function* (also called *Euler's totient function*) is the function

$$\phi\colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto |\{a \in \{1, \ldots, n\} \mid \gcd(a, n) = 1\}|.$$

**1.20 Proposition** (a) $\phi(1) = 1$.

(b) *For every prime $p$ and every $k \in \mathbb{N}$ one has $\phi(p^k) = (p-1)p^{k-1}$. In particular, $\phi(p) = p - 1$.*

**Proof** The statemtent in (a) is clear. In order to prove part (b) we count all elements $a \in \{1, \ldots, p^k\}$ with the property that $\gcd(a, p^k) \neq 1$. This last condition is equivalent to $p \mid a$. But the number of elements $a \in \{1, \ldots, p^k\}$ which are divisible by $p$ is precisely $p^{k-1}$. Thus, $\phi(p^k) = p^k - p^{k-1} = (p - 1)p^{k-1}$. □

## Exercises for Section 1

**1.** Write a computer program that uses the Euclidean Algorithm to compute the greatest common divisor $d$ of two natural numbers $a$ and $b$ and also integers $u$ and $v$ such that $d = ua + vb$. Use the program to compute $d, u, v$ for $(a, b) = (2458437443, 903827662)$.

**2.** Let $(a, b) = (153680, 79269)$. Compute by hand $d := \gcd(a, b)$ and determine $u, v \in \mathbb{Z}$ satisfying $d = ua + vb$.

**3.** Show that for $a, b \in \mathbb{N}$ and for $d \in \mathbb{N}$ the following are equivalent:
(i) $d = \gcd(a, b)$.
(ii) $d$ is a common divisor of $a$ and $b$, and every other common divisor of $a$ and $b$ divides $d$.

**4.** Let $a$ and $b$ be natural numbers, set $d := \gcd(a, b)$, and let $u_0$ and $v_0$ be integers such that $d = u_0a+v_0b$. Show that the set of pairs $(u, v) \in \mathbb{Z}\times\mathbb{Z}$ satisfying $d = ua + vb$ is given as $\{(u_0, v_0) + t(r, -s) \mid t \in \mathbb{Z}\}$, where $r := b/d$ and $s := a/d$.

**5.** Let $p$ be a prime number and let $a_1, \ldots, a_n \in \mathbb{Z}$. Show that if $p|a_1 \cdots a_n$ then $p|a_i$ for some $i \in \{1, \ldots, n\}$.

**6.** Let $a, b \in \mathbb{Z}$, not both equal to 0, and let $d := \gcd(a, b)$. Show that

$$\{ua + vb \mid u, v \in \mathbb{Z}\} = \{qd \mid q \in \mathbb{Z}\}.$$

**7.** Compute $\phi(36)$. Compare it with $\phi(4)$ and $\phi(9)$. Formulate a general conjecture and verify it in some cases.

# 2 Rings and Fields

**2.1 Definition** A *ring* is a set $R$ equipped with two operations, called *addition* and *multiplication*, which satisfy the ring axioms.

Addition is a function $R \times R \to R$, denoted by $(r, s) \mapsto r + s$ and multiplication is a function $R \times R \to R$, denoted by $(r, s) \mapsto r \cdot s$ or just $rs$. The following axiom (a)–(c) are required to hold. The ring $R$ is called *commutative* if additionally axiom (d) holds.

(a) (i) $(r + s) + t = r + (s + t)$ for all $r, s, t \in R$. (Associativity of addition)

(ii) $r + s = s + r$ for all $r, s \in R$. (Commutativity of addition)

(iii) There exists an element $z \in R$ such that $z + r = r = r + z$ for all $r \in R$. (There can only be one such element: If also $z'$ has the property then $z = z + z' = z'$.) This element is usually denoted by 0 and is called the *zero element*.

(iv) For every $r \in R$ there exists an element $s \in R$ such that $r + s = 0 = s + r$. (For given $r$ there can only be one such element: If also $s'$ has the property then $s = s + 0 = s + (r + s') = (s + r) + s' = 0 + s' = s'$.) This element is usually denoted by $-r$ and is called the *additive inverse* of $r$. (Thus, by definition $r + (-r) = 0 = (-r) + r$.)

(b) (i) $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ for all $r, s, t \in R$. (Associativity of multiplication)

(ii) There exists an element $e \in R$ such that $r \cdot e = r = e \cdot r$ for all $r \in R$. (There can only be one such element: If also $e' \in R$ has the property then $e = e \cdot e' = e'$.) This element is usually denoted by 1 and is called the *one element* or the *identity element* of $R$.

(c) $r \cdot (s + t) = (r \cdot s) + (r \cdot t)$ and $(r + s) \cdot t = (r \cdot t) + (s \cdot t)$ for all $r, s, t \in R$. (Distributivity)

(d) $r \cdot s = s \cdot r$ for all $r, s \in R$.

**2.2 Remark** When working with rings one usually has the following conventions.

(a) $r - s := r + (-s)$ for all $r, s \in R$.

(b) In order to save parentheses, one gives priority to multiplication over addition. For example $rs + t$ means $(rs) + s$ but not $r(s + t)$.

**2.3 Remark** For a ring $(R, +, \cdot)$ one can derive the following rules easily from the axioms:

(a) $0 \cdot r = 0 = r \cdot 0$.

(b) $-(r+s) = -r - s$.
(c) $(-r) \cdot s = -(r \cdot s) = r \cdot (-s)$.
(d) $(-1) \cdot (-1) = 1$.
(e) $-r = (-1) \cdot r$.

**2.4 Examples** (a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are commutative rings with the usual addition and multiplication.

(b) Every set $R$ with just one element equipped with the only possible addition and multiplication is a ring. Every such ring is called a *trivial ring* or "the" *zero ring*. In a trivial ring we have $0 = 1$. Conversely, if $R$ is a ring in which $0 = 1$, then $R$ is a trivial ring (verify!).(

(c) The polynomial ring $\mathbb{R}[X]$ with real coefficients is a commutative ring. More generally, if $R$ is any ring, one can form the polynomial ring $R[X]$ with coefficients in $R$. Its elements are formal polynomials $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, with $a_n, \ldots, a_0 \in R$ and we use the usual addition and multiplication of polynomials. If $R$ is commutative then also $R[X]$ is commutative. (Warning: We do not define polynomials as function! This is an important difference. For instance, if $R$ has only finitely many elements then there are only finitely many functions from $R$ to $R$, but there are still infinitely many polynomials if $R$ is not the trivial ring.)

(d) For any ring $R$ and $n \in \mathbb{N}$ we define $M_n(R)$ as the set of all square $n \times n$-matrices with entries in $R$. The usual matrix addition and matrix multiplication satisfy the axioms (a)–(c) in Definition 2.1. The zero matrix and the identity matrix are the respective zero and identity element of $M_n(R)$. Note that if $R$ is not the zero-ring, then $M_n(R)$ is not commutative whenever $n \geqslant 2$, even if $R$ is commutative.

**2.5 Definition** Let $R$ and $S$ be rings.

(a) A function $f\colon R \to S$ is called a *ring homomorphism* if

$$f(r_1 + r_2) = f(r_2) + f(r_2) \quad \text{and} \quad f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)\,, \quad \text{for all } r_1, r_2 \in R,$$

and

$$f(1) = 1\,.$$

(b) An element $u \in R$ is called a *unit* (or *invertible*) if there exists an element $v \in R$ such that $uv = 1 = vu$. In this case $v$ is uniquely determined (if also $v'u = 1 = uv'$ then $v = v(uv') = (vu)v' = v'$) and we call $v$ the *(multiplicative) inverse* of $u$ and denote it by $v = u^{-1}$. The set of units of $R$

is denoted by $R^\times$. If $u, u_1, u_2$ are units of $R$ then also $u^{-1}$ and $u_1u_2$ are units of $R$ with inverses $(u^{-1})^{-1} = u$ and $(u_1u_2)^{-1} = u_2^{-1}u_1^{-1}$. Note that $1 \in R^\times$ with $1^{-1} = 1$.

(c) The ring $R$ is called a field if $R$ is commutative, $1 \neq 0$, and $R^\times = R \setminus \{0\}$. (For instance, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, $\mathbb{Z}$ is not a field.)

**2.6 Lemma** *Let $R$ be a commutative ring. Then*

$$M_2(R)^\times = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \in R^\times \}\,.$$

**Proof** For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$ we write $\det(A) := ad - bc$. It is easy to verify that, for $A, B \in M_2(R)$, one has $\det(AB) = \det(A)\det(B)$.

Let $A \in M_2(R)^\times$. Then there exists $B \in M_2(R)$ such that $AB = 1 = BA$. Applying determinants we obtain $\det(A)\det(B) = \det(AB) = \det(1) = 1$. This implies that $\det(A) \in R^\times$. Conversely, assume that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$ and that $\det(A) = ad - bc \in R^\times$. Set $v := \det(A)^{-1} \in R$ and consider $B = \begin{pmatrix} dv & -bv \\ -cv & av \end{pmatrix}$ then

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} dv & -bv \\ -cv & av \end{pmatrix} = \begin{pmatrix} (ad-bc)v & 0 \\ 0 & (ad-bc)v \end{pmatrix} = 1 \in M_2(R)$$

and

$$BA = \begin{pmatrix} dv & -bv \\ -cv & av \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} (ad-bc)v & 0 \\ 0 & (ad-bc)v \end{pmatrix} = 1 \in M_2(R)\,.$$

This implies that $A \in M_2(R)^\times$ and $A^{-1} = B$. □

## Exercises for Section 2

**1.** Prove the statements in Remark 2.3.

**2.** Let $S$ and $T$ be rings and let $R := S \times T$.

(a) Show that $R$ is again a ring if one defines $(s_1, t_1)+(s_2, t_2) := (s_1+s_2, t_1+t_2)$ and $(s_1, t_1) \cdot (s_2, t_2) := (s_1 \cdot s_2, t_1 \cdot t_2)$ for $s_1, s_2 \in S$ and $t_1, t_2 \in T$. What is the zero-element and what is the one-element of $R$?

(b) Show that $R^\times = S^\times \times T^\times$.

**3.** Let $R$ and $S$ be rings and let $f : R \to S$ be a ring homomorphism.

(a) Show that $f(0) = 0$ and that $f(-r) = -f(r)$ for all $r \in R$.

(b) Show that if $u \in R^\times$, then $f(u) \in S^\times$ and $f(u)^{-1} = f(u^{-1})$.

**4.** Let $R$ be a commutative ring. Show that the function

$$\det\colon M_2(R) \to R\,, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc\,,$$

satisfies $\det(AB) = \det(A)\det(B)$ for all $A, B \in M_2(R)$. Is this still true if one drops the commutativity assumption on $R$?

**5.** Determine the set $R^\times$ of units of the following rings $R$:

(a) $R = \mathbb{Z}$.

(b) $R = \mathbb{R}[X]$.

(c) $R = \{a + bi \mid a, b \in \mathbb{Z}\}$, the so-called ring of *Gaussian integers* (here $i$ is the complex number with the property $i^2 = -1$.)

# 3 Congruences and the Ring $\mathbb{Z}/m\mathbb{Z}$

**3.1 Definition** Let $m \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. We write

$$a \equiv b \mod m \qquad (\text{and say } a \textit{ is congruent to } b \textit{ modulo } m)$$

if $m \mid a - b$. This is equivalent to $a$ and $b$ having the same remainder after division by $m$. Therefore, 'being congruent modulo $m$' is an equivalence relation on $\mathbb{Z}$. We write $\mathbb{Z}/m\mathbb{Z}$ ($\mathbb{Z}$ *modulo* $m\mathbb{Z}$) for the set of equivalence classes. The equivalence class of $a$ is given by $a + m\mathbb{Z} := \{a + mk \mid k \in \mathbb{Z}\}$. It is also called the *congruence class* or *residue class* of $a$ modulo $m$. We have

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}$$

and $\mathbb{Z}/m\mathbb{Z}$ has $m$ elements. If we pick one element from each of the $m$ congruence classes we call the resulting set a *complete set of residues* modulo $m$. Note that

$$a \equiv b \mod m \iff m \mid a - b \iff a + m\mathbb{Z} = b + m\mathbb{Z}$$
$$\iff a \text{ and } b \text{ have the same remainder after division by } m.$$

**3.2 Example** For $m = 5$ we have

$$3 \equiv -2 \equiv 8 \mod 5 \quad \text{and} \quad 3 + 5\mathbb{Z} = -2 + 5\mathbb{Z} = 8 + 5\mathbb{Z}\,.$$

Obviously, $\{0, 1, 2, 3, 4\}$ is a complete set of residues modulo 5. But also $\{5, -4, 7, 18, -11\}$ is one.

**3.3 Remark** The following rules for congruences are immediate from the definitions.

(a) If $a \equiv b \mod m$ and $c \equiv d \mod m$ then

$$a + c \equiv b + d \mod m\,,\ ac \equiv bd \mod m\,,\ a - c \equiv b - d \mod m\,.$$

So we can add, multiply and subtract congruences.

(b) The set $\mathbb{Z}/m\mathbb{Z}$ with addition and multiplication given by

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}\,, (a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = (ab) + m\mathbb{Z}\,,$$

is a commutative ring. (It follows from (a) that addition and multiplication is well-defined, i.e., not dependent on the choice of $a$ and $b$ in its residue class.) The zero element is $0 + m\mathbb{Z} = m\mathbb{Z}$, the 1-element is $1 + m\mathbb{Z}$.

(c) If $a \equiv b \mod m$ and $d \mid m$ then $a \equiv b \mod d$.

(d) If $a \equiv b \mod m$ and $a \equiv b \mod n$ with $\gcd(m,n) = 1$ then $a \equiv b \mod mn$.

**3.4 Notation** If $u$ is an element a ring $R$ the symbol $u^n$ has a meaning for all $n \in \mathbb{N}_0$. If $n > 0$, it is just equal to $u \cdots u$, the product with $n$ factors. If $n = 0$ we set $u^n = 1$. If $u$ is a unit with inverse $v \in R$ we can also define $u^{-n}$ for $n \in \mathbb{N}$ by $u^{-n} := v^n$. Thus, if $u \in R^\times$, $u^n$ is defined for all $n \in \mathbb{Z}$ and we have $u^{m+n} = u^m u^n$ and $(u^m)^n = u^{mn}$ for all $m, n \in \mathbb{Z}$.

**3.5 Proposition** *Let $m \in \mathbb{N}$ and let $a \in \mathbb{Z}$. The residue class $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ if and only if $\gcd(a,m) = 1$. In particular $\phi(m)$ is the number of units in $\mathbb{Z}/m\mathbb{Z}$.*

**Proof** "$\Rightarrow$": Assume that there exists $b \in \mathbb{Z}$ with $(a+m\mathbb{Z})(b+m\mathbb{Z}) = 1+m\mathbb{Z}$. Then $ab + m\mathbb{Z} = 1 + m\mathbb{Z}$ and there exists $q \in \mathbb{Z}$ with $ab - 1 = qm$ or $1 = ab - qm$. It follows that $\gcd(a,m)$ is a divisor of $ab - qm = 1$. This implies $\gcd(a,m) = 1$.

"$\Leftarrow$": If $\gcd(a,m) = 1$ then there exist $u, v \in \mathbb{Z}$ with $1 = ua + vm$. This implies $1 \equiv ua \mod m$ and $1 + m\mathbb{Z} = ua + m\mathbb{Z} = (u + m\mathbb{Z})(a + m\mathbb{Z})$ so that $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$. □

**3.6 Corollary** *Let $m \in \mathbb{N}$. Then $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if $m$ is a prime.*

**Proof** First, if $m = 1$ then $m$ is not a prime and $\mathbb{Z}/m\mathbb{Z}$ is the trivial ring and therefore not a field. So assume from now on that $m \geqslant 2$. In this case we have $0 + m\mathbb{Z} \neq 1 + m\mathbb{Z}$. And it remains to be shown that every non-zero element $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ if and only if $m$ is a prime. First, if $m$ is a prime then $\gcd(a,m) = 1$ for all $a = 1, \ldots, m-1$ and by Proposition 3.5 every such element $a + m\mathbb{Z}$ is invertible. Conversely, if $m$ is not a prime then we can write $m = ab$ with $a, b \in \mathbb{N}$ and $2 \leqslant a, b \leqslant m - 1$. Thus, $a + m\mathbb{Z}$ is not the zero element and also not invertible by Proposition 3.5, since $\gcd(a,m) = a$. It follows that $\mathbb{Z}/m\mathbb{Z}$ is not a field. □

**3.7 Corollary** *Let $m \in \mathbb{N}$, let $a, b \in \mathbb{Z}$ and let $d := \gcd(a,m)$.*

(a) *The congruence $ax \equiv b \mod m$ has a solution $x \in \mathbb{Z}$ if and only if $d \mid b$.*

(b) *If $ax \equiv b \mod m$ has a sloution $x_0 \in \mathbb{Z}$ then the set of all solutions is given by $x_0 + (m/d)\mathbb{Z}$.*

**Proof** (a) "⇒": If $ax_0 \equiv b \mod m$ for some $x_0 \in \mathbb{Z}$ then $d \mid m \mid ax_0 - b$ and also $d \mid a \mid ax_0$. This implies $d \mid b$.

"⇐": Since $\gcd(a, m) = d$, there exist $u, v \in \mathbb{Z}$ such that $d = ua + vm$. Multiplication with $b/d$ yields $b = d(b/d) = (ub/d)a + (vb/d)m$ with integers $ub/d$ and $(vb/d)$. This implies that $x_0 := ub/d$ solves the congruence.

(b) Assume that $x_0 \in \mathbb{Z}$ is a solution of the above congruence and let $x \in \mathbb{Z}$ be arbitrary. Then, with $a' := a/d, b' := b/d, m' := m/d \in \mathbb{Z}$ we have

$$\begin{aligned} ax \equiv b \mod m &\iff m \mid ax - b \iff m \mid (ax - b) - (ax_0 - b) \\ &\iff m \mid a(x - x_0) \iff m' \mid a'(x - x_0) \\ &\iff m' \mid x - x_0 \iff x \in x_0 + m'\mathbb{Z}\,. \end{aligned}$$

□

**3.8 Proposition (Fermat's Little Theorem)** *Let $p$ be a prime and let $a \in \mathbb{Z}$. Then $a^p \equiv a \mod p$. Moreover, if $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$. In particular, if $a + p\mathbb{Z} \neq 0 + p\mathbb{Z}$ then $(a + p\mathbb{Z})^{-1} = (a + p\mathbb{Z})^{p-2}$.*

**Proof** If $p \mid a$ then $a \equiv 0 \mod p$ and $a^p \equiv 0 \mod p$. Therefore, we can assume from now on that $p \nmid a$. It suffices to show that $a^{p-1} \equiv a \mod p$, since then, multiplying by $a$ we also obtain $a^p \equiv a \mod p$.

Consider the $p$ numbers $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$. They form again a complete set of residues modulo $p$. In fact, if $ia \equiv ja \mod p$ for $0 \leqslant i \leqslant j \leqslant p - 1$ then $p \mid (j - i)a$. Since $p \nmid a$, we have $p \mid j - i$. But $j - i \in \{0, \ldots, p-1\}$ and we can conclude that $i = j$. So we know that the elements $a + p\mathbb{Z}, 2a + p\mathbb{Z}, \ldots, (p-1)a + p\mathbb{Z}$ of $\mathbb{Z}/p\mathbb{Z}$ are the same as the elements $1 + p\mathbb{Z}, 2 + p\mathbb{Z}, (p-1) + p\mathbb{Z}$, just possibly in a different order. Multiplying them together in the ring $\mathbb{Z}/p\mathbb{Z}$ yields $(p-1)! \cdot a^{p-1} + p\mathbb{Z} = (p-1)! + p\mathbb{Z}$. Since $p \nmid (p-1)!$, the element $(p-1)^! + p\mathbb{Z}$ is invertible and multiplying the last equation with this element's inverse yields $a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z}$ (or, equivalently, $a^{p-1} \equiv 1 \mod p$). □

**3.9 Corollary** *If $p$ is a prime, $a \in \mathbb{Z}$ with $p \nmid a$, and $m, n \in \mathbb{Z}$ are such that $n \equiv m \mod p - 1$ then $a^m \equiv a^n \mod p$.*

**Proof** Since $n \equiv m \mod p - 1$, we have $m = n + k(p-1)$ for some $k \in \mathbb{Z}$. Moreover, since $p \nmid a$, Proposition 3.8 implies

$$a^m = a^{n+k(p-1)} = a^n(a^{p-1})^k \equiv a^n 1^k = a^n \mod p$$

and the corollary is proven. □

**3.10 Theorem (Chinese Remainder Theorem)** *Let $m_1, \ldots, m_r \in \mathbb{N}$ be pairwise coprime (i.e., $\gcd(m_i, m_j) = 1$ for $i \neq j$ in $\{1, \ldots, r\}$) and set $m := m_1 m_2 \cdots m_r$. For any choice of $a_1, \ldots, a_r \in \mathbb{Z}$ there exists a solution $x \in \mathbb{Z}$ to the system of congruences*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

*Moreover, if $x_0$ is a solution then the set of all solutions is equal to $x_0 + m\mathbb{Z}$.*

**Proof** Existence: Set $n_i := m/m_i$ for $i = 1, \ldots, r$. Then $\gcd(n_i, m_i) = 1$ and there exist $b_i \in \mathbb{Z}$ with $b_i n_i \equiv 1 \mod m_i$ for all $i = 1, \ldots, r$. Set $x := a_1 b_1 n_1 + \cdots a_r b_r n_r$. Then, for each $i = 1, \ldots, r$ we have $x \equiv a_i b_i n_i \equiv a_i \mod m_i$ since $n_j \equiv 0 \mod m_i$ for all $j \neq i$.

Uniqueness: Assume that $x$ and $x'$ in $\mathbb{Z}$ are solutions to the above system of congruences. Then $x \equiv a_i \equiv x' \mod m_i$ for all $i = 1, \ldots, r$. In other words, $m_i \mid x - x'$ for all $i = 1, \ldots, r$. Since $m_1, \ldots, m_r$ are pairwise coprime, we obtain $m \mid x - x'$. Conversely, if $x_0$ is a solution and $k \in \mathbb{Z}$ then also $x_0 + km$ is a solution, since $m_i \mid m \mid x_0 - a_i$ for all $i = 1, \ldots, r$ implies $m_i \mid x_0 + km - a_i$ for all $i = 1, \ldots, r$. □

**3.11 Example** Find all numbers $x \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv 3 \mod 7\,, \\ x &\equiv 5 \mod 11\,, \\ \text{and } x &\equiv -1 \mod 13\,. \end{aligned}$$

We follow the construction of a solution in the proof of the Chinese Remainder Theorem. $m_1 = 7$, $m_2 = 11$, $m_3 = 13$ and $m = 7 \cdot 11 \cdot 13 = 1001$. Further, $n_1 = 11 \cdot 13 = 143$, $n_2 = 7 \cdot 13 = 91$, $n_3 = 7 \cdot 11 = 77$. We find $b_1 = -2$, $b_2 = 4$, $b_3 = -1$ as possible solutions to $b_i n_i \equiv 1 \mod m_i$, for $i = 1, 2, 3$. Thus, $x_0 := 3 \cdot (-2) \cdot 143 + 5 \cdot 4 \cdot 91 + (-1) \cdot (-1) \cdot 77 = -858 + 1820 + 77 = 1039$ is a solution, and the set of solutions is $1039 + 1001\mathbb{Z} = 38 + 1001\mathbb{Z}$.

**3.12 Corollary** *Let $m_1, \ldots, m_r$ and $m$ be as in Theorem 3.10. Then the function*

$$\begin{aligned} \rho\colon \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \\ a + m\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}) \end{aligned}$$

*is a bijective ring homomorphism (i.e., injective and surjective, or a one-to-one correspondence). Moreover, $\phi(m) = \phi(m_1) \cdots \phi(m_r)$.*

**Proof** Well-defined ($\rho$ is a function): If $a \equiv b \mod m$ then also $a \equiv b \mod m_i$ for all $i = 1, \ldots, r$.

$\rho$ is a ring homomorphism: For $a, b \in \mathbb{Z}$ we have

$$\begin{aligned} \rho((a + m\mathbb{Z}) + (b + m\mathbb{Z})) = \rho((a + b) + m\mathbb{Z}) &= \Big((a + b) + m_1\mathbb{Z}, \ldots, (a + b) + m_r\mathbb{Z}\Big) \\ &= \Big(a + m_1\mathbb{Z}) + (b + m_1\mathbb{Z}), \ldots, (a + m_r\mathbb{Z}) + (b + m_r\mathbb{Z})\Big) \\ &= \Big(a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}\Big) + \Big(b + m_1\mathbb{Z}, \ldots, b + m_r\mathbb{Z}\Big) \\ &= \rho(a + m\mathbb{Z}) + \rho(b + m\mathbb{Z})\,. \end{aligned}$$

Similarly, we obtain $\rho((a+m\mathbb{Z})(b+m\mathbb{Z})) = \rho(a+m\mathbb{Z}) + \rho(b+m\mathbb{Z})$. Finally,

$$\rho(1 + m\mathbb{Z}) = (1 + m_1\mathbb{Z}, \ldots, 1 + m_r\mathbb{Z})$$

which is the 1-element in the product ring.

$\rho$ is surjective: This follows immediately from the existence statement in the Chinese Remainder Theorem.

$\rho$ is injective: This follows immediately from the uniqueness statement in the Chinese Remainder Theorem.

Formula for $\phi(m)$: The ring isomorphism $\rho$ and its inverse $\rho^{-1}$ restrict to inverse bijections between the sets of units. But

$$\Big(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}\Big)^\times = (\mathbb{Z}/m_1\mathbb{Z})^\times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})^\times\,.$$

Now we obtain $\phi(m) = \phi(m_1) \cdots \phi(m_r)$ immediately from Proposition 3.5. □

**3.13 Corollary** *Let $m = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of $m \in \mathbb{N}$. Then*

$$\begin{aligned} \varphi(m) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}) &= p_1^{e_1 - 1} \cdots p_r^{e_r - 1}(p_1 - 1) \cdots (p_r - 1) \\ &= m(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})\,. \end{aligned}$$

**Proof** This is clear from Corollary 3.12 and Proposition 1.20. □

**3.14 Example** $\phi(99) = \phi(9)\phi(11) = 6 \cdot 10 = 60$ and $\phi(1001) = \phi(7)\phi(11)\phi(13) = 6 \cdot 10 \cdot 12 = 720$.

**3.15 Remark** Assume that $n \in \mathbb{N}$ is given together with the information that $n = pq$ is the product of two unknown prime numbers $p < q$. The following arguments will show that knowledge of the primes $p$ and $q$ is equivalent to knowledge of $\phi(n)$.

(a) If $p$ and $q$ are known then $\phi(n)$ can be computed as above: $\phi(n) = (p-1)(q-1)$.

(b) If $\phi(n)$ is known then $p$ and $q$ can be computed as follows: We first check if $n$ is even. If yes, then $p = 2$ and $q = n/2$. This was the trivial case. So assume that $n$, $p$ and $q$ are odd. We have $n = pq$ and $\phi(n) = (p-1)(q-1)$. Substituting $q = n/p$ in the second equation gives a quadratic equation in $p$ with known coefficients:

$$\phi(n) = (p-1)(\frac{n}{p}-1) \iff p\phi(n) = (p-1)(n-p) \iff p^2+(\phi(n)-n-1)p+n = 0\,.$$

With $a := \phi(n) - n - 1$ we obtain $p = \frac{1}{2}(-a \pm \sqrt{a^2 - 4n})$.

**3.16 Theorem (Euler's Theorem)** *Let $a \in \mathbb{Z}$ and let $m \in \mathbb{N}$ with $\gcd(a, m) = 1$. Then*

$$a^{\phi(m)} \equiv 1 \mod m\,.$$

**Proof** The ring $\mathbb{Z}/m\mathbb{Z}$ has $\phi(m)$ units. We enumerate them by $b_1 + m\mathbb{Z}, \ldots, b_{\phi(m)}+m\mathbb{Z}$ and set $b+m\mathbb{Z} := (b_1+m\mathbb{Z}) \cdots (b_{\phi(m)}+m\mathbb{Z})$ which is again a unit in $\mathbb{Z}/m\mathbb{Z}$. First we claim that if $(a+m\mathbb{Z})(b_i+m\mathbb{Z}) = (a+m\mathbb{Z})(b_j+m\mathbb{Z})$ for $i, j \in \{1, \ldots, \phi(m)\}$ then $i = j$. In fact, this follows immediately by multiplication with the inverse of $a + m\mathbb{Z}$. The $\phi(m)$ distinct elements $(a + m\mathbb{Z})(b_1 + m\mathbb{Z}), \ldots, (a_m\mathbb{Z})(b_{\phi(m)} + m\mathbb{Z})$ are again units of $\mathbb{Z}/m\mathbb{Z}$. Therefore, up to reordering, they are again the elements $b_1 + m\mathbb{Z}, \ldots, b_{\phi(m)} + m\mathbb{Z}$. Thus, their product is also $b + m\mathbb{Z}$. On the other hand their product is also $a^{\phi(m)}b + m\mathbb{Z}$. This implies $b + m\mathbb{Z} = a^{\phi(m)}b + m\mathbb{Z} = (a^{\phi(m)} + m\mathbb{Z})(b + m\mathbb{Z})$. Multiplication with the inverse of $b + m\mathbb{Z}$ yields $1 + m\mathbb{Z} = a^{\phi(m)} + m\mathbb{Z}$ and $a^{\phi(m)} \equiv 1 \mod m$. □

**3.17 Corollary** *If $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ with $\gcd(a,m) = 1$ and if $n, n' \in \mathbb{N}$ with $n \equiv n' \mod \phi(m)$ then*

$$a^n \equiv a^{n'} \mod m\,.$$

**Proof** Same proof as for Corollary 3.9. □

**3.18 Remark** Let $m \in \mathbb{N}$ and let $m = p^{e_1} \cdots p^{e_r}$ be its prime factorization. From the proof of Corollary 3.12 we have the bijection

$$\begin{aligned} \rho\colon (\mathbb{Z}/m\mathbb{Z})^\times &\to (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{e_r})^\times \\ a + m\mathbb{Z} &\mapsto (a + p_1^{e_1}\mathbb{Z}, \ldots, a + p_r^{e_r}\mathbb{Z})\,, \end{aligned}$$

which is multiplicative (i.e., $\rho((a+m\mathbb{Z})(b+m\mathbb{Z})) = \rho(a+m\mathbb{Z})\rho(b+m\mathbb{Z})$). This implies that already the natural number

$$e := \operatorname{lcm}\Big(p_1^{e_1}(p_1-1), \ldots, p_r^{e_r}(p_r-1)\Big)$$

has the property that

$$a^e \equiv 1 \mod m$$

for all $a \in \mathbb{Z}$ with $\gcd(a,m) = 1$. Similarly, the previous corollary holds with $\phi(m)$ replaced with $e$: If $n, n'$ are natural numbers with $n \equiv n' \mod e$ then

$$a^n \equiv a^{n'} \mod m$$

**3.19 Examples** (a) Let $m = 15$. Then $\phi(m) = \phi(3)\phi(5) = 2 \cdot 4 = 8$ and we obtain $a^8 \equiv 1 \mod 15$ for all $a \in \mathbb{Z}$ with $\gcd(a,15) = 1$. But with $e = \operatorname{lcm}(2,4) = 4$ we already have $a^4 \equiv 1 \mod 15$ for every $a \in \mathbb{Z}$ as before.

(b) We want to compute the remainder of $5^{2009}$ after division by 99. Thus, $m = 99$, $a = 5$ and $n = 2009$. Note that $\gcd(5,99) = 1$. We have $\phi(m) = \phi(9)\phi(11) = 6 \cdot 10 = 60$ and $e = \operatorname{lcm}(6,10) = 30$. Therefore, we know that $(5 + 99\mathbb{Z})^{30} = 1 + 99\mathbb{Z}$. Moreover, $2009 \equiv 29 \equiv -1 \mod 30$. Therefore, $(5 + 99\mathbb{Z})^{2009} = (5 + 99\mathbb{Z})^{29} = (5 + 99\mathbb{Z})^{-1}$. We can compute $(5 + 99\mathbb{Z})^{29}$ by computing

$$\begin{aligned} (5 + 99\mathbb{Z})^2 &= 25 + 99\mathbb{Z}\,, \\ (5 + 99\mathbb{Z})^4 &= (25 + 99\mathbb{Z})^2 = 625 + 99\mathbb{Z} = 31 + 99\mathbb{Z}\,, \\ (5 + 99\mathbb{Z})^8 &= (31 + 99\mathbb{Z})^2 = 961 + 99\mathbb{Z} = -29 + 99\mathbb{Z}\,, \\ (5 + 99\mathbb{Z})^{16} &= (-2 + 99\mathbb{Z})^2 = 841 + 99\mathbb{Z} = -50 + 99\mathbb{Z}\,, \end{aligned}$$

and then noting that

$$\begin{aligned}(5+99\mathbb{Z})^{29} &= (5+99\mathbb{Z})^{1+4+8+16} = (5+99\mathbb{Z})(31+99\mathbb{Z})(-29+99\mathbb{Z})(-50+99\mathbb{Z}) \\ &= (155+99\mathbb{Z})(1450+99\mathbb{Z}) = (-43+99\mathbb{Z})(-35+99\mathbb{Z}) \\ &= (1505+99\mathbb{Z}) = 20+99\mathbb{Z}\,.\end{aligned}$$

Thus the remainder of $5^{2009}$ after division by 99 is 20.

Alternatively, we could have computed the inverse of $5+99\mathbb{Z}$ with the Euclidean Algorithm to obtain $20+99\mathbb{Z}$.

Another alternative is to compute $(5+9\mathbb{Z})^{2009}$ and $(5+11\mathbb{Z})^{2009}$ and then use the Chinese Remainder Theorem: ...

**3.20 Remark (Modular exponentiation)** We can compute $(a+m\mathbb{Z})^n$ for large $n$ even when $\gcd(a,m) \neq 1$ with the method in the last example. We first write the exponent $n$ in its binary form: $n = d_0 + 2d_1 + 4d_2 + \cdots + 2^k d_k$ with $d_0, d_1, \ldots, d_k \in \{0,1\}$ the digits of $n$ in its binary expansion. Then we compute $(a+m\mathbb{Z})^{2^i}$ for $i = 0, \ldots, k$ and finally compute

$$(a+m\mathbb{Z})^n = (a+m\mathbb{Z})^{d_0} + ((a+m\mathbb{Z})^2)^{d_1} + ((a+m\mathbb{Z})^4)^{d_2} + \cdots + ((a+m\mathbb{Z})^{2^k})^{d_k}$$

as in the previous example. Note we never have to deal with numbers that are larger than $m^2$.

**3.21 Proposition** *Let $n \in \mathbb{N}$. Then $\sum_{0<d|n} \phi(d) = n$. Here, the sum runs over all positive divisors $d$ of $n$.*

**Proof** Induction on the number of different prime divisors of $n$.

If $n$ is equal to 1 this is clear.

If $n = p^e$ for some prime $p$ and some $e \in \mathbb{N}$ then

$$\begin{aligned}\sum_{d|n} \phi(d) &= \sum_{i=0}^{e} \phi(p^i) = 1 + (p-1) + p(p-1) + p^2(p-1) + p^{e-1}(p-1) \\ &= 1 + (p-1)(1 + p + p^2 + \cdots + p^{e-1}) = 1 + (p-1)\frac{p^e - 1}{p-1} = p^e\end{aligned}$$

and the equation holds in this case.

Next we assume that $n$ can be written as $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$ and that the equation already is proved for $n_1$ and for $n_2$. Note that we have

a bijection

$$\{(d_1, d_2) \in \mathbb{N} \times \mathbb{N} \mid d_1 \mid n_1, d_2 \mid n_2\} \to \{d \in \mathbb{N} \mid d \mid n\}\,,$$
$$(d_1, d_2) \mapsto d_1 d_2\,.$$

Using this we obtain

$$\begin{aligned}\sum_{d|n} \phi(d) &= \sum_{(d_1,d_2)} \phi(d_1 d_2) = \sum_{(d_1,d_2)} \phi(d_1)\phi(d_2) \\ &= \Big(\sum_{d_1|n_1} \phi(d_1)\Big)\Big(\sum_{d_2|n_2} \phi(d_2)\Big) = n_1 \cdot n_2 = n\end{aligned}$$

and the proposition is proved. □

**3.22 Proposition** *For all $a \in \mathbb{Z}$ and all $n, d \in \mathbb{N}$ one has*

$$a^{nd} - 1 = (a^d - 1)(a^{(n-1)d} + a^{(n-2)d} + \cdots + a^d + 1)$$

**Proof** Easy verification. □

**3.23 Proposition** *Let $m \in \mathbb{N}$ and let $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. Moreover assume that $r, s \in \mathbb{N}$ satisfy $a^r \equiv 1 \mod m$ and $a^s \equiv 1 \mod m$. Then $a^d \equiv 1 \mod m$ where $d = \gcd(r, s)$.*

**Proof** There exist $u, v \in \mathbb{Z}$ with $d = ur + vs$. This implies that

$$\begin{aligned}(a + m\mathbb{Z})^d &= (a + m\mathbb{Z})^{ur+vs} = ((a + m\mathbb{Z})^r)^u \cdot ((a + m\mathbb{Z})^s)^v \\ &= (1 + m\mathbb{Z})^u \cdot (1 + m\mathbb{Z})^v = 1 + m\mathbb{Z}\end{aligned}$$

which implies the desired congruence. □

**3.24 Proposition** *Assume that $p$ is a prime dividing $a^n - 1$ for some $n, a \in \mathbb{N}$. Then one of the two following must hold:*

(a) *$p \mid a^d - 1$ for some divisor $d$ of $n$ which is smaller than $n$, or*
(b) *$p \equiv 1 \mod n$.*

*Moreover, if $p$ and $n$ are odd and $p \equiv 1 \mod n$ then $p \equiv 1 \mod 2n$.*

**Proof** Note that since $p \mid a^n - 1$ we have $p \nmid a$. We have $p \mid a^n - 1$ and $p \mid a^{p-1} - 1$ by Fermat's Little Theorem. Proposition 3.23 implies that $p \mid a^d - 1$ for $d = \gcd(p-1, n)$.

If $d < n$ then we are in case (a).

If $d = n$ then $n \mid p - 1$ and we are in case (b).

The last statement is obvious, since $2 \mid p - 1$. □

**3.25 Proposition** *Let $a, n \in \mathbb{N}$ and assume that $n$ is odd. Then*

$$a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + - \cdots - a + 1)\,.$$

**Proof** Easy verification. □

**3.26 Remark** The last propositions are useful when one tries to factor numbers of the form $a^n - 1$ or $a^n + 1$ into primes. Primes of the form $2^n + 1$ are called *Fermat primes* and primes of the form $2^n - 1$ are called *Mersenne primes*. Fermat primes: $2, 3, 5, 17, 257, \ldots$. Mersenne primes: $3, 7, 31, 127, \ldots$. It is unknown if there are infinitely many Fermat primes or Mersenne primes.

## Exercises for Section 3

**1.** Prove the statements in Remark 3.3.

**2.** Determine the units of the ring $\mathbb{Z}/30\mathbb{Z}$ and find their inverses.

**3.** For $a = -286, 12, -5690$, determine if the element $a + 12001\mathbb{Z}$ is invertible in $\mathbb{Z}/12001\mathbb{Z}$, and if yes, compute the inverse.

**4.** Decide if the matrix

$$A = \begin{pmatrix} 3 + 1001\mathbb{Z} & 120 + 1001\mathbb{Z} \\ 14 + 1001\mathbb{Z} & 73 + 1001\mathbb{Z} \end{pmatrix} \in M_2(\mathbb{Z}/1001\mathbb{Z})$$

is invertible and if yes, determine its inverse.

**5.** Find $x \in \{0, \dots, 17016\}$ such that the three congruences

$$\begin{aligned} x &\equiv 3 \mod 119 \\ x &\equiv -2 \mod 11 \\ x &\equiv 8 \mod 13 \end{aligned}$$

are simultaneously satisfied.

**6.** Let $n = n_k 10^k + \cdots + n_2 100 + n_1 10 + n_0$ with $n_0, \dots, n_k \in \{0, \dots, 9\}$. Thus, $n_0, \dots, n_k$ are the digits of $n$ as decimal number. Show that

(a) $n \equiv n_0 + n_1 + n_2 + \cdots + n_k \mod 9$.

(b) $3 \mid n \iff 3 \mid n_0 + n_1 + \cdots + n_k$.

(c) $9 \mid n \iff 9 \mid n_0 + n_1 + \cdots + n_k$.

(d) $n \equiv n_0 - n_1 + n_2 - + \cdots \mod 11$.

(e) $11 \mid n \iff 11 \mid n_0 - n_1 + n_2 - + \cdots$.

**7.** Compute $289^{3812} \mod 121$.

**8.** (a) Assume that $p = 2^n + 1$ is a Fermat prime with $n \geqslant 1$. Show that $n = 2^r$ for some $r \in \mathbb{N}_0$.

(b) Assume that $p = 2^n - 1$ is a Mersenne prime with $n \geqslant 2$. Show that $n$ is a prime.

**9.** Let $n > 2$ be a natural number. Show that $\phi(n)$ is a power of 2 if and only if $n$ is a product of Fermat primes and each odd Fermat prime occurs at most once in $n$. (One can show that a regular $n$-gon can be constructed with compass and straight edge if and only if $\varphi(n)$ is a power of 2.)

# 4 First Simple Crypto Systems

**4.1 (The basic setup and terminology)**

- *Cryptography* is the study of disguising messages.
- A message in undisguised form is called a *plain text*.
- A message in disguised form is called a *cipher text*.
- Plain text and cipher text are written in some *alphabet*. The number of *letters* is usually denoted by $N$.
- The process of converting plain text to cipher text is called *enciphering*, the reverse process is called *deciphering*.
- Plain text and cipher text are usually broken up into *message units*. A message unit could be a single letter, or a pair of letters (*digraph*), or a triple of letters (*trigraph*), or a block of any number of letters. We denote the set of message units of the plain text (resp. cipher text) $\mathcal{P}$ (resp. $\mathcal{C}$). An *enciphering transformation* is a function $f\colon \mathcal{P} \to \mathcal{C}$. It is usually bijective and its inverse $f^{-1}\colon \mathcal{C} \to \mathcal{P}$ is called the *deciphering transformation*.
- A setup as above is called a *crypto system*. It is of advantage to translate $\mathcal{C}$ and $\mathcal{P}$ into mathematical objects with rich structure that makes the computation of $f$ and $f^{-1}$ easy and allows statements about the security of the setup.

**4.2 Example** We can label the letters from $A$ to $Z$ and the 'blank' by the elements of $\mathbb{Z}/27\mathbb{Z}$:

| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

| $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ |
|---|---|---|---|---|---|---|---|---|---|
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |

| $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | |
|---|---|---|---|---|---|---|
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |

In this case, our alphabet consists of the elements in $\mathbb{Z}/27\mathbb{Z}$. We can use single letter blocks and set $\mathcal{P} = \mathcal{C} = \mathbb{Z}/27\mathbb{Z}$. For instance, the letter $8 + 27\mathbb{Z}$ of the alphabet $\mathbb{Z}/27\mathbb{Z}$ represents the usual letter 'I'.

(a) **Shift transformation:** We can choose an element $b \in \mathbb{Z}/27\mathbb{Z}$ and use the bijective function

$$f_b \colon \mathbb{Z}/27\mathbb{Z} \to \mathbb{Z}/27\mathbb{Z}\,, \quad p \mapsto p + b\,,$$

as enciphering transformation. The corresponding deciphering transformation is $f_b^{-1} = f_{-b}$. We call $b$ the *key* of this crypto system. For $b = 3 + 27\mathbb{Z}$ we obtain

$$\text{TOMORROW} \overset{f_b}{\mapsto} \text{WRPRUURZ}\,.$$

(b) **Affine transformation:** We can choose two elements $a \in (\mathbb{Z}/27\mathbb{Z})^\times$ and $b \in \mathbb{Z}/27\mathbb{Z}$ and define the enciphering transformation

$$f_{a,b} \colon \mathbb{Z}/27\mathbb{Z} \to \mathbb{Z}/27\mathbb{Z}\,, \quad p \mapsto ap + b\,.$$

Note that $f_{a,b}$ is bijective, since $a$ is invertible in the ring $\mathbb{Z}/27\mathbb{Z}$. The deciphering transformation $f_{a,b}^{-1}$ is again of this form, namely

$$f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}\,.$$

We call the pair $(a, b)$ the *key* of this crypto system, and the crypto system itself is called the *affine crypto system*. Note that if $a = 1$ we obtain as a special case the *shift crypto system* from part (a). If we choose $a = 2 + 27\mathbb{Z}$ and $b = 3 + 27\mathbb{Z}$ then we obtain

$$\text{TOMORROW} \overset{f_{a,b}}{\mapsto} \text{OEAEKKEU}\,.$$

We have $a^{-1} = 14 + 27\mathbb{Z}$ and can verify that

$$f_{14+27\mathbb{Z},12+27\mathbb{Z}} \colon \text{OEAEKKEU} \mapsto \text{TOMORROW}\,.$$

**4.3 Remark** The study of breaking codes is called *cryptanalysis*. For the above crypto systems (shift and affine), an easy way to find the key is *frequency analysis*. In English language, of all the letters, the blank occurs most often, then E, then T, etc.

For instance, if one knows that the crypto system used is an affine crypto system with the ring $R = \mathbb{Z}/27\mathbb{Z}$, and if X is the most frequent letter and

K the second most frequent in the cipher texts then we can assume that X stands for the blank and K stands for E. This gives equations:

$$23 + 27\mathbb{Z} = X = f_{a,b}(\text{blank}) = a(-1 + 27\mathbb{Z}) + b\,,$$
$$10 + 27\mathbb{Z} = K = f_{a,b}(E) = a(4 + 27\mathbb{Z}) + b\,.$$

These two equations simplify to

$$23 + 27\mathbb{Z} = -a + b \quad \text{and} \quad 10 + 27\mathbb{Z} = (4 + 27\mathbb{Z})a + b\,.$$

Subtraction gives $13+27\mathbb{Z} = (-5+27\mathbb{Z})a$. Finding $(-5+27\mathbb{Z})^{-1} = 16+27\mathbb{Z}$ and multiplication by this element allows us to find $a = (16 + 27\mathbb{Z})(13 + 27\mathbb{Z}) = 21+27\mathbb{Z} = -6+27\mathbb{Z}$. Then we can substitute into the first equation to find $b = (23 + 27\mathbb{Z}) + a = 17 + 27\mathbb{Z} = -10 + 27\mathbb{Z}$.

**4.4 Example (Affine digraph crypto system)** (a) We use the same alphabet as before and label the digraphs $AA$, $AB$, $AC$, ... by the elements $0+729\mathbb{Z}$, $1+729\mathbb{Z}$, $2+729\mathbb{Z}$, .... Note that $729 = 27^2$. Thus, $DK$ is labeled by $(3 \cdot 27 + 10) + 729\mathbb{Z}$, using that $D$ is labeled by 3 and $K$ is labeled by 10. This way we have identified the sets $\mathcal{P}$ and $\mathcal{C}$ of message units ($AA$, $AB$, ...) with the ring $\mathbb{Z}/729\mathbb{Z}$.

Again we can use an affine enciphering transformation

$$f_{a,b}\colon \mathcal{P} \to \mathcal{C}\,, \quad p \mapsto ap + b\,,$$

for an enciphering key $(a, b) \in (\mathbb{Z}/729\mathbb{Z})^\times \times \mathbb{Z}/729\mathbb{Z}$.

For example, if $a = 283 + 729\mathbb{Z}$ and $b = 500 + 729\mathbb{Z}$ then

$$\text{TOMORROW} \overset{f_{a,b}}{\mapsto} \text{HHYHMT D}\,.$$

In fact,

$$\begin{aligned}\text{TO} \leftrightarrow (19 \cdot 27 + 14) + 729\mathbb{Z} &= 527 + 729\mathbb{Z} \mapsto (283 \cdot 527 + 500) + 729\mathbb{Z} \\ &= 196 + 729\mathbb{Z} = (7 \cdot 27 + 7) + 729\mathbb{Z} \leftrightarrow \text{HH}\,,\end{aligned}$$

and similarly for the other three digraphs.

As in the previous example $f_{a,b}^{-1}$ is again of the form $f_{a',b'}$ with $a' = a^{-1}$ and $b' = -a^{-1}b$. In our case, with $a = 283 + 729\mathbb{Z}$ and $b = 500 + 729\mathbb{Z}$ we obtain $a' = 322 + 729\mathbb{Z}$ and $b' = 109 + 729\mathbb{Z}$.

(b) In English language the three most frequent digraphs are 'E ', 'S ', and ' T', in this order. Assume that you have intercepted some cipher text that you know was enciphered using the affine digraph crypto system above with an unknown key $(a, b)$. You conduct frequency analysis and find out that the most frequent diagraphs in the cipher text are 'YK', then 'ZK', then 'KR'. This gives you the following equations:

$$\begin{aligned}(24 \cdot 27 + 10) + 729\mathbb{Z} &= a \cdot ((4 \cdot 27 + 26) + 729\mathbb{Z}) + b \\ (25 \cdot 27 + 10) + 729\mathbb{Z} &= a \cdot ((18 \cdot 27 + 26) + 729\mathbb{Z}) + b \\ (10 \cdot 27 + 17) + 729\mathbb{Z} &= a \cdot ((26 \cdot 27 + 19) + 729\mathbb{Z}) + b\end{aligned}$$

Simplifying, we obtain

$$\begin{aligned}658 + 729\mathbb{Z} &= (134 + 729\mathbb{Z})a + b \quad (1) \\ 685 + 729\mathbb{Z} &= (512 + 729\mathbb{Z})a + b \quad (2) \\ 287 + 729\mathbb{Z} &= (721 + 729\mathbb{Z})a + b \quad (3)\end{aligned}$$

Subtracting Equation (1) from Equation (2) we obtain

$$27 + 729\mathbb{Z} = (378 + 729\mathbb{Z})a \quad (4)\,.$$

Unfortunately, 378 and 729 are not coprime so that $(378 + 729\mathbb{Z})$ does not have an inverse. But dividing by $\gcd(378, 729) = 27$ we still obtain $1+27\mathbb{Z} = (14+27\mathbb{Z})a_1$, where $a_1 \in \mathbb{Z}/27\mathbb{Z}$ arises from $a$ as the image under the function

$$\mathbb{Z}/729\mathbb{Z} \to \mathbb{Z}/27\mathbb{Z} \quad x + 729\mathbb{Z} \mapsto x + 27\mathbb{Z}\,.$$

The equation $1 + 27\mathbb{Z} = (14 + 27\mathbb{Z}) \cdot a_1$ now implies

$$a_1 = 2 + 27\mathbb{Z}\,. \quad (5)$$

This leaves us with 27 possibilities for $a$, namely $a = 2+729\mathbb{Z}$, $a = 29+729\mathbb{Z}$, $a = 56 + 729\mathbb{Z}$, etc.

Instead of investigating each of these possibilities individually, we start again with Equations (1)–(3) and this time we subtract Equation (3) from Equation (2) to obtain

$$398 + 729\mathbb{Z} = (-209 + 729\mathbb{Z})a = (520 + 729\mathbb{Z})a\,.$$

Now we are lucky, since $\gcd(-209, 729) = 1$. Using the Euclidean Algorithm we find $(520 + 729\mathbb{Z})^{-1} = -293 + 729\mathbb{Z}$ and therefore

$$a = (-293 + 729\mathbb{Z})(398 + 729\mathbb{Z}) = 26 + 729\mathbb{Z}\,.$$

Obviously, this is not consistent with Equation (5). This means that there is no solution for $a$ that satisfies all three Equations (1)–(3). We probably had the wrong match-up from our frequency analysis. One should try to match up the most frequent digraphs in a different way and try again.

(c) Returning to our concrete choice of $a$ and $b$ in part (a), the digraphs ON and NO are enciphered as

$$\begin{aligned}
\mathrm{ON} &\leftrightarrow (14 \cdot 27 + 13) + 729\mathbb{Z} = 391 + 729\mathbb{Z} \mapsto a \cdot (391 + 729\mathbb{Z}) + b \\
&\quad = 345 + 729\mathbb{Z} \leftrightarrow \mathrm{MV}\,, \\
\mathrm{NO} &\leftrightarrow (13 \cdot 27 + 14) + 729\mathbb{Z} = 365 + 729\mathbb{Z} \mapsto a \cdot (365 + 729\mathbb{Z}) + b \\
&\quad = 277 + 729\mathbb{Z} \leftrightarrow \mathrm{KH}\,.
\end{aligned}$$

Thus, in contrast to the single letter affine crypto system, one can not use simple one letter frequency analysis.

However, also note that in

$$\mathrm{T\underline{O}|M\underline{O}|RR|OW} \mapsto \mathrm{H\underline{H}|Y\underline{H}|MT|\ D}$$

the first two O's, both occurring in even positions, are both turned into H's. This is no coincidence, as a simple computation modulo 27 shows. Thus, one can decipher by 1-letter frequency analysis of the even places all letters in even places. Moreover, one can determine $a$ and $b$ modulo 27.

**4.5 Remark** Instead of digraphs one can also use message units of $k$ letter, interpret them as elements in the ring $\mathbb{Z}/N^k\mathbb{Z}$ (where $N$ is the number of letters in the alphabet that is used). Again, one can use affine transformations

$$f_{a,b}\colon \mathbb{Z}/N^k\mathbb{Z} \to \mathbb{Z}/N^k\mathbb{Z}\,, \quad p \mapsto ap + b\,,$$

with $a \in (\mathbb{Z}/N^k\mathbb{Z})^\times$ and $b \in \mathbb{Z}/N^k\mathbb{Z}$. The principles are very similar to those we have seen for $k = 1$ and $k = 2$.

## Exercises for Section 4

**1.** Assume the letters A-Z are labeled by $0, \ldots, 25$ and the blank is labeled by 26. Encipher the message "everything is ok" using the affine cryptosystem for $R = \mathbb{Z}/27\mathbb{Z}$ with the key $(a, b) = (8, 13)$.

**2.** Assume that the following message is enciphered with the labeling of letters and the blank as in Problem 1 using an affine cryptosystem for $R = \mathbb{Z}/27\mathbb{Z}$. Try to find the key (a,b) using frequency analysis and decipher the message. The message is:
15 8 1 17 13 9 17 10 11 1 9 10 22 2 7 17 21 1 24 22 7 12 17 10 1 21 25 24 11 1 2 17 1 17 8 3 22 26 17 3 1 26 19 11 5 1 11 26 22 1 19 8 16 22 21 9 15 11 19 2 7 17 1 23 25 15 7 19 11 19 17 24 1 1 15 1 10 17 24 11 7 17 24 24 1 19 21 15 18 19 8 15 11 19 22 8 1 15 8 3 1 15 1 9 15 11 19 17 8 11 1 9 17 10 11 19 8 15 16 19 11 0 1 1 5 22 26 15 10 3 1 26 1 17 12 17 24.

**3.** Assume you intercept the message "PSQIUF" and you know it has been enciphered using the affine digraph cryptosystem for the ring $R = \mathbb{Z}/729\mathbb{Z}$ and the labeling as in Example 4.4 with the key $(a, b) = (320, 155)$. Decipher the message.

# 5 Crypto Systems Using Matrices

**5.1 Example (Affine matrix crypto system)** Assume we use an alphabet with $N$ letters. We label a digraph by a column vector $\begin{pmatrix} x \\ y \end{pmatrix} \in (\mathbb{Z}/N\mathbb{Z})^2$ with $x, y \in \mathbb{Z}/N\mathbb{Z}$. A text $a_1b_1a_2b_2a_3b_3 \dots a_nb_n$ will be translated into a matrix

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \end{pmatrix} .$$

For instance, with $N = 27$ and the labeling from Section 4 we could translate TOMORROW into

$$\begin{pmatrix} 19 & 12 & 17 & 14 \\ 14 & 14 & 17 & 22 \end{pmatrix} , \tag{5.1.a}$$

omitting the '$+27\mathbb{Z}$', but keeping in mind that we actually mean the classes of these numbers as elements in the ring $\mathbb{Z}/27\mathbb{Z}$. As enciphering transformation we might choose a matrix $A \in \mathrm{Mat}_2(\mathbb{Z}/N\mathbb{Z})^\times$ and define

$$f_A \colon \mathcal{P} = (\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2 = \mathcal{C} , \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix} .$$

The deciphering transformation is of the same form, namely $(f_A)^{-1} = f_{A^{-1}}$. Recall that $A$ is invertible if and only if $\det A$ is a unit in $\mathbb{Z}/N\mathbb{Z}$. $A$ is called the *key* of this crypto system. Note that instead of multiplying $A$ consecutively to $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$, $\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$, …, $\begin{pmatrix} x_n \\ y_n \end{pmatrix}$, one can instead multiply $A$ to the matrix in (5.1.a).

Slightly more generally one can additionally choose a vector $B \in (\mathbb{Z}/N\mathbb{Z})^2$ and use the enciphering transformation

$$f_{A,B} \colon (\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2 , \quad P \mapsto AP + B .$$

Its inverse is again of the same form: $(f_{A,B})^{-1} = f_{A^{-1},-A^{-1}B}$ and $(A, B)$ (resp. $(A^{-1}, -A^{-1}B)$) is called the enciphering (resp. deciphering) key of this *affine matrix crypto system.*

**5.2 Example** We use $N = 27$ as in Section 4 and choose the key $(A, B)$ with

$$A = \begin{pmatrix} 23 + 27\mathbb{Z} & -1 + 27\mathbb{Z} \\ 4 + 27\mathbb{Z} & 12 + 27\mathbb{Z} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 3 + 27\mathbb{Z} \\ 19 + 27\mathbb{Z} \end{pmatrix} .$$

We encipher

$$\text{TOMORROW} \leftrightarrow \begin{pmatrix} 19 & 12 & 17 & 14 \\ 14 & 14 & 17 & 22 \end{pmatrix} \overset{f_{A,B}}{\mapsto} \begin{pmatrix} 21 & 22 & 26 & 6 \\ 20 & 19 & 21 & 15 \end{pmatrix} \leftrightarrow \text{VUWT VGP}\,.$$

We compute the deciphering key: $\det(A) = 10 + 27\mathbb{Z}$ and $\det(A)^{-1} = 19 + 27\mathbb{Z} = -8 + 27\mathbb{Z}$. Thus,

$$A^{-1} = \begin{pmatrix} 12 & 19 \\ 5 & 5 \end{pmatrix} \quad \text{and} \quad -A^{-1}B = \begin{pmatrix} 8 \\ -2 \end{pmatrix},$$

again omitting the '$+27\mathbb{Z}$'. Now we can verify that the deciphering transformation indeed returns our original message 'TOMORROW'.

**5.3 Remark** (a) The affine matrix crypto system does not have the same flaw as the affine crypto system for digraphs used in Section 4. In fact, in the previous example we saw that 'TO' and 'MO' were enciphered into 'VU' and 'WT', respectively. Although both plaintext digraphs 'TO' and 'MO' end in 'O', the enciphered digraphs end in different letters, namely 'U' and 'T'.

(b) One can easily attack the affine matrix crypto system with digraph frequency analysis. However, instead of using $2 \times 2$-matrices we could use $k \times k$-matrices with entries in $\mathbb{Z}/N\mathbb{Z}$ and message units of $k$ letters, for any $k \in \mathbb{N}$ we want. For large $k$, this crypto system would have none of the disadvantages we found with the previous systems.

**5.4 Example** Assume you intercepted an enciphered message beginning with

$$CU|.T|G\ |CG|NF|CG|.?|BK$$

and assume you know from some source that the corresponding plain text message starts with $GI|VE|\ M|E$ and that it was created by affine matrix encryption for the alphabet A–Z, the blank, and the punctuations ',', '.' and '?' with $N = 30$ letters. Also assume that you know that $B = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ in the key $(A, B)$.

From this information we can derive equations

$$\begin{pmatrix} 2 \\ 20 \end{pmatrix} = A \begin{pmatrix} 6 \\ 8 \end{pmatrix} \qquad (1)$$

$$\begin{pmatrix} 28 \\ 19 \end{pmatrix} = A \begin{pmatrix} 21 \\ 4 \end{pmatrix} \qquad (2)$$

$$\begin{pmatrix} 6 \\ 26 \end{pmatrix} = A \begin{pmatrix} 26 \\ 12 \end{pmatrix} . \qquad (3)$$

We can combine equations (1) and (2) to obtain

$$\begin{pmatrix} 2 & 28 \\ 20 & 19 \end{pmatrix} = A \begin{pmatrix} 6 & 21 \\ 8 & 4 \end{pmatrix} .$$

But

$$\det \begin{pmatrix} 6 & 21 \\ 8 & 4 \end{pmatrix} = 24 - 168 = -144 \equiv 6 \mod 30$$

which is not good, since it is not invertible modulo 30. If the determinant were invertible, we could compute the inverse of the matrix and solve for $A$. Similarly, combining equations (2) and (3) lead to

$$\begin{pmatrix} 28 & 6 \\ 19 & 26 \end{pmatrix} = A \begin{pmatrix} 21 & 26 \\ 4 & 12 \end{pmatrix} \qquad (4)$$

with

$$\det \begin{pmatrix} 21 & 26 \\ 4 & 12 \end{pmatrix} = 252 - 104 = 148 \equiv -2 \mod 30 \qquad (5)$$

and combining equations (1) and (3) lead to

$$\begin{pmatrix} 2 & 6 \\ 20 & 26 \end{pmatrix} = A \begin{pmatrix} 6 & 26 \\ 8 & 12 \end{pmatrix}$$

with

$$\det \begin{pmatrix} 6 & -4 \\ 8 & 12 \end{pmatrix} = 72 + 32 = 104 \equiv 14 \mod 30 .$$

We will work with the equations (4) and (5) in $\mathbb{Z}/30\mathbb{Z}$ and view them as equations in $\mathbb{Z}/15\mathbb{Z}$:

$$\begin{pmatrix} -2 & 6 \\ 4 & -4 \end{pmatrix} = A' \begin{pmatrix} 6 & -4 \\ 4 & -3 \end{pmatrix}$$

with $A' \in \mathrm{Mat}_2(\mathbb{Z}/15\mathbb{Z})$ arising from $A$ by viewing the entries of $A$ modulo 15. Again,

$$\det \begin{pmatrix} 6 & -4 \\ 4 & -3 \end{pmatrix} = -2 + 15\mathbb{Z}.$$

Thus, the matrix $\begin{pmatrix} 6 & -4 \\ 4 & -3 \end{pmatrix}$ is invertible in $\mathrm{Mat}_2(\mathbb{Z}/15\mathbb{Z})$, its determinant has inverse $7 + 15\mathbb{Z}$ and its inverse is given by

$$\begin{pmatrix} 6 & -4 \\ 4 & -3 \end{pmatrix}^{-1} = 7 \begin{pmatrix} -3 & 4 \\ -4 & 6 \end{pmatrix} = \begin{pmatrix} -21 & 28 \\ -28 & 42 \end{pmatrix} = \begin{pmatrix} -6 & -2 \\ 2 & -3 \end{pmatrix}$$

as matrix with entries in $\mathbb{Z}/15\mathbb{Z}$. This implies that

$$A' = \begin{pmatrix} -2 & 6 \\ 4 & -4 \end{pmatrix} \begin{pmatrix} -6 & -2 \\ 2 & -3 \end{pmatrix} = \begin{pmatrix} 24 & -14 \\ -32 & 4 \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 13 & 4 \end{pmatrix}$$

as matrix with entries in $\mathbb{Z}/15\mathbb{Z}$. Using this result for $A'$, we are left with 16 possibilities for $A$:

$$A = \begin{pmatrix} 9 + 15\varepsilon_1 & 1 + 15\varepsilon_2 \\ 13 + 15\varepsilon_3 & 4 + 15\varepsilon_4 \end{pmatrix}$$

with $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 \in \{0, 1\}$.

We will investigate each of these 16 cases:

Case $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (0, 0, 0, 0)$:

$$A = \begin{pmatrix} 9 & 1 \\ 13 & 4 \end{pmatrix}, \quad \det A = 36 - 13 = 23 \equiv -7 \mod 30\,.$$

This leads to

$$A^{-1} = (-13) \begin{pmatrix} 4 & -1 \\ -13 & 9 \end{pmatrix} = \begin{pmatrix} -52 & 13 \\ 169 & -117 \end{pmatrix} = \begin{pmatrix} 8 & 13 \\ 19 & 3 \end{pmatrix}$$

and to the deciphered message beginning with

$$GIVE\_ME\_TWE\_\ldots$$

which doesn't make sense.

Case $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (0, 0, 0, 1)$:

$$A = \begin{pmatrix} 9 & 1 \\ 13 & 19 \end{pmatrix}, \quad \det A \text{ is even}.$$

This is impossible, since $\det A$ must be invertible in $\mathbb{Z}/30\mathbb{Z}$.

Case $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (0, 0, 1, 0)$:

$$A = \begin{pmatrix} 9 & 1 \\ -2 & 4 \end{pmatrix}, \quad \det A \text{ is even}.$$

Again, this is not possible.

Case $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (0, 0, 1, 1)$:

$$A = \begin{pmatrix} 9 & 1 \\ -2 & -11 \end{pmatrix}, \quad \det A = -99 + 2 = -97 \equiv -7 \mod 30.$$

This leads to

$$A^{-1} = (-13) \begin{pmatrix} -11 & -1 \\ 2 & 9 \end{pmatrix} = \begin{pmatrix} 143 & 13 \\ -26 & -117 \end{pmatrix} = \begin{pmatrix} -7 & 13 \\ 4 & 3 \end{pmatrix}$$

and to the deciphered message beginning with

$$GIVE\_ME\_EHE\_BX$$

which doesn't make sense.

Case $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (0, 1, 0, 0)$:

$$A = \begin{pmatrix} 9 & 16 \\ 13 & 4 \end{pmatrix}, \quad \det A \text{ is even}.$$

This is not possible.

$\vdots$

## Exercises for Section 5

**1.** Let $N = 30$ and use the labeling of the alphabet A-Z, " ", ",", ".", "?" as in Example 5.4. Use the affine matrix crypto system with key $(A, B)$, where

$$A = \begin{pmatrix} 1+30\mathbb{Z} & -1+30\mathbb{Z} \\ 3+30\mathbb{Z} & -2+30\mathbb{Z} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 4+30\mathbb{Z} \\ 1+30\mathbb{Z} \end{pmatrix}.$$

Encipher the message "COLLUSION?" and compute the key for the deciphering transformation.

**2.** You intercepted the message

"U?DIPPWKCKIKFBWZERRXTV AXN,FG.SAYCHY"
"VTMIMBG.LHTV KCPEAF?.FSGGZ.YOQMZQL.D"
"WKLHYCHIVT,REEKQMJSLEAFXWWVFMKQQUQEW"
"OQHI .BOG.UN.JGNIZQYESRMOQGNWMTVZHF,"
"OKQYZQBLVNQ.MJSLMKQQUQRXKMJEG.ZH WRM"
".HYNDV,REE,RGBJR.F?NFHMHGHSFMKTZPDKA"
"?EVJEM W?T MDOYU.FSFYCKWSHKNGEG.LH?N"
"FHMHGHSFOQCCESRM?N,RZBE,.HZZQLIHWWCZ"
".KHIIJOWIHW..HQQUQUNRMJR.F?TWANUEGSE"
"GTSHFXWZGHDOOQGNVFMKWE,MBFE,.H,XOQWK"
"ZBOTRZON.ECJQLWZFXWZQQUQ.GMZCIG.VZKW"
"V.Q.NXVTG.QQUQ.USFMKBOBFEM WYCHIVTJR"
".FJLVZGNMJSL?Z QIOWCESRMSFSWSEYRWK"

Assume that an affine matrix crypto system was used and that the underlying alphabet consists of the thirty letters A-Z, " ", ",", ".", "?", labeled by the elements in $\mathbb{Z}/30\mathbb{Z}$. Assume that you further know that the plaintext message ends with the four letters "LES " and that $B = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ in the enciphering key $(A, B)$. Find the matrix $A$ of the enciphering key, compute the deciphering key and decipher the first 8 letters of the message.

**3.** Decipher the full message in Exercise 2 using a computer. (Bonus points)

**4.** Finish Example 5.4 from class: Find the correct matrix $A$ and decipher the beginning of the message.

# 6 Public Key Crypto Systems

**6.1 Definition (Public key crypto system)** A large list of persons shares the same sets $\mathcal{P}$ of plain text message units and $\mathcal{C}$ of cipher text message units. Each person $X$ publishes an enciphering key $k_{X,e}$ in a phone book. This key allows everybody to compute an enciphering transformation $f_X : \mathcal{P} \to \mathcal{C}$. This transformation is used to send messages to person $X$. The characteristic property of a public key crypto system is that even knowing $k_{X,e}$ (and $f_X$) it is impossible to compute the deciphering key $k_{X,d}$ or the deciphering transformation $f_X^{-1} : \mathcal{C} \to \mathcal{P}$ in reasonable time. Such functions $f_X$ are also called *one way functions* or *trap functions*.

If person $A$ wants to send a message to person $B$, he/she looks up the key $k_{B,e}$ in the phone book under B's name, computes the enciphering transformation $f_B : \mathcal{P} \to \mathcal{C}$, enciphers the plain text message $P$ as $f_B(P)$ and sends this to $B$. Only $B$ has knowledge of the deciphering key $k_{B,d}$ and the deciphering transformation $f_B^{-1}$.

**6.2 Remark** Public key crypto systems have the following advantages:

(a) One can have a large network of people communicating with each other. If $x$ is the number of people in the network then one only needs $x$ keys to allow to communicate everybody with everybody else. In contrast to the previous system, every pair of persons in the network would have to choose a key that only is used among those two. This leads to $x(x-1)/2 \sim x^2/2$ keys. Each person would have to keep track of as many deciphering keys as there are persons he/she wants to communicate with.

(b) Authentication: If Alice (A for short) wants to send a message to Bob (B for short), she can use the following trick to make sure that Bob knows the message can only come from her. She can include a so-called signature:

P=Plain text message: Blablabla

S=Signature: Alice, April 30, 2009, some random meaningful text

She sends $f_B(P)$ and appends $f_B(f_A^{-1}(S))$. Bob can read the message using $f_B^{-1}$ and verify the signature using $f_A$ in addition to the last part. Since only Alice knows $f_A^{-1}$, the message must come from her. But there is still a problem: Someone who obtained a message from Alice before can use her signature $f_A^{-1}(S)$. A remedy would be to include a precise time in the signature.

(c) HASH FUNCTIONS: One can also make sure that nobody intercepts the message, changes the message part and keeps Alice's signature in place. This is done through so-called *hash-functions* $h\colon \mathcal{P}^r \to \mathcal{P}^s$. Such a function is publicly known and $r$ is large compared to $s$. Now, Alice adds to her signature the part $h(P)$, so altogether she sends $f_B(P), f_B(f_A^{-1}(S)), f_B(f_A^{-1}(h(P)))$. Bob can verify that no one has changed the message part $f_B(P)$ by deciphering the message part, computing $h(P)$ and comparing it with the deciphered second part of the signature.

(d) KEY EXCHANGE: It lies in the nature of public key crypto systems that enciphering and deciphering messages takes longer than for 'private crypto systems'. If speed is essential one can still use a public crypto system to exchange keys for a private crypto system.

# 7 The RSA Crypto System

This crypto system is name after its inventors Rivest, Shamir and Adleman (∼1978).

**7.1 Definition (RSA crypto system)** Each person $X$ chooses two large primes $p_X < q_X$ (about 100 decimal digits) and computes $n_X := p_X q_X$. Person $X$ keeps $p_X$ and $q_X$ secret. Next, person $X$ computes $\phi(n_X)$ and chooses some number $e_X \in \{1, \dots, \phi(n_X)\}$ with $\gcd(e_X, \phi(n_X)) = 1$. Person $X$ publishes her/his enciphering key $(n_X, e_X)$ in a list under her name. Only person $X$ can compute the inverse $d_X$ of $e_X$ modulo $\phi(n_X)$, since only person $X$ knows $\phi(n_X)$ (or equivalently $p_X$ and $q_X$, cf. Remark 3.15). To encipher a message you want to send to person $X$, you use the enciphering transformation

$$f_X \colon \mathbb{Z}/n_X\mathbb{Z} \to \mathbb{Z}/n_X\mathbb{Z}\,, \quad a + n_X\mathbb{Z} \mapsto a^{e_X} + n_X\mathbb{Z}\,.$$

Using her deciphering key $(n_X, d_X)$, Person $X$ can decipher the message by the transformation

$$f_X^{-1} \colon \mathbb{Z}/n_X\mathbb{Z} \to \mathbb{Z}/n_X\mathbb{Z}\,, \quad b + n_X\mathbb{Z} \mapsto b^{d_X} + n_X\mathbb{Z}\,.$$

We need to show that no matter what $a$ is, we have

$$(a^{e_X})^{d_X} \equiv a \mod n_X\,. \tag{7.1.a}$$

For that we first show that $p_X \mid a - a^{e_X d_X}$. If $p_X \mid a$, this is clear, and if $p_X \nmid a$ this follows from the corollary to Fermat's Theorem, since $e_X d_X \equiv 1 \mod \phi(n_X)$. Similarly, we can see that $q_X \mid a - a^{e_X d_X}$, and therefore $n_X \mid a - a^{e_X d_X}$, which means the congruence in (7.1.a) holds.

**7.2 Remark** In the above definition it seems that $\mathcal{C}$ and $\mathcal{P}$ are equal to $\mathbb{Z}/n_X\mathbb{Z}$ and depend on the person $X$. We can make $\mathcal{P}$ and $\mathcal{C}$ independent of $X$ by the following slight modification. Assume we use an alphabet with $N$ letters. Choose natural numbers $k < l$ and require that everybody chooses $n_X$ satisfying

$$N^k < n_X < N^l\,.$$

We will use plain text message units consisting of blocks of $k$ letters and cipher text message units consisting of blocks of $l$ letters. Thus, $|\mathcal{P}| = N^k$

and $|\mathcal{C}| = N^l$. If, for instance, $k = 3$ we translate the plain text message unit 'CAT' into the number $a := 2 \cdot N^2 + 0 \cdot N + 19$. This number is smaller than $n_X$, we take its class modulo $n_X$ and apply the enciphering transformation $f_X \colon \mathbb{Z}/n_X\mathbb{Z} \to \mathbb{Z}/n_X\mathbb{Z}$ to obtain a number $b < n_X$. Thus, $b < N^l$ and we can translate $b$ into a block of $l$-letters, i.e. into a cipher text message unit. Deciphering just reverses this process: Person $X$ translates the block of of $l$-letters again into the number $b$. This number is smaller than $n_X$. Person $X$ computes the remainder of $b^{d_X}$ modulo $n_X$ and obtains the original number $a$ which was smaller than $N^k$, and translates it into a block of $k$ letters.

**7.3 Example** Alice choses $p_A = 167$ and $q_A = 281$. Then $n_A = p_A q_A = 46,927$ and $\phi(n_A) = (p_A - 1)(q_A - 1) = 46,480$. Alice chooses $e_A = 39,423$ and makes sure that $\gcd(39,423\ ,\ 46,480) = 1$. Then Alice computes $d_A = 26,767$. She publishes $(46,927\ ,\ 39,423)$ and keeps $\phi(n_A)$ and $d_A$ (along with $p_A$ and $q_A$ secret).

Next assume that we only use the letters A-Z as our alphabet, i.e., $N = 26$, and that we choose $k = 3$ and $l = 4$. (Note that $N^3 = 17,576 < n_A < 456,976 = N^4$). To send the message 'YES' to Alice we proceed as follows:

$$YES \leftrightarrow 24 \cdot 26^2 + 4 \cdot 26 + 18 = 16,346(\mathrm{mod} n_A\mathbb{Z})\,,$$
$$16,346(\mathrm{mod}\ n_A\mathbb{Z}) \quad \overset{f_A}{\mapsto} \quad 16,346^{39,423}(\mathrm{mod}\ 46,927) = 21,166\,,$$
$$21,166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 \leftrightarrow BFIC\,.$$

Now Alice obtains this message, translates it into the number $21,166$, computes the remainder of $21,166^{26,767}$ modulo $46,927$ and obtains $16,346$ which she translates into 'YES'.

For the exponentiation one can use the the repeated squaring method.

**7.4 Remark** Assume the situation of Remark 7.2: Everyone has chosen primes $p_X, q_X$ such that $N^k < n_X < N^l$. If $A$ wants to send a message to $B$ and wants to apply $f_B f_A^{-1}$ to her signature, this only works if $n_A < n_B$. In the other case she must use $f_A^{-1} f_B$. This should be a common rule for all participants.

**7.5 Remark** We will show that, for a participant of the RSA crypto system, it is not a good idea to choose $p < q$ with large $\gcd(p-1, q-1)$. In this case $r := \mathrm{lcm}(p-1, q-1)$ is a small multiple of $q-1$ and $p-1$, therefore

small compared to $\phi(n) = (p-1)(q-1)$ and to $n = pq$. If $f$ is an inverse of $e$ modulo $r$ then we have for every $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$:

$$a^{ef-1} = a^{tr} = a^{(p-1)s} \equiv 1 \mod p$$

with $t, s \in \mathbb{N}$. Therefore $p \mid a^{ef-1} - 1$. Similarly, we obtain $q \mid a^{ef-1} - 1$. Thus, $n = pq \mid a^{ef-1} - 1 \mid a^{ef} - a$ and

$$(a^e)^f \equiv a \mod n\,, \quad \text{for all } a \in \mathbb{Z} \text{ with } \gcd(a, n) = 1, \tag{7.5.a}$$

and a relatively small number $f$. Since most of the numbers $a$ are coprime to $n$, one can decipher the cipher text message unit $a^e$ easily by raising it to the $f$-th power, although $f$ might be different from $d$. Just by trial and error, one might find a small number $f$ with that property.

Next we will show that if we have found a number $f$ satisfying (7.5.a) we can even find the primes $p$ and $q$. Set $m := ef - 1$. Then

$$a^m \equiv 1 \mod n \quad \text{for all } a \in \mathbb{Z} \text{ with } \gcd(a, n) = 1. \tag{7.5.b}$$

Note that $m$ must be even since otherwise $(-1)^m \equiv (-1) \not\equiv 1 \mod n$. We check if also $m' := m/2$ has the property in (7.5.b) by choosing random elements $a$ which are coprime to $n$. If $m'$ does not have this property for all $a$, then the test will fail for at least 50 percent of all $a$'s (this will be shown later using group theory, see Corollary 8.4(c)). So, if $m'$ passes this test for $r$ independently chosen elements $a$, the chance that $m'$ does not have the property for all $a$ is less than $1/2^r$. So after enough tests (say $r = 20$), one can basically decide if $m'$ has property (7.5.b). Now, $m'$ has to be even (use also $a = -1$ as additional test) and we continue the same way with $m'' = m'/2$. Since these numbers will become smaller and smaller, at some point this test will fail and we have a number $m$ such that (7.5.b) holds for $m$ but not for $m/2$. This implies that $m/2$ is not a multiple of both $p-1$ and $q-1$ (by the first paragraph in this remark).

Now we distinguish two cases:

(i) $m/2$ is a multiple of one of the numbers $p-1$ and $q-1$ but not of the other. Say $m/2$ is a multiple of $p-1$ but not of $q-1$ (the opposite case is handled symmetrically). Then $a^{m/2} \equiv 1 \mod p$ for all $a$ with $\gcd(a, n) = 1$, but $a^{m/2} \equiv \pm 1 \mod q$ with each case occurring exactly 50 percent of the time (justification with group theory later, see Corollary 8.14(i),(ii) and Corollary 8.4(c)).

(ii) $m/2$ is not a multiple of either $p-1$ or $q-1$. Then we have 4 possibilities, namely $a^{m/2} \equiv \pm 1 \mod p$ and $a^{m/2} \equiv \pm 1 \mod q$, each occurring precisely 25 percent of the time (justification with group theory later, see Corollary 8.14(iii) and Corollary 8.4(c)).

Therefore, in any case, by trying random $a's$, coprime to $n$, the chance that $a^{m/2}-1$ is divisible by exactly one of the primes $p$ and $q$ but not by the other is precisely 50 percent. If $a$ has this property then $\gcd(a^{m/2}-1, n)$ is equal to the prime dividing $a^{m/2}-1$. Computing $\gcd(a^{m/2}-1, n)$ for randomly chosen $a$ will produce $p$ or $q$ with probability $1-\frac{1}{2^r}$ after $r$ steps.

## Exercises for Section 7

**1.** Find primes $p, q$ for yourself such that $n := pq$ is in the range between $N^3 = 27,000$ and $N^4 = 810,000$ (where $N = 30$). Find a possible $e$ for the RSA cryptosystem and compute the deciphering exponent $d$.

This part is voluntary: If you feel comfortable with giving away your email address to others in this class, indicate it on your homework together with your email address and key $(n, e)$. We will publish the resulting phone book for the RSA crypto system to those participating and you can use it to communicate.

**2.** Assume that with the RSA cryptosystem somebody's phone book entry is $(n, e) = (11247661, 268729)$ and assume you found out that it is very likely that $a^{7169e} \equiv a \mod n$ for all $a \in \{0, \ldots, n-1\}$. Find the prime decomposition of $n$ using this information and the deciphering key $(n, d)$ from this information.

# 8 Groups

**8.1 Definition** (a) A *group* is a set $G$ together with a binary operation

$$G \times G \to G\,, \quad (a,b) \mapsto ab\,, \quad (\text{or } a \cdot b \text{ or } a * b \text{ or } a \circ b, \text{ etc.})$$

containing an element $e$ such that

(i) $(ab)c = a(bc)$ for all $a, b, c \in G$;

(ii) $ae = a = ea$ for all $a \in G$;

(iii) For all $a \in G$ there exists an element $b \in G$ with $ab = e = ba$.

The cardinality $|G|$ is called the *order* of $G$. The element $e$ is uniquely determined by the property in (ii). It is called the *identity element* of $G$ and is often denoted by $1_G$ or just 1. Also, for given $a \in G$, the element $b$ from (iii) is uniquely determined by $a$. It is called the *inverse* and is denoted by $a^{-1}$. For $a \in G$ and $k \in \mathbb{Z}$ we set $a^k$ to be the $k$-fold product of $a$ if $k > 0$, we set $a^k = 1_G$ if $k = 0$ and we set $a^k := (a^{-1})^{|k|}$ if $k < 0$.

(b) Assume that $G$ and $H$ are groups. A function $f\colon G \to H$ is called a *group homomorphism* if it satisfies $f(ab) = f(a)f(b)$ for all $a, b \in G$. Note that this implies $f(1_G) = 1_H$. If additionally $f$ is bijective we call $f$ an *isomorphism*. The group $G$ and $H$ are called *isomorphic* (notation $G \cong H$) if there exists an isomorphism $f\colon G \to H$.

(c) If $f\colon G \to H$ is a group homomorphism then the *kernel* of $f$ is defined as

$$\ker(f) := \{a \in G \mid f(a) = 1_H\}$$

and the *image* of $f$ is defined as

$$\operatorname{im}(f) := \{f(a) \mid a \in G\}\,.$$

(d) For two subsets $X, Y \subseteq G$ of a group $G$ we define

$$XY := \{xy \mid x \in X, y \in Y\}\,.$$

which is again a subset of $G$.

**8.2 Example** If $R$ is a ring then $R^\times$ together with the ring multiplication is a group. Also, $R$ together with addition is a group.

**8.3 Lemma** *Let $G$ and $H$ be groups and let $f\colon G \to H$ be group homomorphism.*

(a) *Let $h \in \mathrm{im}(f)$ and let $g \in G$ with $f(g) = h$. Then*

$$\{a \in G \mid f(a) = h\} = g\ker(f)\,.$$

(b) *If $G$ is finite then $|g\ker(f)| = |\ker(f)|$ and $|G| = |\mathrm{im}(f)| \cdot |\ker(f)|$.*

(c) *Assume that $G$ is finite and that $h \in \mathrm{im}(f)$. Then the probability that $f$ sends a random element $a$ of $G$ to $h$ is*

$$\frac{|\ker(f)|}{|G|} = \frac{1}{|\mathrm{im}(f)|}\,.$$

**Proof** (a) Let $a \in G$ with $f(a) = h$. Then $f(a) = h = f(g)$ and multiplication from the left by $f(g)^{-1}$ yields $1_G = f(g)^{-1}f(a) = f(g^{-1})f(a) = f(g^{-1}a)$, so that $g^{-1}a \in \ker(f)$. Therefore, $a = g(g^{-1}a) \in g\ker(f)$. Conversely, let $a \in g\ker(f)$. Then there exists $x \in \ker(f)$ with $a = gx$ and $f(a) = f(gx) = f(g)f(x) = f(g)1_H = f(g)$.

(b) The function $\phi\colon \ker(f) \to g\ker(f)$, $x \mapsto gx$ is surjective by definition of $g\ker(f)$ and injective, since $gx = gy$ implies $x = y$ for $x, y \in \ker(f)$. Therefore $|\ker(f)| = |g\ker(f)|$.

The relation $a \sim b$ if and only of $f(a) = f(b)$ defines an equivalence relation on $G$. Each equivalence class is characterized by the element $h \in \mathrm{im}(f)$ to which its elements are mapped to. Therefore, the number of equivalence class is $|\mathrm{im}(f)|$. Moreover, by (a), the equivalence class of an element $g$ in $G$ is equal to $g\ker(f)$. Therefore $|G| = |\mathrm{im}(f)| \cdot |\ker(f)|$.

(c) Now let $h \in \mathrm{im}(f)$. The probability that a random element $a \in G$ is mapped to $h$ via $f$ is $|\{a \in G \mid f(a) = h\}|/|G|$. Now (a) and (b) imply the rest. □

**8.4 Corollary** *Let $n \in \mathbb{N}$ and let $m \in \mathbb{N}$ be even such that*

$$a^{m/2} \not\equiv 1 \mod n \quad \textit{for at least one } a \in \mathbb{Z} \textit{ with } \gcd(a, n) = 1.$$

*Then, among all the elements $a \in \{1, \ldots, n\}$ with $\gcd(a, n) = 1$, at least 50% have the property $a^{m/2} \not\equiv 1 \mod n$.*

**Proof** Note that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group under multiplication (called the *unit group* of the ring $\mathbb{Z}/n\mathbb{Z}$). Consider the function

$$f\colon (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times\,, \quad a+n\mathbb{Z} \mapsto (a+n\mathbb{Z})^{m/2} = a^{m/2}+n\mathbb{Z}\,.$$

It is easy to check that $f$ is a group homomorphism:

$$\begin{aligned} f((a+n\mathbb{Z})(b+n\mathbb{Z})) &= f(ab+n\mathbb{Z}) = (ab)^{m/2}+n\mathbb{Z} = a^{m/2}b^{m/2}+n\mathbb{Z} \\ &= (a^{m/2}+n\mathbb{Z})(b^{m/2}+n\mathbb{Z}) = f(a+n\mathbb{Z})f(b+n\mathbb{Z})\,, \end{aligned}$$

for $a+n\mathbb{Z}, b+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. By our hypothesis we have $|\mathrm{im}(f)| \geqslant 2$. Now, Lemma 8.3(c), the probability for an element $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ that $a^{m/2} \equiv 1 \mod n$ is equal to $1/|\mathrm{im}(f)| \leqslant 1/2$. □

**8.5 Definition** Let $G$ be a group.

(a) A non-empty subset $H$ of $G$ is called a *subgroup* of $G$ (notation: $H \leqslant G$) if for any two elements $h_1, h_2 \in H$ also $h_1h_2 \in H$, and for every element $h \in H$ also $h^{-1} \in H$.

(b) For any element $g$ we set $\langle g\rangle := \{g^k \mid k \in \mathbb{Z}\}$. This is a subgroup of $G$ and it is called the subgroup generated by $g$.

(c) Let $g \in G$. The smallest $n \in \mathbb{N}$ (if it exists) such that $g^n = 1$ is called the *order* of $g$. It is denoted by $\mathrm{ord}(g)$. If $g^n \neq 1$ for all $n \in \mathbb{N}$ then we set $\mathrm{ord}(g) := \infty$.

(d) $G$ is called a *cyclic* group if there exists an element $g \in G$ such that $G = \langle g\rangle$. In this case the element $g$ is called a *generator* of $G$.

**8.6 Remark** Let $G$ be a group.

(a) If $g \in G$ and $\mathrm{ord}(g) = n \in \mathbb{N}$ then $1 = g^0, g^1, g^2, \ldots, g^{n-1}$ are $n$ distinct elements. In fact, if $g^i = g^j$ for some $0 \leqslant i < j \leqslant n-1$ then $1 = g^{j-i}$, a contradiction. Moreover, for $k, l \in \mathbb{Z}$ one has:

$$g^k = g^l \iff g^{k-l} = 1 \iff k \equiv l \mod n\,.$$

In fact, the first equivalence comes from multiplying the first equation by $g^{-l}$ (or in backwards direction by $g^l$). To see the second equivalence, write $k-l = qn+r$ with $q \in \mathbb{Z}$ and $r \in \{0, \ldots, n-1\}$. Then $g^{k-l} = g^{qn+r} = (g^n)^q g^r = g^r$. Now, by the first statement, $g^r = 1$ if and only if $r = 0$.

(b) If $G$ is finite and $H \leqslant G$ then $|H|$ divides $|G|$ (Lagrange's Theorem). In fact, the relation

$$g_1 \sim g_2 : \iff \exists h \in H \colon g_1 h = g_2$$

is an equivalence relation on $G$. Moreover, the equivalence class of $g$ is given by $gH$. The latter is in bijection with $H$ under $H \to gH$, $h \mapsto gh$. Therefore, each equivalence class has size $|H|$ and their disjoint union is $G$. If there are $n$ equivalence classes, then $|G| = n \cdot |H|$.

(c) For any $g \in G$, the set $\langle g \rangle$ is a subgroup of $G$ and $\operatorname{ord}(g) = |\langle g \rangle|$ by Part (a). In particular, if $G$ is finite then $\operatorname{ord}(g)$ divides $|G|$.

(d) Let $g \in G$ and suppose $\operatorname{ord}(g) = n \in \mathbb{N}$. For any $k \in \mathbb{Z}$ one has $\langle g^k \rangle \leqslant \langle g \rangle$. Therefore, $\operatorname{ord}(g^k) \mid \operatorname{ord}(g)$. Moreover, one has

$$\begin{aligned} \langle g^k \rangle = \langle g \rangle &\iff \exists l \in \mathbb{Z} \colon g^{kl} = g \overset{\text{(a)}}{\iff} \exists l \in \mathbb{Z} \colon kl \equiv 1 \mod n \\ &\iff k + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \gcd(k, n) = 1 \,. \end{aligned}$$

Therefore, if $G = \langle g \rangle$ with $\operatorname{ord}(g) = n$ then $G$ has exactly $\phi(n)$ generators (i.e., elements of order $n$), namely $g^a$, where $a \in \{1, \ldots, n\}$ with $\gcd(a, n) = 1$.

**8.7 Lemma** *Let $G$ be a finite group of order $n$ and assume that for every $d \mid n$ one has*

$$|\{g \in G \mid g^d = 1\}| \leqslant d \,.$$

*Then $G$ is cyclic.*

**Proof** For $d \mid n$ we set

$$X_d := \{g \in G \mid g^d = 1\} \quad \text{and} \quad Y_d := \{g \in G \mid \operatorname{ord}(g) = d\} \,.$$

Obviously, $G$ equals the disjoint union $\bigcup_{d|n} Y_d$ and $Y_d \subseteq X_d$.

We show next that $|Y_d|$ is either 0 or $\phi(d)$. In fact, assume that $Y_d \neq \emptyset$ and let $x \in Y_d$. Then $\langle x \rangle \subseteq X_d$ and we obtain $d = |\langle x \rangle| \leqslant |X_d| \leqslant d$ by our hypothesis. This implies $X_d = \langle x \rangle$ and, since $Y_d \subseteq X_d$, also that $Y_d$ is the set of generators of $\langle x \rangle$. Note that there are precisely $\phi(d)$ generators, by Remark 8.6(d), so that $|Y_d| = \phi(d)$. This proves that $|Y_d|$ either 0 or $\phi(d)$.

Assume that $|Y_n| = 0$. Then we obtain the contradiction

$$n = |G| = \sum_{d|n} |Y_d| < \sum_{d|n} \phi(d) \overset{3.21}{=} n \,.$$

Therefore $Y_n \neq \emptyset$ and $G$ has an element $g$ of order $n$. Thus $G = \langle g \rangle$ and $G$ is cyclic. □

**8.8 Remark (Division with remainder in the polynomial ring)** Let $F$ be a field.

(a) Let $f(X), g(X) \in F[X]$. We write $f(X) \mid g(X)$ if $f(X)$ divides $g(X)$, i.e., if there exists $q(X) \in F[X]$ such that $g(X) = f(X)q(X)$. Note that if $0 \neq \alpha \in F$ then $f(X) \mid g(X)$ if and only if $\alpha f(X) \mid g(X)$ and if and only if $f(X) \mid \alpha g(X)$. Thus, when considering divisibility properties we may freely multiply polynomials with non-zero constants.

(b) For two polynomials $f(X), g(X) \in F[X]$ with $f(X) \neq 0$ we can divide $g(X)$ by $f(X)$ with remainder and obtain polynimials $q(X), r(X) \in F[X]$ with

$$g(X) = q(X)f(X) + r(X) \text{ and } \deg(r) < \deg(g)\,.$$

Here we have the convention that the zero polynomial has degree $-\infty$. As for integers, we can show that $q(X)$ and $r(X)$ are uniquely determined. We define the *greatest common divisor* of $f(X)$ and $g(X)$ as the polynomial $d(X) \in F[X]$ of highest possible degree which is *monic* (i.e., has leading coefficient 1) and divides both $f(X)$ and $g(X)$. It is denoted by $\gcd(f(X), g(X))$. Using division with remainder, one can apply the Euclidean algorithm as for integers to find $d(X) = \gcd(f(X), g(X))$ and again, it can be expressed as linear combination

$$d(X) = u(X)f(X) + v(X)g(X)$$

for polynomials $u(X), v(X) \in F[X]$.

For example, if $f(X) = X^3 - 3X^2 + X + 2$ and $g(X) = X^2 - 4$ in $\mathbb{Q}[X]$ we obtain

$$\begin{aligned} f(X) &= g(X)(X-3) + (5X-10) \\ g(X) &= (5X-10)(\frac{1}{5}X - \frac{2}{5})\,. \end{aligned}$$

This shows that $d(X) = \gcd(f(X), g(X)) = X - 2$ and we can express $d(X)$ as

$$X-2 = \frac{1}{5}(5X-10) = \frac{1}{5}\Big(f(X)-(X-3)g(X)\Big) = \frac{1}{5}\cdot f(X)+(-\frac{1}{5}X+\frac{3}{5})\cdot g(X)\,.$$

**8.9 Proposition** *Let $F$ be a field and let $0 \neq f \in F[X]$ have degree $n$. Then $f$ has at most $n$ zeroes in $F$.*

**Proof** We prove this by induction on $n$: If $n = 0$ then $f = a$ is constant for some $a \in F$ with $a \neq 0$. Thus, $f$ has no zeroes. If $n = 1$ then $f = aX + b$ with $a, b \in F$ and $a \neq 0$. In this case, $f$ has precisely one zero, namely $-ba^{-1}$. Now assume that $n > 1$ and the the proposition holds for all values smaller than $n$. If $f$ has no zero, we are done. If $f$ has a zero $a \in F$ we can divide $f$ by $X - a$ and obtain $f = q \cdot (X - a) + r$ with a constant polynomial $r$. Evaluating the equation at $a$ we obtain $r = 0$. Thus, $f = q \cdot (X - a)$ and $q$ is a polynomial of degree $n - 1$. By induction, $q$ has at most $n - 1$ zeroes. If $b \in F$ is a zero $f$ then $0 = f(b) = q(b)(X - b)$. Since $F$ is a field this implies that $b$ is a zero of $q$ or $b = a$. Thus, $f$ has at most $n$ zeroes. □

**8.10 Theorem** *Every finite subgroup of the unit group $F^\times = F \setminus \{0\}$ of a field $F$ is cyclic. In particular, $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group with $p-1$ elements.*

**Proof** Let $U \leqslant F^\times$ with $|U| = n$. According to Lemma 8.7 it suffices to show that $|\{u \in U \mid u^d = 1\}| \leqslant d$ for all $d \mid n$. But $\{u \in U \mid u^d = 1\}$ is contained in the set of zeroes of the polynomial $X^d - 1 \in F[X]$ of degree $d$. Now Proposition 8.9 finishes the proof. □

**8.11 Definition** Let $p$ be a prime number. An integer $a$ is called a *primitive root modulo $p$* if $a+p\mathbb{Z}$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. For example, 2 is a primitive root modulo 5: $2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1 \mod 5$, and therefore $2+5\mathbb{Z}$ generates the group $(\mathbb{Z}/5\mathbb{Z})^\times$ of order 4.

**8.12 Remark** It is an open famous conjecture (by E. Artin) if the number 2 is a primitive root for infinitely many primes.

**8.13 Corollary** *Let $p$ be a prime and let $m \in \mathbb{Z}$. Then*

$$a^m \equiv 1 \mod p \text{ for all } a \in \{1, \ldots, p-1\} \iff (p-1) \mid m\,.$$

**Proof** $\Rightarrow$: Let $r \in \{1, \ldots, p-1\}$ be a primitive root modulo $p$. Then $\operatorname{ord}(r + p\mathbb{Z}) = p - 1$ and by our hypothesis we have $r^m + p\mathbb{Z} = 1 + p\mathbb{Z}$. Now Remark 8.6(a) implies that $m \equiv 0 \mod p - 1$.

$\Leftarrow$: This follows from Fermat's Little Theorem. □

**8.14 Corollary** *Assume that $n = pq$ for two odd primes $p < q$ and assume that $m \in \mathbb{N}$ is even and has the property that*

$$a^m \equiv 1 \mod n \text{ for all } a \in \mathbb{Z} \text{ with } \gcd(a, n) = 1$$

*but*

$$a^{m/2} \not\equiv 1 \mod n \text{ for at least one } a \in \mathbb{Z} \text{ with } \gcd(a, n) = 1.$$

*Then, the group homomorphism*

$$\begin{aligned} f\colon (\mathbb{Z}/n\mathbb{Z})^\times &\to (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \\ a + n\mathbb{Z} &\mapsto (a^{m/2} + p\mathbb{Z}, a^{m/2} + q\mathbb{Z}) \end{aligned}$$

*is not trivial and one has $(p-1) \nmid \frac{m}{2}$ or $(q-1) \nmid \frac{m}{2}$. Moreover:*

*(i) If $(p-1) \mid \frac{m}{2}$ and $(q-1) \nmid \frac{m}{2}$ then* $\mathrm{im}(f) = \{(1 + p\mathbb{Z}, 1 + q\mathbb{Z}), (1 + p\mathbb{Z}, -1 + q\mathbb{Z})\}$.

*(ii) If $(p-1) \nmid \frac{m}{2}$ and $(q-1) \mid \frac{m}{2}$ then* $\mathrm{im}(f) = \{(1 + p\mathbb{Z}, 1 + q\mathbb{Z}), (-1 + p\mathbb{Z}, 1 + q\mathbb{Z})\}$.

*(iii) If $(p-1) \nmid \frac{m}{2}$ and $(q-1) \nmid \frac{m}{2}$ then* $\mathrm{im}(f)$ *consists of the 4 elements* $(\pm 1 + p\mathbb{Z}, \pm 1 + q\mathbb{Z})$.

**Proof** Clearly, $f$ is a group homomorphism. It is not trivial, since there exists some $a_0 + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})$ with $a_0^{m/2} + n\mathbb{Z} \neq 1 + n\mathbb{Z}$. This element corresponds under the bijective function in the Chinese Remainder theorem to the element $(a_0^{m/2} + p\mathbb{Z}, a_0^{m/2} + q\mathbb{Z})$. This implies that $a_0^{m/2} + p\mathbb{Z} \neq 1 + p\mathbb{Z}$ or $a_0^{m/2} + q\mathbb{Z} \neq 1 + q\mathbb{Z}$, or both. By Fermat's little Theorem this implies that $(p-1) \nmid \frac{m}{2}$ or $(q-1) \nmid \frac{m}{2}$. Now the result follows from Corollary 8.13, the fact that $X^2 = 1$ has only the solutions $x = \pm 1$ in any field (e.g. in $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$). □

## Exercises for Section 8

**1.** Show that if $f\colon G \to H$ is a group homomorphism then $f(1_G) = 1_H$ and $f(g^{-1}) = f(g)^{-1}$ for all $g \in G$.

**2.** Show that for every ring $R$, the set $R^\times$ of invertible elements forms a group under multiplication.

**3.** Let $G$ and $G'$ be groups and let $f\colon G \to G'$ be a group homomorphism.

(a) Show that if $H \leqslant G$ and $H' \leqslant G'$, then $f(H) := \{f(h) \mid h \in H\} \leqslant G'$ and $f^{-1}(H') := \{g \in G \mid f(g) \in H'\} \leqslant G$.

(b) Show that $\ker(f) \leqslant G$ and $\operatorname{im}(f) \leqslant G'$.

**4.** Assume that $G = \langle x \rangle$ and that $\operatorname{ord}(x) = n \in \mathbb{N}$. Moreover, let $k \in \mathbb{Z}$ and set $y := x^k$. Show that $\operatorname{ord}(y) = n/\gcd(n,k)$

**5.** Compute the greatest common divisor of the polynomials $\bar{2}X^5 + \bar{3}X^4 + X^2 + \bar{4}$ and $X^4 + \bar{2}X^3 + X + \bar{3}$ in the polynomial ring $F[X]$ with $F = \mathbb{Z}/5\mathbb{Z}$, where the 'bar' means taking the class in $\mathbb{Z}/5\mathbb{Z}$ (e.g., $\bar{2} = 2 + 5\mathbb{Z}$).

**6.** (a) Find a generator of the group $G = (\mathbb{Z}/17\mathbb{Z})^\times$.

(b) Find all primitive roots modulo 13.

(c) Is the group $(\mathbb{Z}/16\mathbb{Z})^\times$ cyclic?

(d) Is the group $(\mathbb{Z}/27\mathbb{Z})^\times$ cyclic?

# 9 Finite Fields

Throughout this section $F$ denotes a field.

**9.1 Definition** Let $f(X) \in F[X]$. For two polynomials $g(X)$ and $h(X)$ in $F[X]$ we define

$$g(X) \equiv h(X) \mod f(X): \iff f(X) \mid g(X) - h(X)\,.$$

This defines an equivalence relation on $F[X]$. The class of $g(X)$ is called the *residue class of* $g(X)$ *modulo* $f(X)$ and is equal to $g(X)+f(X)F[X]$. We will often abbreviate $f(X)F[X]$ by $(f(X))$. The set of equivalence classes will be denoted by $F[X]/(f(X))$. The set $F[X]/(f(X))$ is again a commutative ring with addition and multiplication defined by

$$(g(X) + (f(X))) + (h(X) + (f(X))) := (g(X) + h(X)) + (f(X))$$

and

$$(g(X) + (f(X))) \cdot (h(X) + (f(X))) := (g(X) \cdot h(X)) + (f(X))\,.$$

The 0-element is $0 + (f(X)) = f(X)F[X]$ and the identity element is $1 + (f(X))$.

**9.2 Proposition** *Let $f(X) \in F[X]$ with $\deg f(X) = n \geqslant 1$. Then the polynomials of degree $< n$ form a complete set of representatives of the congruence classes of $F[X]$ modulo $f(X)$.*

**Proof** Let $g(X) \in F[X]$ be arbitrary. Dividing $g(X)$ by $f(X)$ with remainder, we obtain $g(X) = q(X)f(X) + r(X)$ with $\deg r(X) < n$. Therefore, $g(X) \equiv r(X) \mod f(X)$ and the congruence class of $g(X)$ contains the polynomial $r(X)$ of degree $< n$.

Now assume that $r(X)$ and $s(X)$ are polynomials in $F[X]$ of degree $< n$ and that $r(X) \equiv s(X) \mod f(X)$. Then there exists $q(X) \in F(X)$ such that $r(X) - s(X) = q(X)f(X)$. But, if $q(X) \neq 0$ then $\deg q(X)f(X) \geqslant n$, while $\deg r(X) - s(X) < n$. This is impossible. Therefore, $q(X) = 0$ and $r(X) = s(X)$. □

**9.3 Definition** A polynomial $f(X) \in F[X]$ is called *irreducible* if $\deg f(X) \geqslant 1$ and if $f(X)$ cannot be written as a product $f(X) = a(X)b(X)$ with polynomials $a(X), b(X) \in F[X]$ of degree $\geqslant 1$.

**9.4 Remark** (a) If $f(X)$ has degree 1 then $f(X)$ is irreducible.

(b) If $f(X)$ has degree 2 or 3 then we have the following irreducibility criterion:

$$f(X) \text{ is irreducible if and only if } f(X) \text{ has not root in } F.$$

In fact, every decomposition of $f(X)$ into a product with non-constant factors must involve a factor of degree 1 and every polynomial of degree 1 has a root.

(c) If $f(X)$ is irreducible then also $\alpha f(X)$ is irreducible for every $0 \neq \alpha \in F$.

**9.5 Theorem** *Let $f(X) \in F[X]$ be irreducible. Then $F[X]/(f(X))$ is a field. In particular, if $F = \mathbb{Z}/p\mathbb{Z}$ for a prime $p$ and $f(X)$ has degree $n$ then, by Proposition 9.2, $F[X]/(f(X))$ is a field with $p^n$ elements.*

**Proof** Let $g(X) \in F[X]$ with $g(X) + (f(X)) \neq 0 + (f(X))$, i.e., with $f(X) \nmid g(X)$. We need to show that $g(X) + (f(X))$ has an inverse in $F[X]/(f(X))$. For this it suffices to show that there exists a polynomial $u(X) \in F[X]$ such that $g(X)u(X) \equiv 1 \mod f(X)$. But, since $f(X)$ is irreducible and $g(X)$ is not a multiple of $f(X)$, every common divisor of $f(X)$ and $g(X)$ must have degree 0. This implies that the constant polynomial 1 is a greatest common divisor of $f(X)$ and $g(X)$. By Remark 8.8 we find polynomials $u(X)$ and $v(X)$ in $F[X]$ such that $1 = u(X)g(X) + v(X)f(X)$. This implies that $u(X)g(X) \equiv 1 \mod f(X)$ and that $g(X) + (f(X))$ is invertible in $F[X]/(f(X))$. □

**9.6 Example** Let $F = \mathbb{Z}/3\mathbb{Z}$. We write the elements in $F$ as $\bar{0}$, $\bar{1}$ and $\bar{2}$. Let $f(X) = X^3 + \bar{2}X + \bar{2} \in F[X]$. We have $f(\bar{0}) = \bar{2}$, $f(\bar{1}) = \bar{2}$ and $f(\bar{2}) = \bar{2}$. Since $f(X)$ has degree 3 and no roots in $F$, we know from Remark 9.4(b) that $f(X)$ is irreducible in $F[X]$. The resulting field $E = F[X]/(f(X))$ has 27 elements. The elements of $E$ can be represented by the polynomials $aX^2 + bX + c$ with $a, b, c \in F$. If we want to find out what the product of the two elements represented by $X^2 + \bar{2}$ and $X^2 + \bar{1}$ is, we can proceed as follows. First multiply as usual in $F[X]$:

$$(X^2 + \bar{2})(X^2 + \bar{1}) = X^4 + \bar{2}\,.$$

Then divide $X^4 + \bar{2}$ by $f(X)$ with remainder. The remainder $r(X)$ is in the same class as $X^4 + \bar{2}$:

$$X^4 + \bar{2} = X \cdot (\underbrace{X^3 + \bar{2}X + \bar{2}X}_{f(X)}) + \underbrace{X^2 + X + \bar{2}}_{r(X)} .$$

Thus,

$$(X^2 + \bar{2} + (f(X))) \cdot (X^2 + \bar{1} + (f(X))) = X^2 + X + \bar{2} + (f(X)) .$$

**9.7 Remark** (a) One can show that for every prime $p$ and every $n \in \mathbb{N}$ there exists an irreducible polynomial $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ of degree $n$. Therefore, there exists a finite field with $p^n$ elements for every prime $p$ and every $n \in \mathbb{N}$.

(b) It is not difficult to show that every finite field $F$ must have $p^n$ elements for some prime $p$ and some $n \in \mathbb{N}$. This is done by showing that $F$ must contain a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$, namely the set $\{0, 1, 1+1, 1+1+1, \ldots\}$. Then one verifies that the field $F$ is a vector space over this subfield using the multiplication in $F$ as scalar multiplication. Finally, if $n$ is the dimension of $F$ over this subfield then $F$ has $p^n$ elements.

(c) It can also be shown that any two finite fields $F$ and $F'$ with the same number of elements are isomorphic, i.e., there exists a ring isomorphism $f\colon F \to F'$.

(d) Recall from Theorem 8.10 that the multiplicative group $F^\times = F \setminus \{0\}$ of a finite field $F$ with $q$ elements is cyclic of order $q - 1$.

## Exercises for Section 9

**1.** Determine all irreducible polynomials in $(\mathbb{Z}/2\mathbb{Z})[X]$ of degree 2,3, and 4.

**2.** Is $X^4 + \bar{3}X^2 - \bar{2}X + \bar{1}$ irreducible in $(\mathbb{Z}/5\mathbb{Z})[X]$?

**3.** Let $F = \mathbb{Z}/3\mathbb{Z}$. Compute an inverse of the polynomial $X^2 + X + \bar{1}$ in $F[X]$ modulo the polynomial $X^3 + X^2 + X + \bar{2}$.

**4.** Let $F = \mathbb{Z}/3\mathbb{Z}$.

(a) Show that $f(X) = X^2 + X + \bar{2}$ is irreducible in $F[X]$.

(b) Consider the multiplicative group $G$ of units of the field $F[X]/(f(X))$. What is the order of $G$? Find an element that generates $G$. How many generators does $G$ have?

# 10 Discrete Logarithms

**10.1 Definition** Let $G$ be a finite group and let $g \in G$. If $x \in \langle g \rangle$ then any integer $k \in \mathbb{Z}$ such that $x = g^k$ is called a *discrete logarithm* of $x$ to the base $g$. If $\mathrm{ord}(g) = n$ and $k$ is a discrete logarithm of $x$ to the base $g$ then the set of all discrete logarithms of $x$ to the base $g$ is equal to $k + n\mathbb{Z}$.

The *discrete logarithm problem*: Given $x \in \langle g \rangle$, find a discrete logarithm of $x$ to the base $g$. Of course, one cannot expect to find a general algorithm that solves the discrete logarithm problem for all $G$ and $g$. But, depending on $G$, e.g., unit groups of finite fields or of finite rings one can try more specific things.

**10.2 Definition** Let $G$ be a finite group and let $g \in G$. We say that the *Diffie-Hellman assumption* holds for $G$ and $g$ if the following is true: Given $g$ and two powers $g^a$ and $g^b$ (without knowing $a$ and $b$) it is unfeasible to compute $g^{ab}$. This is related to the discrete logarithm problem: If one can solve the discrete logarithm problem then the Diffie-Hellman assumption does not hold. It is conjectured that the converse is also true.

**10.3 Remark (Diffie-Hellman key exchange system)** Assume we have a finite group $G$ and an element $g \in G$ of order $n$, both publicly known, satisfying the Diffie-Hellman assumption. Assume that two parties $A$ and $B$ want to use a private key crypto system (as for example the $k$-graph matrix crypto system) and assume that one has a publicly known translation function $t\colon \langle g \rangle \to \mathcal{K}$ to the set of all possible keys. In order to agree on a key, $A$ and $B$ can do the following: $A$ chooses a random number $a$ between 0 and $n-1$ and keeps it secret. Similarly, $B$ chooses a random number $b$ between 0 and $n-1$ and keeps it secret. $A$ computes $g^a$ and publishes it. Similarly, $B$ computes $g^b$ and publishes it (and so does everybody else participating in the network). Then both are able to compute $g^{ab} = (g^a)^b = (g^b)^a$ (since $A$ knows $a$ and $B$ knows $b$). But a third party cannot compute $g^{ab}$ from the knowledge of $g^a$ and $g^b$. Now, $A$ and $B$ use the key $t(g^{ab})$ for their communication. This is safer than transmitting the key itself.

**10.4 Example** Assume one uses single letter shift encryption and a 26-letter alphabet:

$$C = P + (k + 26\mathbb{Z}),$$

where $k \in \{0, 1, \ldots, 25\}$ is the key (previously called $b$). Suppose a field with at least 26 units, say $\mathbb{F}_{53}$, and a generator of $\mathbb{F}_{53}^{\times}$, say 2, is chosen and is

publicly known. Alice chooses $a = 29$ and looks up Bob's entry $2^b = 12 \in \mathbb{F}_{53}$ (without knowing $b$). She computes $12^{29} = 21$ in $\mathbb{F}_{53}$. So, she uses the key $k = 21$ when communicating with Bob. Meanwhile, Alice publishes $2^{29} = 45 \in \mathbb{F}_{53}$ and Bob (who has chosen $b = 19$) computes $k = 45^{19} = 21 \in \mathbb{F}_{53}$ and uses the same key when communicating with Alice.

Of course in this simple example it would be easy to crack the system and also the Diffie-Hellman assumption does not hold for such a small order $n = 52$. The example was chosen for the sake of simplicity of calculation.

**10.5 Remark (Massey-Omura crypto system)** In this crypto system one works with a publicly known field $\mathbb{F}_q$ with $q$ elements. Plain text message units are labeled by certain elements in $P \in \mathbb{F}_q^\times$.

Every participant $A$ randomly chooses $e_A \in \{1, \ldots, q-1\}$ with $\gcd(e_A, q-1) = 1$ and computes $d_A \in \{1, \ldots, q-1\}$ with $e_A d_A \equiv 1 \mod q-1$. $A$ keeps $e_A$ and $d_A$ secret.

If $A$ wants to send a message $P$ to $B$ then this is done in 3 steps:

$$A \xrightarrow{P^{e_A}} B \xrightarrow{P^{e_A e_B}} A \xrightarrow{P^{e_A e_B d_A}} B\,.$$

Note that $P^{e_A e_B d_A} = P^{e_B}$. Therefore, $B$ can compute $P^{e_B d_B} = P$. One must use a good authentication system to prevent $C$ from sending back $P^{e_A e_C}$ to $A$ after the first step. No exchange of keys is necessary. It is essential that the discrete logarithm problem cannot be solved.

**10.6 Remark (El Gamal crypto system)** For this crypto system one works with a publicly known field $\mathbb{F}_q$ with $q$ elements and a publicly known generator $g$ of $\mathbb{F}_q^\times$. Plain text messages are labeled by certain elements $P \in \mathbb{F}_q^\times$. Every user $X$ chooses a number $a_X \in \{1, \ldots, q-2\}$, keeps it secret, computes $g^{a_X}$ and publishes it.

Person $A$ sends a message unit $P \in \mathbb{F}_q$ to person $B$ by choosing some integer $k$ and sending the pair $(g^k, g^{a_B k} P)$ of elements in $\mathbb{F}_q^\times$ to $B$. The first entry $g^k$ is called the *clue* and the part $g^{a_B k}$ of the second entry is called the *mask*. Now, $B$ computes $(g^k)^{a_B} = g^{a_B k}$ and and then computes $(g^k)^{q-1-a_B} \cdot g^{a_B k} P = P$.

Again, one doesn't need a key exchange. It is essential that the Diffie-Hellman assumption holds.

## Exercises for Section 10

For both exercises below we use the 31-letter alphabet A-Z (labeled by the numbers 0-25) together with the 'blank', 'period', ?, !, and 'apostrophe', labeled by 26-30.

**1.** You and your friend communicate using affine enciphering transformations $p \mapsto ap + b$, where $a, b \in \mathbb{F}_{31} = \mathbb{Z}/31\mathbb{Z}$. Consider the field $\mathbb{F}_{31^2} = \mathbb{F}_{961}$ realized as $F := \mathbb{F}_{31}[X]/(X^2+1)$. The key $(a, b)$ for the enciphering transformation is viewed as the class of $a + bX$ in $F$. You exchange keys using the Diffie-Hellman system with the group $F^\times$ and $g = 4 + X + (X^2 + 1) \in F^\times$. As your secret exponent you choose $a = 209$. Your friend sends you her $g^b = 1 + 19X + (X^2 + 1) \in F$.

(a) Find the element in $F^\times$ that describes your common enciphering key.

(b) What is the element $g^a \in F^\times$ you send your friend, so she also can compute the enciphering.

(c) What is the key $(a, b)$ that both of you are using for the affine single letter crypto system?

(d) Read the message 'BUVCFIWOUJTZ!H." from your friend.

**2.** Let $p$ be the Fermat prime $p = 65537$, use the field $F = \mathbb{Z}/p\mathbb{Z}$ and let $g = 5 + p\mathbb{Z} \in F^\times$. You receive the message $(29095, 23846)$, which your friend composed using the ElGamal cryptosystem in $F^\times$, using your public key $g^a$. Your secret exponent $a$ is 13908. For message units you use the alphabet from the top of this page and trigraphs. You translate them into elements in $F$ by $AAA = 0$, $AAB = 1, \ldots, ''' = 29790 = 31^3 - 1$, similar to Example 4.4. Decipher the message.

# 11 The Knapsack Crypto System

**11.1 Definition** (a) Let $k \in \mathbb{N}_0$, $v_0, v_1, \ldots, v_{k-1} \in \mathbb{N}$ and let $V \in \mathbb{N}$. The *knapsack problem* is to determine if it is possible to find a subset $I \subseteq \{0, \ldots, k-1\}$ such that $\sum_{i \in I} v_i = V$, and if possible to find such an $I$. $V$ is interpreted as the volume of the knapsack and $v_0, \ldots, v_{k-1}$ are the volumes of items one might pack in to fill the knapsack completely. Note that the existence of such a subset $I$ is equivalent to the existence of a base 2 number $(\varepsilon_{k-1}, \ldots, \varepsilon_1, \varepsilon_0)_2$ with digits $\varepsilon_i \in \{0, 1\}$ such that $V = \sum_{i=0}^{k-1} \varepsilon_i v_i$.

(b) A sequence $v_0, \ldots, v_{k-1}$ as above is called *superincreasing* if $v_i > v_0 + v_1 + \cdots + v_{i-1}$ for all $i = 1, \ldots, k-1$.

**11.2 Example** (a) Let $(v_0, \ldots, v_4) = (3, 4, 1, 12, 9)$ and let $V = 17$. Then one has the solutions $(1, 0, 1, 1, 1)$ and $(0, 1, 1, 1, 0)$ to the corresponding knapsack problem. But there is no solution if $V = 2$, $V = 6$ or $V = 23$.

(b) The sequence $(1, 3, 6, 12, 25)$ is superincreasing. For $V = 17$ there is no solution. For $V = 19$ there is the unique solution $(1, 0, 1, 1, 0)$.

**11.3 Proposition** *Let $(v_0, \ldots, v_{k-1})$ be superincreasing and let $V \in \mathbb{N}$. then there exists at most one solution to the knapsack problem. The following algorithm decides if there is a solution and finds the solution if it exists:*

(0) *Start with $I := \emptyset$.*

(1) *Find the largest index $i \in \{0, \ldots, k-1\}$ such that $v_i \leqslant V$ and include $i$ into $I$. Then go to* (2)*. If there is no such $i$ then stop.*

(2) *Redefine $k$ as $i$, $V$ as $V - v_i$ and go back to* (1)*.*

*If at the end one has $V = \sum_{i \in I} v_i$, then $I$ is the only solution. If $V \neq \sum_{i \in I} v_i$ then there is no solution.*

**Proof** Clear with some thinking. The only chance to fill the knapsack completely, is to take the largest $v_i$ which fits into it and then proceed with the remaining volume and $v_0, \ldots, v_{i-1}$ to fill the remaining volume. □

**11.4 Remark (Knapsack crypto system)** It is conjectured that the general knapsack problem cannot be solved in polynomial time in $k$, $\log V$ and $\log v_i$, although for special classes, like superincreasing sequences, the problem can be solved very quickly as the previous proposition shows. This motivated the knapsack crypto system:

Assume that message units are labeled by base 2 numbers $(\varepsilon_{k-1}, \ldots, \varepsilon_1, \varepsilon_0)_2$ of length $k$. Every participant $X$ chooses a superincreasing sequence $(v_0, \ldots, v_{k-1})$ of length $k$, a number $m \in \mathbb{N}$ with $m > v_0 + \cdots + v_{k-1}$, a number $a \in \{1, \ldots, m-1\}$ with $\gcd(a, m) = 1$, and then determines $b \in \{1, \ldots, m-1\}$ with $ab \equiv 1 \mod m$. Next, $X$ computes $w_0, \ldots, w_{k-1} \in \{1, \ldots, m-1\}$ such that $w_i \equiv av_i \mod m$ and publishes the sequence $w_0, \ldots, w_{k-1}$. The numbers $v_0, \ldots, v_{k-1}, m, a, b$ are kept secret.

If $A$ wants to send a message unit $P = (\varepsilon_{k-1}, \ldots, \varepsilon_1, \varepsilon_0)_2$ to $X$, she computes $C := \sum_{i=0}^{k-1} \varepsilon_i w_i$ and sends it to $X$. Since the knapsack problem is difficult to solve, knowledge of $C$ and $(w_0, \ldots, w_{k-1})$ is not enough to compute $(\varepsilon_{k-1}, \ldots, \varepsilon_1, \varepsilon_0)$. But $X$ can compute $V \in \{0, \ldots, m-1\}$ such that $V \equiv bC \mod m$. Then

$$V \equiv bC = \sum_{i=0}^{k-1} b\varepsilon_i w_i \equiv \sum_{i=0}^{k-1} b\varepsilon_i a v_i \equiv \sum_{i=0}^{k-1} \varepsilon_i v_i \mod m\,.$$

Since the first and last expression in this equation are both contained in $\{1, \ldots, m-1\}$ one has

$$V = \sum_{i=0}^{k-1} \varepsilon_i v_i\,,$$

and since $(v_0, \ldots, v_{k-1})$ is superincreasing, $X$ can easily find $(\varepsilon_{k-1}, \ldots, \varepsilon_1, \varepsilon_0)_2$ from $V$ and $(v_0, \ldots, v_{k-1})$.

**11.5 Example** Suppose that plain text message units are single letters $A-Z$, labeled by $(00000)_2 = 0$ through $(11001)_2 = 25$ (so $k = 5$). Assume that $B$ chooses the sequence $(v_i) = (2, 3, 7, 15, 31)$, $m = 61$, and $a = 17$. Then $b = 18$ and $B$ publishes $(w_i) = (34, 51, 58, 11, 39)$. If $A$ wants to send the message 'WHY' to $B$ she uses the base 2 numbers $(10110)_2 = 22$, $(00111)_2 = 7$, $(11000)_2 = 24$, computes the integers $39 + 58 + 51 = 148$, $58 + 51 + 34 = 143$, $39 + 11 = 50$ and sends $148, 143, 50$ to $B$. Because the sequence $(34, 51, 58, 11, 39)$ is not superincreasing, it is difficult for an interceptor to reconstruct how the knapsack volumes 148, 143 and 50 were filled by small item volumes from this sequence.

Now, $B$ multiplies 148, 143, and 50 by 18, reduces mod 61 to obtain 41, 12, and 46. Then, $B$ solves the knapsack problem for $(2, 3, 7, 15, 31)$ and these volumes to obtain (10110), (00111) and (11000).

**11.6 Remark** In 1982, Shamir found a polynomial time algorithm to solve the knapsack problem $C = \varepsilon_0 w_0 + \cdots + \varepsilon_{k-1} w_{k-1}$ (with the notation from

Remark 11.4). This was based on the fact that $w_0, \ldots, w_{k-1}$ is not an arbitrary sequence, but a multiple of a superincreasing sequence (modulo $m$). This led to modifications of the original knapsack crypto system which are still safe (see [K] pp. 114–115).

## Exercises for Section 11

**1.** Assume you use the knapsack cryptosystem and that you have chosen $(v_0, \ldots, v_4) = (3, 4, 10, 19, 40)$, $m = 100$, and $a = 19$.

(a) What do you publish?

(b) Assume that another person wants to send the message "YESTERDAY" to you, using 5 digit base-2 numbers to label the letters A-Z. What does that person send?

(c) You get the message $(166, 227, 227, 133)$. What does it mean?

# 12 Pseudoprimes

Recall that Fermat's Little Theorem says that if $p$ is a prime and $a \in \mathbb{Z}$ with $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$. We want to investigate if this can be used for a primality test.

**12.1 Definition** Let $1 < n \in \mathbb{N}$ be odd and composite (i.e., not a prime) and let $b \in \mathbb{Z}$ with $\gcd(b, n) = 1$. The number $n$ is called a *pseudoprime to the base* $b$ if

$$b^{n-1} \equiv 1 \mod n\,. \tag{12.1.a}$$

If (12.1.a) holds for $b$, then also for all $b' \in \mathbb{Z}$ with $b' \equiv b \mod n$.

**12.2 Example** The number $n = 7.13 = 91$ is a pseudoprime to the base $b = 3$: We compute $3^{90} = 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3^2$ using the repeated squaring method.

$$\begin{aligned}
3^2 &\equiv 9 \mod 91\\
3^4 &\equiv 81 \equiv -10 \mod 91\\
3^8 &\equiv 100 \equiv 9 \mod 91\\
3^{16} &\equiv 81 \equiv -10 \mod 91\\
3^{32} &\equiv 100 \equiv 9 \mod 91\\
3^{64} &\equiv 81 \equiv -10 \mod 91
\end{aligned}$$

This yields $3^{90} \cong (-10) \cdot (-10) \cdot 9 \cdot 9 = (-90) \cdot (-90) \cong 1 \cdot 1 = 1 \mod 91$.

However, $n = 91$ is not a pseudoprime to the base $b = 2$:

$$\begin{aligned}
2^2 &\equiv 4 \mod 91\\
2^4 &\equiv 16 \mod 91\\
2^8 &\equiv 74 \equiv -17 \mod 91\\
2^{16} &\equiv 16 \mod 91\\
2^{32} &\equiv -17 \mod 91\\
2^{64} &\equiv 16 \mod 91
\end{aligned}$$

and $2^{90} = 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^2 \equiv 16 \cdot 16 \cdot (-17) \cdot 4 \equiv 64 \mod 91$.

**12.3 Proposition** *Let* $1 < n \in \mathbb{N}$.

(a) *For every* $b \in \mathbb{Z}$ *with* $\gcd(b,n) = 1$ *one has:* $b^{n-1} \equiv 1 \mod n$ *if, and only if, the order of* $b + n\mathbb{Z}$ *in the group* $(\mathbb{Z}/n\mathbb{Z})^\times$ *divides* $n - 1$.

(b) *The elements* $b + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ *such that* $n$ *is a pseudoprime to the base* $b$ *form a subgroup of* $(\mathbb{Z}/n\mathbb{Z})^\times$.

(c) *If (12.1.*a*) fails for one* $b \in \{1, \ldots, n-1\}$ *with* $\gcd(b,n) = 1$ *then it fails for at least* 50% *of all* $b \in \{1, \ldots, n-1\}$ *with* $\gcd(b,n) = 1$.

**Proof** (a) This is immediate from Remark 8.6.

(b) Clearly $1 + n\mathbb{Z}$ satisfies (12.1.a). Assume that $b_1, b_2 \in \mathbb{Z}$ are such that $b_1^{n-1} \equiv 1 \equiv b_2^{n-1} \mod n$. Multiplying these congruences yields $(b_1 b_2)^{n-1} \equiv 1 \mod n$. Finally, if $b \in \mathbb{Z}$ is such that $b + n\mathbb{Z}$ satisfies (12.1.a) and $a \in \mathbb{Z}$ with $ab \equiv 1 \mod n$ then $a^{n-1} \equiv a^{n-1}b^{n-1} = (ab)^{n-1} \equiv 1^{n-1} = 1 \mod n$.

(c) Let $G = (\mathbb{Z}/n\mathbb{Z})^\times$ and let $H$ be the subset of $G$ consisting of those $b + n\mathbb{Z}$ with $b^{n-1} \equiv 1 \mod n$. By Part (b), $H$ is a subgroup of $G$, and by Remark 8.6(b), we have $|G| = |H| \cdot k$ for some $k \in \mathbb{N}$. Since $H$ is not equal to $G$, we have $k \geqslant 2$. The statement follows now from $\frac{|G \smallsetminus H|}{|G|} = \frac{|G|-|H|}{|G|} = 1 - \frac{|H|}{|G|} = 1 - \frac{1}{k} \geqslant 1 - \frac{1}{2} = \frac{1}{2}$. □

**12.4 Remark** Let $1 < n \in \mathbb{N}$. By Proposition 12.3(c) we can conclude: If $n$ passes the test (12.1.a) for $k$ random elements $b \in \{1, \ldots, n-1\}$ with $\gcd(b,n) = 1$, then the chance that $n$ does not pass it for all such $b$ is $\leqslant \frac{1}{2^k}$.

**12.5 Definition** Let $1 < n \in \mathbb{N}$ be odd and composite. If $n$ is a pseudoprime to the base $b$ for all $b \in \{1, \ldots, n-1\}$ with $\gcd(b,n) = 1$ then $n$ is called a *Carmichael number*. At this point we don't know if Carmichael numbers exist.

We will write $\mathrm{ord}_G(g)$ for the order of a group element $g$ in a group $G$, if $G$ is not immediate from the context.

The next proposition gives a criterion that will help to find Carmichael numbers.

**12.6 Proposition** *Let* $1 < n \in \mathbb{N}$ *be odd.*

(a) *If* $p^2 \mid n$ *for some prime* $p$ *then* $n$ *is not a Carmichael number.*

(b) $n$ *is a Carmichael number if and only if* $n = p_1 \cdots p_r$ *with pairwise distinct primes* $p_1, \ldots, p_r$ *and* $r \geqslant 2$ *such that* $(p_i - 1) \mid (n-1)$ *for all* $i = 1, \ldots, r$.

**Proof** (a) Assume that $p^2 \mid n$. By Proposition 12.7 there exists $g \in \mathbb{Z}$ such that $g + p^2\mathbb{Z}$ is a generator of $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Write $n = p^a \cdot n'$ with $p \nmid n'$ and $2 \leqslant a \in \mathbb{N}$. By the Chinese Remainder Theorem, there exists $b \in \mathbb{Z}$ with $b \equiv g \mod p^a$ and $b \equiv 1 \mod n'$ (since $\gcd(p^a, n') = 1$). Next we show that $\gcd(b, n) = 1$. Assume that $b$ and $n$ have a common prime divisor $q$. Then either $q = p$ or $q$ divides $n'$. In the first case, $p$ divides $b$ and then also divides $g$ (which is impossible since $g + p^2\mathbb{Z} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$), and in the second case, $q$ divides $b$ and $n'$ (which is impossible because $b \equiv 1 \mod n'$). Therefore, $\gcd(b, n) = 1$. Next we show that $b^{n-1} \not\equiv 1 \mod n$. Assume that $b^{n-1} \equiv 1 \mod n$, which implies that $b^{n-1} \equiv 1 \mod p^2$. Since $b \equiv g \mod p^2$, we have $p(p-1) = \mathrm{ord}_{(\mathbb{Z}/p^2\mathbb{Z})^\times}(b + p^2\mathbb{Z}) \mid (n-1)$. This implies $p \mid (n-1)$ and $n \equiv 1 \mod p$ which is a contradiction to $p \mid n$. Therefore, we have shown that $b^{n-1} \not\equiv 1 \mod n$ and $\gcd(b, n) = 1$, which implies that $n$ cannot be a Carmichael number.

(b) First assume that $n$ is a Carmichael number. By Part (a) this implies that $n = p_1 \dots p_r$ with pairwise distinct primes $p_1, \dots, p_r$ and $r \geqslant 2$. Let $i \in \{1, \dots, r\}$, let $g \in \mathbb{Z}$ such that $g + p_i\mathbb{Z}$ generates $(\mathbb{Z}/p_i\mathbb{Z})^\times$, and write $n = p_i \cdot n'$. By the Chinese Remainder Theorem there exists $b \in \mathbb{Z}$ such that $b \equiv g \mod p_i$ and $b \equiv 1 \mod n'$ (since $\gcd(p_i, n') = 1$). Since $p_i \nmid b$ and $b \equiv 1 \mod n'$ we have $\gcd(b, n) = 1$. Since $n$ is a Carmichael number we obtain $b^{n-1} \equiv 1 \mod n$, which implies $b^{n-1} \equiv 1 \mod p_i$ and $p_i - 1 = \mathrm{ord}_{(\mathbb{Z}/p_i\mathbb{Z})^\times}(b + p_i\mathbb{Z}) \mid (n-1)$.

Next assume that $n = p_1 \cdots p_r$ with pairwise distinct primes $p_1, \dots, p_r$ and $r \geqslant 2$ such that $(p_i - 1) \mid (n-1)$ for all $i = 1, \dots, r$. Let $b \in \mathbb{Z}$ with $\gcd(b, n) = 1$. We will show that $b^{n-1} \equiv 1 \mod n$. For each $i = 1, \dots, r$ we have $\gcd(b, p_i) = 1$ and by Fermat's Little Theorem $b^{p_i - 1} \equiv 1 \mod p_i$. Since $(p_i - 1) \mid (n-1)$, we obtain $b^{n-1} \equiv 1 \mod p_i$ and $p_i \mid b^{n-1} - 1$. Thus, $n = p_1 \cdots p_r \mid b^{n-1} - 1$ and $b^{n-1} \equiv 1 \mod n$. □

**12.7 Proposition** *Let $p$ be an odd prime and let $a \in \mathbb{N}$. Then the group $(\mathbb{Z}/p^a\mathbb{Z})^\times$ is cyclic. More precisely, if $g \in \mathbb{Z}$ is a primitive root modulo $p$, then $g + p^a\mathbb{Z}$ or $(g + p) + p^a\mathbb{Z}$ generates $(\mathbb{Z}/p^a\mathbb{Z})$.*

**Proof** First note that with $g$ also $g + p$ is a primitive root modulo $p$.

Next we show that there exists $h \in \{g, g + p\}$ such that $h^{p-1} = 1 + h_1 p$ with $h_1 \in \mathbb{Z}$ and $p \nmid h_1$. Since $g^{p-1} \equiv 1 \mod p$, we can write $g^{p-1} = 1 + pg_1$

with $g_1 \in \mathbb{Z}$. If $p \nmid g_1$, then we can take $h = g$ and we are done. If $p \mid g_1$ then

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + \sum_{i=1}^{p-1} \binom{p-1}{i} g^{p-1-i} p^i = 1 + pg_1 + (p-1)g^{p-2}p + f_1 p^2 \\ &= 1 + p(g_1 - g^{p-2}) + f_2 p^2\end{aligned}$$

for some $f_1, f_2 \in \mathbb{Z}$. Now choose $h = g + p$ and $h_1 = g_1 - g^{p-2} + f_2 p$. Then $h_1 \equiv g^{p-2} \not\equiv 0 \mod p$.

Choose $h$ as in the previous paragraph and set $k := \operatorname{ord}_{(\mathbb{Z}/p^a\mathbb{Z})^\times}(h + p^a\mathbb{Z})$. Since $|(\mathbb{Z}/p^a\mathbb{Z})^\times| = \phi(p^a) = p^{a-1}(p-1)$, we have $k \mid p^{a-1}(p-1)$. It suffices to show that $k = p^{a-1}(p-1)$. First we show that $(p-1) \mid k$. Since $h^k \equiv 1 \mod p^a$, we have $h^k \equiv 1 \mod p$, which implies $(p-1) = \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(h + p\mathbb{Z}) \mid (n-1)$.

Now it suffices to show that $p^{a-1} \mid k$. By induction on $j \in \mathbb{N}_0$ we first show that

$$(1 + h_1 p)^{p^j} \equiv 1 + h_1 p^{j+1} \mod p^{j+2}. \tag{12.7.a}$$

This is clear for $j = 0$. Moreover, for $j = 1$ we have

$$(1 + h_1 p)^p = 1 + p h_1 p + \sum_{j=2}^{p} \binom{p}{j} h_1^j p^j \equiv 1 + h_1 p^2 \mod p^3,$$

since $p \mid \binom{p}{j}$ for $j = 2, \ldots, p-1$ and $p \geqslant 3$. For the induction step assume that (12.7.a) holds for some $j \geqslant 1$. Then there exists $f \in \mathbb{Z}$ such that

$$\begin{aligned}(1 + h_1 p)^{p^{j+1}} &= \left((1 + h_1 p)^{p^j}\right)^p = \left(1 + h_1 p^{j+1} + f p^{j+2}\right)^p \\ &= \left(1 + p^{j+1}(h_1 + fp)\right)^p \\ &= 1 + p \cdot p^{j+1}(h_1 + fp) + \sum_{i=2}^{p} \binom{p}{i} p^{(j+1)i}(h_1 + fp)^i \\ &= 1 + h_1 p^{j+2} + f' p^{j+3},\end{aligned}$$

for some $f' \in \mathbb{Z}$, since $p \mid \binom{p}{i}$ and $(j+1)i + 1 \geqslant j + 3$ for $i = 2 \ldots, p-1$.

Since $k \mid p^{a-1}(p-1)$ and $(p-1) \mid k$, we already have $k = p^b(p-1)$ for some $b \in \{0, \ldots, a-1\}$, and it suffices to show that $b = a - 1$. Assume that $b < a - 1$. Then

$$1 \equiv (h^{p-1})^{p^b} \mod p^a \quad \text{and} \quad (h^{p-1})^{p^b} = (1 + h_1 p)^{p^b} \equiv 1 + h_1 p^{b+1} \mod p^{b+2}.$$

Since $b+2 \leqslant a$, we obtain $1 \equiv 1 + h_1 p^{b+1} \mod p^{b+2}$ and $h_1 p^{b+1} \equiv 0 \mod p^{b+2}$. But this implies $p \mid h_1$, a contradiction. Thus, $b = a-1$ and the proof is complete. □

**12.8 Proposition** *Every Carmichael number is divisible by at least three distinct primes.*

**Proof** Let $n$ be a Carmichael number. Then, by Proposition 12.6(b), we know that $n = p_1 \cdots p_r$ for pairwise distinct odd primes $p_1, \ldots, p_r$ and that $r \geqslant 2$. Therefore, we only have to rule out the case $r = 2$. So assume that $n = pq$ with primes $p < q$. Then Proposition 12.6(b) implies that $(p-1) \mid (n-1)$ and $(q-1) \mid (n-1)$. Thus,

$$0 \equiv n - 1 = p(q-1) + (p-1) \equiv p - 1 \mod q - 1$$

which implies $(q-1) \mid (p-1)$. But this contradicts $q - 1 > p - 1$, and the proof is complete. □

**12.9 Remark** Using Propositions 12.6 and 12.8, it is easy to actually find Carmichael numbers. For instance, $n = 561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. In fact, $2 \mid 560$, $10 \mid 560$, and $16 \mid 560$. It is the smallest Carmichael number. Alford, Granville, and Pomerance proved in 1992 that there are infinitely many Carmichael numbers. Unfortunately, the existence of infinitely many Carmichael numbers forbids using (12.1.a) as a primality test for $n$ in conjunction with Proposition 12.3(c). We continue with another attempt for a primality test, using a beautiful theory by Gauss about how to determine if a number $a \in \{1, \ldots, p-1\}$ is a a square modulo $p$, where $p$ is a prime.

**12.10 Definition** Let $p$ be an odd prime and let $a \in \mathbb{Z}$. One defines the *Legendre symbol* $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ by

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and there exists } b \in \mathbb{Z} \text{ with } a \equiv b^2 \mod p, \\ -1 & \text{if } p \nmid a \text{ and there exists no } b \in \mathbb{Z} \text{ with } a \equiv b^2 \mod p. \end{cases}$$

If $\left(\frac{a}{p}\right) = 1$, then $a$ is called *quadratic residue modulo p*.

The following properties of the Legendre symbol follow relatively easy from the definition, using that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic at some places.

**12.11 Proposition** *Let $p$ be a prime and let $a, b \in \mathbb{Z}$.*

(a) *If $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

(c) *If $p \nmid a$ then $\left(\frac{a^2}{p}\right) = 1$, in particular $\left(\frac{1}{p}\right) = 1$.*

(d) *If $p \nmid a$ then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$ (Euler's criterion).*

(e) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, *i.e., if $p \equiv 1 \mod 4$ then $\left(\frac{-1}{p}\right) = 1$, and if $p \equiv 3 \mod 4$ then $\left(\frac{-1}{p}\right) = -1$.*

(f) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, *i.e., $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \mod 8$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3 \mod 8$.*

The following theorem is due to Gauss and a highlight of his career. See [K, Proposition II.2.5] for a proof.

**12.12 Theorem (Gauss' quadratic reciprocity law)** *Let $p$ and $q$ be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \mod 4 \text{ and } q \equiv 3 \mod 4. \end{cases}$$

**12.13 Example** Consider the prime $p = 9283$. Is $a = 1002$ a square modulo $p$? We compute $\left(\frac{a}{p}\right)$ to find the answer:

$$\begin{aligned} \left(\frac{a}{p}\right) = \left(\frac{1002}{9283}\right) &= \left(\frac{2 \cdot 3 \cdot 167}{9283}\right) = \left(\frac{2}{9283}\right) \cdot \left(\frac{3}{9203}\right) \cdot \left(\frac{167}{9283}\right) \\ &= (-1) \cdot \left(\frac{9283}{3}\right) \cdot (-1) \cdot \left(\frac{9283}{167}\right) \cdot (-1) = -\left(\frac{1}{3}\right) \cdot \left(\frac{98}{167}\right) \\ &= -\left(\frac{7^2 \cdot 2}{167}\right) = -\left(\frac{7^2}{167}\right) \cdot \left(\frac{2}{167}\right) = -1 \cdot 1 = -1\,. \end{aligned}$$

Therefore, there exists no $x \in \mathbb{Z}$ such that $1002 \equiv x^2 \mod 9283$.

**12.14 Definition** Let $3 \leqslant n \in \mathbb{N}$ be an odd number with prime decomposition $n = p_1^{e_1} \cdots p_r^{e_r}$ and let $a \in \mathbb{Z}$. One defines the *Jacobi symbol* $\left(\frac{a}{n}\right) \in \{-1, 0, 1\}$ by

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r},$$

using the Legendre symbols $\left(\frac{a}{p_i}\right)$. Note that this extends the definition of the Legendre symbol: if $n = p$ is a prime then the Jacobi symbol $\left(\frac{a}{p}\right)$ is equal to the Legendre symbol $\left(\frac{a}{p}\right)$. However, the Jacobi symbol does not have the same interpretation as the Legendre symbol about squares modulo $n$.

**12.15 Proposition** *Let $3 \leqslant m, n \in \mathbb{N}$ be odd and $a, b \in \mathbb{Z}$.*

(a) *If $a \equiv b \mod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.*

(b) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$, *and if* $\gcd(m, n) = 1$ *then* $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{a}{n}\right)$.

(c) *If* $\gcd(a, n) = 1$ *then* $\left(\frac{a^2}{n}\right) = 1$, *in particular* $\left(\frac{1}{n}\right) = 1$.

(d) *If* $\gcd(a, n) = 1$ *then* $\left(\frac{a}{n}\right) \in \{-1, 1\}$ *and if* $\gcd(a, n) \neq 1$ *then* $\left(\frac{a}{n}\right) = 0$.

(e) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$, *i.e.,* $\left(\frac{-1}{n}\right) = 1$ *if* $n \equiv 1 \mod 4$ *and* $\left(\frac{-1}{n}\right) = -1$ *if* $n \equiv 3 \mod 4$.

(f) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$, *i.e.,* $\left(\frac{2}{n}\right) = 1$ *if* $n \equiv \pm 1 \mod 8$ *and* $\left(\frac{2}{n}\right) = -1$ *if* $n \equiv \pm 3 \mod 8$.

(g) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \cdot (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$, *i.e., if* $n \equiv 1 \mod 4$ *or* $m \equiv 1 \mod 4$ *then* $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$, *and if* $n \equiv 3 \mod 4$ *and* $m \equiv 3 \mod 4$ *then* $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

**Proof** All the statements can be reduced to the corresponding statements about the Legendre symbol in Proposition 12.11. □

**12.16 Remark** One can compute the Jacobi symbol $\left(\frac{m}{n}\right)$ very quickly even without knowing the prime decompositions of $m$ and $n$, by applying division with remainder and Proposition 12.15(g). This was not possible for the Legendre symbol, because there "denominator" had to be a prime and one

first had to decompose the "numerator" into primes. For instance:

$$\begin{aligned}\left(\frac{2724}{4003}\right) &= \left(\frac{4}{4003}\right)\cdot\left(\frac{681}{4003}\right) = 1\cdot\left(\frac{681}{4003}\right) = \left(\frac{4003}{681}\right)\\ &= \left(\frac{598}{681}\right) = \left(\frac{2\cdot 299}{681}\right) = \left(\frac{2}{681}\right)\cdot\left(\frac{299}{681}\right) = 1\cdot\left(\frac{299}{681}\right)\\ &= \left(\frac{681}{299}\right) = \left(\frac{183}{299}\right) = -\left(\frac{299}{183}\right) = -\left(\frac{116}{183}\right) = -\left(\frac{4}{183}\right)\left(\frac{29}{183}\right)\\ &= -\left(\frac{29}{183}\right) = -\left(\frac{183}{29}\right) = -\left(\frac{9}{29}\right) = -1\,.\end{aligned}$$

**12.17 Definition** Let $3 \leqslant n \in \mathbb{N}$ be odd and composite, and let $b \in \mathbb{Z}$ be such that $\gcd(b,n) = 1$. The number $n$ is called an *Euler pseudoprime to the base* $b$, if

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \mod n\,. \tag{12.17.a}$$

**12.18 Remark** Let $3 \leqslant n \in \mathbb{N}$ be odd.

(a) If $n = p$ is a prime then $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \mod n$ for all $b \in \mathbb{Z}$ with $\gcd(b,n) = 1$, by Euler's Criterion, see Proposition 12.11(d).

(b) Let $b \in \mathbb{Z}$ with $\gcd(b,n) = 1$. If $n$ is an Euler pseudoprime to the base $b$ then $n$ is a pseudoprime to the base $b$. In fact, squaring the congruence in (12.17.a) yields the congruence in (12.1.a).

(c) It is easy to see that the elements $b+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that (12.17.a) holds form a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. This implies that if (12.17.a) does not hold for all $b \in \{1,\dots,n-1\}$ with $\gcd(b,n) = 1$, then it holds for at most 50% of all $b \in \{1,\dots,n-1\}$ with $\gcd(b,n) = 1$.

(d) If (12.17.a) holds for all $b \in \mathbb{Z}$ with $\gcd(b,n) = 1$, then $n$ is a prime. In fact, assume that (12.17.a) holds for all $b \in \mathbb{Z}$ with $\gcd(b,n) = 1$ and that $n$ is not a prime. Then $n$ is a Carmichael number, by (b). By Proposition 12.6(b), we can write $n = p\cdot n'$ with $p \nmid n'$. Let $a \in \mathbb{Z}$ be a primitive root modulo $p$. Then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$, by Euler's criterion (Proposition 12.11(d)). Since $a + p\mathbb{Z}$ has order $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, we obtain $a^{(p-1)/2} \equiv -1 \mod p$ and $\left(\frac{a}{p}\right) = -1$. Now let $b \in \mathbb{Z}$ be such that $b \equiv a \mod p$ and $b \equiv 1 \mod n'$. Then $\gcd(b,n) = 1$ and $\left(\frac{b}{n}\right) = \left(\frac{b}{p}\right)\cdot\left(\frac{b}{n'}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{1}{n'}\right) = -1$. Since (12.17.a) holds for $b$, we obtain $b^{(n-1)/2} \equiv -1 \mod n$. This implies $b^{(n-1)/2} \equiv -1 \mod n'$. But, since $b \equiv 1 \mod n'$, we also have $b^{(n-1)/2} \equiv 1 \mod n'$. This is a contradiction.

(e) By (d), there does not exist the analogue of a Camichael number for Euler pseudoprimes. Using (c), one obtains a very good primality test, called the *Solovay-Strassen test*. This basic test can be refined to an even better test, the Miller-Rabin test, see [K, pp. 129–131].

## Exercises for Section 12

**1.** Find a Carmichael number different from 561

**2.** Find a generator of the group $(\mathbb{Z}/625\mathbb{Z})^{\times}$.

**3.** Consider the prime $p = 123121$ and the number $a := 85734$. Find out if the congruence $x^2 \equiv a \mod p$ has a solution.

**4.** Compute the Jacobi symbol $\left(\frac{2018}{4567}\right)$.

**5.** Find the next prime after the prime $p = 123121$ using the Solovay-Strassen test.

# References

[K] N. Koblitz: A course in number theory and cryptography. Second Edition. Springer, 1994.