Chapter I: Elementary number theory

30% HW 30% test 40% exam
in class test end of March/April.

1 Division in $\mathbb{Z}$. The Euclidean algorithm

Definition. Let $x, y \in \mathbb{Z}$. It is said that x **divides** y (or, y is **divisible by** x) if there exists $z \in \mathbb{Z}$ such that $y = xz$. Notation: $x \mid y$ or $y : x$.

Proposition 1.1. *For any integers x, y, z:*

1. $x \mid x$, $1 \mid x$, $(-x) \mid x$, $(-1) \mid x$;
2. *if $x \mid y$ and $y \mid z$ then $x \mid z$;*
3. *if $x \mid y$ and $x \mid z$ then $x \mid y + z$;*
4. *if $x \mid y$ then $x \mid yz$;*
5. *if $z \neq 0$ then $xz \mid yz$ if and only if $x \mid y$;*
6. $x \mid 0$; *if $0 \mid x$ then $x = 0$.*

Proof. 1. $x = x \cdot 1 = 1 \cdot x = (-x) \cdot (-1) = (-1) \cdot (-x)$.

2. If $y = xk$, $z = yl$ then $z = (xk)l = x(kl)$.
3. If $y = xk$, $z = xl$ then $y + z = x(k + l)$.
4. If $y = xk$ then $yz = (xk)z = x(kz)$.
5. If $y = xk$ then $yz = xzk$; conversely, if $yz = xzk$ then $(y - xk)z = 0$. Now $z \neq 0$ implies $y - xk = 0$, i.e., $y = xk$.
6. $0 = x \cdot 0$; if $x = 0 \cdot k$ then $x = 0$.

□

Problem 1.2. *Prove that $10x + y$ is divisible by 7 if and only if $x - 2y$ is divisible by 7*

Solution. Notice that $x - 2y = 21x - 2(10x + y)$ and $10x + y = 10(x - 2y) + 21y$ and use properties of divisibility. □

Exercise 1.1. *Prove the divisibility rule by 3: an integer is divisible by 3 iff the sum of its digits is divisible by 3.* for 11. $\overline{a_n a_{n-1} \cdots a_2 a_1} \vdots 11 \Leftrightarrow a_n - a_{n-1} + a_{n-2} - \cdots \vdots 11$.

Definition. If $x \mid y$ and $y \mid x$, the integers x and y are **associated.** It is equivalent to the fact that $y = \pm x$.

Proposition 1.3. *If a, a' and b, b' are two pairs of associated integers then $a \mid b$ iff $a' \mid b'$.*

Proof. Let $a \mid b$. Then $a' \mid a, a \mid b, b \mid b'$ imply $a' \mid b'$. □

Theorem 1.4 (Integral division). *Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then there exist unique integers q (the quotient) and r (the remainder) such that $a = bq + r$ and $0 \leq r \leq |b| - 1$.*

Proof. First consider the case $b > 0, a \geq 0$. Use induction on a. If $a < b$ then $a = b \cdot 0 + a$ and $0 \leq a \leq b - 1$. Consider the case $a \geq b$ and assume that the statement is valid for all pairs a', b with $a' < a$. Then $a' = a - b \geq 0$ and $a' = a - b < a$. By the induction assumption there are q', r' such that $a' = a - b = bq' + r'$ and $0 \leq r' \leq b - 1$. Then $a = b(q' + 1) + r'$.

The second case is $b > 0, a < 0$. Then $-a > 0$ and there are q', r' such that $-a = bq' + r'$, $0 \leq r' \leq b - 1$. Then $a = -bq' - r'$. If $r' = 0$ then $a = b(-q') + 0$ and we are done. If $1 \leq r' \leq b - 1$, then $a = b(-q') - r' = b(-q' - 1) + (b - r')$ and $1 \leq b - r' \leq b - 1$ as required.

Finally, suppose $b < 0$; then $-b > 0$ and one can find q', r' such that $a = (-b)q' + r'$ and $0 \leq r' \leq -b - 1$. Then $a = b(-q') + r'$ and $0 \leq r' \leq |b| - 1$.

It remains to prove the uniqueness. Let $a = bq + r = bq' + r'$; then $b(q - q') = (r' - r)$. If $q = q'$, then $r = r'$. If $q \neq q'$, then $|b| \leq |b| \cdot |q - q'| = |r - r'|$. On the other hand, $0 \leq r, r' \leq |b| - 1$, so $|r - r'| \leq |b| - 1$, a contradiction. □

Definition. Let $a_1, \ldots, a_n \in \mathbb{Z}$. An integer $d = \gcd(a_1, \ldots, a_n)$ is the **greatest common divisor** of $a_1, \ldots, a_n$ if

I. d is a common divisor of $a_1, \ldots, a_n$, i.e. $d \mid a_1, \ldots, d \mid a_n$;

II. if d' is another common divisor of $a_1, \ldots, a_n$, then $d' \mid d$.

Remarks. 1. The GCD (if exists) is unique up to associativity. Indeed, if d and d' are the two greatest common divisors of $a_1, \ldots, a_n$, then $d \mid d'$ and $d' \mid d$. Thus $\gcd(a_1, \ldots, a_n)$ denotes one of (two) GCD of a and b.

2. It is easy to see that $\gcd(0, a) = a$.

Proposition 1.5 (Bézout's identity). *The greatest common divisor of $a_1, \ldots, a_n \in \mathbb{Z}$ exists and is of the form $d = a_1u_1 + \cdots + a_nu_n$ for some integers $u_1, \ldots, u_n$.*

Proof. The case $a_1 = \cdots = a_n = 0$ is trivial. Assume that $a_1 \neq 0$. Consider S, the set of all positive integers of the form $a_1u_1 + \cdots + a_nu_n$ for all $u_1, \ldots, u_n \in \mathbb{Z}$ and its smallest element d (this set is nonempty: for example, it contains $|a_1|$). Then $d = a_1u_1 + \cdots + a_nu_n$ for some $u_1, \ldots, u_n \in \mathbb{Z}$ and $a_1 = dq + r = (a_1u_1 + \cdots + a_nu_n)q + r$ for some $q, r \in \mathbb{Z}, 0 \leq r < d$. Then $r = a_1(1 - u_1q) + a_2(-u_2q) + \cdots + a_n(-u_nq) \in S$ whence $0 \leq r < d$ implies $r = 0$ and d divides a_1. Similarly, d divides $a_2, \ldots, a_n$ and d is a common divisor of $a_1, \ldots, a_n$.

Let d' be another common divisor of $a_1, \ldots, a_n$. Then $d' \mid a_1u_1 + \cdots + a_nv_n = d$ as required. □

Proposition 1.6. *Let $x, y, z \in \mathbb{Z}$. Then*

1. $\gcd(x, y) = x$ *if and only if* $x \mid y$.
2. $\gcd(\gcd(x, y), z) = \gcd(x, y, z) = \gcd(x, \gcd(y, z))$.
3. $\gcd(zx, zy) = z \cdot \gcd(x, y)$.

Proof. 1. If $\gcd(x, y) = x$, then $x \mid y$ by definition. Conversely, let $x \mid y$, then x is a common divisor of x and y, and if d' is another common divisor of x, y, then, in particular, $d' \mid x$. Thus $\gcd(x, y) = x$.

2. Any common divisor of $\gcd(x, y)$ and z is a common divisor of x, y and z and vice versa, any common divisor of x, y and z is a common divisor of $\gcd(x, y)$ and z; the same is valid for any common divisor of x and $\gcd(y, z)$. Consequently, the "maximum" elements (that are divisible by any other element) in these sets are equal (up to associativity!).

3. If $z = 0$, the identity is trivial. Let $\gcd(x, y) = d$ then $d \mid x$, $d \mid y$ and $zd \mid zx$ and $zd \mid zy$, therefore $zd \mid \gcd(zx, zy)$. Conversely, it is clear that $z \mid zx$, $z \mid zy$, so $z \mid \gcd(zx, zy)$. If $\gcd(zx, zy) = zc$ for some c then $zc \mid zx$, $zc \mid zy$ and one gets $c \mid x$ and $c \mid y$ since $z \neq 0$. Therefore $c \mid \gcd(x, y) = d$, whence $zc \mid zd$, that is, $\gcd(zx, zy) \mid zd$.

□

Corollary 1.7. *Let $x, y \in \mathbb{Z}$ and $d = \gcd(x, y)$. Then $x = x'd, y = y'd$ and $\gcd(x', y') = 1$.*

Lemma 1.8. *Let $a, b, q, r \in \mathbb{Z}$. If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.* (subtractive Euclidean Algorithm)

Proof. Let $d = \gcd(a, b)$ and $d' = \gcd(b, r)$. One has $d \mid a$, $d \mid b$ whence $d \mid (a - bq) = r$ and $d \mid d'$. Furthermore, $d' \mid b$, $d' \mid r$, whence $d' \mid bq + r = a$, and $d' \mid d$. Thus d and d' are associated. □

The **Euclidean algorithm** for $a \geq b > 0$:

Step 1. Division with remainder on a, b gives $q_0, r_0 \geq 0$ such that $a = bq_0 + r_0, r_0 < b$.

Step 2. Division with remainder on b, r_0 gives $q_1, r_1 \geq 0$ such that $b = r_0q_1 + r_1, r_1 < r_0$.

⋮

Step n. Division with remainder on r_{n-1}, r_n gives $q_{n+1}, r_{n+1} \geq 0$ such that $r_{n-1} = r_nq_{n+1} + r_{n+1}, r_{n+1} < r_n$.

⋮

Since $b > r_0 > r_1 > \cdots$, the process must terminate with $r_m = 0$ for some m. Lemma 1.8 implies $\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_{m-1}, r_m) = r_{m-1}$, thus the greatest common divisors appears in the sequence $a, b, r_0, r_1 \ldots$ as the last non-zero remainder.

Problem 1.9. *Use the Euclidean algorithm to find the GCD and Bézout's coefficients for* $(46, 20)$.

Solution. $46 = 1 \cdot 20 + 26$

$26 = 1 \cdot 20 + 6$

$20 = 3 \cdot 6 + 2$

$6 = 3 \cdot 2 + 0$

Thus $2 = \gcd(46, 20)$. In order to find Bézout's coefficients, use the above equalities:

$$2 = 20 - 3 \cdot 6 = 20 - 3 \cdot (26 - 1 \cdot 20) = 4 \cdot 20 - 3 \cdot 26 = 4 \cdot 20 - 3 \cdot (46 - 1 \cdot 20) = 7 \cdot 20 - 3 \cdot 46.$$

□

Exercise 1.2. *Use the Euclidean algorithm to find the GCD and Bézout's coefficients for* $(75, 54)$.

Definition. The numbers a, b are **coprime** if $\gcd(a, b) = 1$.

Proposition 1.10. *Let* $a, b, c \in \mathbb{Z}$.

1. *If* a, b *are coprime, then* $\gcd(a, bc) = \gcd(a, c)$.
2. a, b *are coprime if and only if there are* $u_0, v_0 \in \mathbb{Z}$ *such that* $au_0 + bv_0 = 1$.
3. *If* $c \mid ab$ *and* a, c *are coprime then* $c \mid b$.
4. *If* $b_1 \mid a$, $b_2 \mid a$ *and* b_1, b_2 *are coprime, then* $b_1 b_2 \mid a$.

Proof. 1. By Proposition 1.6 one has $\gcd(a, bc) = \gcd(\gcd(a, ac), bc) = \gcd(a, \gcd(ac, bc)) = \gcd(a, c\gcd(a, b)) = \gcd(a, c)$.

2. If $\gcd(a, b) = 1$ then $1 = au_0 + bv_0$ for some $u_0, v_0 \in \mathbb{Z}$. Conversely, if $au_0 + bv_0 = 1$ and $d = \gcd(a, b)$, then $d \mid au_0 + bv_0 = 1$ and d is associated with 1.

3. There are $u_0, v_0 \in \mathbb{Z}$ such that $au_0 + cv_0 = 1$. Then $b = abu_0 + cbv_0$ is divisible by c.

4. Since $a = b_1 k$ is divisible by b_2 and b_1, b_2 are coprime, the previous property gives $k = b_2 \ell$, whence $a = b_1 k = b_1 b_2 \ell$.

□

Problem 1.11. *Find* $\gcd(7^{13} - 2, 7^{11} + 2)$.

Solution. By Lemma 1.8

$$\begin{aligned}\gcd(7^{13} - 2, 7^{11} + 2) &= \gcd(7^{13} - 2 - 7^2(7^{11} + 2), 7^{11} + 2) \\ &= \gcd(2 \cdot 7^2 + 2, 7^{11} + 2) = \gcd(7^2 + 1, 7^{11} + 2) \\ &= \gcd(7^2 + 1, 7^{11} + 2 - (7^2 + 1)(7^9 - 7^7 + 7^5 - 7^3 + 7)) \\ &= \gcd(7^2 + 1, -5) = 5.\end{aligned}$$

□

Exercise 1.3. *Find* $\gcd(2 \cdot 3^{15} + 1, 2 \cdot 3^7 - 5)$.

Exercise 1.4. *If* $\gcd(a, 4) = \gcd(b, 4) = 2$, *find* $\gcd(a + b, 4)$.

Exercise 1.5. *For every* $a \in \mathbb{Z}$ *find* $\gcd(5a^2 + 2, a - 3)$.

Problem 1.12. *Prove that* $\gcd(x^n - 1, x^m - 1) = x^{\gcd(m,n)} - 1$ *for any positive integers* x, m, n.

Solution. The *subtractive* Euclidean algorithm at each step changes the pair $(a, b), a \geq b$ for $(a - b, b)$. By repeating the same arguments as in the case of the Euclidean algorithm, one can easily see that it leads to the pair $(\gcd(a, b), 0)$.

Let $n \geq m$. Then $\gcd(x^n - 1, x^m - 1) = \gcd(x^m(x^{n-m} - 1), x^m - 1) = \gcd(x^{n-m} - 1, x^m - 1)$ and one can mimic the subtractive Euclidean algorithm to get

$$\gcd(x^n - 1, x^m - 1) = \gcd(x^{n-m} - 1, x^m - 1) = \cdots = \gcd(x^{\gcd(m,n)} - 1, x^0 - 1) = x^{\gcd(m,n)} - 1.$$

□

2 Linear Diophantine equations

Proposition 2.1. *Let $a, b, c \in \mathbb{Z}$, $a, b \neq 0$ and $d = \gcd(a, b)$.*

1. *The equation $ax + by = c$ has an integer solution if and only if $d \mid c$.*
2. *If (x_0, y_0) is one of the solutions of $ax + by = c$ and $a = da', b = db'$, then the other solutions are of the form $(x, y) = (x_0 + b't, y_0 - a't), t \in \mathbb{Z}$.*

Proof. 1. Note that $d \mid a$, $d \mid b$ thus $d \mid ax + by$ for all x, y. Therefore if d does not divide c, the equation has no solution.

Now let $c = dh$. Bézout's identity gives $au_0 + bv_0 = d$ for some $u_0, v_0 \in \mathbb{Z}$. Then $a(u_0h) + b(v_0h) = dh = c$, thus $(x_0, y_0) = (u_0h, v_0h)$ is a solution.

2. Let (x_1, y_1) be a solution to the equation $ax + by = c$. Then $a(x_1 - x_0) = b(y_0 - y_1)$ and $a'(x_1 - x_0) = b'(y_0 - y_1)$, where $a = a'd, b = b'd$ and $\gcd(a', b') = 1$ by Corollary 1.7. Hence, $b' \mid a'(x_1 - x_0)$ gives $b' \mid (x_1 - x_0)$ by Proposition 1.10. Denote $x_1 - x_0 = b't$, then $a'b't = b'(y_0 - y_1)$ and $y_0 - y_1 = a't$. Thus an arbitrary solution (x_1, y_1) to the equation has the form $x_1 = x_0 + b't$, $y_1 = y_0 - a't$ for $t \in \mathbb{Z}$. Conversely, it is easy to see that $(x_0 + b't, y_0 - a't)$ is indeed a solution for any $t \in \mathbb{Z}$.

□

Problem 2.2. *Solve the equation $62x + 38y = 4$.*

Solution. First, divide the coefficients by $\gcd(62, 38) = 2$ to get the equation $31x + 19y = 2$. Using the Euclidean algorithm, one can find Bézout's coefficients for $(31, 19)$: $31 \cdot 8 + 19 \cdot (-13) = 1$ whence $31 \cdot 2 \cdot 8 + 19 \cdot 2 \cdot (-13) = 2$. Then $(x_0, y_0) = (2 \cdot 8, 2 \cdot (-13)) = (16, -26)$ is a solution to the equation and $(x, y) = (16 + 19t, -26 - 31t), t \in \mathbb{Z}$ is its complete solution. □

Remark. Notice that the form of the solution to the above equation is not unique. For instance, $(x, y) = (-3 + 19t, 5 - 31t), t \in \mathbb{Z}$ defines the same set of solutions.

Exercise 2.1. *Solve the equation $126x - 51y = 9$.*

Problem 2.3. *Solve the equation $9x + 5y + 7z = 2$.*

Solution. The original equation is equivalent to the system of linear equations

$$\begin{cases} 9x + 5y = a \\ a + 7z = 2 \end{cases}.$$

Consider the equation $9x' + 5y' = 1$. One of its solutions is $(x'_0, y'_0) = (-1, 2)$ whence $(-a, 2a)$ is a solution to the equation $9x + 5y = a$. Thus its complete solution has the form $(x, y) = (-a + 5t, 2a - 9t), t \in \mathbb{Z}$. The complete solution to the equation $a + 7z = 2$ has the form $(a, z) = (2 - 7s, s), s \in \mathbb{Z}$ and

$$\begin{aligned} x &= -a + 5t = 7s - 2 + 5t, \\ y &= 2a - 9t = 4 - 14s - 9t, \\ z &= s \end{aligned}$$

for $s, t \in \mathbb{Z}$ is the complete solution to the original equation. □

Exercise 2.2. *Solve the equation* $2x - 4y + 5z = 3$.

Exercise 2.3. *Solve the system*

$$\begin{cases} 4x + 5y + 7z = 2 \\ 7x - 2y + 3z = -1 \end{cases}.$$

Exercise 2.4. *Let* $a, b, c, n \in \mathbb{Z}$, $a, b, c \neq 0$ *and* $d = \gcd(a, b, c)$. *Show that the equation* $ax + by + cz = n$ *has an integer solution if and only if* $d \mid n$.

3 Prime factorization theorem

Definition. An integer $p > 1$ is a **prime** number or a **prime** if $p = xy$ for $x, y \in \mathbb{Z}$ implies either x or y is associated with p. Alternatively, an integer $p \neq 1$ is a prime if it has no positive divisors other than 1 and p.

Proposition 3.1. *Let* p *be a prime.*

1. *if* $a \in \mathbb{Z}$ *and* p *does not divide* a, *then* p *and* a *are coprime;*
2. *if* $a, b \in \mathbb{Z}$ *and* p *divides* ab, *then* p *divides either* a *or* b *(Euclid's lemma);*
3. *if* p *divides the product of several integers, then* p *divides at least one of them;*
4. *every integer* $a > 1$ *is divisible by at least one prime number;*
5. *there are infinitely many primes (Euclid's theorem);*
6. *two distinct primes are coprime.*

Proof.

1. Put $d = \gcd(a, p) > 0$. Then $d \mid p$, so either $d = 1$ or $d = p$. If $d = p$ then $p \mid a$, a contradiction. Thus $d = 1$ and a, p are coprime.
2. Assume p does not divide a. By (1), a and p are coprime, hence $p \mid b$ by Proposition **??**.
3. Follows by induction on the number of multipliers.
4. Follows by induction on a; the case $a = 2$ is obvious. Further, if a is prime, there is nothing to prove. If a is not prime, then $a = bc$ for some positive integers b, c with $b, c < a$. Then by the induction assumption b is divisible by some prime p, hence a is also divisible by p.
5. Assume the contrary; let $p_1, \ldots, p_n$ be all the prime numbers. Consider $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$. By (4), a is divisible by some prime p_i, $1 \leq i \leq n$ which is impossible.
6. Assume primes p_1 and p_2 are not coprime; then by (1) $p_1 \mid p_2$ and $p_2 \mid p_1$, therefore they are equal.

□

Theorem 3.2 (Fundamental theorem of arithmetic, prime factorization theorem)**.** *Every integer $n > 1$ can be represented uniquely as a product of prime numbers, up to the order of the factors.*

Proof. The existence of factorization of n follows by induction on n. If $n = 2$, the statement is trivial. Let $n > 1$. Then $n = p_1 n_1$ for some prime p_1 by Proposition 3.1. The induction assumption for $n_1 < n$ yields $n_1 = p_2 \cdots p_k$ for some prime $p_2, \ldots, p_k$. Then $n = p_1 p_2 \cdots p_k$ as required.

The uniqueness also follows by induction on n. If $n = 2$, there is nothing to prove. Let $n = p_1 \cdots p_k = q_1 \cdots q_l$. The product $p_1 \cdots p_k$ is divisible by q_1, hence by Proposition 3.1 one of the factors, say p_i, is divisible by q_1. Then $p_i = q_1$ by Proposition 3.1, and $p_1 \cdots p_{i-1} p_{i+1} \cdots p_k = q_2 \cdots q_l < n$. By the induction assumption these factorizations differ only in the order of the prime factors. Hence the original factorizations $p_1 \cdots p_k = q_1 \cdots q_l$ also differ only in the order of the factors. □

Definition. Let $n \in \mathbb{N}$. Group together equal primes in its factorization and put them in the ascending order: $n = p_1^{k_1} \cdots p_s^{k_s}$, where $p_1 < \cdots < p_s$ are primes and $k_1, \ldots, k_s \in \mathbb{N}$. This representation is unique and is called the **canonical representation** of n.

Exercise 3.1. *Find the canonical representation of* 12000.

Remark. In some cases it is useful to allow the exponents $k_1, \ldots, k_s$ to be 0. For example, one can represent $m, n \in \mathbb{N}$ in the form $m = p_1^{k_1} \ldots p_s^{k_s}$, $n = p_1^{l_1} \ldots p_s^{l_s}$ with common prime factors $p_1, \ldots, p_s$ and non-negative integers $k_1, \ldots, k_s, l_1, \ldots, l_s$: if a prime factor is present in the canonical representation of m and not in that of n, one can include it into the factorization of n with zero exponent.

Example. 50 and 36 can be decomposed with common set of prime factors as $50 = 2^1 \cdot 3^0 \cdot 5^2, 36 = 2^2 \cdot 3^2 \cdot 5^0$

Proposition 3.3. *Let $m = p_1^{k_1} \cdots p_s^{k_s}$, $n = p_1^{l_1} \cdots p_s^{l_s}$ for primes $p_1, \ldots, p_s$. Then $m \mid n$ iff $k_i \le l_i$ for all $i = 1, \ldots, s$.*

Proof. If $k_i \le l_i$ for all $i = 1, \ldots, s$, then $n = m \cdot p_1^{l_i - k_i} \cdots p_s^{l_s - k_s}$.

Conversely, assume $n = mr$ for $r \in \mathbb{Z}$. If $r = q_1 \cdots q_t$ is a prime factorization of then

$$p_1^{l_1} \cdots p_s^{l_s} = p_1^{k_1} \cdots p_s^{k_s} q_1 \cdots q_t.$$

Two prime factorizations of n coincide up to permutation of the factors. Then $p_i^{k_i}$ occurs in the left-hand side product which implies $k_i \le l_i$. □

Proposition 3.4. *If $m = p_1^{k_1} \cdots p_s^{k_s}$, $n = p_1^{l_1} \cdots p_s^{l_s}$ be the canonical representations of integers m, n with common prime factors and $d = \gcd(m, n)$, then $d = p_1^{\min(k_1, l_1)} \cdots p_s^{\min(k_s, l_s)}$.*

Proof. Put $d = p_1^{\min(k_1, l_1)} \cdots p_s^{\min(k_s, l_s)}$. Since $k_i, l_i \ge \min(k_i, l_i)$ for all $i = 1, \ldots, s$, Proposition 3.3 implies that d is a common divisor of m and n. Let d' be another common divisor of m and n. Note that all prime factors of d' are among $p_1, \ldots, p_s$. Then $d' = p_1^{r_1} \cdots p_s^{r_s}$ for some $r_1, \ldots, r_s \ge 0$ and Proposition 3.3 gives $k_i, l_i \ge r_i$ for all $i = 1, \ldots, s$. Thus $\min(k_i, l_i) \ge r_i$, whence $d' \mid d$ again by Proposition 3.3. □

The **least common multiple** $\operatorname{lcm}(m,n)$ of $m,n\in\mathbb{N}$ is the smallest positive integer divisible by both m and n.

Proposition 3.5. *Let $m=p_1^{k_1}\cdots p_s^{k_s}$, $n=p_1^{l_1}\cdots p_s^{l_s}$ be the canonical representations of integers m,n with common prime factors and $e=\operatorname{lcm}(m,n)$. Then $e=p_1^{\max(k_1,l_1)}\cdots p_s^{\max(k_s,l_s)}$.*

Proof. Similar to the proof of Proposition 3.4. Put $e=p_1^{\max(k_1,l_1)}\cdots p_s^{\max(k_s,l_s)}$, then e is a common multiple of m and n by Proposition 3.3. Let e' be another common multiple of m and n. Then $e'=p_1^{t_1}\cdots p_s^{t_s}q$ for q being coprime to $p_1,\ldots,p_s$. Then $t_i\geq k_i,l_i$ for all $1\leq i\leq s$ by Proposition 3.3 whence $t_i\geq\max(k_i,l_i)$. Thus $e|e'$ by Proposition 3.3. □

Corollary 3.6. *$mn=\gcd(m,n)\operatorname{lcm}(m,n)$.*

Proof. Follows from the identity $k+l=\min(k,l)+\max(k,l)$. □

Proposition 3.7. *For any $m,n\in\mathbb{Z}$ there exist $m',n'\in\mathbb{Z}$ such that $n'\mid n, m'\mid m, \gcd(n',m')=1$ and $n'm'=\operatorname{lcm}(n,m)$.*

Proof. Let $n=p_1^{k_1}\cdots p_s^{k_s}$, $m=p_1^{l_1}\cdots p_s^{l_s}$ be the canonical representations of m,n with common prime factors. Then $\gcd(n,m)=p_1^{\min(k_1,l_1)}\cdots p_s^{\min(k_s,l_s)}$ and $\operatorname{lcm}(n,m)=p_1^{\max(k_1,l_1)}\cdots p_s^{\max(k_s,l_s)}$ by Propositions 3.4 and 3.5. Define

$$\Delta_1(k,l)=\begin{cases}k, & k\geq l\\ 0, & k<l\end{cases},\qquad \Delta_2(k,l)=\begin{cases}0, & k\geq l\\ l, & k<l\end{cases}.$$

Then $\Delta_1(k,l)\leq k, \Delta_2(k,l)\leq l, \min(\Delta_1(k,l),\Delta_2(k,l))=0$ and $\Delta_1(k,l)+\Delta_2(k,l)=\max(k,l)$. Put $n'=p_1^{\Delta_1(k_1,l_1)}\cdots p_s^{\Delta_1(k_s,l_s)}, m'=p_1^{\Delta_2(k_1,l_1)}\cdots p_s^{\Delta_2(k_s,l_s)}$, and the required properties of n',m' follow. □

Problem 3.8. *Let $n=p_1^{k_1}\cdots p_s^{k_s}$ be the canonical representation of n. The number of all positive integer divisors of n is $(1+k_1)\cdots(1+k_s)$.*

Solution. By Proposition 3.3 each divisor of n is of the form $p_1^{l_1}\cdots p_s^{l_s}$ for $0\leq l_i\leq k_i$, and Fundamental theorem of arithmetic implies that different s-tuples $(l_1,\ldots,l_s)$ correspond to different divisors. Thus the number of positive integer divisors of n is equal to the number of such s-tuples which is $(1+k_1)\cdots(1+k_s)$. □

Problem 3.9. *Let n,m be coprime integers and $d\mid mn$. Prove that $d=ab$ where $a\mid n, b\mid m$.*

Solution. Let $m=p_1^{k_1}\cdots p_s^{k_s}$, $n=q_1^{l_1}\cdots q_s^{l_s}$ be the canonical representations of m,n. Since they are coprime, $p_i\neq q_j$ for all i,j. Since $d\mid p_1^{k_1}\cdots p_s^{k_s}q_1^{l_1}\cdots q_s^{l_s}$, by Proposition 3.3 $d=p_1^{k_1'}\cdots p_s^{k_s'}q_1^{l_1'}\cdots q_s^{l_s'}$ with $k_i'\leq k_i, l_j'\leq l_j$. Then $a=p_1^{k_1'}\cdots p_s^{k_s'}, b=q_1^{l_1'}\cdots q_s^{l_s'}$ satisfy the required conditions. □

Exercise 3.2. *Prove that $a^3\mid b^2$ implies $a\mid b$*

Exercise 3.3. *Prove that if ab, bc, ac are integer cubes then a,b,c are integer cubes.*

Exercise 3.4. *Let a,n be positive integers. Prove that $\sqrt[n]{a}\in\mathbb{Q}$ implies $\sqrt[n]{a}\in\mathbb{Z}$.*

4 Chinese remainder theorem

Theorem 4.1 (Chinese remainder theorem). *Let $m_1, \dots, m_n \in \mathbb{N}$, and m_i, m_j be coprime for any $i \neq j$. Then for any $a_1, \dots, a_n \in \mathbb{Z}$ the system of congruences (同余).*

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

has a solution, and its general solution has the form $x \equiv x_0 \mod m_1 \cdots m_n$ where x_0 is a particular solution.

Proof. First prove the second part of the statement. Let $x \in \mathbb{Z}$ be such that $x \equiv a_i \pmod{m_i}, 1 \leq i \leq n$. Then $x - x_0$ is divisible by $m_i, 1 \leq i \leq n$. Since $m_1, \dots, m_n$ are coprime, Proposition 1.10 gives $m_1 \cdots m_n \mid x - x_0$, whence $x \equiv x_0 \pmod{m_1 \cdots m_n}$. Conversely, if $x \equiv x_0 \pmod{m_1 \cdots m_n}$, then $x - x_0$ is divisible by all $m_i, 1 \leq i \leq n$, thus $x \equiv x_0 \equiv a_i \pmod{m_i}$ for all $i, 1 \leq i \leq n$ and x is a solution of the system.

For a proof of the existence, we use the induction on n. Let $n = 2$. The system

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

is solvable if and only if the system of equations

$$\begin{cases} x = a_1 + m_1 y_1, \\ x = a_2 + m_2 y_2 \end{cases}.$$

is solvable. The latter system implies $m_1 y_1 - m_2 y_2 = a_1 - a_2$. Since m_1, m_2 are coprime, $y_1, y_2 \in \mathbb{Z}$ exist by Proposition 2.1. If one put $x = a_1 + m_1 y_1$ then $x = a_2 + m_2 y_2$, i.e. the system is solvable.

Assume the statement holds for n and consider the system (归纳. 假设 n 个同余式有解. 证 n+1 个~).

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \dots \\ x \equiv a_{n+1} \pmod{m_{n+1}} \end{cases}$$

By the induction assumption, the system

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

is equivalent to the congruence $x \equiv x_0 \pmod{m_1 \cdots m_n}$, where x_0 is a partial solution of this system. Therefore, the original system is equivalent to the system

$$\begin{cases} x \equiv x_0 \pmod{m_1 \cdots m_n}, \\ x \equiv a_{n+1} \pmod{m_{n+1}} \end{cases},$$

which has a solution since $m_1 \cdots m_n, m_{n+1}$ are coprime. □

Problem 4.2. *Solve the system*

$$\begin{cases} x \equiv 3 \pmod{13} \\ x \equiv 1 \pmod{9} \end{cases}.$$

Solution. The system can be rewritten as the system of equations

$$\begin{cases} x = 3 + 13y \\ x = 1 + 9z \end{cases}.$$

Subtracting the first equation from the second one gets $13y - 9z = -2$. Let $y_0 = 4, z_0 = 6$ be its particular solution. Then $x_0 = 1 + 9z_0 = 55$ is a particular solution of the system of congruences and $x = 55 + 117t, t \in \mathbb{Z}$ is its general solution. □

Exercise 4.1. *Solve the system*

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{6} \\ x \equiv 3 \pmod{7} \end{cases}.$$

Hint. Let x_0 be a solution of the system

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{6} \end{cases}.$$

Then solve the system

$$\begin{cases} x \equiv x_0 \pmod{30} \\ x \equiv 3 \pmod{7} \end{cases}.$$

Exercise 4.2. *Is the system*

$$\begin{cases} x \equiv 1 \pmod{30} \\ x \equiv -5 \pmod{21} \\ x \equiv 16 \pmod{35} \end{cases}.$$

solvable?

5 Euler's totient function

Definition. Let $n \in \mathbb{N}$. The number of positive integers not exceeding n coprime to n is denoted by $\varphi(n)$ and called **Euler's totient function.** (不超过n、与n互质)

Example. $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$.

Let $x, n \in$ and $n > 0$. Denote by $[x]_n$ the residue class of x modulo n.

Proposition 5.1. *Let $n \in \mathbb{N}$. Then $\varphi(n)$ equals the number of invertible elements (units) of the ring $\mathbb{Z}/n\mathbb{Z}$.*

Proof. As it was proven before, $[x]_n$ is invertible if and only if x, n are coprime. □

Theorem 5.2. *Let $m, n \in \mathbb{Z}$ be positive and coprime. The map $f\colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ given by $f([x]_{mn}) = ([x]_m, [x]_n)$ is well-defined and bijective.*

Moreover, $[x]_{mn}$ is invertible in $\mathbb{Z}/mn\mathbb{Z}$ if and only if $[x]_m$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ and $[x]_n$ is invertible in $\mathbb{Z}/n\mathbb{Z}$.

Proof. If $[x]_{mn} = [x']_{mn}$, then $mn \mid x - x'$, so $m \mid x - x'$ and $n \mid x - x'$. Thus $[x]_m = [x']_m$ and $[x]_n = [x']_n$ whence f is well-defined.

Assume $f([x]_{mn}) = f([x']_{mn})$. Then $[x]_m = [x']_m, [x]_n = [x']_n$ and $m \mid x - x'$ and $n \mid x - x'$. Since m, n are coprime, $mn \mid x - x'$ by Proposition 1.10, i.e. $[x]_{mn} = [x']_{mn}$. This proves the injectivity of f.

By the Chinese remainder theorem, for any $a, b \in \mathbb{Z}$ there is $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}.$$

Then $f([x]_{mn}) = ([x]_m, [x]_n) = ([a]_m, [b]_n)$ which implies that f is surjective.

If $[x']_{mn}$ is the inverse of $[x]_{mn}$ in $\mathbb{Z}/mn\mathbb{Z}$ and, then $[x']_m$ is the inverse to $[x]_m$, and $[x']_n$ is the inverse to $[x]_n$. Indeed, $[x]_m \cdot [x']_m = [x \cdot x']_m$, but $xx' \equiv 1 \pmod{mn}$ implies $xx' \equiv 1 \pmod{m}$. Similarly $[x]_n[x']_n = [1]_n$.

Conversely, let $a, b \in \mathbb{Z}$ be such that $[x]_m[a]_m = [1]_m$ and $[x]_n[b]_n = [1]_n$. The map f is bijective, so there is $x' \in \mathbb{Z}$ such that $[x']_m = [a]_m$, $[x']_n = [b]_n$. Then $[xx']_m = [x]_m \cdot [x']_m = [1]_m$ and $[xx']_n = [1]_n$. Thus $xx' \equiv 1 \pmod{m}$ and $xx' \equiv 1 \pmod{n}$, whence by Proposition 1.10 $xx' \equiv 1 \pmod{mn}$ and $[x]_{mn}$ is invertible. □

Theorem 5.3. *Let $m, n \in \mathbb{Z}$ be positive and coprime. Then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. By Proposition 5.1, $\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^*|$ and $\varphi(m)\varphi(n) = |(\mathbb{Z}/m\mathbb{Z})^*| \cdot |(\mathbb{Z}/n\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*|$. Theorem 5.2 states that f establishes a bijection between $(\mathbb{Z}/mn\mathbb{Z})^*$ and $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$, so these sets are of the same size. □

Corollary 5.4. *If $n = p_1^{k_1} \cdots p_s^{k_s}$ is the canonical representation of $n \in \mathbb{N}$ then $\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdots p_s^{k_s-1}(p_s - 1)$.*

Proof. First show that $\varphi(p^k) = p^{k-1}(p-1)$ if p is prime, $k > 0$. Evidently x is coprime to p^k iff x is coprime to p, that is, x is not divisible by p. The number of positive integers not greater than p^k and divisible by p is $p^k/p = p^{k-1}$, therefore the number of positive integers not greater than p^k and not divisible by p $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Now notice that all the factors of the form $p_i^{k_i}$ in the canonical representation of n are coprime and Theorem 5.3 implies $\varphi(n) = \varphi(p_1^{k_1} \cdots p_s^{k_s}) = \varphi(p_1^{k_1}) \cdot \cdots \varphi(p_s^{k_s}) = p_1^{k_1-1}(p_1 - 1) \cdots p_s^{k_s-1}(p_s - 1)$ as required. □

Problem 5.5. *Show that $\sum_{d|n} \varphi(d) = n$.*

Solution. Consider the list of n fractions

$$\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$$

and reduce each number to the lowest terms; that is, express it as a quotient of coprime integers. The denominator of the fraction in the new list is a divisor of n. If $d \mid n$, exactly $\varphi(d)$ fractions will have d as their denominator. Indeed, if $n = dk$, any fraction $\frac{s}{d}$ where $1 \le s \le d$ and s, d are coprime, originates from the fraction $\frac{sk}{n}$. Hence, there are $\sum_{d|n} \varphi(d)$ elements in the list. □

Exercise 5.1. *Compute* $\varphi(60)$.

Exercise 5.2. *Show that* $\varphi(n)$ *is even for every* $n \ge 3$.

Exercise 5.3. *Prove the identity* $\sum_{d|n} \varphi(d) = n$ *by induction on* n.

Hint. Choose a prime divisor p of n and write $n = mp^k$ for m coprime p, then use the induction assumption for m.

6 Modular arithmetic and Euler's theorem

Remind properties of congruences:

Proposition 6.1. *Let* $m \in \mathbb{N}$.

1. $a \equiv a \pmod m$ *for any* $a \in \mathbb{Z}$
2. *if* $a \equiv b \pmod m$, *then* $b \equiv a \pmod m$ *for any* $a, b \in \mathbb{Z}$
3. *if* $a \equiv b \pmod m$ *and* $b \equiv c \pmod m$, *then* $a \equiv c \pmod m$ *for any* $a, b, c \in \mathbb{Z}$
4. *if* $a_1 \equiv a_2 \pmod m$ *and* $b_1 \equiv b_2 \pmod m$, *then* $a_1 + b_1 \equiv a_2 + b_2 \pmod m$ *and* $a_1 b_1 \equiv a_2 b_2 \pmod m$ *for any* $a_1, a_2, b_1, b_2 \in \mathbb{Z}$
5. *every integer is congruent modulo* m *exactly to one of* $0, 1, \dots, m-1$.

Problem 6.2. *Find* $2000^{17} \pmod{13}$

Solution. First, $2000 \equiv 11 \equiv -2 \pmod{13}$, thus $2000^{17} \equiv (-2)^{17} = -2^{17} \pmod{13}$. Further, $2^6 = 64 \equiv -1 \pmod{13}$, thus $-2^{17} = -(2^6)^2 \cdot 2^5 \equiv -(-1)^2 \cdot 2^5 = -32 \equiv 7 \pmod{13}$. □

Problem 6.3. *Find* $10^{100} \pmod{77}$

Proof. First we find $10^{100} \pmod 7$ and $10^{100} \pmod{11}$. Since $10^3 \equiv 3^3 = 27 \equiv -1 \pmod 7$ and $100 \equiv 4 \mod 6$, one has $10^{100} \equiv 3^{100} \equiv 3^4 \equiv 9^2 \equiv 2^2 = 4 \pmod 7$. Further, $10^{100} \equiv (-1)^{100} = 1 \pmod{11}$. Thus $x = 10^{100}$ satisfies the following conditions

$$\begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 1 \pmod{11} \end{cases}.$$

The solution of this system yields $x \equiv 67 \pmod{77}$. □

Exercise 6.1. *Find* $10^{200} \pmod{91}$

Exercise 6.2. *Prove that*

1. $43^{101} + 23^{101}$ *is divisible by 66*
2. $2^{70} + 3^{70}$ *is divisible by 13.*

Exercise 6.3. *Prove that if* $a^2 + b^2$ *is divisible by 7 then* $a^2 + b^2$ *is divisible by 49.*

Theorem 6.4 (Euler's Theorem)**.** *Let* $n \in \mathbb{N}$, $a \in \mathbb{Z}$ *and* a, n *are coprime. Then* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corollary 6.5 (Fermat's Little Theorem)**.** *If* p *is prime, and* $a \in \mathbb{Z}$, *then* $a^p \equiv a \pmod{p}$.

Proof. If $p \mid a$, then $a^p \equiv 0 \pmod{p}$ and $a \equiv 0 \pmod{p}$. If $p \nmid a$, then by Euler's theorem, $a^{p-1} \equiv 1 \pmod{p}$. Multiplying both parts by a, one gets the required congruence. □

Problem 6.6. *Find* $7^{96} \pmod{27}$.

Solution. Since $\varphi(27) = 18$, Euler's theorem implies that $7^{18} \equiv 1 \pmod{27}$. Then $7^{96} = (7^{18})^5 \cdot 7^6 \equiv 7^6 \pmod{27}$. Finally $7^2 = 49 \equiv -5 \pmod{27}$, whence $7^6 = (7^2)^3 \equiv (-5)^3 = -125 \equiv 10 \pmod{27}$. □

Exercise 6.4. *Find* $7^{120} \pmod{19 \cdot 23}$.

Exercise 6.5. *Find* $14^{100} \pmod{34}$. *Notice that Euler's theorem can not be directly applied.*

Exercise 6.6. *Solve the equation* $x^{99} + x^{71} + 2x^{49} + x^{20} + \overline{1} = \overline{0}$ *in* $\mathbb{Z}/11\mathbb{Z}$

Problem 6.7. *Find all integer* x *satisfying the congruence* $3x^2 + 2x + 4 \equiv 0 \pmod{55}$.

Solution. The congruence is equivalent to the system

$x = \frac{-b \pm \sqrt{\Delta}}{2a}$ is suitable for any field.

$$\begin{cases} 3x^2 + 2x + 4 \equiv 0 \pmod{5} \\ 3x^2 + 2x + 4 \equiv 0 \pmod{11} \end{cases}$$

Using the formula for the roots of the quadratic equations in a field, one gets

$$\begin{cases} \overline{x} = (-\overline{2} \pm \sqrt{-\overline{44}})(2 \cdot \overline{3})^{-1} = \overline{2}, \overline{4}, & \text{in } \mathbb{Z}/5\mathbb{Z} \\ \overline{x} = (-\overline{2} \pm \sqrt{-\overline{44}})(2 \cdot \overline{3})^{-1} = \overline{7}, & \text{in } \mathbb{Z}/11\mathbb{Z} \end{cases}$$

Thus

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 7 \pmod{11} \end{cases} \quad \text{and} \quad \begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 7 \pmod{11} \end{cases}.$$

The solutions of the above systems give $x \equiv 7, 29 \pmod{77}$. □

Exercise 6.7. *Find all integer* x *satisfying* $8x^2 - 7x + 17 \equiv 0 \pmod{105}$.

Proposition 6.8. *Let p be an odd prime, $p \nmid b$ and $n \in \mathbb{N}$. The congruence $x^2 \equiv b \pmod{p^n}$ is solvable iff the congruence $x^2 \equiv b \pmod{p}$ is solvable.*

Moreover if the congruence $x^2 \equiv b \pmod{p^n}$ is solvable then it has exactly two solutions.

Proof. Suppose $x^2 \equiv b \pmod{p}$ is solvable and prove that $x^2 \equiv b \pmod{p^n}$ is solvable by induction on n. Assume that $a^2 - b = kp^n$ for some $a, k \in \mathbb{Z}$ and put $a' = a + cp^n$, $c \in \mathbb{Z}$. Then $a'^2 = (a + cp^n)^2 \equiv a^2 + 2acp^n = b + (k + 2ac)p^n \pmod{p^{n+1}}$. Clearly $p \nmid 2a$ and there is c such that $k + 2ac \equiv 0 \pmod{p}$. Then a' satisfies $a'^2 \equiv b \pmod{p^{n+1}}$.

The inverse statement is trivial.

Finally assume $x^2 \equiv y^2 \equiv b \pmod{p^n}$. Then $p^n \mid (x-y)(x+y)$ whence $p^m \mid (x-y), p^{n-m} \mid (x+y)$ for some $0 \le m \le n$. If $0 < m < n$ then $p \mid (x-y), (x+y)$ whence $p \mid x$ and $p \mid b$, a contradiction. Thus $m = 0$ or n, that is $y \equiv \pm x \pmod{p^n}$. □

Exercise 6.8. *Find all integer x satisfying $x^2 \equiv 59 \pmod{125}$.*

Hint. Follow the proof of Proposition 6.8.

7 Primitive roots

Lemma 7.1. *If G is an abelian group, $a, b \in G$ and $\operatorname{ord} a = n, \operatorname{ord} b = m$, with $\gcd(n, m) = 1$, then $\operatorname{ord} ab = nm$.*

Proof. Obviously, $(ab)^{nm} = a^{nm}b^{nm} = e$. Suppose that $(ab)^k = e$ for some $k > 0$. Then $b^{nk} = (ab)^{nk} = e$, whence $m \mid nk$. Since $\gcd(n, m) = 1$, it implies $m \mid k$. Similarly, $n \mid k$. Now $\gcd(n, m) = 1$ implies $nm \mid k$, hence $k \ge mn$. □

Lemma 7.2. *If G is an abelian group, $a, b \in G$ and $\operatorname{ord} a = n, \operatorname{ord} b = m$, then there exists $c \in G$ such that $\operatorname{ord} c = \operatorname{lcm}(n, m)$.*

Proof. By Proposition 3.7, there are n', m' such that $n' \mid n, m' \mid m, \gcd(n', m') = 1$ and $n'm' = \operatorname{lcm}(n, m)$. If $\operatorname{ord} a = n$ and $n = n's$, then obviously $\operatorname{ord} a^s = n'$. Similarly, for $m = m'r$ we have $\operatorname{ord} b^r = m'$. Then $\operatorname{ord} a^s b^r = n'm' = \operatorname{lcm}(n, m)$ by Lemma 7.1. □

Theorem 7.3. *The multiplicative group of a finite field is cyclic*

Proof. Let K be a finite field and $|K^*| = m$. Choose $\alpha \in K^*$ with maximum order, $\operatorname{ord} \alpha = s$. By Lagrange's theorem, $s \mid m$, in particular, $m \ge s$. Let $\beta \in K^*$ and $\operatorname{ord} \beta = r$. By Lemma 7.2 one can find $\gamma \in K^*$ such that $\operatorname{ord} \gamma = \operatorname{lcm}(s, r) \ge s$. Since α has maximum order, $\operatorname{lcm}(s, r) = s$, whence $r \mid s$. Thus, the order of any element of K^* is a divisor of s.

Consider the polynomial $x^s - 1$ over K. Any $\beta \in K^*$ is its root, since $\beta^s = (\beta^r)^k = 1$ if $\operatorname{ord} \beta = r$ and $s = rk$. The number of roots of a polynomial cannot exceed its degree, so $m \le s$. Hence, $m = s$ and α is a generator of K^*. □

Example. The polynomial $f(x) = x^2 + \overline{1}$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$ whence $K = \mathbb{Z}/3\mathbb{Z}[x]/(f)$ is a field of 9 elements. The element $\alpha = x + \overline{1}$ is a generator of K^*.

Indeed, $\alpha^2 = -\overline{x}, \alpha^4 = -\overline{1}$, and so the order of α, being a divisor of 8, is not equal to $1, 2, 4$.

Definition. A generator of the multiplicative group of a field is called its **primitive** element.

Definition. Let $n \in \mathbb{Z}, n \geq 2$. An integer g is a **primitive root** modulo n if every $a \in \mathbb{Z}$ coprime to n is congruent to a power of g modulo n. This is equivalent to the fact that $\overline{g}$ is a generator of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$.

Remark. If p is prime, g is a primitive root modulo p iff $\overline{g}$ is a primitive element of the field $\mathbb{Z}/p\mathbb{Z}$. Thus Theorem 7.3 implies that primitive roots modulo p exist. There are composite numbers which possess primitive roots (for example, -1 is a primitive root modulo 4) and which don't (for example, there is no primitive root modulo 8).

Proposition 7.4. *If $n = ab$, where $a, b > 1$ are odd and coprime, then n does not have a primitive root*

Proof. For $m = \operatorname{lcm}(\varphi(a), \varphi(b))$ one has $x^m \equiv 1 \pmod{n}$ for all x coprime with n by Euler's Theorem. Note that $m < \varphi(a)\varphi(b) = \varphi(n)$ because $\varphi(a)$ and $\varphi(b)$ are both even. □

Problem 7.5. *Find the least primitive root modulo 73:*

Solution. One has $\varphi(73) = 72 = 2^3 \cdot 3^2$. Thus a is a primitive root modulo 73 iff $a^{36} \not\equiv 1 \pmod{73}$ and $a^{24} \not\equiv 1 \pmod{73}$.

Testing $a = 2$: $2^{36} \equiv 1 \pmod{73}$

Testing $a = 3$: $3^{36} \equiv 1 \pmod{73}$

Testing $a = 5$: $5^{36} \equiv -1 \pmod{73}$, $5^{24} \equiv 8 \pmod{73}$, hence 5 is the least primitive root modulo 73. □

Proposition 7.6. *Let $p > 2$ be a prime and a be a primitive root modulo p. If $a^{p-1} \not\equiv 1 \pmod{p^2}$ then a is a primitive root modulo p^2. If $a^{p-1} \equiv 1 \pmod{p^2}$ then $a + p$ is a primitive root modulo p^2.*

Proof. Let $m = \operatorname{ord} \overline{a}$ in $(\mathbb{Z}/p^2\mathbb{Z})^*$. Since the order of this group equals $\varphi(p^2) = p(p-1)$, one has $m \mid p(p-1)$. Further, $a^m \equiv 1 \mod p^2$ implies $a^m \equiv 1 \mod p$. The order of the residue class of a in $(\mathbb{Z}/p\mathbb{Z})^*$ is $p-1$, whence $p-1 \mid m$. Thus $m = p-1$ or $m = p(p-1)$.

If $a^{p-1} \not\equiv 1 \pmod{p^2}$ then $m = p(p-1)$ and a is a primitive root modulo p^2. Assume $a^{p-1} \equiv 1 \pmod{p^2}$ and consider $a+p$ which is also a primitive root modulo p. If $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$ then it is a primitive root modulo p^2 as it was shown above. Otherwise $(a+p)^{p-1} \equiv 1 \pmod{p^2}$ gives $a + p \equiv (a+p)^p \equiv a^p \equiv a \pmod{p^2}$, a contradiction. □

Proposition 7.7. *Let $p > 2$ be a prime and a be a primitive root modulo $p^n, n \geq 2$ then a is a primitive root modulo p^{n+1}.*

Proof. Let $m = \operatorname{ord} \overline{a}$ in $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$. Since the order of this group equals $\varphi(p^{n+1}) = p^n(p-1)$, one has $m \mid p^n(p-1)$. Further, $a^m \equiv 1 \pmod{p^{n+1}}$ implies $a^m \equiv 1 \pmod{p^n}$. The order of the residue class of a in $(\mathbb{Z}/p^n\mathbb{Z})^*$ is $\varphi(p^n) = p^{n-1}(p-1)$, whence $p^{n-1}(p-1) \mid m$. Thus $m = p^{n-1}(p-1)$ or $m = p^n(p-1)$.

It remains to show that $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$. Euler's theorem gives $a^{p^{n-2}(p-1)} = 1 + sp^{n-1}$ for $s \in \mathbb{Z}$. Since a is a primitive root modulo p^n, $a^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$, whence $p \nmid s$. Hence $a^{p^{n-1}(p-1)} = (1 + sp^{n-1})^p \equiv 1 + sp^n \not\equiv 1 \pmod{p^{n+1}}$. □

Corollary 7.8. *For any n and prime $p > 2$ there exists a primitive root modulo p^n.*

Problem 7.9. *Let p be an odd prime. Prove that*

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p}, & \text{if } p-1 \nmid n \\ -1 \pmod{p}, & \text{if } p-1 \mid n \end{cases}$$

Solution. Let g be a primitive root modulo p. Then

$$\begin{aligned} 1^n + 2^n + \cdots + (p-1)^n \equiv & (g^0)^n + (g^1)^n + \cdots + (g^{p-2})^n \\ = & (g^n)^0 + (g^n)^1 + \cdots + (g^n)^{p-2} = \frac{(g^n)^{p-1} - 1}{g^n - 1} \equiv 0 \pmod{p} \end{aligned}$$

if $g^n \not\equiv 1 \pmod{p}$, that is if $p-1 \nmid n$. If $p-1 \mid n$ then $g^n \equiv 1 \pmod{p}$ and the above sum is equivalent to -1 modulo p. □

Exercise 7.1. i) *Find the least primitive root modulo* 41.
ii) *Prove that there is no primitive root modulo* 12.

Exercise 7.2. *Let $g \in \mathbb{Z}$ be a primitive root modulo n and $h \in \mathbb{Z}, gh \equiv 1 \mod n$. Show that h is a primitive root modulo n.*

Exercise 7.3. *Let p be an odd prime. Prove that*

$$1^n + 2^n + \cdots + (p^2-1)^n \equiv \begin{cases} 0 \pmod{p^2}, & \text{if } p-1 \nmid n \\ -p \pmod{p^2}, & \text{if } p-1 \mid n \end{cases}$$

Hint. Follow the proof of Problem 7.9. If g is a primitive root modulo p^2 and $p-1 \nmid n$ then $g^n \not\equiv 1 \pmod{p}$.

8 Legendre symbol

Definition. Let p be an odd prime and a be an integer coprime to p. If the congruence $x^2 \equiv a \pmod{p}$ is solvable, then a is a **quadratic residue** modulo p, otherwise a is a **quadratic nonresidue** modulo p. Clearly if $a \equiv b \mod p$ then a is a quadratic residue modulo p iff b is a quadratic residue modulo p.

Example. Since $\overline{1}^2 = \overline{1}, \overline{2}^2 = \overline{4}, \overline{3}^2 = \overline{4}, \overline{4}^2 = \overline{1}$ in $\mathbb{Z}/5\mathbb{Z}$, -1 is a quadratic residue modulo 5 and 7 is a quadratic nonresidue modulo 5.

Lemma 8.1. *Let p be an odd prime and $a \in \mathbb{Z}$. The number of integer solutions modulo p of the congruence $x^2 \equiv a \pmod{p}$ equals*

$$\begin{cases} 2, & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } p \nmid a \\ 0, & \text{if } a \text{ is a quadratic nonresidue modulo } p \\ 1, & \text{if } p \mid a \end{cases}$$

Proof. If $p \mid a$ then $x^2 \equiv a \mod p$ is equivalent to $x \equiv 0 \mod p$, that is the solution modulo p is unique. If a is a quadratic residue modulo p and $p \nmid a$ then $a \equiv b^2 \pmod p$ for some $b \in \mathbb{Z}$. Then $x^2 \equiv b^2 \mod p$ is equivalent to $(x-b)(x+b) \equiv 0 \mod p$. This congruence has 2 solutions modulo p. (They are distinct since $-b \equiv b \mod p$ implies $2 \mid p$ or $p \mid b$ whence $a \equiv 0 \pmod p$ and the both cases are impossible.) Finally if a is a quadratic nonresidue modulo p, the congruence $x^2 \equiv a \pmod p$ has no solution. □

exclude $\bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$

Proposition 8.2. *Let p be an odd prime. There are exactly $(p-1)/2$ quadratic residues modulo p in any p consecutive integers.* p个连续整数←研究时等价于$\mathbb{Z}/p\mathbb{Z}$

Proof. It suffices to prove that there are exactly $(p-1)/2$ squares in $\mathbb{Z}/p\mathbb{Z}$. Consider the partitioning of $\mathbb{Z}/p\mathbb{Z}$ into the subsets of elements with equal squares. By Lemma 8.1, the partition contains a unique one-element subset and N two-element subsets where N is the number of quadratic residues modulo p. Therefore $N = (p-1)/2$. □

除去 $\bar{0}$. $\bar{x}^2 = \bar{y}^2 = a \pmod p$ 的数 两两对应.

Lemma 8.3. *Let p be an odd prime, $g \in \mathbb{Z}$ be a primitive root modulo p. Then $a \in \mathbb{Z}, a \equiv g^j \pmod p$ is a quadratic residue iff j is even.*

Proof. If $j = 2k$ then $\overline{a} = (\overline{g}^k)^2$ and if $\overline{a} = \overline{b}^2, \overline{b} = \overline{g}^k$ then $g^j = g^{2k}$ and $p-1 \mid j-2k$ whence j is even. □

Proposition 8.4 (Euler's criterion)**.** *Let p be an odd prime and $a \in \mathbb{Z}, p \nmid a$. Then*

$$a^{(p-1)/2} \equiv \begin{cases} 1 \mod p, \text{ if } a \text{ is a quadratic residue modulo } p \\ -1 \mod p, \text{ if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

Proof. By Fermat's Little theorem, $(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \pmod p$. Thus $a^{(p-1)/2} \equiv \pm 1 \pmod p$ by Lemma 8.1.

Let $g \in \mathbb{Z}$ be a primitive root modulo p and $a \equiv g^j \pmod p$. By Lemma 8.3 a is a quadratic residue iff j is even. On the other hand $\overline{a}^{(p-1)/2} = \overline{g}^{j(p-1)/2} = \overline{1}$ iff $j(p-1)/2$ is divisible by $p-1$, that is, iff j is even, which proves the statement. □

Definition. Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ if } a \text{ is a quadratic residue modulo } p \\ 0, \text{ if } a \text{ is divisible by } p \\ -1, \text{ if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p.$

Euler criterion 的 Legendre symbol 形式.

Example. $\left(\frac{2}{11}\right) = -1$ since 2 is a quadratic nonresidue modulo 11 , while $\left(\frac{3}{11}\right) = 1$ since $3 \equiv 5^2 \mod 11$ is a quadratic residue modulo 11.

Proposition 8.5. *Let p be an odd prime and $a, b \in \mathbb{Z}$. Then*

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

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. *In other words, the product of two quadratic residues is a quadratic residue, the product of two quadratic nonresidues is a quadratic residue, and the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue.*

Proof. The first part is obvious. By Euler's criterion $\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \pmod p$ for any $x \in \mathbb{Z}, (x,p) = 1$. Thus $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$ if $p \nmid ab$. If $p \mid ab$ then either $p \mid a$ or $p \mid b$ and the equality also follows. □

Exercise 8.1. *Prove that*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, \text{ if } p \equiv 1 \pmod 4 \\ -1, \text{ if } p \equiv 3 \pmod 4 \end{cases}$$

Hint. Use Euler's criterion.

Exercise 8.2. *Let $p > 3$ be a prime. Prove that the sum of quadratic residues modulo p in the interval $[1, p-1]$ is divisible by p.*

Hint. Multiply all the residues by an integer $a \not\equiv 0, \pm 1 \pmod 3$.

Lemma 8.6 (Gauss Lemma)**.** *Let p be an odd prime and $a \in \mathbb{Z}, p \nmid a$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{n(a,p)},$$

where $n(a,p)$ denotes the number of integers in the set $A = \{a, 2a, \ldots, \frac{(p-1)}{2}a\}$ such that the remainder of the division by p is greater than $p/2$.

Proof. First notice that the elements of A modulo p are all distinct since $ka \equiv \ell a \pmod p$ implies $k \equiv \ell \pmod p$ and $k = \ell$ as $1 \le k, \ell \le (p-1)/2$. Partition A into subsets A_1 and A_2 where A_1 consists of the elements whose remainders of the division by p are less than $p/2$. If m is the size of A_1, then the size of A_2 is $n = n(a,p)$ and $n + m = (p-1)/2$.

Let $r_1, r_2, \ldots, r_m$ be the remainders of the elements of A_1 divided by p and $s_1, s_2, \ldots, s_n$ be the remainders of the elements of A_2 divided by p. Then $0 < r_1, \ldots, r_m, p - s_1, \ldots, p - s_n < \frac{p}{2}$.

We will prove that the above integers are all distinct. Indeed, assume that $p - s_u = r_v$ for some $1 \le v \le m, 1 \le u \le n$. There are $k, \ell \in \mathbb{Z}$, $1 \le k, \ell \le (p-1)/2$ such that $r_v \equiv ka \pmod p, s_u \equiv \ell a \pmod p$, hence $(k+\ell)a \equiv r_v + s_u = p \equiv 0 \pmod p$. This implies $k + \ell \equiv 0 \pmod p$ which is a contradiction since $0 < k + \ell \le p - 1$.

As all of $r_1, \ldots r_m, p - s_1, \ldots, p - s_n$ are distinct, they coincide up to permutation with the integers $1, 2, \ldots, (p-1)/2$. Thus

$$\left(\frac{p-1}{2}\right)! = r_1 \cdots r_m (p - s_1) \cdots (p - s_n) \equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod p.$$

As $r_1, r_2, \ldots, r_m, s_1, s_2, \ldots, s_n$ are the remainders of the elements of A divided by p, one has

$$r_1 \cdots r_m s_1 \cdots s_n \equiv a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$

As $p \nmid (p-1)/2!$, the above two congruences yield $a^{(p-1)/2} \equiv (-1)^n \pmod{p}$. It remains to apply Euler's criterion. □

Example. Let $p = 17$ and $a = 3$, then $A = \{3, 6, 9, 12, 15, 18, 21, 24\}$ and the set of their remainders divided by 3 is $\{3, 6, 9, 12, 15, 1, 4, 7\}$. Hence, $n(3, 17) = 3$ and $\left(\frac{3}{17}\right) = -1$.

Proposition 8.7. *Let p be an odd prime and a be an odd integer, $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\tau(a,p)}, \text{ where } \tau(a,p) = \sum_{i=1}^{(p-1)/2} \left[\frac{ia}{p}\right].$$

Proof. By Gauss Lemma, it is sufficient to prove that $\tau(a, p) \equiv n(a, p) \pmod{2}$.

Dividing the integers $a, 2a, \ldots, \frac{(p-1)a}{2}$ by p with remainder, one gets $ia = p\left[\frac{ia}{p}\right] + \rho_i, 0 \leq \rho_i < p$ for $1 \leq i \leq (p-1)/2$. With the same notation as in the proof of Gauss Lemma, the remainders $\rho_1, \ldots, \rho_{(p-1)/2}$ coincide up to permutation with $r_1, \ldots, r_m, s_1, \ldots, s_n$. On the other hand, $r_1, \ldots, r_m, p-s_1, \ldots, p-s_n$ coincide up to permutation with $1, 2, \ldots, (p-1)/2$. Therefore

$$a \sum_{i=1}^{(p-1)/2} i = p \sum_{i=1}^{(p-1)/2} \left[\frac{ia}{p}\right] + \sum_{v=1}^{m} r_v + \sum_{u=1}^{n} s_u$$

and

$$\sum_{i=1}^{(p-1)/2} i = \sum_{h=1}^{m} r_v + \sum_{u=1}^{n} (p - s_u) = pn + \sum_{v=1}^{m} r_v - \sum_{u=1}^{n} s_u.$$

By subtracting the above equalities one gets

$$(a-1) \sum_{i=1}^{(p-1)/2} i = p\tau(a,p) - pn + 2\sum_{u=1}^{n} s_u.$$

Since a, p are odd, $\tau(a, p) \equiv n \pmod{2}$ as required. □

Proposition 8.8. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 \text{ if } p \equiv \pm 1 \pmod 8 \\ -1 \text{ if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Proof. Apply Gauss Lemma to $a = 2$, where $A = \{2, 4, \ldots, p-1\}$. Then one has to find the number n of elements of A that are greater than $p/2$. If $p = 8h + 1$ then n is the number of integers $4h + 1, \ldots, 8h$, that is, $n = 4h$ is even. If $p = 8h + 3$ then n is the number of integers $4h + 2, \ldots, 8h + 2$, that is, $n = 4h + 1$ is odd. The other cases $p = 8h + 5$ and $p = 8h + 7$ are treated similarly. □

Theorem 8.9 (Law of quadratic reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

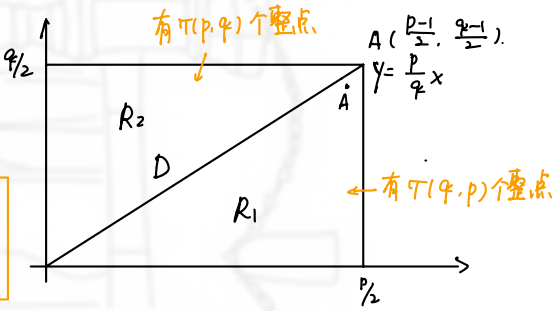
unless $p \equiv q \equiv 3 \pmod 4$, in which case

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Equivalently,

$$\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.}$$

D上无整数点



Proof. Consider the open rectangle R with vertices $(0,0), (p/2,0), (0,q/2), (p/2,q/2)$. Clearly, it includes $(p-1)(q-1)/4$ points with integer coordinates. Let D be the diagonal from $(0,0)$ to $(p/2,q/2)$ with equation $py = qx$. As p, q are coprime, no point with integer coordinates in R lies on D. Denote by R_1 the subset of R lying below D, and by R_2 the subset of R lying above D. Count the points of R_1 with integer coordinates, that is, the points of the form (i,j), with $1 \le i \le (p-1)/2, 1 \le j \le [qi/p]$. Their number is $\tau(q,p) = \sum_{i=1}^{(p-1)/2}[qi/p]$. Analogously, the number of points of R_2 having integer coordinates is $\tau(p,q) = \sum_{i=1}^{(q-1)/2}[pi/q]$. Thus

$$\frac{(p-1)(q-1)}{4} = \tau(p,q) + \tau(q,p)$$

and the statement immediately follows from Proposition 8.7. □

Problem 8.10. *Compute* $(\frac{47}{131})$.

利用二次互反律(8.9). 不断缩小分子分母

Solution.

$$\begin{aligned}\left(\frac{47}{131}\right) &= -\left(\frac{131}{47}\right) = -\left(\frac{37}{47}\right) = -\left(\frac{47}{37}\right) = -\left(\frac{10}{37}\right)\\ &= -\left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = \left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1.\end{aligned}$$

by 8.8. $37 \equiv -3 \pmod 8$

Alternatively,

$$\begin{aligned}\left(\frac{47}{131}\right) &= -\left(\frac{131}{47}\right) = -\left(\frac{84}{47}\right) = -\left(\frac{4}{47}\right)\left(\frac{3}{47}\right)\left(\frac{7}{47}\right)\\ &= -\left(\frac{47}{3}\right)\left(\frac{47}{7}\right) = -\left(\frac{2}{3}\right)\left(\frac{5}{7}\right) = \left(\frac{5}{7}\right) = -1.\end{aligned}$$

↑ 对7. quadratic residue 只有 1, 2, 4.

□

Problem 8.11. *Does there exist an integer x satisfying the congruence $3x^2 - 7x + 5 \equiv 0 \pmod{31}$?*

Solution. The question is equivalent to the solvability of the equation $\overline{3}t^2 - \overline{7}t + \overline{5} = \overline{0}$ in $\mathbb{Z}/31\mathbb{Z}$. Its discriminant equals $D = (-\overline{7})^2 - 4 \cdot \overline{3} \cdot \overline{5} = -\overline{11}$ and $(\frac{-11}{31}) = (\frac{20}{31}) = (\frac{5}{31}) = (\frac{31}{5}) = (\frac{1}{5}) = 1$. Thus the equation is solvable. □

Exercise 8.3. *Compute* $(\frac{41}{151}), (\frac{43}{151})$.

Problem 8.12. *Characterise the odd primes p such that 5 is a quadratic residue modulo p.*

Solution. By the law of quadratic reciprocity, $(\frac{5}{p}) = 1$ iff $(\frac{p}{5}) = 1$. Clearly ± 1 are the only quadratic residues modulo 5, thus 5 is a quadratic residue modulo p iff $p \equiv \pm 1 \mod 5$. □

Exercise 8.4. *Show that* $166 \mid 13^{41} + 1$.

Hint. Use Euler's criterion.

Exercise 8.5. *Show that 3 is a quadratic residue modulo prime p iff $p \equiv \pm 1 \mod 12$.*

Problem 8.13. *Prove that there are infinitely many primes p such that $p \equiv -1 \pmod{12}$.*

Solution. Suppose $p_1, \ldots, p_n$ are the only primes of the form $12n - 1, n \in \mathbb{Z}$. Let $P = p_1 \cdots p_n$ and $Q = 12P^2 - 1$. Then every prime divisor of Q is $\pm 1 \pmod{12}$. Indeed, let q be an odd prime such that $q \mid 12P^2 - 1$. Then $3(2P)^2 \equiv 1 \pmod{q}$ implies that 3 is a quadratic residue modulo q. This only happens when $q \equiv \pm 1 \pmod{12}$ (Exercise 8.5). Thus every prime divisor of Q is of the form $12n + 1$ or $12n - 1$. They cannot all be of the form $12n + 1$, otherwise the product would also be of this form. Thus there is a prime of the form $12n - 1$ dividing Q and it cannot be one of $p_1, \ldots, p_n$, a contradiction. □

Exercise 8.6. *Prove that* $(\frac{-3}{p}) = (\frac{p}{3})$ *for any odd prime p.*

Problem 8.14. *Show that for any $a \in \mathbb{Z}$ every divisor of $a^4 - a^2 + 1$ satisfies $a \equiv 1 \pmod{12}$.*

Solution. Let p be a prime divisor of $a^4 - a^2 + 1$. Then $\alpha^4 - \alpha^2 + \overline{1} = \overline{0}$ for $\alpha = \overline{a} \in \mathbb{Z}/p\mathbb{Z}$. This can be rewritten as $(\overline{2}\alpha^2 - 1)^2 = -\overline{3}$ and $((\alpha^2 - 1)\alpha^{-1})^2 = -\overline{1}$. These equalities imply $(\frac{-1}{p}) = 1$ whence $p \equiv 1 \pmod{4}$ and $(\frac{p}{3}) = (\frac{-3}{p}) = 1$ whence $p \equiv 1 \pmod{3}$. □

Problem 8.15. *Prove that for a prime p and integers a, b, $p \nmid ab$, the number of solutions of the congruence $ax^2 + by^2 \equiv 1 \pmod{p}$ is $p - \left(\frac{-ab}{p}\right)$.*

Solution. The congruence $ax^2 + by^2 \equiv 1 \pmod{p}$ is equivalent to the congruence $(ax)^2 + aby^2 \equiv a \pmod{p}$. Using Legendre symbol, the number of its solutions can be written as

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{a - aby^2}{p}\right)\right) = p + \sum_{y=0}^{p-1} \left(\frac{a - aby^2}{p}\right) = p + \left(\frac{-ab}{p}\right) \sum_{y=0}^{p-1} \left(\frac{y^2 + d}{p}\right),$$

where $db \equiv -1 \pmod{p}$.

Further, consider the expression $\left(1+\left(\frac{z}{p}\right)\right)\left(\frac{z+d}{p}\right)$. If $z=0$, it is $\left(\frac{d}{p}\right)$; if z is a quadratic nonresidue, it is 0; if z is a quadratic residue, it is $2\left(\frac{z+d}{p}\right)=\left(\frac{y^2+d}{p}\right)+\left(\frac{(p-y)^2+d}{p}\right)$ where $y^2\equiv z \pmod p$. Hence

$$\sum_{y=0}^{p-1}\left(\frac{y^2+d}{p}\right)=\sum_{z=0}^{p-1}\left(1+\left(\frac{z}{p}\right)\right)\left(\frac{z+d}{p}\right)=\sum_{z=0}^{p-1}\left(\frac{z}{p}\right)\left(\frac{z+d}{p}\right)$$

since $\sum_{z=0}^{p-1}\left(\frac{z+d}{p}\right)=0$ by Proposition 8.2. If $z'\in\mathbb{Z}, zz'\equiv 1 \pmod p$ then $\left(\frac{z}{p}\right)=\left(\frac{z'}{p}\right)$ and thus

$$\begin{aligned}\sum_{z=0}^{p-1}\left(\frac{z}{p}\right)\left(\frac{z+d}{p}\right)&=\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)\left(\frac{z+d}{p}\right)=\sum_{z=1}^{p-1}\left(\frac{z'}{p}\right)\left(\frac{z+d}{p}\right)=\sum_{z=1}^{p-1}\left(\frac{1+dz'}{p}\right)\\&=\sum_{z'=1}^{p-1}\left(\frac{1+dz'}{p}\right)=\left(\frac{d}{p}\right)\sum_{z'=1}^{p-1}\left(\frac{-b+z'}{p}\right)=-\left(\frac{d}{p}\right)\left(\frac{-b}{p}\right)=-1\end{aligned}$$

which gives the desired identity. □

9 Primality tests

Theorem 9.1 (Wilson's Theorem)**.** *Let n be a positive integer. Then $(n-1)!\equiv -1 \pmod n$ iff n is a prime.*

Proof. Suppose $n=kl$ with $k,l>1$, then $k\mid(n-1)!$. If $(n-1)!\equiv -1 \pmod n$ then $(n-1)!\equiv -1 \pmod k$ and $-1\equiv 0 \pmod k$, a contradiction.

Let $n=p$ be a prime. Since the residue classes modulo p form a field, every non-zero residue $\overline{a}$ has a unique multiplicative inverse $\overline{a}^{-1}$. If $\overline{a}=\overline{a}^{-1}$ then $p\mid(a-1)(a+1)$, thus the only values of $\overline{a}$ for which $\overline{a}=\overline{a}^{-1}$ are $\overline{a}=\pm\overline{1}$. Therefore, with the exception of $1, p-1$, the factors in the expanded form of $(p-1)!$ can be arranged in disjoint pairs such that product of each pair is congruent to 1 modulo p. This proves the theorem. □

Alternative proof. Let $n=p$ be a prime. Then the polynomials $x^{p-1}-1$ and $(x-\overline{1})\cdots(x-\overline{p-1})$ over $\mathbb{Z}/p\mathbb{Z}$ are equal. Indeed, consider their difference. Each non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is its root, thus it has $p-1$ roots. On the other hand its degree is less then $p-1$, which implies that the difference is zero. The statement of the Theorem follows from considering the constant terms of the polynomials. □

Exercise 9.1. *Find the remainder of* 90! *divided by* 97.

Hint. Use Wilson's Theorem.

Fermat numbers and Pépin's primality test

Definition. The nth **Fermat number** is $F_n = 2^{2^n} + 1$.

Exercise 9.2. *Prove that 641 is a factor of F_5.*

Hint. Use the identities $641 = 27 \cdot 5 + 1$ and $641 = 2^4 + 5^4$.

Lemma 9.2. *If the number $2^k + 1$ is prime, then k is a power of 2.*

Proof. If k has an odd factor s and $k = rs$ then

$$a^{rs} + 1 = (a^r + 1)(a^{r(s-1)} - a^{r(s-2)} + \cdots + a^2 r - ar + 1).$$

□

Proposition 9.3 (Pépin's primality test)**.** *For $n \geq 1$, the nth Fermat number F_n is prime iff* $3^{(F_n-1)/2} \equiv -1 \mod F_n$.

Proof. Assume that $3^{(F_n-1)/2} \equiv -1 \mod F_n$. Then $3^{F_n-1} \equiv 1 \mod F_n$, thus the order of $\overline{3}$ in $(\mathbb{Z}/F_n\mathbb{Z})^*$ divides $F_n - 1 = 2^{2^n}$. On the other hand, this order does not divide $(F_n - 1)/2$, and therefore it must be equal to $F_n - 1$. Therefore $(\mathbb{Z}/F_n\mathbb{Z})^*$ contains at least $F_n - 1$ elements, and this can happen only if F_n is prime.

Conversely, assume that F_n is prime. Clearly $F_n \equiv (-1)^{2^n} + 1 \equiv 2 \mod 3$, and $(\frac{F_n}{3}) = -1$. Finally $(\frac{3}{F_n}) = (\frac{F_n}{3}) = -1$ by the law of quadratic reciprocity and $3^{(F_n-1)/2} \equiv (\frac{3}{F_n}) \mod F_n$ by Euler's criterion. □

F_0, F_1, F_2, F_3, F_4 are the only known prime Fermat numbers. Some Fermat numbers like F_{24} fail Pépin's test but no factors have been found yet.

Deterministic primality tests determine whether a number is prime or not *with certainty* (the sieve of Eratosthenes, the test based on Wilson's theorem, Pépin's primality test etc) but are often too computationally expensive to be practical. *Probabilistic* primality tests sort out composite numbers but allow an input number to be composite even if it passes the test (a *false positive*) with a small probability. Their advantage is computational efficiency.

Fermat primality test (不是完美的. 有合数可以通过; 但是很简单. 对大数很有效).

(1) choose a random integer a with $1 < a < n$;
(2) if the condition $a^{n-1} \equiv 1 \pmod{n}$ does not hold, then n is not prime

Definition. A **pseudoprime** or **Fermat's pseudoprime** to base a is a composite number n such that $a^{n-1} \equiv 1 \pmod{n}$.

Example. The number $91 = 7 \cdot 13$ is a pseudoprime to base 3 since $3^{90} \equiv 1 \pmod{91}$.

Definition. A **Carmichael number** is a composite number n such that $a^{n-1} \equiv 1 \pmod{n}$ for every a, $1 < a < n$ and coprime to n. ↖ 通过 Fermat test 的合数.

Proposition 9.4. *An integer n is a Carmichael number if and only if it is square-free and $p-1$ divides $n-1$ for every prime factor p of n.*

Proof. Suppose $n = p_1 \cdots p_s$ with $p_1, \ldots, p_h$ distinct primes. Let a be an integer with $1 < a < n$ coprime to $p_1, \ldots, p_s$. For any $1 \le i \le s$ the congruence $a^{p_i - 1} \equiv 1 \pmod{p_i}$ implies $a^{n-1} \equiv 1 \pmod{p_i}$ since $p_i - 1 \mid n - 1$. Then $a^{n-1} \equiv 1 \pmod{n}$.

Now assume $a^{n-1} \equiv 1 \pmod{n}$ for every a, $1 < a < n$ and coprime to n. If n is even then $-1 \equiv (n-1)^{n-1} \equiv 1 \pmod{n}$ whence $n = 2$, which is a contradiction since n is composite.

Let $n = p_1^{k_1} \cdots p_s^{k_s}$ be its canonical representation, $p_i \neq 2$. By Corollary 7.9 there are primitive roots a_i modulo $p_i^{k_i}$, $1 \le i \le s$. By the Chinese Remainder Theorem there exists $a \in \mathbb{Z}$ such that $a \equiv a_i \pmod{p_i^{k_i}}, 1 \le i \le s$. Further, $a^{n-1} \equiv 1 \pmod{n}$ implies $a_i^{n-1} \equiv a^{n-1} \equiv 1 \pmod{p_i^{k_i}}$. Since a_i is a primitive root modulo $p_i^{k_i}$, the order of a_i in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$ is $\varphi(p_i^{k_i}) = p_i^{k_i - 1}(p_i - 1)$ and thus $p_i^{k_i-1}(p_i - 1) \mid n - 1$. This readily implies $p_i - 1 \mid n - 1$. Finally if $k_i > 1$ then both $n - 1$ and n are divisible by p_i, a contradiction. □

Example. $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number, as 560 is divisible by $3 - 1 = 2, 11 - 1 = 10, 17 - 1 = 16$.

Exercise 9.3. *Find a Carmichael numbers in the interval* $(1700, 1800)$.

Miller–Rabin primality test

Fix an odd integer $n > 2$. Write $n = 2^s d + 1$ with odd d.

(1) choose a random integer a be coprime to n;
(2) verify that $a^d \equiv 1 \mod n$. If it does not hold, then n is not prime;
(3) verify that the congruence $a^{2^r d} \equiv -1 \mod n$ holds for some $0 \le r < s$. If it is not true, then n is not prime.

Proposition 9.5. *Any odd prime $n = p$ passes the Miller–Rabin test to any base a.*

Proof. First, remark that the only square roots of 1 modulo p are 1 and -1. Each term of the sequence $a^{2^s d}, a^{2^{s-1} d}, \cdots, a^{2d}, a^d$ is a square root of the preceding term. The first term is congruent to 1 modulo p by Fermat's little theorem, thus the second term is congruent to either 1 or -1 modulo p. If it is congruent to -1, we are done. Otherwise, it is congruent to 1 and the reasoning can be iterated. At the end, either one of the terms is congruent to -1, or all of them are congruent to 1, and in particular the last term a^d. □

Definition. A **strong pseudoprime** to base a is a composite number that passes the Miller–Rabin test to base a.

Example. Let $n = 3277 = 29 \cdot 113$, then $3276 = 2^2 \cdot 819$.

$$2^{819} \equiv 128 \mod 3277, \quad 2^{2 \cdot 819} \equiv -1 \mod 3277 - \text{passed}$$
$$3^{819} \equiv 2564 \mod 3277, \quad 3^{2 \cdot 819} \equiv 434 \mod 3277 - \text{failed}$$

A composite number n is a strong pseudoprime to at most one quarter of all bases below n; in particular there are no numbers that are strong pseudoprimes to all bases.

The first strong pseudoprime to base 2 is 2047; the first strong pseudoprimes to bases 2, 3, and 5 is greater than 2^{24} and there is no strong pseudoprime to base 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, and 37 less than 2^{64}.

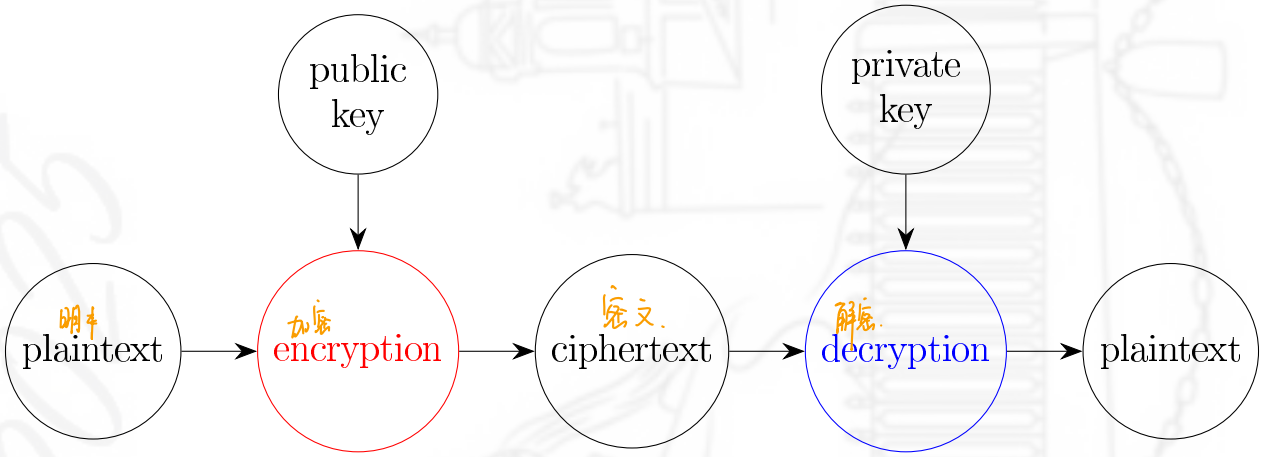
Exercise 9.4. *Show that every strong pseudoprime to base a is a pseudoprime to base a*

Exercise 9.5. *Determine if* 3281 *is a pseudoprime to base* 3*?*

Chapter II: Applications of number theory

10 Public-key cryptosystems. RSA algorithm

A *public-key cryptosystem* uses a *private key* that is kept secret and *a public key* which is freely provided to others. Messages encrypted with the public key are transmitted over an open channel and decrypted with the private key. The two keys have the property that, given the public key, it is computationally infeasible to derive the private key.



RSA algorithm

I. Key creation (Bob)

(a) Choose secret primes p and q, set $n = pq$;
(b) Select an integer $1 < e < \varphi(n)$ coprime to $\varphi(n)$;
(c) Calculate the multiplicative inverse d of e modulo $\varphi(n)$ (i.e., $ed \equiv 1 \pmod{\varphi(n)}$);
(d) Publish the public key (e, n);
(e) Keep secret the private key d.

Theorem 6.4 (Euler's Theorem). *Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and a, n are coprime. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Corollary 6.5 (Fermat's Little Theorem). *If p is prime, and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.*

Proof. If $p \mid a$, then $a^p \equiv 0 \pmod{p}$ and $a \equiv 0 \pmod{p}$. If $p \nmid a$, then by Euler's theorem, $a^{p-1} \equiv 1 \pmod{p}$. Multiplying both parts by a, one gets the required congruence. □

II. Encryption (Alice)

(a) Take a number (plaintext) m;
(b) Encrypt m using the public key: $c \equiv m^e \pmod{n}$;
(c) Send the cyphertext c to Bob.

III. Decryption (Bob)

(a) Receive c;

(b) Decrypt c using the private key: $c^d \equiv m^{ed} \equiv m \pmod{n}$.

An intruder who intercepts the cyphertext c and knows the public key (e, n), needs to find d such that $ed \equiv 1 \pmod{\varphi(n)}$ and therefore, $\varphi(n)$. Computation of $\varphi(n)$ is based on the prime factorization of n. Thus, decryption of the intercepted message requires prime factorization, which is time-consuming.

In implementation of RSA algorithm, not primes but strong pseudoprimes p, q are used.

11 Error-correcting codes. BCH code

Definition. Fix a finite set of symbols, which will be called an **alphabet.** In this course the alphabet is the elements of a finite field K (mainly $\mathbb{Z}/2\mathbb{Z}$). A **word** in the alphabet is a finite sequence of its elements. The **Hamming distance** between two words is the number of bits at which the corresponding symbols are different. The **weight** of a word is the number of its non-zero symbols.

A **code** is a set of words of equal length, its elements are called **codewords.** The **power** of the code is the number of its codewords. The **distance** of the code is the minimum Hamming distance between different codewords.

Codewords are transmitted over a noisy communication channel and the received words may differ from the transmitted ones.

Examples. 1. The code $\{000, 011, 101, 110\}$ has the distance 2 (the *parity bit code*)

2. The code $\{0000, 0101, 1010, 1111\}$ has the distance 2, the code $\{000000, 010101, 101010, 11111$ has the distance 3 (the *repetition code*)

3. The code $\{00000, 01101, 10110, 11011\}$ has the distance 3

When a transmission is received, the recipient will assume that the transmitted codeword is the closest (in the Hamming distance) to the received word.

Definition. A code can **correct** up to r errors if any codeword can be uniquely recovered if there are errors in no more than r positions in the received codeword.

Example. The code $\{000000, 010101, 101010, 111111\}$ corrects up to 1 error but can't correct 2 errors. Indeed, the word 011111 may be either 010101 or 111111 transmitted with ≤ 2 errors.

Proposition 11.1. *A code with distance d can correct up to $r = [\frac{d-1}{2}]$ errors.*

Proof. For each codeword, consider a set of words whose Hamming distance does not exceed r (= the closed balls of radius r centered at the codewords). These sets do not overlap since otherwise the distance between the corresponding codewords would be at most $2r < d$, which is impossible. Therefore, a word that differs from the codeword in no more than r bits lies exactly in one of such sets, and thus the codeword can be recovered unambiguously. □

Definition. The **linear code** generated by a matrix $A \in \mathrm{M}_{m,n}(K)$ consists of the codewords of the form $AX, X \in \mathrm{M}_{n,1}(K)$. The **polynomial code** generated by a polynomial $f \in K[x]_n$ consists of the words of length $m \geq n+1$, having the form $c_0 \cdots c_{m-1}$, where $f \mid \sum_{j=0}^{m-1} c_j x^j$.

Example. Consider the 6-bit polynomial code generated by $f(x) = x^3 + x + \overline{1}$ over $\mathbb{Z}/2\mathbb{Z}$. Its codewords are obtained be multiplying f by the polynomials of degree not greater than 2. For instance, $(x^3 + x + \overline{1})(x^2 + x + \overline{1}) = x^5 + x^4 + \overline{1}$ with corresponds to the codeword 100011. The code contains 8 codewords: $000000, 110100, 011010, 101110, 001101, 111001, 010111, 100011$.

Proposition 11.2. *1. The power of the linear code generated by a matrix A is $|K|^r$, where $r = \operatorname{rk} A$.*

2. A polynomial code is a particular case of a linear code.

3. The distance of a linear code is equal to the minimum weight of its non-zero codeword.

Proof. (1) The codewords of the linear code generated by $A \in \mathrm{M}_{m,n}(K)$ coincide with the subspace $\{AX \mid X \in \mathrm{M}_{n,1}(K)\}$, which is in turn equal to the span of the columns of A. Its dimension is r, thus this subspace contains $|K|^r$ elements.

(2) If a code is generated by a polynomial $f = \sum_{j=0}^{n} a_j x^j$, then for $g = \sum_{i=0}^{m-n-1} b_i x^i$ one has $fg = \sum_{\ell=0}^{m-1} (\sum_{j=0}^{n} a_j b_{\ell-j}) x^\ell$. Thus the code is generated by the matrix $A \in \mathrm{M}_{m,m-n}(K)$

$$A = \begin{pmatrix} a_0 & 0 & \cdots & 0 & 0 \\ a_1 & a_0 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ & & & a_0 & 0 \\ & & & a_1 & a_0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & a_n & a_{n-1} \\ 0 & 0 & \cdots & 0 & a_n \end{pmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} m-n-1 \\ \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} n \end{matrix}$$

(3) Let AX_1, AX_2 be two codewords at a distance d then the codeword $A(X_1 - X_2) = AX_1 - AX_2$ is of weight d. Conversely, if a codeword AX is of weight d, then it is at a distance d from of the codeword $0 \cdots 0$. □

Definition. Let L/K be an extension, $\alpha \in L$. A non-zero polynomial $f \in K[t]$ is called **minimal** for α if $f(\alpha) = 0$ and $\deg g \geq \deg f$ for any $g \in K[t]$ such that $g(\alpha) = 0$.

Proposition 11.3. *Let L/K be a field extension, $\alpha \in L$.*

Definition. If a subset K of a field L is a field with respect to the operations induced from L, then K is called a **subfield** of L and L is an **extension** of K (notation: L/K).
A **basis** of an extension L/K is a basis of L as a vector space over K. The **degree** of L/K is the dimension of L as a vector space over K (notation: $[L : K]$). An extension is **finite** if its degree is finite.

1. A minimal polynomial for α is irreducible.

2. *If f is a minimal polynomial for α and $g \in K[t], g(\alpha) = 0$, then $f \mid g$.*

3. *If $f \in K[t]$ is irreducible and $f(\alpha) = 0$, then f is a minimal polynomial for α*

4. *A minimal polynomial is uniquely defined up to associativity. A monic minimal polynomial is unique.*

Corollary 11.4. *If $f \in K[t]$ is a minimal polynomial for $\alpha \in L$, then* $\deg f \mid [L : K]$

Let $|K| = p^n$. Fix $d \leq p^n - 1$. Let α be a primitive element of K. Denote by $g_1, \ldots, g_{d-1} \in \mathbb{Z}/p\mathbb{Z}[x]$ minimal polynomials for $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ respectively and put $g = \operatorname{lcm}(g_1, \ldots, g_{d-1})$.

Note that $\alpha^{p^n-1} - 1 = 0$ for any $\alpha \in K^*$ by a corollary to Lagrange's theorem, whence $g_i \mid x^{p^n-1} - 1$ for any $1 \leq i \leq d-1$. Thus $g \mid x^{p^n-1} - 1$ and in particular $\deg g \leq p^n - 1$.

Proposition 11.5. *The distance of the polynomial code of length $p^n - 1$ generated by g is not less than d.*

Proof. Suppose there is a codeword with weight less than d. Then $g \mid f$ for some $f(x) = b_1 x^{s_1} + \cdots + b_{d-1} x^{s_{d-1}}$, where $0 \leq s_1 < \cdots < s_{d-1} \leq p^n - 2$ and $b_1, \ldots, b_{d-1} \in \mathbb{Z}/p\mathbb{Z}$. Then $f(\alpha) = f(\alpha^2) = \cdots = f(\alpha^{d-1}) = 0$, which gives

$$\begin{pmatrix} \alpha^{s_1} & \alpha^{s_2} & \cdots & \alpha^{s_{d-1}} \\ \alpha^{2s_1} & \alpha^{2s_2} & \cdots & \alpha^{2s_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-1)s_1} & \alpha^{(d-1)s_2} & \cdots & \alpha^{(d-1)s_{d-1}} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{d-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

The determinant of the above matrix can be calculated using the Vandermonde determinant:

$$\begin{vmatrix} \alpha^{s_1} & \alpha^{s_2} & \cdots & \alpha^{s_{d-1}} \\ \alpha^{2s_1} & \alpha^{2s_2} & \cdots & \alpha^{2s_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-1)s_1} & \alpha^{(d-1)s_2} & \cdots & \alpha^{(d-1)s_{d-1}} \end{vmatrix} = \alpha^{s_1+\cdots+s_{d-1}} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{s_1} & \alpha^{s_2} & \cdots & \alpha^{s_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-2)s_1} & \alpha^{(d-2)s_2} & \cdots & \alpha^{(d-2)s_{d-1}} \end{vmatrix}$$
$$= \alpha^{s_1+\cdots+s_{d-1}} \prod_{1 \leq i < j \leq d-1} (\alpha^{s_j} - \alpha^{s_i}).$$

Since α generates K^*, and $0 \leq s_i < s_j \leq p^n - 2$, this determinant is nonzero, which implies that the above linear system has only zero solution $b_1 = \cdots = b_{d-1} = 0$, which contradicts to our assumption. □

The code constructed above is called the **Bose—Chaudhuri—Hocquenghem code (BCH)**.

Example. Consider the case $p = 2, n = 4$ and $K = \mathbb{Z}/2\mathbb{Z}[t]/(t^4 + t + 1)$. Then $\alpha = \overline{t}$ is a primitive element of K. Indeed, $\operatorname{ord}\alpha \neq 1, 3, 5$, and hence, the order of α is 15. Next, we have

$$g_1(x) = g_2(x) = g_4(x) = g_8(x) = x^4 + x + \overline{1}$$
$$g_3(x) = g_6(x) = g_9(x) = g_{12}(x) = x^4 + x^3 + x^2 + x + \overline{1}$$
$$g_5(x) = g_{10}(x) = x^2 + x + \overline{1}$$
$$g_7(x) = g_{11}(x) = g_{13}(x) = g_{14}(x) = x^4 + x^3 + \overline{1},$$

We prove the first chain of equalities. Clearly $\alpha^4 + \alpha + \overline{1} = \overline{t}^4 + \overline{t} + \overline{1} = \overline{t^4 + t + 1} = \overline{0}$. Then $(\alpha^2)^4 + \alpha^2 + \overline{1} = (\alpha^4 + \alpha + \overline{1})^2 = \overline{0}$ and similarly $(\alpha^4)^4 + \alpha^4 + \overline{1} = (\alpha^8)^4 + \alpha^8 + \overline{1} = \overline{0}$.

It remains to show that there is no quadratic polynomial over $\mathbb{Z}/2\mathbb{Z}$ which has $\alpha, \alpha^2, \alpha^4, \alpha^8$ as its root. If $\overline{0} = c_2\alpha^2 + c_1\alpha + c_0$ for $c_2, c_1, c_0 \in \mathbb{Z}/2\mathbb{Z}$ then $t^4 + t + \overline{1} \mid c_2t^2 + c_1t + c_0$, whence $c_2 = c_1 = c_0 = \overline{0}$. If $\overline{0} = c_2\alpha^4 + c_1\alpha^2 + c_0 = c_2(\alpha + \overline{1}) + c_1\alpha^2 + c_0$, then $t^4 + t + \overline{1} \mid c_1t^2 + c_2t + (c_0 + c_2)$, whence $c_2 = c_1 = c_0 = \overline{0}$. If $\overline{0} = c_2\alpha^8 + c_1\alpha^4 + c_0 = c_2(\alpha + \overline{1})^2 + c_1\alpha^4 + c_0$, then $t^4 + t + \overline{1} \mid c_1t^4 + c_2t^2 + (c_0 + c_2)$, whence $c_2 = c_1 = c_0 = \overline{0}$. Finally, if $\overline{0} = c_2\alpha^{16} + c_1\alpha^8 + c_0 = c_2(\alpha + \overline{1})^4 + c_1(\alpha + \overline{1})^2 + c_0$, then $t^4 + t + \overline{1} \mid c_2t^4 + c_1t^2 + (c_0 + c_1 + c_2)$, whence $c_2 = c_1 = c_0 = \overline{0}$.

Now

$$\begin{aligned}
d = 2, 3 \qquad & g(x) = g_1(x) = x^4 + x + \overline{1} \\
d = 4, 5 \qquad & g(x) = g_1(x)g_3(x) = x^8 + x^7 + x^6 + x^4 + \overline{1} \\
d = 6, 7 \qquad & g(x) = g_1(x)g_3(x)g_5(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + \overline{1} \\
d = 8, \ldots, 15 \qquad & g(x) = g_1(x)g_3(x)g_5(x)g_7(x) = x^{14} + x^{13} + \cdots + \overline{1}.
\end{aligned}$$

Definition. . A code is **cyclic** if for any of its codewords $c_0c_1 \cdots c_{m-1}$ the word $c_{m-1}c_0c_1 \cdots c_{m-2}$ also belongs to the code.

Proposition 11.6. *The BCH code is cyclic.*

Proof. Denote $m = p^n - 1$. Each of $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ is a root of $x^m - 1$. Then Proposition 11.3 implies that the minimal polynomials $g_1, \ldots, g_{d-1}$ divide $x^m - 1$, and hence so does their least common multiple g. If $c_0c_1 \cdots c_{m-1}$ is a codeword, then $f_1 = c_0 + c_1x + \cdots + c_{m-1}x^{m-1}$ is divisible by g. We need to show that $f_2 = c_{m-1} + c_0x + \cdots + c_{m-2}x^{m-1}$ is also divisible by g, which follows from the equality $f_2 = xf_1 - c_{m-1}(x^m - 1)$. □

Exercise 11.1. *Prove the formulas for g_3, g_6, g_9, g_{12} from the above example.*

Exercise 11.2. *Consider the BCH code from the above example for $d = 5$.*

i) *Are* 110100010000001, 100000010001011 *its codewords?*

ii) *The received word* 101100000001010 *has errors in two bits. Find the original codeword.*

Exercise 11.3. *Let $p = 2, n = 5$ and $K = \mathbb{Z}/2\mathbb{Z}[t]/(t^5 + t^2 + \overline{1})$. Calculate the generator polynomials for BCH codes corresponding to $d = 1, \ldots 8$.*

Definition. The **linear code** generated by a matrix $A \in \mathrm{M}_{m,n}(K)$ consists of the codewords of the form $AX, X \in \mathrm{M}_{n,1}(K)$. The **polynomial code** generated by a polynomial $f \in K[x]_n$ consists of the words of length $m \geq n+1$, having the form $c_0 \cdots c_{m-1}$, where $f \mid \sum_{j=0}^{m-1} c_j x^j$.

Example. Consider the 6-bit polynomial code generated by $f(x) = x^3 + x + \overline{1}$ over $\mathbb{Z}/2\mathbb{Z}$. Its codewords are obtained be multiplying f by the polynomials of degree not greater than 2. For instance, $(x^3 + x + \overline{1})(x^2 + x + \overline{1}) = x^5 + x^4 + \overline{1}$ with corresponds to the codeword 100011. The code contains 8 codewords: $000000, 110100, 011010, 101110, 001101, 111001, 010111, 100011$.

Proposition 11.2. *1. The power of the linear code generated by a matrix A is $|K|^r$, where $r = \operatorname{rk} A$.*

2. A polynomial code is a particular case of a linear code.

3. The distance of a linear code is equal to the minimum weight of its non-zero codeword.

Proof. (1) The codewords of the linear code generated by $A \in \mathrm{M}_{m,n}(K)$ coincide with the subspace $\{AX \mid X \in \mathrm{M}_{n,1}(K)\}$, which is in turn equal to the span of the columns of A. Its dimension is r, thus this subspace contains $|K|^r$ elements.

(2) If a code is generated by a polynomial $f = \sum_{j=0}^{n} a_j x^j$, then for $g = \sum_{i=0}^{m-n-1} b_i x^i$ one has $fg = \sum_{\ell=0}^{m-1} (\sum_{j=0}^{n} a_j b_{\ell-j}) x^\ell$. Thus the code is generated by the matrix $A \in \mathrm{M}_{m,m-n}(K)$

$$A = \begin{pmatrix} a_0 & 0 & \cdots & 0 & 0 \\ a_1 & a_0 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ & & & a_0 & 0 \\ & & & a_1 & a_0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & a_n & a_{n-1} \\ 0 & 0 & \cdots & 0 & a_n \end{pmatrix}$$

(3) Let AX_1, AX_2 be two codewords at a distance d then the codeword $A(X_1 - X_2) = AX_1 - AX_2$ is of weight d. Conversely, if a codeword AX is of weight d, then it is at a distance d from of the codeword $0 \cdots 0$. □

Definition. Let L/K be an extension, $\alpha \in L$. A non-zero polynomial $f \in K[t]$ is called **minimal** for α if $f(\alpha) = 0$ and $\deg g \geq \deg f$ for any $g \in K[t]$ such that $g(\alpha) = 0$.

Proposition 11.3. *Let L/K be a field extension, $\alpha \in L$.*

Definition. If a subset K of a field L is a field with respect to the operations induced from L, then K is called a **subfield** of L and L is an **extension** of K (notation: L/K).
A **basis** of an extension L/K is a basis of L as a vector space over K. The **degree** of L/K is the dimension of L as a vector space over K (notation: $[L : K]$). An extension is **finite** if its degree is finite.

1. A minimal polynomial for α is irreducible.

2. *If f is a minimal polynomial for α and $g \in K[t], g(\alpha) = 0$, then $f \mid g$.*

3. *If $f \in K[t]$ is irreducible and $f(\alpha) = 0$, then f is a minimal polynomial for α*

4. *A minimal polynomial is uniquely defined up to associativity. A monic minimal polynomial is unique.*

Corollary 11.4. *If $f \in K[t]$ is a minimal polynomial for $\alpha \in L$, then* $\deg f \mid [L : K]$

Let $|K| = p^n$. Fix $d \leq p^n - 1$. Let α be a primitive element of K. Denote by $g_1, \ldots, g_{d-1} \in \mathbb{Z}/p\mathbb{Z}[x]$ minimal polynomials for $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ respectively and put $g = \operatorname{lcm}(g_1, \ldots, g_{d-1})$.

Note that $\alpha^{p^n-1} - 1 = 0$ for any $\alpha \in K^*$ by a corollary to Lagrange's theorem, whence $g_i \mid x^{p^n-1} - 1$ for any $1 \leq i \leq d-1$. Thus $g \mid x^{p^n-1} - 1$ and in particular $\deg g \leq p^n - 1$.

Proposition 11.5. *The distance of the polynomial code of length $p^n - 1$ generated by g is not less than d.*

Proof. Suppose there is a codeword with weight less than d. Then $g \mid f$ for some $f(x) = b_1 x^{s_1} + \cdots + b_{d-1} x^{s_{d-1}}$, where $0 \leq s_1 < \cdots < s_{d-1} \leq p^n - 2$ and $b_1, \ldots, b_{d-1} \in \mathbb{Z}/p\mathbb{Z}$. Then $f(\alpha) = f(\alpha^2) = \cdots = f(\alpha^{d-1}) = 0$, which gives

$$\begin{pmatrix} \alpha^{s_1} & \alpha^{s_2} & \cdots & \alpha^{s_{d-1}} \\ \alpha^{2s_1} & \alpha^{2s_2} & \cdots & \alpha^{2s_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-1)s_1} & \alpha^{(d-1)s_2} & \cdots & \alpha^{(d-1)s_{d-1}} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{d-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

The determinant of the above matrix can be calculated using the Vandermonde determinant:

$$\begin{vmatrix} \alpha^{s_1} & \alpha^{s_2} & \cdots & \alpha^{s_{d-1}} \\ \alpha^{2s_1} & \alpha^{2s_2} & \cdots & \alpha^{2s_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-1)s_1} & \alpha^{(d-1)s_2} & \cdots & \alpha^{(d-1)s_{d-1}} \end{vmatrix} = \alpha^{s_1+\cdots+s_{d-1}} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{s_1} & \alpha^{s_2} & \cdots & \alpha^{s_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-2)s_1} & \alpha^{(d-2)s_2} & \cdots & \alpha^{(d-2)s_{d-1}} \end{vmatrix}$$
$$= \alpha^{s_1+\cdots+s_{d-1}} \prod_{1 \leq i < j \leq d-1} (\alpha^{s_j} - \alpha^{s_i}).$$

Since α generates K^*, and $0 \leq s_i < s_j \leq p^n - 2$, this determinant is nonzero, which implies that the above linear system has only zero solution $b_1 = \cdots = b_{d-1} = 0$, which contradicts to our assumption. □

The code constructed above is called the **Bose—Chaudhuri—Hocquenghem code (BCH)**.

Example. Consider the case $p = 2, n = 4$ and $K = \mathbb{Z}/2\mathbb{Z}[t]/(t^4 + t + 1)$. Then $\alpha = \bar{t}$ is a primitive element of K. Indeed, $\operatorname{ord}\alpha \neq 1, 3, 5$, and hence, the order of α is 15. Next, we have

$$g_1(x) = g_2(x) = g_4(x) = g_8(x) = x^4 + x + \bar{1}$$
$$g_3(x) = g_6(x) = g_9(x) = g_{12}(x) = x^4 + x^3 + x^2 + x + \bar{1}$$
$$g_5(x) = g_{10}(x) = x^2 + x + \bar{1}$$
$$g_7(x) = g_{11}(x) = g_{13}(x) = g_{14}(x) = x^4 + x^3 + \bar{1},$$

We prove the first chain of equalities. Clearly $\alpha^4 + \alpha + \bar{1} = \bar{t}^4 + \bar{t} + \bar{1} = \overline{t^4 + t + 1} = \bar{0}$. Then $(\alpha^2)^4 + \alpha^2 + \bar{1} = (\alpha^4 + \alpha + \bar{1})^2 = \bar{0}$ and similarly $(\alpha^4)^4 + \alpha^4 + \bar{1} = (\alpha^8)^4 + \alpha^8 + \bar{1} = \bar{0}$.

It remains to show that there is no quadratic polynomial over $\mathbb{Z}/2\mathbb{Z}$ which has $\alpha, \alpha^2, \alpha^4, \alpha^8$ as its root. If $\bar{0} = c_2\alpha^2 + c_1\alpha + c_0$ for $c_2, c_1, c_0 \in \mathbb{Z}/2\mathbb{Z}$ then $t^4 + t + \bar{1} \mid c_2t^2 + c_1t + c_0$, whence $c_2 = c_1 = c_0 = \bar{0}$. If $\bar{0} = c_2\alpha^4 + c_1\alpha^2 + c_0 = c_2(\alpha + \bar{1}) + c_1\alpha^2 + c_0$, then $t^4 + t + \bar{1} \mid c_1t^2 + c_2t + (c_0 + c_2)$, whence $c_2 = c_1 = c_0 = \bar{0}$. If $\bar{0} = c_2\alpha^8 + c_1\alpha^4 + c_0 = c_2(\alpha + \bar{1})^2 + c_1\alpha^4 + c_0$, then $t^4 + t + \bar{1} \mid c_1t^4 + c_2t^2 + (c_0 + c_2)$, whence $c_2 = c_1 = c_0 = \bar{0}$. Finally, if $\bar{0} = c_2\alpha^{16} + c_1\alpha^8 + c_0 = c_2(\alpha + \bar{1})^4 + c_1(\alpha + \bar{1})^2 + c_0$, then $t^4 + t + \bar{1} \mid c_2t^4 + c_1t^2 + (c_0 + c_1 + c_2)$, whence $c_2 = c_1 = c_0 = \bar{0}$.

Now

$$\begin{aligned}
d = 2, 3 \quad & g(x) = g_1(x) = x^4 + x + \bar{1} \\
d = 4, 5 \quad & g(x) = g_1(x)g_3(x) = x^8 + x^7 + x^6 + x^4 + \bar{1} \\
d = 6, 7 \quad & g(x) = g_1(x)g_3(x)g_5(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + \bar{1} \\
d = 8, \ldots, 15 \quad & g(x) = g_1(x)g_3(x)g_5(x)g_7(x) = x^{14} + x^{13} + \cdots + \bar{1}.
\end{aligned}$$

Definition. . A code is **cyclic** if for any of its codewords $c_0c_1 \cdots c_{m-1}$ the word $c_{m-1}c_0c_1 \cdots c_{m-2}$ also belongs to the code.

Proposition 11.6. *The BCH code is cyclic.*

Proof. Denote $m = p^n - 1$. Each of $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ is a root of $x^m - 1$. Then Proposition 11.3 implies that the minimal polynomials $g_1, \ldots, g_{d-1}$ divide $x^m - 1$, and hence so does their least common multiple g. If $c_0c_1 \cdots c_{m-1}$ is a codeword, then $f_1 = c_0 + c_1x + \cdots + c_{m-1}x^{m-1}$ is divisible by g. We need to show that $f_2 = c_{m-1} + c_0x + \cdots + c_{m-2}x^{m-1}$ is also divisible by g, which follows from the equality $f_2 = xf_1 - c_{m-1}(x^m - 1)$. □

Exercise 11.1. *Prove the formulas for g_3, g_6, g_9, g_{12} from the above example.*

Exercise 11.2. *Consider the BCH code from the above example for $d = 5$.*

i) *Are* 110100010000001, 100000010001011 *its codewords?*

ii) *The received word* 101100000001010 *has errors in two bits. Find the original codeword.*

Exercise 11.3. *Let $p = 2, n = 5$ and $K = \mathbb{Z}/2\mathbb{Z}[t]/(t^5 + t^2 + \bar{1})$. Calculate the generator polynomials for BCH codes corresponding to $d = 1, \ldots 8$.*