BIE-DML - Discrete Mathematics and Logic

Tutorial 7

Number Theory – Integers and primes, modular arithmetics and congruences

Francesco Dolce, Eva Pernecká and Jitka Rybníčková

Faculty of Information Technology
Czech Technical University in Prague

Winter semester 2024/2025

updated: 21/10/2024, 14:03

7.1 Introduction

7.1.1 Integers and primes

In this section we present some elements of number theory Let us stress that in the whole section we work exclusively with integers (and their subsets).

$\mathbb{Z}$ denotes the set of integers, i.e., $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, on which the operations of addition and multiplication are defined as usual. To define subtraction, we simply use addition of opposite numbers. Similarly, if we want to introduce division, we use multiplication. However, it is necessary to define what exactly should the division of two integers express. We call this operation *division with remainder* and we call the property meaning that one number divides another with zero remainder, *divisibility*. Let us define it properly.

Definition 7.1 (Divisibility)**.** A number a **divides** a number b (or, b is **divisible** by a) if there is an integer k such that $b = k \cdot a$. This fact is denoted by $a \mid b$. Similarly, if a does not divide b, we write $a \nmid b$. The number a is called a **divisor** (or a **factor**) of the number b and, conversely, b is called a **multiple** of a.

Remark 7.2. The number 1 is a divisor of any integer by this definition. Moreover 0 is divisible by any integer, i.e., 0 is divisible also by 0 since $0 = k \cdot 0$.

Theorem 7.3 (Properties of divisibility)**.** *Consider $a, b, c \in \mathbb{Z}$.*

- *If $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.*
- *If $a \mid b$ then $a \mid (nb)$ for every $n \in \mathbb{Z}$.*
- *$a \mid b$ if and only if $|a| \mid |b|$.*
- *If $a \mid b$ and $b \neq 0$ then $|\,a\,| \leq |\,b\,|$.*
- *$a \mid b \wedge a \mid c$ if and only if $a \mid (mb + nc)$ for every $m, n \in \mathbb{Z}$.*
- *If $a \mid (b + c) \wedge a \mid b$ then $a \mid c$.*

Theorem 7.4 (The Division Algorithm)**.** *Let $a \in \mathbb{Z},\ b \in \mathbb{N}$. Then there exist unique $q \in \mathbb{Z}$ and unique $r \in \mathbb{N}_0$, with $0 \leq r < |\,b\,|$, such that*

$$a = b \cdot q + r.$$

*The integer q is called the **quotient** of a, b, and r is called the **remainder** of the division of a by b. We also write $r = a \mod b$ (operation modulo).*

Having already defined the division we can define more:

Definition 7.5. Let $a, b \in \mathbb{Z}$, then:

- A positive integer d is a common divisor of a, b, if $d \mid a$ and $d \mid b$.
- A positive integer d is the **greatest common divisor** of a, b (and we write $d = \gcd(a, b)$) if at least one of a, b is nonzero and d is the greatest of all divisors of a, b, i.e., for every $c \in \mathbb{N}$, if $c \mid a$ and $c \mid b$, then also $c \mid d$.
- If $\gcd(a, b) = 1$ then positive integers a, b are **relatively prime** (or, **co-prime**).
- $\gcd(0, 0)$ is explicitly defined as 0.
- A positive integer ℓ is a common multiple of a, b if $a \mid \ell$ and $b \mid \ell$.

- A positive integer ℓ is the **least common multiple** of a, b (and we write $\ell = \operatorname{lcm}(a, b)$) if both a, b are nonzero and ℓ is the least of all multiples of a, b, i.e., for every $c \in \mathbb{N}$, if $a \mid c \wedge b \mid c$ then also $\ell \mid c$. If $a = 0$ or $b = 0$ then $\operatorname{lcm}(a, b) = 0$.

Theorem 7.6 (Properties of gcd and lcm)**.** *Let $a, b \in \mathbb{Z}$, then:*

- *If n is a common multiple of a, b, then $\operatorname{lcm}(a, b)$ divides n.*
- *If $a|n$ and $b|n$, then $\operatorname{lcm}(a, b)|n$.*
- $\gcd(a, b) = \gcd(|a|, |b|)$ *and* $\operatorname{lcm}(a, b) = \operatorname{lcm}(|a|, |b|)$.
- *Denote $d = \gcd(a, b)$. Then* $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
- $\gcd(a + cb, b) = \gcd(a, b)$ *for any $c \in \mathbb{Z}$.*
- *If $a|bc$ for some $c \in \mathbb{Z}$ and a, b are co-prime (i.e.,* $\gcd(a, b) = 1$*), then $a|c$.*
- *The greatest common divisor of positive integers a, b is the least positive integer which is a linear combination of a, b. Very often you can find this fact named by French mathematician Étienne Bézout –* ***Bézout's identity****:*

$$gcd(a, b) = d = \alpha \cdot a + \beta \cdot b\,,$$

where α, β are integer coefficients of this linear combination.

Primes and factorization

Definition 7.7. A positive integer $p > 1$ is a **prime** if p is divisible only by 1 and p.
The **factorization** of a positive integer $n > 1$ is the identity

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k},$$

where $k \geq 1$ is an integer, $p_1 < p_2 < \cdots < p_k$ are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers.

Theorem 7.8. *The set of all primes is infinite.*

Theorem 7.9 (Fundamental Theorem of Number Theory)**.** *Every positive integer $n \geq 2$ can be uniquely represented as the product of prime numbers. This unique form is called* ***canonical factorization*** *of n (or* ***prime factorization*** *of n).*

Corollary 7.10. *Let p be a prime and let $p \mid (a_1 \cdot a_2 \cdots a_k)$, where a_i is a non-negative integer for every $i = 1, \ldots, k$. Then there is a_j, $1 \leq j \leq k$, such that $p \mid a_j$.*

Proposition 7.11. *Consider two numbers $a, b \in \mathbb{N}$ and the factorizations of a, b of the form*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \qquad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k},$$

where p_i are primes (here, we allow possible zero exponent) less or equal to a, b. Then

$$\gcd(a, b) = p_1^{min\{\alpha_1, \beta_1\}} \cdot p_2^{min\{\alpha_2, \beta_2\}} \cdots p_k^{min\{\alpha_k, \beta_k\}}.$$

Similarly,

$$\operatorname{lcm}(a, b) = p_1^{max\{\alpha_1, \beta_1\}} \cdot p_2^{max\{\alpha_2, \beta_2\}} \cdots p_k^{max\{\alpha_k, \beta_k\}}.$$

Corollary 7.12.

$$\operatorname{lcm}(a, b) = \frac{|a| \cdot |b|}{\gcd(a, b)} \qquad \forall\ a, b \in Z \setminus \{0\}.$$

Eukleid's algorithm

Eukleid's algorithm (or, Euclid's algorithm, EA) is a very old algorithm to find the greatest common divisor of two positive integers efficiently (i.e., without factorization).

Theorem 7.13. *Let a, b be two positive integers s.t. $a \geq b > 0$. Consider the sequence $\{r_n\}_{n=0}^{k+1}$ of decreasing remainders defined by*

$$r_{n+2} = r_n \mod r_{n+1}$$

with initial conditions $r_0 = a, r_2 = 1$, where $r_{k+1} = 0$ (if $k > 0$) is the first zero element of this sequence. Then the last nonzero element r_k (i.e., the last nonzero remainder) is the greatest common divisor of a, b. That is, $\gcd(a, b) = r_k$.

Moreover, there is an extended version of Eukleid's algorithm (or, Euclid's, EEA) which generates the integer coefficients α, β of Bézout's identity:

$$gcd(a, b) = d = \alpha \cdot a + \beta \cdot b.$$

Let us introduce two implementations of EEA – in a table and in a matrix.

Algorithm 7.14 (EEA in table)**.**

1. Consider $a \geq b > 0$. Then set $r_0 := a$, $r_1 = b$. Denote the table header as r_i, α_i, β,q_i.
2. Fill the first row of the table representing r_0, α_0, β_0, q_0 with values a, 1, 0, $-$ (which in fact means $r_0 = 1 \cdot a + 0 \cdot b$).
3. Fill the next row r_1, α_1, β_1, q_1 with values: b, 0, 1, $\left\lfloor \frac{a}{b} \right\rfloor$ (which means $r_1 = 0 \cdot a + 1 \cdot b$ and integer quotient $q_1 = a \mod b$).
4. If $i \geq 2$, then set
$$r_i := r_{i-2} - q_{i-1} \cdot r_{i-1}\,.$$
If $r_i \neq 0$ then use the following formulas to fill in this row:
$$\begin{aligned} \alpha_i &:= & \alpha_{i-2} - q_{i-1} \cdot \alpha_{i-1} \\ \beta_i &:= & \beta_{i-2} - q_{i-1} \cdot \beta_{i-1} \\ q_i &:= & \lfloor r_{i-1}/r_i \rfloor \end{aligned}$$
5. If $r_i \neq 0$, repeat step 4 for the next row ($i := i + 1$). If $r_i = 0$, set $k = i - 1$ and stop.

The greatest common divisor is in the second to last row of the table:

$$\gcd(a, b) = r_k, \quad \alpha = \alpha_k, \quad \beta = \beta_k.$$

Moreover, α, β are the coefficients of the linear combination $\gcd(a, b) = \alpha \cdot a + \beta \cdot b$. Beware of the order of a, b.

r_i	α_i	β_i	q_i
a	1	0	$-$
b	0	1	$q_1 = \lfloor \frac{a}{b} \rfloor$
$r_2 = a - q_1 \cdot b$	$1 - q_1 \cdot 0$	$0 - q_2 \cdot 1$	q_2
$\ldots$	$\ldots$	$\ldots$	$\ldots$
$r_k = \gcd(a, b)$	α	β	q_k
$r_{k+1} = 0$	$-$	$-$	$-$

EEA can be also implemented as a special Gaussian elimination on matrix 2×3:

Algorithm 7.15 (EEA in matrix)**.**

1. The first column of the matrix consists of a, b, where $a \geq b$.
2. After the first column, write the 2×2-identity matrix.
3. Eliminate: Subtract a multiple of the second row from the first one such that the result is a remainder, i.e., $a_{1,1} \mod a_{2,1}$. Write the eliminated first row to the second row and the previously second row write as a first row of the new matrix.
4. Repeat step 3 until the value of $a_{2,1}$ is 0.

Results in the matrix:

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \begin{array}{l} \leftarrow + \\ \leftarrow -q \end{array} \sim \begin{pmatrix} b & 0 & 1 \\ (a \mod b) & 1 & -q \end{pmatrix} \sim \cdots \text{ modif. GEM } \cdots \sim \begin{pmatrix} \gcd(a,b) & \alpha & \beta \\ 0 & x' & y' \end{pmatrix},$$

where α, β are the coefficients of linear combination $gcd(a, b) = \alpha \cdot a + \beta \cdot b$. Beware of the order of a, b!

Diophantine equations

An equation $ax + by = c$ with unknowns x, y and $a, b, c \in \mathbb{Z}$ is called a (linear) Diophantine equation, if the only solutions of interest are the integers ones (i.e., $x, y \in \mathbb{Z}$).

Theorem 7.16 (The existence of a solution)**.** *Let $d = \gcd(|a|, |b|)$ for a Diophantine equation $ax+by = c$. Then*

- *the equation has no solution in $\mathbb{Z}$ iff d does NOT divide c.*
- *the equation has (at least one) solution in $\mathbb{Z}$ iff d divides c.*

Therefore, we are able to decide when a solution exists. But are we able to construct it?

Algorithm 7.17 (Finding solution of $ax + by = c$)**.**

1. There is no solution if c is not a multiple of $\gcd(a, b)$.
2. If c is a multiple of $\gcd(a, b)$, then find $\alpha, \beta \in \mathbb{Z}$ such that $\gcd(a, b) = \alpha \cdot a + \beta \cdot b$ using EEA.
3. Multiply the Bézout's identity from step 2. by number $\dfrac{c}{\gcd(a,b)}$, so that

$$gcd(a, b) = \alpha \cdot a + \beta \cdot b \quad \Rightarrow \quad c = \gcd(a, b) \cdot \frac{c}{\gcd(a,b)} = \alpha \cdot \frac{c}{\gcd(a,b)} \cdot a + \beta \cdot \frac{c}{\gcd(a,b)} \cdot b;$$

thus the numbers

$$x = \alpha \cdot \frac{c}{\gcd(a,b)} \qquad \text{and} \qquad y = \beta \cdot \frac{c}{\gcd(a,b)}$$

are solutions of the given Diophantine equation.

Having found some solution $(x, y) \in \mathbb{Z}^2$ of $ax + by = c$, we can easily obtain other solutions using zero addition cleverly:

$$\begin{aligned} c &= ax + by \\ &= ax + by + (ab - ab) \\ &= a(x + b) + b(y - a)\,, \end{aligned}$$

thus, the pair $(x + b, y - a)$ is a solution as well. This idea can be applied many times, therefore it is no surprise that the difference of any two solutions of the type $(k \cdot b, -k \cdot a)$, with $k \in \mathbb{Z}$, are solutions of the associated homogeneous equation.

Definition 7.18. Given a Diophantine equation $ax+by=c$, the equation $ax+by=0$ is an associated homogeneous equation of the original one.

Theorem 7.19. *Consider a Diophantine equation $ax+by=c$ and $\gcd(a,b)\,|\,c$. Then:*

- *If $(x_p,y_p)\in\mathbb{Z}^2$ is some solution (a particular solution) and $(x_h,y_h)\in\mathbb{Z}^2$ is some solution of the associated homogeneous equation, then $(x,y)=(x_p,y_p)+(x_h,y_h)\in\mathbb{Z}^2$ is also a solution of the given Diophantine equation.*
- *Consider a homogeneous Diophantine equation $ax+by=0$ where $a,b\in\mathbb{Z}$ are co-prime. Then all solutions are of the form $(x,y)=k\cdot(b,-a)$, where $k\in\mathbb{Z}$.*
- *Consider $a,b\in\mathbb{Z}$ not co-prime, i.e., with $\gcd(a,b)>1$. Then the homogeneous equation should be simplified to*

  $$\frac{a}{\gcd(a,b)}\cdot x+\frac{b}{\gcd(a,b)}\cdot y=0$$

  (both coefficients are now co-prime integers, see Theorem 7.6). Then every solution is of type $(x,y)=k\cdot\left(\frac{b}{\gcd(a,b)},\frac{-a}{\gcd(a,b)}\right)$ for $k\in\mathbb{Z}$.

We can summarize the items above as follows: Consider $\alpha,\beta\in\mathbb{Z}$ and $\gcd(a,b)=a\cdot\alpha+b\cdot\beta$, where $\gcd(a,b)\,|\,c$. Then the solution set of a Diophantine equation $ax+by=c$ is

$$\left\{\left(\alpha\cdot\frac{c}{\gcd(a,b)}+k\frac{b}{\gcd(a,b)},\beta\cdot\frac{c}{\gcd(a,b)}-k\frac{a}{\gcd(a,b)}\right)\;;\;k\in\mathbb{Z}\right\}.$$

7.1.2 Modular arithmetic

In this section we introduce modular arithmetic and linear congruences.

Powers and inversions

For a given positive integer m we will denote $\mathbb{Z}_m$ (or, $\mathbb{Z}\mod m$) the set of integers modulo m. The most common notation is

$$\mathbb{Z}_m=\{0,1,2\ldots,m-1\}.$$

Definition 7.20. In this structure, every $b\in\mathbb{Z}$ is replaced by its remainder $r\in\mathbb{Z}_m=\{0,1,\ldots,m-1\}$ of b when divided by m (i.e., $b \mod m$).

We define arithmetic on the set $\mathbb{Z}_m$. When adding or multiplying, every number (remainder) of $\mathbb{Z}_m$ represents all integers equivalent to it*.

- $a+b$ in $\mathbb{Z}_m$ is performed as a sum of two integers, only the result is "moduled" by modulus m, i.e., the result is divided by m and its remainder is returned.
- $a\cdot b$ is computed in the same way.

Both operations (addition and multiplication) possess the same properties as in $\mathbb{Z}$ – associativity, commutativity and distributivity – which allows us to use brackets and change the order of summands/factors in $\mathbb{Z}_m$. We can also "module" during the operations of addition and multiplication, not only "at the end" of the process. This way we will never work with unnecessarily big numbers.

Formally, we can define the equivalence relation $\equiv \pmod m$ (or $\equiv_m$) on $\mathbb{Z}$ as follows.

*This is a binary relation on set $\mathbb{Z}$ (stay tuned for Tutorial 8), as a property of two numbers having the same remainder after division by m.

Definition 7.21 (Congruence)**.** Let $a, b, m \in \mathbb{Z}$, where $m > 1$. If $m|(a-b)$, then a is congruent with b modulo m, denoted by $a \equiv b \pmod{m}$ (or, $a = b \pmod{m}$). If $m \nmid (a-b)$, then a is not congruent with b modulo m, denoted by $a \not\equiv b \pmod{m}$.

The set $\mathbb{Z}/\equiv_m = \mathbb{Z}_m$ can be expressed by different representatives of classes of equivalence, e.g.,:

$$\begin{aligned}\mathbb{Z}_m &= \{0, 1, 2, \ldots, m-1\} \\ &= \{m, m+1, m+2, \ldots, 2m-1\} \\ &= \{k \cdot m, k \cdot m + 1, k \cdot m + 2, \ldots, 2k \cdot m - 1\} \\ &= \{-m, -m+1, -m+2, \ldots, -1\} \\ &= \cdots .\end{aligned}$$

Thus, we can work with any number with the same remainder modulo m. E.g.,

$$m - 1 \equiv 2m - 1 \equiv 3m - 1 \equiv -1 \equiv -2m - 1 \equiv -3m - 1 \pmod{m}.$$

This can simplify calculations, as in the following example.

Example 7.22. Evaluate this expression in the standard arithmetic of $\mathbb{Z}$ and **then** find the representative modulo 23. Compare with calculations done directly in $\mathbb{Z}_{23}$.

$$\begin{aligned}(3 \cdot 5 \cdot 24 + 4 \cdot 13 \cdot 5 + 9 \cdot 5) \cdot 22 &\equiv (360 + 260 + 45) \cdot 22 \pmod{23} \\ &\equiv 665 \cdot 22 \pmod{23} \\ &\equiv 14630 \pmod{23} \\ &\equiv 2 \pmod{23} \\ &\textit{versus} \\ (3 \cdot 5 \cdot 24 + 4 \cdot 13 \cdot 5 + 9 \cdot 5) \cdot 22 &\equiv (3 \cdot 5 \cdot 1 + 4 \cdot 13 \cdot 5 + 9 \cdot 5)(-1) \pmod{23} \\ &\equiv (15 + 6 \cdot 5 + (-1))(-1) \pmod{23} \\ &\equiv (15 + 7 - 1)(-1) \pmod{23} \\ &\equiv 21(-1) \pmod{23} \\ &\equiv (-2)(-1) \pmod{23} \\ &\equiv 2 \pmod{23}\,.\end{aligned}$$

The latter seems to be longer but we are only working with small numbers so the result can be obtained without any extra electronic help.

Remark 7.23. Consider $a, b, c, d, m \in \mathbb{Z}$, with $m \geq 2$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then also

$$\begin{aligned}a + c &\equiv b + d \pmod{m}\,, \\ a - c &\equiv b - d \pmod{m}\,, \\ a \cdot c &\equiv b \cdot d \pmod{m}\,.\end{aligned}$$

Remark: We cannot reduce the congruence as in standard arithmetic. We need to apply the following rule:

$$a \cdot c \equiv b \cdot c \pmod{m} \quad \Rightarrow \quad a \equiv b \left(\mathrm{mod}\, \frac{m}{\gcd(c, m)}\right),$$

thus we change the modulus as well!

$\mathbb{Z}_m$ has (compared to $\mathbb{Z}$) this additional property – the existence of multiplicative inverse elements.

Theorem 7.24 (The Existence of Multiplicative Inverse in $\mathbb{Z}_m$)**.**
If $a \neq 0$ is an arbitrary number in $\mathbb{Z}_m$, then there is a unique number $x \in \mathbb{Z}_m$, such that

$$a \cdot x \equiv x \cdot a \equiv 1 \pmod{m} \qquad \Longleftrightarrow \qquad \gcd(a, m) = 1.$$

The number x is called a multiplicative inverse of a modulo m and is denoted by $x \equiv a^{-1} \pmod{m}$ (or, $x = a^{-1}$ in $\mathbb{Z}_m$).

If m is prime, then the equation has a solution for every $a \neq 0$ in $\mathbb{Z}_m$ (i.e., an inverse element exists for any nonzero $a \in \mathbb{Z}_m$).

We will practise the finding of inverse elements in the exercises below.

The last operation we define for $\mathbb{Z}_m$ is the power. This can be inherited from $\mathbb{Z}$ as well (only "modulo" the result), however, there are better methods in modular arithmetic. We will practise it using two theorems.

Theorem 7.25 (Fermat's Little Theorem (FLT))**.** *Let p be a prime. If $a \in \mathbb{N}$, then $a^p \equiv a \pmod{p}$.*

We will use this version of the theorem: If a prime p is co-prime with a, then

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

By this theorem, we can reduce exponentials by multiples of $p - 1$.

We can reduce the exponent for non-prime modulus as well. We need to use a more general theorem than Fermat's Little Theorem: Euler's Theorem.

Theorem 7.26 (Euler's Theorem)**.** *Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. If $\gcd(m, a) = 1$ then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}\,,$$

where $\varphi(m)$ is Euler's totient function.

Euler's totient function is difficult to evaluate. By the definition, $\varphi(m)$ is the number of all positive integers less than or equal to m co-prime with m. The properties of this function are:

- if $p \in \mathbb{N}$ is a prime then $\varphi(p) = p - 1$;
- if $p \in \mathbb{N}$ is a prime then $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$;
- if $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$, then $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$;
- if $m \in \mathbb{N}$ has prime factorization $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k}$, then

$$\begin{aligned}\varphi(m) &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\ &= m \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right),\end{aligned}$$

  where $k \geq 1$ is a non-negative integer, $p_1 < p_2 < \cdots < p_k$ are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers.

Linear congruences, systems of linear congruences

In the previous section, we presented the greatest common divisor of integers a, b (that we denoted $\gcd(a, b)$) and the Eukleid's algorithm by which gcd can be calculated. An extended version of this algorithm allowed us to find coefficients in Bézout's identity, which has an extensive application in the number theory. Recall that Bézout's identity is given as

$$\gcd(a, b) = a \cdot x + b \cdot y$$

where x, y are integers.

Theorem 7.27 (Existence and number of solutions for congruences Theorem)**.** *Let $a, b, m \in \mathbb{Z}$, with $m > 1$. A linear congruence*

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

has $\gcd(a, m)$ solutions iff $\gcd(a, m)|b$. Otherwise, there are no solutions. All solutions in $\mathbb{Z}_m$ can be obtained by the formula

$$x \equiv x_0 + k \cdot \frac{m}{\gcd(a, m)} \pmod{m},$$

where k is an arbitrary integer and given x_0 there is a y_0 such that the pair (x_0, y_0) is a solution of the equation

$$ax_0 + my_0 = b.$$

Furthermore, $k \in \mathbb{Z}$ can be restricted. There are only finitely many solutions in $\mathbb{Z}_m$, namely $\gcd(a, m)$ elements of $\mathbb{Z}_m$. The set of all solutions of a congruence $a \cdot x \equiv b \pmod{m}$ is given as

$$\left\{ x_0 + k \cdot \frac{m}{\gcd(a, m)} \pmod{m} \ : \ k \in \{0, 1, \ldots, \gcd(a, m) - 1\} \right\}.$$

Theorem 7.28 (Chinese Remainder Theorem (ChRTh))**.** *Consider a system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots \\ x &\equiv a_N \pmod{m_N}, \end{aligned}$$

*where $\gcd(m_i, m_j) = 1$ for every $i, j \in \{1, 2, \ldots, N\}$, $i \neq j$ (i.e., all pairs of m_i's are co-prime). Then a solution of the system **exists and is unique in** $\mathbb{Z}_M$, where $\boldsymbol{M = m_1 \cdot m_2 \cdots m_N}$.*

This theorem does not give us any algorithm to find a solution. Let us work it out. Put $M_i = \frac{M}{m_i}$. Since $\gcd(m_i, M_i) = 1$, then solutions x_i of linear congruences

$$M_i \cdot x_i \equiv 1 \pmod{m_i}$$

exist for every $i \in \{1, \ldots, N\}$, where N is the number of equations. Moreover

$$M_i \cdot x_i \equiv 0 \pmod{m_j} \qquad \forall\ j \neq i.$$

A solution of the system can be constructed as follows:

$$x \equiv a_1 \cdot x_1 \cdot M_1 + a_2 \cdot x_2 \cdot M_2 + \cdots + a_N \cdot x_N \cdot M_N \pmod{M}.$$

Theorem 7.29 (Chinese Remainder Theorem – general case)**.** *Consider a system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots \\ x &\equiv a_N \pmod{m_N}, \end{aligned}$$

*where $\gcd(m_i, m_j)$ divides $a_i - a_j$ for all $i, j \in \{1, 2, \ldots, N\}$, $i < j$. Then a solutions exists and **is unique in** $\mathbb{Z}_M$, where $\boldsymbol{M = \mathrm{lcm}(m_1, m_2, \ldots, m_N)}$.*

An application of this theorem will be presented in exercises.

Reference:

1. original materials of BIE-ZDM at FIT:
   https://courses.fit.cvut.cz/courses/BIE-ZDM/

7.2 Exercises

7.2.1 Integers and primes

Exercise 7.1. Prove that the divisibility relation $a \mid b$ on the set $\mathbb{N}$ (positive integers) has the following properties:

- it is *reflexive*, i.e., for every $a \in \mathbb{N}$, we have $a \mid a|$;
- it is *antisymmetric*, i.e., for every $a, b \in \mathbb{N}$, if $a \mid b$ and $b \mid a$ then $a = b$;
- it is *transitive*, i.e., for every $a, b, c \in \mathbb{N}$, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Exercise 7.2. Prove the following statements regarding divisibility, for every $a, b, c, d \in \mathbb{Z}$:

a) $a \mid b$ if and only if $b \pmod a = 0$ (mod is the operation of remainder after division);

b) if $a \mid b$ and $c \mid d$, then $ac \mid bd$;

c) If $ac \mid bc$ and $c \neq 0$, then $a \mid b$;

d) prove or disprove: if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Exercise 7.3. Prove that the product of three consecutive integers is divisible by 6.

Exercise 7.4. Use a direct proof and/or mathematical induction to prove the following statements for every $n \in \mathbb{N}$:

a) $2 \mid (n^2 - n)$,

b) $3 \mid (n^3 + 2n)$,

c) $6 \mid (n^3 - n)$,

d) $2 \mid (n^2 + n)$,

e) $5 \mid (n^5 - n)$,

f) $21 \mid (4^{n+1} + 5^{2n-1})$ (where $n \geq 1$).

Exercise 7.5. For each of the following pairs $a, b \in \mathbb{Z}$, find $\gcd(a, b)$ both using the factorization and the extended Eukleid's algorithm, express the Bézout's identity (i.e., write $\gcd(a, b)$ as a linear combination of a and b) and calculate $\operatorname{lcm}(a, b)$.

a) $a = 420, \quad b = 231$,

b) $a = -60, \quad b = -156$,

c) $a = 118, \quad b = -131$.

Exercise 7.6. Prove that the prime factorization of a number $n \geq 2$ contains at most $\lceil \log_2 n \rceil$ factors.

Exercise 7.7. Find a solution set of the following Diophantine equations $a \cdot x + b \cdot y = c$:

a) $2 \cdot x + 3 \cdot y = 4$,

b) $2 \cdot x + 4 \cdot y = 3$,

c) $2 \cdot x + 4 \cdot y = 6$,

d) $3 \cdot x + 6 \cdot y = 2$,

e) $3 \cdot x + 6 \cdot y = 9$.

Exercise 7.8. Consider two hourglasses with limit 11 minutes and 5 minutes. Is it possible to measure an interval of 7 minutes with this pair of hourglasses? If so, how? Is it possible to describe all the ways in which we measure the interval of 7 minutes?

Exercise 7.9. The head of the scout camp goes to the store to purchases bangers and sausages for the evening picnic by the camp fire. One sausage costs 11 CZK and one banger 6 CZK. The scout has only 350 CZK with them.

a) Decide how many bangers and how many sausages they can buy to spend all the money.

b) Find the solution so that each scout has one banger and one sausage (and at the same time the sum is spent completely).

c) Using the previous result find the possible numbers of scouts in the camp if you know there are at least 10 of them.

7.2.2 Modular arithmetic

Exercise 7.10. Find the additive inverse $-a$ and a multiplicative inverse a^{-1} (if it exists) in $\mathbb{Z}_n$ for the given a and modulus n:

a) $n = 35, a = 12$;

b) $n = 36, a = 15$;

c) $n = 42, a = 25$;

d) $n = 146, a = 75$.

Remark 7.30. Note that there is another way to find the inverse of a in $\mathbb{Z}_n$: such an element must be uniquely determined (if it exists) and can therefore be found by brute force – by testing all numbers in $\mathbb{Z}_n$ one by one. Verifying by multiplying this number by a we should get 1. This procedure is usually faster for small modulus like $\mathbb{Z}_3, \mathbb{Z}_5, \ldots$. We would not recommend this method in any of the given examples from the previous exercise.

Exercise 7.11. Find the multiplicative inverse a^{-1} (if it exists) in $\mathbb{Z}_n$ for the given a and modulus n:

a) $n = 8, a = 3$;

b) $n = 5, a = 4$;

c) $n = 13, a = 9$.

Exercise 7.12. Define the addition and the multiplication table of $\mathbb{Z}_4$ (remainder system $\pmod 4$).

a) Discuss the solution set (and the uniqueness of this solution) of the equation $a + x \equiv b \pmod 4$, where x is undetermined and a, b are arbitrary constants.

b) Discuss the solution set (and the uniqueness of this solution) of the equation $a \cdot x \equiv b \pmod 4$, where x is undetermined and a, b are arbitrary constants.

Exercise 7.13. Calculate powers in the given modulus:

a) $3^{33} \mod 11$,

b) $4^{44} \mod 13$,

c) $5^{55} \mod 17$,

d) $6^{66} \mod 19$,

e) $13^{33} \mod 15$,

f) $14^{44} \mod 15$,

g) $16^{55} \mod 21$,

h) $17^{67} \mod 21$,

i) $242\ 162^{123^{234}}$[†] $\mod 121$,.

j) $360\ 240\ 142^{123} \mod 120$.

[†]Exponentiation is not associative. By convention, when we write a^{b^c} we mean $a^{(b^c)}$.

Exercise 7.14. Find all solutions of the linear congruences below.

a) $2 \cdot x \equiv 3 \pmod 7$,

b) $6 \cdot x \equiv 4 \pmod 3$,

c) $9 \cdot x \equiv 1 \pmod{256}$,

d) $3 \cdot x \equiv 2 \pmod{340}$,

e) $4 \cdot x \equiv 4 \pmod{12}$,

f) $14 \cdot x \equiv 7 \pmod{35}$,

g) $39 \cdot x \equiv 27 \pmod{123}$.

Exercise 7.15. Find all solutions of the systems of linear congruences below.

a) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 3 \end{cases}$

b) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases}$

c) $\begin{cases} x \equiv 3 \pmod 8 \\ x \equiv 7 \pmod{12} \\ x \equiv 4 \pmod{15} \end{cases}$

d) $\begin{cases} x \equiv 4 \pmod 6 \\ x \equiv 6 \pmod 8 \\ x \equiv 10 \pmod{20} \end{cases}$

e) $\begin{cases} 2 \cdot x \equiv 3 \pmod 5 \\ 3 \cdot x \equiv 4 \pmod 7 \\ 5 \cdot x \equiv 7 \pmod{11} \end{cases}$

Exercise 7.16. Return back to the power $360\,240\,142^{123} \pmod{120}$ (see Exercise 7.13 point *j)*). Now we apply the Chinese Remainder Theorem to calculate the powers in case the modulus and base are not co-prime.

Exercise 7.17. A food factory produces the same amount of products per day. The products are packed in boxes of one of three types – `A`, `B` and `C` (one type throughout the day). When packed in type `A` boxes (with a capacity of 32 pieces), 14 products remain unpacked, when packed in type `B` boxes (25 pieces each), 16 products remain unpacked and when using box `C` (27 pieces each), 8 products remain. Unpackaged products can no longer be used the next day, so they are discarded. Determine the number of products that the factory produces per day and then design the smallest possible number of products by which it is enough to increase the daily production so that no products are discarded, regardless of the type of boxes used.

Exercise 7.18. A farmer took eggs to the market in a small cart. On the way to the market place, a motorcyclist hit the cart and broke all the eggs. The farmer demands 2 000 CZK as a compensation for the broken eggs. Determine the number of eggs in the cart knowing that:

- there is one egg left when pairing eggs;
- there are two left when packing eggs in groups of 3;
- there are three left when packing eggs in groups of four;
- there are four left when packing eggs in groups of five;
- there are five left when packing eggs in groups of six;
- there are no eggs when packing eggs in groups of seven.

Suppose tht the price per egg is between 2.50 CZK and 4 CZK.

7.3 More exercises

7.3.1 Integers and primes

Exercise 7.19. Find the solution sets of the following Diophantine equations:

a) $4 \cdot x + 7 \cdot y = 12$,

b) $4 \cdot x + 6 \cdot y = 12$,

c) $51 \cdot x + 9 \cdot y = 3$,

d) $3 \cdot x + 51 \cdot y = 9$,

e) $4 \cdot x + 6 \cdot y = 20$,

f) $13 \cdot x + 14 \cdot y = 15$,

g) $42 \cdot x + 24 \cdot y = 20$,

h) $42 \cdot x + 24 \cdot y = 10$,

i) $6 \cdot x + 7 \cdot y = 1$,

j) $8 \cdot x + 7 \cdot y = 1$,

k) $6 \cdot x + 8 \cdot y = 1$,

l) $35 \cdot x + 45 \cdot y = 15$.

Exercise 7.20. Divisibility Criteria: Formulate criteria of divisibility for 3, 4, 5, 10, 11 and prove them using number theory and modular arithmetic.

7.3.2 Modular arithmetic

Exercise 7.21. Find all solutions of systems the of linear congruences below.

a) $\begin{cases} 3x \equiv 2 \pmod 5 \\ 2x \equiv 1 \pmod 3 \end{cases}$

b) $\begin{cases} x \equiv 3 \pmod 5 \\ 5x \equiv 4 \pmod 7 \\ 9x \equiv 7 \pmod{11} \end{cases}$

c) $\begin{cases} 4x \equiv 4 \pmod 6 \\ x \equiv 6 \pmod 8 \end{cases}$

Exercise 7.22. (*) Find the last two digits of the following integers in binary, octal, system with base 5, and hexadecimal representation:

a) 3401,

b) 4804,

c) 33356,

d) 7403.