Lecture notes:
Number theory with applications

Vladimir Oleshchuk

October 10, 2022

Contents

1 Introduction

In this notes we introduce notation, notions and some basic results from number theory. This will serve as a basis for understanding many applications where number theory was utilized in the recent years.

We consider numbers from $\mathbb{Z} = \{, ..., -2, -1, 0, 1, 2, ...\}$, $\mathbb{Z}^+ = \{1, 2, ...\}$ and $\mathbb{N} = \{0, 1, ...\}$.

2 Divisibility and divisors

The notion of *divisibility* that is the fact that one number is divided by another is a fundamental in number theory. If a and d are two numbers from $\mathbb{Z}$ such that $a = kd$ for an integer k, then d is said to divide a and denoted as $d|a$. If $d|a$ then a is called *multiple* of d. If d does not divide a we write $d \not| a$.If $d|a$ and $d > 0$ then d is called a *divisor* of a. Each integer a has always at least two divisors (called trivial divisors) such as 1 and a. Divisors of a that are not trivial are called *factors*. For example, 12 has factors $2, 3, 4$ and 6.

Properties of integer division can be summarized in the following theorem:

Theorem 1 *Let $a, b, c \in \mathbb{Z}$. Then*

- $1|a$;
- $a|0, a \neq 0$;
- $(a|b \wedge b|a) \Rightarrow a = \pm b$;
- $(a|b \wedge b|c) \Rightarrow a|c$;
- $a|b \Rightarrow a|bx \ \forall x \in \mathbb{Z}$;
- *If $x = y + z$,where $x, y, z \in \mathbb{Z}$ and a divides two of these three integers then a must divide the third number $(a|b \wedge a|c) \Rightarrow a|\left(bx + cy\right)$, for all $x, y \in \mathbb{Z}$ expression $bx + cy$ is called a* linear combination *of b and c).*
- *Let $c_i \in \mathbb{Z}$, $1 \leq i \leq n$. If $a|c_i$ for all i, then $a|\left(c_1x_1 + c_2x_2 + ... + c_nx_n\right)$ for all choices of $x_1, x_2, \ldots, x_n$ from $\mathbb{Z}$.*

Proof: Assume that $a|y$ and $a|z$. It means that $y = an$ and $z = am$ for $n, m \in \mathbb{Z}$, and $x = an + am = a(n + m)$. According to definition it means that $a|x$. Similarly, if a divides x and y then we have $x = an$ and $y = am$ for $n, m \in \mathbb{Z}$. Thus $z = x - y = an - am = a(n - m)$.

3 Prime and composite numbers

An integer $a > 1$ that has only trivial divisors 1 and a is called *prime*. An integer $a > 1$ that is not a prime number is called a *composite* number. Prime numbers have many properties that distinguish them from composite and make it possible to use them in many important applications. Examples of prime number are: $2, 3, 5, 7, 11, 13$.

For example 12 is composite because $2, 3, 6$ are divisors of 12. Number 1 is neither prime or composite number and is called a *unit*. Similarly 0 and negative integers are either prime or composite integers.

Lemma 1 *If $n \in \mathbb{Z}^+$ is a composite integer then there is a prime p such that $p|n$.*

Proof: Suppose that S is a set of all composite integers that don't have prime divisors. Let us assume that $S \neq \emptyset$. Since $S \subseteq \mathbb{Z}^+$, then there is least element m in S. Since m is from S then m is a composite integer. Therefore $m = m_1 \cdot m_2$ and since m is from S, integers m_1, m_2 are not primes. However both $1 < m_1 < m$ and $1 < m_2 < m$, and therefore $m_1, m_2 \notin S$.Therefore either m_1 or m_2 have prime divisors. Contradiction.

Theorem 2 (Euclid) *There are infinitely many prime numbers.*

Proof: Assume that it is not true, that is, there exists only k primes $p_1, p_2, ..., p_k$. Let us study an integer $T = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$. T cannot be a prime since $T > p_i$ for all $i = 1, 2, ..., k$. Therefore T is a composite integer. Therefore there is a prime p_j such that $p_j|T$, but then p_j must also be a divisor for 1. Contradiction. It means that assumption that there are only finite many primes is not true.

4 Division theorem

Theorem 3 (Division theorem) *Let a be a number from $\mathbb{Z}$ and b be a number from $\mathbb{Z}^+$. Then there are two unique integers q and r such that $0 \leq r < b$ and $a = bq + r$.*

Assume that $a \in \mathbb{Z}$ and that we have integers q and r such that $a = qn+r$ and $0 \leq r < n$. Then $q = \lfloor a/n \rfloor$ is called a *quotient* of division and $r = a \bmod n$ is a *remainder* of division. Therefore we can state that $n|a$ if and only if $a \bmod n = 0$. It follows also that

$$a = \lfloor a/n \rfloor n + (a \bmod n)$$

or

$$a \bmod n = a - \lfloor a/n \rfloor n.$$

5 The great common divisor (GCD)

If d is a divisor of both a and b then d is called a *common divisor* of a and b. For example, 12 has divisors $1, 2, 3, 4, 6, 12$ and 20 has divisors $1, 2, 4, 5, 10, 20$. Thus $1, 2$ and 4 are common divisors for 12 and 20.

Generally there are finite number of divisors for a and b if they are not equal 0 simultaneously, and 1 is always the common divisor. Therefore there is always a great common divisor (gcd) for two integers (not equal 0 simultaneously), and it is denoted as $\gcd(a, b)$ for integers a and b. For example, $\gcd(12, 20) = 4$.

To have function $\gcd(a, b) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ defined for all elements from $\mathbb{Z} \times \mathbb{Z}$ we assume that $\gcd(0, 0) = 0$.

Formally, great common divisor is defined as following.

Definition 1 *Let $a, b \in \mathbb{Z}$ be not equal 0 simultaneously. An integer $c \in \mathbb{Z}^+$ is called a great common divisor of a and b if*

(a) *$c|a$ and $c|b$*

(b) *for all common divisors d of a and b we have that $d|c$.*

Let $a, b \in \mathbb{Z}$. Following properties of gcd follow immediately from the definition:

- $\gcd(a, b) = \gcd(b, a)$,
- $\gcd(a, 0) = |a|$,
- $\gcd(a, na) = |a|$, for $n \in \mathbb{Z}$
- $\gcd(-a, -b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(a, b) = \gcd(|a|, |b|)$

The following question

Theorem 4 *For $a, b \in \mathbb{Z}$ (not equal 0 simultaneously) there exists $c \in \mathbb{Z}^+$ that is equal to $c = \gcd(a, b)$ and is a least positive integer of $\{ax + by | x, y \in \mathbb{Z}\}$.*

Proof: Given $a, b \in \mathbb{Z}$ and let S is defined as

$$S = \{as + bt | s, t \in \mathbb{Z} \text{ and } as + bt > 0\}$$

Since $S \neq \emptyset$ and $S \subseteq \mathbb{Z}^+$, then there is a least integer c in S. We shall show that a least element c is equal to $\gcd(a, b)$.

Since $c \in S$, then $c = ax + by$ for some $x, y \in \mathbb{Z}$. Assume that d is a common divisor a and b. From $d|a$ and $d|b$ follows that $d|(ax + by)$ for all $x, y \in \mathbb{Z}$. It means that $d|c$ and $0 < d \leq c$. The last statement holds for all common divisors of a and b, that is all common divisors of a and b divides c.

Now we shall show that c is also a divisor of a and b.

Assume that it is not true, that is either $c \nmid a$ or $c \nmid b$. If $c \nmid a$ then $a = cq + r$, where $0 < r < c$. Therefore $r = a - cq = a - (ax + by)q = a - axq - bxq = a(1 - qx) + b(-qy) \in S$. Contradiction since c is a least element in S. Similarly we can come to contradiction if $c \nmid b$. It shows that a great common divisor always exists, since c is a common divisor of a and b and all common divisors of a and b divides c.

Assume that c_1 and c_2 satisfy Definition 1. Then $c_2|c_1$ and $c_1|c_2$, and therefore $c_1 = c_2$.

Corollary 1 *For all $a, b \in \mathbb{Z}^+$ there is a unique c such that $c = \gcd(a, b)$.*

Proof: This is the least positive integer that can be presented in the form $ax + by$.

Corollary 2 *For all $a, b \in \mathbb{Z}^+$, if $d|a$ and $d|b$ then $d| \gcd(a, b)$.*

Proof: Since $\gcd(a, b) = ax + by$, $x, y \in \mathbb{Z}$, from $d|a$ and $d|b$ follows that $d| (ax + by)$.

Corollary 3 *For all $a, b \in \mathbb{Z}^+$ and $n \in \mathbb{N}$, $\gcd(an, bn) = n \gcd(a, b)$.*

Proof: If $n = 0$, then statement is true. If $n > 0$, then $\gcd(an, bn)$ is the least positive integer in $\{anx + bny|x, y \in \mathbb{Z} \text{and} ax + by > 0\}$. Assume that the integer is $anx_1 + bny_1 = n(ax_1 + by_1)$ that is n time greater than the least positive integer in $\{ax + by|x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$.If $ax_1 + by_1$ was not a least positive integer in $\{ax + by|x, y \in \mathbb{Z}, ax + by > 0\}$, then $(anx_1 + bny_1)$ could not be the least positive integer in $\{anx + bny|x, y \in \mathbb{Z}, ax + by > 0\}$).

Corollary 4 *For all $a, b \in \mathbb{Z}^+$ and $n \in \mathbb{Z}^+$, if $n|ab$ and $\gcd(a, n) = 1$ then $n|b$.*

Proof: From $\gcd(a, n) = 1$ and Corollary 3 follow that $b \gcd(a, n) = \gcd(ab, nb) = b$. It means that $b = abx + nby$ for some $x, y \in \mathbb{Z}$. Since $n|abx$ and $n|nby$, then $n|b$.

6 Relatively prime numbers (co-primes)

Two integers a and b from $\mathbb{Z}$ are called relatively primes (co-primes) if $\gcd(a, b) = 1$. For example, integers 8 and 9 are relatively prime, but 8 and 10 are not relatively prime.

We say that $n_1, n_2, ..., n_k \in \mathbb{Z}^+$ are pairwise relatively prime if $\gcd(n_i, n_j) = 1$ where $i \neq j$.

Theorem 5 *For $a, b, p \in \mathbb{Z}^+$, if $\gcd(a, p) = 1$ and $\gcd(b, p) = 1$ then $\gcd(ab, p) = 1$.*

Proof: There are x_1, y_1, x_2, y_2 such that $ax_1 + py_1 = 1$ and $bx_2 + py_2 = 1$. By multiplying these equations we get

$$(ax_1 + py_1)(bx_2 + py_2) = ab(x_1x_2) + p(ax_1y_2 + bx_2y_1 + py_1y_2) = 1.$$

Since 1 is the least positive integer and can be expressed as a linear combination of ab and p, then $\gcd(ab, p) = 1$.

7 Fundamental theorem of arithmetic (Unique prime factorization theorem)

The following theorem is sometimes referred as Euclid's lemma.

Theorem 6 *For any prime p and all $a, b \in \mathbb{Z}$, if $p|ab$, then $p|a$ or $p|b$.*

Proof: If $p|a$ then the theorem is correct. Assume that $p \nmid a$. Since p is a prime then $\gcd(a, p) = 1$. Therefore there are $x, y \in \mathbb{Z}$ such that $ax+py = 1$. Then $bax + bpy = b$ and $b = (ba)x + p(by)$. But $p|ba$ and $p|p$. Thus $p|b$.

Theorem 7 *Let $a_i \in \mathbb{Z}^+$, $1 \leq i \leq n$. If p is a prime and $p|a_1a_2...a_n$, then there is a_j such that $p|a_j$ for some $1 \leq j \leq n$.*

Fundamental theorem of arithmetics can be formulated as following.

Theorem 8 *Every integer $a > 1$ can be uniquely presented in the form:*

$$a = p_1^{e_1} p_2^{e_2} ... p_r^{e_r}$$

where p_i, $i = 1, 2, ..., r$ is a prime, $p_1 < p_2 < ... < p_r$ and $e_i \in \mathbb{Z}^+$.

Proof: First we show that all integers m where $m > 1$ can be presented as a product of primes $p_1^{e_1} p_2^{e_2} ... p_r^{e_r}$.

Assume that there is m, $m > 1$ that is a least positive cannot be presented as a product of primes. Since m is not a prime should $m = m_1 \cdot m_2$ where $1 < m_1 < m$ and $1 < m_2 < m$. Therefore can both m_1 and m_2 be presented as a product of primes. Therefore m can be presented as a product of primes.

Now we show that such factoring is unique. It is easy to see that 2 can be uniquely factorized as 2^1, and 3 can uniquely factorized as 3^1. Assume that all $2, 3, 4, ..., n-1$ can be uniquely factorized. Assume that

$$n = p_1^{s_1} p_2^{s_2} ... p_k^{s_k} = q_1^{t_1} q_2^{t_2} ... q_r^{t_r},$$

where p_i is a prime and $s_i \in \mathbb{Z}^+$ for all $1 \leq i \leq k$, q_i is a prime and $t_i \in \mathbb{Z}^+$ for all $1 \leq i \leq r$, and $p_1 < p_2 < ... < p_k$, $q_1 < q_2 < ... < q_k$.

Since $p_1|n$ må $p_1|q_1^{t_1} q_2^{t_2} ... q_r^{t_r}$ and $p_1|q_j$ for some j, $1 \leq j \leq r$. Both p_1 and q_j are primes, therefore $p_1 = q_j$. Similarly, since $q_1|n$ so $q_1|p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$

and $q_1|p_i$ for some i, $1 \leq i \leq k$. Both q_1 and p_i are primes and therefore $q_1 = p_i$. From $p_1 \leq p_i = q_1 \leq q_j$ and $p_1 = q_j$ follow that $p_1 = p_i = q_1 = q_j$. Therefore

$$n_1 = n/p_1 = p_1^{s_1-1} p_2^{s_2} ... p_k^{s_k} = q_1^{t_1-1} q_2^{t_2} ... q_r^{t_r}$$

But since $n_1 < n$ it can according to assumption be factorized uniquely.

Example 1 *Find presentation of* 100 *as a product of primes.*

$$100 = 2 \cdot 50 = 2 \cdot 2 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$$

Example 2 *How many positive divisors has an integer $a \in \mathbb{Z}^+$?*

If $a = p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}$, where p_i is a prime then every $b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$, where $0 \leq s_i \leq t_i$ is a divisor of a. The number of such integers are $(t_1 + 1)(t_2 + 1) \cdots (t_n + 1)$. *For example,* $100 = 2^2 \cdot 5^2$ *has* $(2 + 1)(2 + 1) = 9$ *positive divisors.*

8 Euclidean algorithm

To find great common divisor we can limit us to $\mathbb{N}$, since for all $a, b \in \mathbb{Z}$, hold $\gcd(a, b) = \gcd(|a|, |b|)$.

In principle, when we know that $a = p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$, so then $\gcd(a, b) = p_1^{\min(t_1,s_1)} p_2^{\min(t_2,s_2)} \cdots p_n^{\min(t_n,s_n)}$.

For example, since $42 = 2^1 \cdot 3^1 \cdot 7^1$ and $27 = 3^3 = 2^0 \cdot 3^3 \cdot 7^0$, are $\gcd(42, 27) = 2^{\min(1,0)} \cdot 3^{\min(1,3)} \cdot 7^{\min(1,0)} = 2^0 \cdot 3^1 \cdot 7^0 = 3$.

However an efficient and fast algorithms to factorize large integers are unknown. Therefore we need some other way to find $\gcd(a, b)$. Euclid algorithm, which is normally used to solve the problem, is fast and efficient. It is based on the following theorem.

Theorem 9 *For all nonnegative integers a and for all positive integers b*

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

Proof: Let us show that $\gcd(a, b)$ and $\gcd(b, a \bmod b)$ divides each other and therefore, according to Theorem 1, must be equal (since both are nonnegative).

Let us show that $\gcd(a, b) | \gcd(b, a \bmod b)$.

If $d = \gcd(a, b)$, then $d|a$ and $d|b$. But $a \bmod b = a - \lfloor a/b \rfloor b$. Therefore $d|(a \bmod b)$. Thus $d|\gcd(b, a \bmod b)$, that is,

$$\gcd(a, b) | \gcd(b, a \bmod b)$$

Now we shall show that $\gcd(b, a \bmod b) | \gcd(a, b)$. Let $d = \gcd(b, a \bmod b)$. Then $d|b$ og $d|(a \bmod b)$. Since $a = \lfloor a/b \rfloor b + (a \bmod b)$, so a is a linear combination of b and $(a \bmod b)$. Therefore $d|a$. Since $d|a$ and $d|b$, so we have that $d|\gcd(a,b)$ or

$$\gcd(b, a \bmod b) | \gcd(a,b)$$

Therefore we conclude that $\gcd(a,b) = \gcd(b, a \bmod b)$.

Now we can present an algorithm that was first described in Elements of Euclid (*ca.* 300B.C.) This is a recursive algorithm that implements above theorem. We assume that a and b are non-negative integers. It holds since $\gcd(a,b) = \gcd(|a|, |b|)$.

```
function $\gcd(a,b)$
if $b = 0$
    then return  $a$
    else return $\gcd(b, a \bmod b)$
```

Example 3 *We will run Euclidean algorithm to find* $\gcd(42, 27)$.

$$\begin{aligned}\gcd(42,27) &= \gcd(27, 42 \bmod 27) = \gcd(27,15) = \gcd(15, 27 \bmod 15)\\ &= \gcd(15,12) = \gcd(12, 15 \bmod 12) = \gcd(12,3)\\ &= \gcd(3, 12 \bmod 3) = \gcd(3,0) = 3\end{aligned}$$

9 Extended Euclidean algorithm

Now we extend Euclidean algorithm such that it will generate coefficients x and y of $d = \gcd(a,b) = ax + by$. These coefficients play an important role in modular arithmetic calculations. The algorithm Extended Euclid takes arbitrary integers a and b, and produce a result in the form (d, x, y).

```
function Ext-gcd$(|a|, |b|)$
if $b = 0$
    then return $(a, 1, 0)$
$(d', x', y') \leftarrow$Ext-gcd$(b, a \bmod b)$
$(d, x, y) \leftarrow (d', y', x' - \lfloor a/b \rfloor y')$
return $(d, x, y)$
```

Brief explanation

If $b = 0$ then the algorithm return $d = a, x = 1$ and $y = 0$. It is correct since $d = \gcd(a, 0) = a$ and $d = a \cdot 1 + b \cdot 0$.

If $b \neq 0$, then the algorithm calculates $d' = \gcd(b, a \bmod b)$ and x', y' such that $d' = bx' + (a \bmod b)y'$. Similarly to the previous algorithm

$d = \gcd(a,b) = \gcd(b, a \bmod b) = d'$. Therefore $d = d' = bx' + (a \bmod d)y' = bx' + (a - \lfloor a/b \rfloor \cdot b)y' = ay' + bx' - \lfloor a/b \rfloor \cdot by' = a\underbrace{y'}_{x} + b\underbrace{(x' - \lfloor a/b \rfloor y')}_{y}$.

It means that if $d = \gcd(a,b) = ax + by$, we may choose $x = y'$ and $y = x' - \lfloor a/b \rfloor y'$ where x' and y' are values from previous recursive call of the algorithm.

Example 4 *Executioon of Ext-gcd algorithm to find* $\gcd(42, 27)$ *together with corresponding coefficients* x *and* y *are presented in the table below..*

a	b	$\lfloor a/b \rfloor$	d	x	y
42	*27*	*1*	*3*	*2*	*-3*
27	*15*	*1*	*3*	*-1*	*2*
15	*12*	*1*	*3*	*1*	*-1*
12	*3*	*4*	*3*	*0*	*1*
3	*0*	—	*3*	*1*	*0*

Therefore $\gcd(42, 27) = 3 = 42 \cdot 2 + 27 \cdot (-3)$.

10 Modular arithmetic

Informally, modular arithmetic can be seen as a calculation system where all calculations are performed modulo n. That is each calculation result x has to be represented as an integer from $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ such that $x \bmod n$, where $x \bmod n = x - \lfloor x/n \rfloor n$.

Definition 2 *Assume that* a *and* b *are two integers and* n *is a positive integer. We write* $a \equiv b \pmod{n}$ *if* $n|(a-b)$ *and say that* a *is* congruent *to* b *modulo* n*.*

Assume that a and b are such that $a = q_1 n + r_1$ and $b = q_2 n + r_2$, where $0 \le r_1 \le n-1$ and $0 \le r_2 \le n-1$. Then $a - b = (q_1 n + r_1) - (q_2 n + r_2) = n(q_1 - q_2) - (r_1 - r_2)$. Therefore $n|\,(a-b)$ if and only if $r_1 - r_2 = 0$. From previous consideration can we conclude that $a \equiv b \pmod{n}$ if and only if $r_1 = r_2$. The last means that $a = b + kn$ for some $k \in \mathbb{Z}$.

Example 5 *From definition above follows that* $21 \equiv 1 \pmod{5}$*,* $21 \equiv 3 \pmod{6}$*,* $21 \equiv 0 \pmod{7}$*.*

We define two operations (denoted as $+_n$ and $\times_n$) on n set $\mathbb{Z}_n$. The operations $+_n$ and $\times_n$ denote addition and multiplication on $\mathbb{Z}_n$ which are similar to the ordinary addition and multiplication on $\mathbb{Z}$ except that results are always calculated modulo n.

Following tables give examples of such operations on $\mathbb{Z}_7$.

$+_7$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times_7$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

For example, if we calculate $11 \times_{16} 13$ (in $\mathbb{Z}_{16}$) we calculate $11 \times 13 = 143$, and since$143 = 8 \times 16 + 15$ we find that $143 \bmod 16 = 15$. Therefore $11 \times_{16} 13 = 15$ (i $\mathbb{Z}_{16}$).

Properties of operations on $\mathbb{Z}_n$ arel summarized (without proofs) below:

1. Addition $+_n$ is a closed operation on $\mathbb{Z}_n$, that is, $a, b \in \mathbb{Z}_n, a +_n b \in \mathbb{Z}_n$.
2. Addition $+_n$ is a commutative operation, that is, $a, b \in \mathbb{Z}_n, a +_n b = b +_n a$.
3. Addition $+_n$ is an associative operation, that is, $a, b, c \in \mathbb{Z}_n, (a +_n b) +_n c = a +_n (b +_n c)$
4. 0 is an additive identity, that is, for each $a \in \mathbb{Z}_n, a +_n 0 = 0 +_n a = a$.
5. Additive inverse to each $a \in \mathbb{Z}_n$ with respect to $+_n$ is equal to $n - a$, that is, $a \in \mathbb{Z}_n$, $a + (n - a) = (n - a) + a = 0$.
6. Multiplication $\times_n$ is a closed operation on $\mathbb{Z}_n$, that is, $a \times_n b \in \mathbb{Z}_n$, for all $a, b \in \mathbb{Z}_n$.
7. Multiplication $\times_n$ is a commutative operation, that is, for all $a, b \in \mathbb{Z}_n, a \times_n b = b \times_n a$.
8. Multiplication $\times_n$ is an associative operation, that is, $(a \times_n b) \times_n c = a \times_n (b \times_n c)$, for all $a, b, c \in \mathbb{Z}_n$.
9. 1 is a multiplicative identity, that is, $a \in \mathbb{Z}_n, a \times_n 1 = 1 \times_n a = a$.
10. Multiplication $\times_n$ is distributive over addition $+_n$, that is, $(a +_n b) \times_n c = a \times_n c +_n b \times_n c$ and $a \times_n (b +_n c) = a \times_n b +_n a \times_n c$, for all $a, b, c \in \mathbb{Z}_n$.

11 Finite groups

Definition 3 *Let S be a set and $\bullet$ denote a binary operation defined on S. A pair $(S, \bullet))$ is called a group if following properties are satisfied:*

1. $\forall a, b \in S$, $a \bullet b \in S$
2. *There is an element* $e \in S$ *such that* $e \bullet a = a \bullet e = a$ *for each* $a \in S$
3. *For all* $a, b, c \in S$, $a\bullet\ (b \bullet c) = (a \bullet b) \bullet c$
4. *For each* $a \in S$ *there is a unique* $b \in S$ *such that* $a\bullet\ b = b \bullet a = e$

If, in addition, $\bullet$ is commutative operation, that is, $a \bullet b = b \bullet a$, then $(S, \bullet)$ is called an Abelian or commutative group. If $(S, \bullet)$ is a group and S is a finite set then $(S, \bullet)$ is a finite group.

Theorem 10 $(\mathbb{Z}_n, +_n)$ *is a finite abelian group.*

Since $(\mathbb{Z}_n, +_n)$ is group then an additive inverse is alway exists, that is, we can perform subtraction in $\mathbb{Z}_n$. For example, $(a - b) \bmod n = (a + (-b)) \bmod n = (a + (n - b)) \bmod n$. We calculate $(11 - 18) \bmod 31$ as $(11 + (-18)) \bmod 31 = (11 + (31 - 18)) \bmod 31 = (11 + 13) \bmod 31 = 24 \bmod 31$. From the other side we could also calculate $(11 - 18) \bmod 31 = (-7) \bmod 31 = (31 - 7) \bmod 31 = 24 \bmod 31$.

Let us consider $(\mathbb{Z}_n, \cdot_n)$. From the table that describe $(\mathbb{Z}_7, \cdot_7)$ we can see that 0 has no inverse elements since $0 \cdot_7 a = a \cdot_7 0 = 0 \neq 1$. Therefore we can conclude that $(\mathbb{Z}_7, \cdot_7)$ is not a group.

Let us denote by $\mathbb{Z}_n^*$ a set of all elements from $\mathbb{Z}_n$ that are relatively prime with n:

$$\mathbb{Z}_n^* = \{a | a \in \mathbb{Z}_n \text{ and } \gcd(a, n) = 1\}$$

then $\mathbb{Z}_7^* = \{1, 2, ..., 6\}$ and $\mathbb{Z}_p^* = \{1, 2, ..., p - 1\}$ where p is a prime. Another example is $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$.

Theorem 11 $(\mathbb{Z}_n^*, \cdot)$ *is a finite Abelian group.*

$(\mathbb{Z}_n^*, \cdot)$ is called a *a multiplicative group modulo n.*

Following table represents multiplicative group $(\mathbb{Z}_{12}^*, \cdot)$.

$\cdot_{12}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Since $(\mathbb{Z}_n^*, \cdot)$ is a finite group$(\mathbb{Z}_n^*, \cdot)$ we can find that a number of elements in the group is number of elements in $\{1, 2, ..., n - 1\}$ that are relatively prime with n. Let us denote it as $|\mathbb{Z}_n^*| = \phi(n)$, where $\phi(n)$ denotes a number of integers that are relatively prime to n and smaller than n. This function is called Euler's ϕ-function and is defined as for all integers n, $n \geq 1$.

Let us consider two examples of simple cryptographic schemes that demonstrate using of modular arithmetics.

Example 6 (Shift Cipher) *Let us define a so called Shift Cipher over* $\mathbb{Z}_{26}$ *(where* 26 *is a number of letter in English alphabet). Encryption is defined as following:*

$$e_K(x) = x + K \bmod 26, x \in \mathbb{Z}_{26}$$

Decryption is defined as following:

$$d_K(y) = y - K \bmod 26, y \in \mathbb{Z}_{26}$$

It is easy to see that $d_K(e_K(x)) = x$ *for each* $x \in \mathbb{Z}_{26}$. [1]

To encrypt an English text letter-by-letter we define correspondence between letters and numbers from $\mathbb{Z}_{26}$*. For example, it can be defined as a function:* $A \leftrightarrow 0$, $B \leftrightarrow 1, ..., \mathbb{Z} \leftrightarrow 25$*, presented in the following table:*

A	***B***	***C***	***D***	***E***	***F***	***G***	***H***	***I***	***J***	***K***	***L***	***M***
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
N	***O***	***P***	***Q***	***R***	***S***	***T***	***U***	***V***	***W***	***X***	***Y***	$\mathbb{Z}$
13	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*

For $K = 12$ *word* $MATHEMATICS$ *corresponds to 12 0 19 7 4 12 0 19 8 2 18 which will be encrypted* $K = 12$ *as 24 12 7 19 16 0 12 7 20 14 6 which is an encoding for word* $YMHTQAMHUOG$

Definition 4 (multiplicative inverse) *Assume that* $a \in \mathbb{Z}_n^*$*.* multiplicative inverse to a, *denoted as* $\left(a^{-1} \bmod n\right)$*, is an integer* $a^{-1} \in \mathbb{Z}_n^*$ *such that* $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{n}$*.*

For example, $5^{-1} \bmod 13 = 8$ because $5 \cdot 8 \equiv 1 \pmod{13}$. Therefore we can define division in Z_n^* as $a/b \equiv a \cdot b^{-1} \pmod{n}$.

Example 7 (Affine Cipher) *In this example we describe a more advanced (but still insecure) cipher over* $\mathbb{Z}_{26}$ *called Affine Cipher.*

Encryption function is defined as following:

$$e_K(x) = (ax + b) \bmod 26, \;\; a, b \in \mathbb{Z}_{26}$$

Since decryption means to find x from $y \equiv ax + b \pmod{26}$ *such that it is a solution for equation* $ax \equiv y - b \pmod{26}$*.*

However as we can see from the theorem below such solution exists only when $\gcd(a, 26) = 1$.

[1] For $K = 3$ the cipher is called Caesar Cypher since it is believed was used by Julius Caesar.

Theorem 12 *Congruence* $ax \equiv b \pmod{n}$ *has a unique solution* $b \in \mathbb{Z}_n$ *if and only if* $\gcd(a, n) = 1$.

12 Finding a multiplicative inverse modulo n

The following observation shows how we can calculate multiplicative inverses modulo n.

If $a, n \in \mathbb{Z}^+$ such that $\gcd(a, n) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. From

$$(ax + ny) \bmod n = 1 \bmod n = 1$$

and

$$(ax + ny) \bmod n = ax \bmod n + ny \bmod n = ax \bmod n$$

follows that

$$ax \bmod n = 1$$

or

$$ax \equiv 1 \pmod{n}.$$

It means $x = a^{-1}$ is a multiplicative inverse to a modulo n. Therefore solution x of $ax \equiv 1 \bmod n$ is equal to $x = \left(a^{-1} \bmod n\right)$.

we can find such x by using Extended Euclid algorithm.

Exercise 12.1 *Find* $28^{-1} \bmod 75$.

By applying Extended Euclidean algorithm (ext-gcd) can we find x, y *such that* $\gcd(28, 75) = 28x + 75y = 1$.

a	b	$\lfloor a/b \rfloor$	d	x	y
28	*75*	*0*	*1*	$\boldsymbol{-8}$	*3*
75	*28*	*2*	*1*	*3*	*-8*
28	*19*	*1*	*1*	*-2*	*3*
19	*9*	*2*	*1*	*1*	*-2*
9	*1*	*9*	*1*	*0*	*1*
1	*0*	-	*1*	*1*	*0*

We have that $\gcd(28, 75) = 28 \cdot (-8) + 75 \cdot 3 = 1$.

Therefore $28^{-1} \bmod 75 = -8 \bmod 75 = (75 - 8) \bmod 75 = 67$.

13 Chinese reminder theorem (CRT)

In ca. A.D.100, following problem was described by Chinese mathematician Sun-Tsû:

Find integer x that has reminders $2, 3$ and 2 when x is divided by $3, 5$ and 7 respectively. One possible solution is $x = 23$, and in general solution can be described as $x = 23 + 105k$, where $k \in \mathbb{Z}$. Chinese reminder theorem describes how we can find solutions generally.

Generally it is an approach to solve system of congruences with respect to modulus $n_1, n_2, ..., n_t$ that are pairwise relatively prime. It means that $\gcd(n_i, n_j) = 1$ if $i \neq j$. Assume that $a_1, a_2, ..., a_t$ are integers. We shall consider following system of congruences.

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_t \pmod{n_t} \end{cases}$$

Chinese remainder theorem states that there is a unique solution modulo $n = n_1 \times n_2 \times ... \times n_t$ where $n_1, n_2, ..., n_t$ are pairwise relatively prime.

Let us consider following relation:

$$a \leftrightarrow (a_1, a_2, ..., a_t),$$

where $a \in \mathbb{Z}_n$, $a_i \in \mathbb{Z}_{n_i}$ and $a_i = a \bmod n_i$, $i = 1, 2, \ldots, t$. We can calculate $(a_1, a_2, ..., a_t)$ from a by using t divisions.

Finding a on the base of $(a_1, a_2, ..., a_t)$ is more difficult and CRT suggests the following approach:

Let us denote $m_i = n/n_i$ for $i = 1, 2, \ldots, t$. Since $m_i = (n_1 \cdot n_2 \cdots n_t)/n_i = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_t$, so $m_j \equiv 0 \pmod{n_i}$, $j \neq i$ and $\gcd(m_i, n_i) = 1$. Let us define

$$y_i = m_i^{-1} \bmod n_i$$

Such inverse element always exists since $\gcd(m_i, n_i) = 1$. But

$$m_i \cdot y_i \equiv 1 \pmod{n_i}$$

and

$$m_j \cdot y_j \equiv 0 \pmod{n_i}, j \neq i$$

for $i = 1, 2, \ldots, t$.

Let us choose a as

$$a \equiv (a_1 m_1 y_1 + a_2 m_2 y_2 + \cdots + a_t m_t y_t) \bmod n$$

In the next we show that a is a solution, which means that $a \equiv a_i \bmod n_i$ for all $i = 1, 2, \ldots, t$. (Since $a \equiv b \bmod n$ means $a = b + kn$ and therefore if $n_1 | n$ then $a \bmod n_i = b \bmod n_i$ which means $a \equiv b \bmod n_i$.)

Since $n_i | n$, then if $a \equiv b \bmod n$ implies that $a \equiv b \bmod n_i$, for all $i = 1, 2, \ldots, t$. Thus if

$$a \equiv (a_1 m_1 y_1 + a_2 m_2 y_2 + \cdots + a_t m_t y_t) \bmod n,$$

so

$$a \equiv (a_1 m_1 y_1 + a_2 m_2 y_2 + \cdots + a_t m_t y_t) \bmod n_i.$$

We have that $a_i m_i y_i \equiv a_i \pmod{n_i}$ and $a_j m_j y_j \equiv 0 \pmod{n_i}$ if $j \neq i$. Therefore

$$\begin{aligned} a &\equiv (a_1 m_1 y_1 + a_2 m_2 y_2 + \cdots + a_t m_t y_t) \pmod{n_i} \\ &\equiv a_i m_i y_i \pmod{n_i} \equiv a_i \pmod{n_i}. \end{aligned}$$

for each $i = 1, 2, \ldots, t$.

Since it is true for all $i = 1, 2, \ldots, t$, so a is a solution of the system of congruences.

Theorem 13 *Assume that $n_1, n_2, ..., n_t$ is pairwise relatively prime and $a_1, a_2, ..., a_t$ are integers. The systems of congruences*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_t \pmod{n_t} \end{cases}$$

has a unique solution x mod n where $n = n_1 \times n_2 \times ... \times n_t$ and

$$x = \sum_{k=1}^{t} a_k m_k \left(m_k^{-1} \bmod n_k\right) \bmod n$$

where $m_i = n/n_i$ for $i = 1, 2, \ldots, t$.

Example 8 *Assume that $t = 3$, $n_1 = 5, n_2 = 7, n_3 = 8$. We shall find a solution for the following system of congruences:*

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \\ x \equiv 6 \pmod 8 \end{cases}$$

First, we find that $n = 280$, $m_1 = 56$, $m_2 = 40$, $m_3 = 35$ and

$m_1^{-1} \bmod n_1 = 56^{-1} \bmod 5 = 1 \bmod 5 = 1$
$m_2^{-1} \bmod n_2 = 40^{-1} \bmod 7 = 3 \bmod 7 = 3$
$m_3^{-1} \bmod n_3 = 35^{-1} \bmod 8 = 3 \bmod 8 = 3$
$x = (3 \cdot m_1 \left(m_1^{-1} \bmod 5\right) + 4 \cdot m_2 \left(m_2^{-1} \bmod 7\right)$
$+6 \cdot m_3 \left(m_3^{-1} \bmod 8\right)) \bmod 280$
$= 3 \cdot 56 \cdot 1 + 4 \cdot 40 \cdot 3 + 6 \cdot 35 \cdot 3 \quad \pmod{280}$
$= 168 + 480 + 630 \quad \pmod{280}$
$= 1278 \pmod{280}$
$= 158.$

We can verify that 158 is a solution since

$$\begin{cases} 158 \equiv 3 \pmod 5 \\ 158 \equiv 4 \pmod 7 \\ 158 \equiv 6 \pmod 8 \end{cases}$$

14 Euler *phi*-function

Euler's ϕ-function is defined for each integer $n \geq 1$ such that $\phi(n)$ denotes a number of positive integers that are equal to or smaller than n and are relatively prime with n. Let us calculate $\phi(n)$ for $n = 1, 2, 3, \ldots, 15$:

$$\begin{array}{lllll} \phi(1) = 1 & \phi(2) = 1 & \phi(3) = 2 & \phi(4) = 2 & \phi(5) = 4 \\ \phi(6) = 2 & \phi(7) = 6 & \phi(8) = 4 & \phi(9) = 6 & \phi(10) = 4 \\ \phi(11) = 10 & \phi(12) = 4 & \phi(13) = 12 & \phi(14) = 6 & \phi(15) = 8 \end{array}$$

If p is a prime, then all integers that are smaller that p are relatively prime with p. Therefore $\phi(p) = p - 1$.

Theorem 14 *If $n = pq$ is a composite integer and p and q are two prime, $p \neq q$, then $\phi(n) = (p-1)(q-1)$.*

Proof: Let us count number of integers in $S = \{1, 2, \ldots, pq - 1\}$ that are relatively prime with n. Since p and q are primes, so each integer that are *not* relatively prime with n is divisible either by p or q. Integers from S that are divisible by p are grouped in the set S_p where $S_p = \{p, 2p, 3p, \ldots, (q-1)p\}$. Integers from S that are divisible by q are grouped in set S_q where $S_q = \{q, 2q, 3q, \ldots, (p-1)q\}$. Therefore a number of integers that are smaller than n and are relatively prime with n is equal to:

$$\begin{aligned} |S| - |S_p| - |S_q| &= (pq - 1) - (q - 1) - (p - 1) \\ &= pq - 1 - q + 1 - p + 1 \\ &= pq - p - q + 1 = (p-1)(q-1) \end{aligned}$$

Example 9 *Find $\phi(143)$.*

Since $143 = 11 \cdot 13$*, then* $\phi(143) = 10 \cdot 12 = 120$.

Theorem 15 *If p is a prime and $k > 0$, then $\phi\left(p^k\right) = p^k - p^{k-1} = p^{k-1}(p-1)$.*

Proof: We will count number of elements in $S = \left\{1, 2, ..., p^k - 1\right\}$ that are smaller than p^k and are not relatively primes with p^k. These are integers grouped in the set $S' = \left\{p, 2p, \ldots, \left(p^{k-1} - 1\right)p\right\}$. Therefore $\phi\left(p^k\right) = |S| - |S'| = \left(p^k - 1\right) - \left(p^{k-1} - 1\right) = p^k - p^{k-1}$.

Theorem 16 *If n, m is such that* $\gcd(n, m) = 1$*, then $\phi(nm) = \phi(n)\phi(m)$.*

Theorem 17 $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$*, where p is a prime and $n \in \mathbb{Z}^+$.*

15 Exponentiation modulo n

The subset of $\mathbb{Z}_n^*$ of elements that are relatively prime with n is denoted as $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | \gcd(a, n) = 1\}$. From definition of $\mathbb{Z}_n^*$ follows that $|\mathbb{Z}_n^*| = \phi(n)$.

Example 10 $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

We can observe that $0 \notin \mathbb{Z}_n^*$, $n > 1$ since $\gcd(0, n) = n$. We can also observe that $\mathbb{Z}_p^* = \{1, 2, ..., p - 1\}$ for every prime p.

Example 11 *Following table describes multiplication in* $\mathbb{Z}_{15}^*$:

$\cdot_{15}$	***1***	***2***	***4***	***7***	***8***	***11***	***13***	***14***
1	*1*	*2*	*4*	*7*	*8*	*11*	*13*	*14*
2	*2*	*4*	*8*	*14*	*1*	*7*	*8*	*13*
4	*4*	*8*	*1*	*13*	*2*	*14*	*7*	*11*
7	*7*	*14*	*13*	*4*	*13*	*2*	*1*	*8*
8	*8*	*1*	*2*	*11*	*4*	*13*	*14*	*7*
11	*11*	*7*	*14*	*2*	*13*	*1*	*8*	*4*
13	*13*	*11*	*7*	*1*	*14*	*8*	*4*	*2*
14	*14*	*13*	*11*	*8*	*7*	*4*	*2*	*1*

From the table we can see that each element from $\mathbb{Z}_{15}^*$ *has a multiplicative inverse since* 1 *appears in each row of the table. Another observation is that* $\mathbb{Z}_{15}^*$ *is closed under multiplication modulo* n.

Following theorems (presented here without proofs) will be used later.

Theorem 18 (Euler) *For each integer* n, $n > 1$ *following holds*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for all $a \in \mathbb{Z}_n^*$.

Theorem 19 (Fermat) *If* p *is a prime, then*

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

for all $a \in \mathbb{Z}_p^*$.

Proof: Follows from Theorem 18 for $n = p$, since $\phi(p) = p - 1$.

The last theorem holds for all integers from $\mathbb{Z}_p$ except 0, since $0 \notin \mathbb{Z}_p^*$. However for all $a \in \mathbb{Z}_p$ we have that $a^p \equiv a \pmod{p}$.

16 Application: Public-key cryptosystem RSA

In this section we describe RSA[2], the most widely used public-key cryptosystem. The system is based on computations in $\mathbb{Z}_n$. The notion “Public-key cryptosystem” means that there are two (different) cryptographic keys: one, normally used for encryption, called ’public-key’, and another one, normally used for decryption, called ’private key’. The key called private is supposed to be secret and the key called ’public’ is publicly available. It is supposed to be not possible (or unknown) to derive one key from another.

RSA algorithm:

1. Choose two large random primes p and q.
2. Calculate $n = p \cdot q$.
3. Select a smaller odd integer a that is relatively prime with $\phi(n)$, where $\phi(n) = (p-1)(q-1)$.
4. Calculate b that is a multiplicative inverse to a modulo $\phi(n)$,that is, $b = a^{-1} \bmod \phi(n)$.
5. Select (a, n) as a public key.
6. Keep (b, n) as a secret key.
7. Encryption function is defined as following:
$$e_K(x) = x^a \pmod{n}$$
8. Decryption function is defined as following:
$$d_K(y) = y^b \pmod{n}$$

Let us verify that encryption and decryption are two inverse functions:

$$e_K(d_K(x)) = d_K(e_K(x)) = x^{ab} \bmod n = x, \forall x \in \mathbb{Z}_n$$

Since $ab \equiv 1 \pmod{\phi(n)}$, then $ab = k\phi(n) + 1 = k(p-1)(q-1) + 1$.

If $x \not\equiv 0 (\bmod p)$, then $x \bmod p$ from $\mathbb{Z}_p^*$ and by applying Fermat theorem we have that

[2] R.**R**ivest, A.**S**hamir, L. **A**dleman

$$\begin{aligned}
x^{ab} &\equiv x^{k\phi(n)+1} \pmod p \\
&\equiv x^{k(p-1)(q-1)} \cdot x \pmod p \\
&\equiv x \left(x^{(p-1)}\right)^{k(q-1)} \pmod p \\
&\equiv x \pmod p
\end{aligned}$$

However if $x \equiv 0(\bmod p)$, then $x^{ab} \equiv x(\bmod p)$.
Therefore $x^{ab} \equiv x \pmod p$ for all $x \in \mathbb{Z}_p$.
Similarly we can show that $x^{ab} \equiv x \pmod q$ for all $x \in \mathbb{Z}_q$.
Therefore

$$\begin{cases} x^{ab} \equiv x(\bmod p) \\ x^{ab} \equiv x(\bmod q) \end{cases}$$

or equivalently

$$\begin{cases} x^{ab-1} \equiv 1(\bmod p) \\ x^{ab-1} \equiv 1(\bmod q) \end{cases}$$

Denoting x^{ab-1} as y we get

$$\begin{cases} y \equiv 1(\bmod p) \\ y \equiv 1(\bmod q) \end{cases}$$

Since p and q are two primes, from Chinese remainder theorem follows that

$$\begin{cases} y \equiv 1(\bmod p) \\ y \equiv 1(\bmod q) \end{cases}$$

if and only if

$$y \equiv 1 \bmod n$$

or

$$x^{ab} \equiv x(\bmod n)$$

Thus we can use $e_K(x)$ to encrypt message x and $d_K(y)$ to decrypt message y.

Let us calculate $d_K(x)$ and send message x together with $d_K(x)$ (as a signature). Then only the owner of private key can create $d_K(x)$. However anyone can use public key and verify that signature is correct by calculating $e_K(d_K(x))$ and comparing the result with x. If $e_K(d_K(x)) = x$, then x was signed and received without change of those who knows the private key.

Example 12 *Assume that Alice choose $p = 101$ and $q = 113$. Then $n = 11413$ and $\phi(n) = 100 \cdot 112 = 11200 = 2^6 5^2 7$. Let us choose a that is not divisible by $2, 5$ or 7. Assume that Alice has selected $a = 3533$. By using Extended Euclid Algorithm we can find that $a^{-1} = 6597 \bmod 11200$. Therefore $b = 6597$. Alice publishes $n = 11413$ and $a = 3533$. Now when*

Bob wants to sent message 9726 *to Alice he computes* $9726^{3533} \bmod 11413 = 5761$ *and sends* 5761*. When Alice receives* 5761*, she decrypts it in the following way:* $5761^{6597} \bmod 11413 = 9726$.

17 Exercises with solutions

Exercise 17.1 *Use Extended Euclid algorithm to find following multiplicative inverse:*

1. $17^{-1} \bmod 101$
2. $357^{-1} \bmod 1234$
3. $3125^{-1} \bmod 9987$

. . . .

$17^{-1} \equiv 6 \pmod{101}$. *Test:* $17 \cdot 6 \equiv 1 \pmod{101}$
$357^{-1} \equiv 1075 \pmod{1234}$. *Test:* $375 \cdot 1075 \equiv 1(\bmod 1234)$
$3125^{-1} \equiv 1844 \pmod{9987}$. *Test:* $3125 \cdot 1844 \equiv 1 \pmod{9987}$

Exercise 17.2 *Find all solutions of the following equation:*

$$35x \equiv 10 \pmod{50}$$

. . . .

There is no unique solution here because $\gcd(35, 50) = 5 > 1$. *From equation above follows that*

$$35x = 50k + 10, k \in \mathbb{Z}$$

or at

$$7x = 10k + 2, k \in \mathbb{Z}$$

It means that

$$7x \equiv 2(\bmod 10)$$

Since $\gcd(7, 10) = 1$, *there exists* $7^{-1} \bmod 10$ *that is equal* 3, *that is* $7^{-1} \equiv 3 \pmod{10}$. *Therefore the last equation can be presented in the form*

$$7^{-1} \cdot 7x \equiv 7^{-1} \cdot 2(\bmod 10)$$
$$\equiv 6(\bmod 10)$$

or $x \equiv 6 \pmod{10}$. *It means that*

$$\mathbf{x = 10k + 6}, \forall \mathbf{k} \in \mathbb{Z}$$

or, since we have find solutions modulo 50 then $x \in \{6, 16, 26, 36, 46\} \subset \mathbb{Z}_{50}$.

To verify that it is a solution we can see that:
$35x = 35\,(10k + 6) = 350k + 210$. *Men* $350k + 210 \equiv 10(\bmod 50)$.

Exercise 17.3 *Find x that satisfy following two equations:*

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{13} \end{cases}$$

. . . .

$a_1 = 2$*,* $a_2 = 3$*,* $n_1 = m_2 = 5$*,* $n_2 = m_1 = 13$*. Since* $13^{-1} \equiv 2(\bmod 5)$ *og* $5^{-1} \equiv 8 \pmod{13}$ *the solution will be:*

$$\begin{aligned} x &\equiv 2 \cdot 13 \cdot 2 + 3 \cdot 5 \cdot 8 \pmod{5 \cdot 13} \\ &\equiv 52 + 120 \pmod{65} \\ &\equiv 172 \pmod{65} \\ &\equiv 42 \pmod{65} \end{aligned}$$

Exercise 17.4 *Find all solutions of the following system of equations:*

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{11} \end{cases}$$

. . . .

$a_1 = 4$*,* $a_2 = 5$*,* $n_1 = m_2 = 5$*,* $n_2 = m_1 = 11$*. Since* $11^{-1} \equiv 6(\bmod 5)$ *og* $5^{-1} \equiv 9 \pmod{11}$

the solution can be found as following:

$$\begin{aligned} x &\equiv 4 \cdot 11 \cdot 6 + 5 \cdot 5 \cdot 9 \pmod{5 \cdot 11} \\ &\equiv 264 + 225 \pmod{55} \\ &\equiv 489 \pmod{55} \\ &\equiv 49 \pmod{55} \end{aligned}$$

Exercise 17.5 *Find all integer x that has remainders $1, 2, 3, 4, 5$ when it will be divided by $2, 3, 4, 5, 6$ respectively.*

. . . .

It means that we have to find a solution for the following system of congruences:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \end{cases}$$

Problem is that not all n_i are pairwise coprime (for example, $2, 4, 6$ or $3, 6$). But if $x \equiv 3 \pmod 4$, then $x = 4k + 3$, $k \in \mathbb{Z}$. Therefore $x \bmod 2 = (4k + 3) \bmod 2 = (2(2k + 1) + 1) \bmod 2 = 1 \bmod 2$. It means that if $x \equiv 3 \pmod 4$ then $x \equiv 1 \pmod 2$ (but not the opposite). In the same way we can see that if $x \equiv 5 \pmod 6$ then $x \equiv 1 \pmod 2$. Therefore we can find solution of the the following system:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

However not all solutions of the above system are solutions of the system we have to solve.

$a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $n_1 = 2$, $n_2 = 3$, $n_3 = 5$, $m_1 = 15$, $m_2 = 10$, $m_3 = 6$. *Since* $15^{-1} \equiv 1 (\bmod 2)$ *and* $10^{-1} \equiv 1 \pmod 3$ *and* $6^{-1} \equiv 1 (\bmod 5)$ *we can find that the solution is:*

$$\begin{aligned} x &\equiv 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 4 \cdot 6 \cdot 1 \pmod{2 \cdot 3 \cdot 5} \\ &\equiv 15 + 20 + 24 \pmod{30} \\ &\equiv 59 \pmod{30} \\ &\equiv 29 \pmod{30} \end{aligned}$$

Solutions of the last system are integers $30k + 29, k \in \mathbb{Z}$. We have to choose among these those integers that are also solutions of the original system.

All integers from $\{30k+29, k \in \mathbb{Z}\}$ are solutions for the last systems (with 3 congruences), but we have to choose those integers that are in additions also solutions for equations

$x \equiv 3 \pmod 4$ *and* $x \equiv 5 \pmod 6$.

We can find that

$$\begin{aligned} (30k + 29) \bmod 4 &= ((28k + 2k) + (28 + 1)) \bmod 4 \\ &= (28(k + 1) + (2k + 1)) \bmod 4 \\ &= (2k + 1) \bmod 4. \end{aligned}$$

Therefore in order to find $k \in \mathbb{Z}$ such that $30k + 29 \equiv 3 \pmod 4$ we analyze $2k + 1 \equiv 3 \pmod 4$. It means that $2k + 1 = 4t + 3$ or $2k = 4t + 2$ or $k = 2t + 1, t \in \mathbb{Z}$. Therefore all integers $30(2t + 1) + 29, t \in \mathbb{Z}$ are solutions of these four equations.

Now we shal find out which of theses integers are (in addition) solutions for equation $x \equiv 5 \pmod 6$. It means that we have to find for which $t \in \mathbb{Z}$

following holds: $30(2t+1)+29 \equiv 5 \pmod 6$. *Since* $30 \equiv 0 (\bmod 6)$ *and* $29 \equiv 5 (\bmod 5)$ *we conclude that* $30(2t+1)+29 \equiv 5 \pmod 6$ *for all* $t \in \mathbb{Z}$.

Thus all x *from* $\{30(2t+1)+29 | t \in \mathbb{Z}\} = \{60t+59 | t \in \mathbb{Z}\}$ *are solutions of the original system of congruences.*

Exercise 17.6 *Solve the following system of equations:*

$$\begin{cases} 13x \equiv 4 \pmod{99} \\ 15x \equiv 56 (\bmod 101) \end{cases}$$

. . . .

Since $\gcd(13, 99) = 1$ *and* $\gcd(15, 111) = 1$*, so there exists a multiplicative inverse to* 13 *modulo* 99*, and to* 15 *modulo* 101*. We can find with by applying extended euclid algorithm that* $13^{-1} \equiv 61 \pmod{99}$ *and* $15^{-1} \equiv 27 \pmod{101}$.

Therefore can consider solving of system instead:

$$\begin{aligned} 13^{-1} \cdot 13x &\equiv 13^{-1} \cdot 4 \pmod{99} \equiv 61 \cdot 4 (\bmod 99) \equiv 46 (\bmod 99) \\ 15^{-1} \cdot 15x &\equiv 15^{-1} \cdot 56 (\bmod 101) \equiv 27 \cdot 56 (\bmod 101) \equiv 98 (\bmod 101) \end{aligned}$$

or

$$\begin{aligned} x &\equiv 46 \pmod{99} \\ x &\equiv 98 (\bmod 101) \end{aligned}$$

Here $a_1 = 46, a_2 = 98, n_1 = m_2 = 99$ *and* $n_2 = m_1 = 101$. *Since* $m_1^{-1} \bmod n_1 = 101^{-1} \bmod 99 = 50$ *and* $m_2^{-1} \bmod n_2 = 99^{-1} \bmod 101 = 50$. *Then the solution for such system will be:*

$$\begin{aligned} x &\equiv 46 \cdot 101 \cdot 50 + 98 \cdot 99 \cdot 50 \pmod{99 \cdot 101} \\ &\equiv 717400 (\bmod 9999) \\ &\equiv \mathbf{7471} \end{aligned}$$

Exercise 17.7 *Compute* $\phi(35), \phi(1111), \phi(1024), \phi(10000)$.

. . . .

$\phi(35) = \phi(5 \cdot 7) = \phi(5) \cdot \phi(7) = 4 \cdot 6 = 24.$

$\phi(1111) = \phi(11 \cdot 101) = 10 \cdot 100 = 1000$

$\phi(1024) = \phi\left(2^{10}\right) = 2^{10-1}(2-1) = 512$

$\phi(10000) = \phi\left(2^4 \cdot 5^4\right) = \phi\left(2^4\right) \cdot \phi\left(5^4\right) = 2^3 \cdot 5^3 (5-1) = 8 \cdot 125 \cdot 4 = 4000$

Exercise 17.8 *Find both private and public keys for RSA if* $p = 11$ *and* $q = 29$. *Encrypt and sign message* $x = 100$ *by using those keys.*

. . . .

1. $n = 11 \cdot 29 = 319$

2. $\phi(n) = \phi(319) = 10 \cdot 28 = 280$

3. Choose a *such that* $\gcd(a, 280) = 1$. *For example, we can select* $a = 17$ *and calculate* b :

$$\begin{aligned} b &\equiv 17^{-1} (\mathrm{mod}\, 280) \\ &\equiv 33 (\mathrm{mod}\, 280) \end{aligned}$$

4. Then we have public key $(17, 319)$ *and private key* $(33, 319)$.
Encrypted integer 100 *is:* $e_K(100) = 100^{17} \bmod 319 = 254$.
We can calculate that

$$\begin{aligned} 100^{17} \bmod 319 &= \left(\left(100^8 \bmod 319\right) \cdot \left(100^8 \bmod 319\right) \cdot 100\right) \bmod 319 \\ &= 45 \cdot 45 \cdot 100 \bmod 319 = 202500 \bmod 319 = \mathbf{254}. \end{aligned}$$

Test: $d_K(254) = 254^{33} \bmod 319 =$
We compute it as following:

$$\begin{aligned} 254^{33} &\equiv \left(254^{10} \bmod 319\right)^3 \left(254^3 \bmod 319\right) (\mathrm{mod}\, 319) \\ &\equiv 111^3 \cdot 34 \,(\mathrm{mod}\, 319) \\ &\equiv \mathbf{100} \end{aligned}$$

where

$$\begin{aligned} 254^{10} \bmod 319 &= \left(\left(254^4 \bmod 319\right) \cdot 254 \bmod 319\right)^2 \bmod 319 \\ &= 100 \cdot 100 \bmod 319 = 111 \end{aligned}$$

Message 100 *can be signed by signature* 122 *that can be computed as:*

$$\begin{aligned} d_K(100) &= 100^{33} \,(\mathrm{mod}\, 319) \\ &= \left(100^5 \bmod 319\right)^6 \left(100^3 \bmod 319\right) \bmod 319 \\ &= \left(\left(122^6 \bmod 319\right) 254\right) \bmod 319 \\ &= 111 \cdot 254 \bmod 319 \\ &= 122 \end{aligned}$$

Verification of validity of such signature can be done as following:

$$\begin{aligned} e_K(122) &= 122^{17} \bmod 319 \\ &= \left(122^5 \bmod 319\right)^3 \cdot \left(122^2 \bmod 319\right) \bmod 319 \\ &= 265^3 \cdot 210 \bmod 319 \\ &= \mathbf{100} \end{aligned}$$
