4.2 Congruence relation modulo n

We have introduced the extended Euclid's algorithm which helped us to solve Diophantic equations; linear equations with two unknowns where we look only for integer solutions. The material of the last lecture will be used for introduction new "numbers", residue classes, and operations with them.

4.2.1 The Relation Modulo n. First of all we introduce an equivalence relation *modulo* n for a natural number $n > 1$. You have already come across it; indeed, consider the imaginary unit i. We have

$$i^2 = -1, \quad i^3 = -i, \quad i^4 = 1, \quad \text{and} \quad i^5 = i.$$

Therefore, it is easy to calculate powers of the imaginary unit i; indeed for example $i^{651} = i^{4\cdot 162+3} = 1^{162} \cdot i^3 = -i$. More generally, to calculate i^k it suffices to know the remainder r when k is divided by 4, and then we have $i^k = i^r$.

Definition. Given two integers a, b and a natural number $n > 1$. We say that a *is congruent to* b *modulo* n and write $a \equiv b \pmod n$ if $a - b$ is divisible by n. □

4.2.2 Equivalent Characterizations of Modulo n. We could introduce the relation modulo n in other two ways.

Proposition. Let a and b be two integers. Then the following is equivalent:

1. $a \equiv b \pmod n$,
2. $a = b + k\,n$ for some integer k,
3. a and b have the same remainders when divided by n.

□

Justification. It is clear that conditions 1. and 2. are equivalent; indeed the fact that $a - b$ is divisible by n means that $a - b = k\,n$ for some integer $k \in \mathbb{Z}$; and this is the same as $a = b + k\,n$.

We show that $a \equiv b \pmod n$ if and only if a and b have the same remainder when divided by n. Assume that $a = q_1\,n + r_1$, $b = q_2\,n + r_2$ and $0 \le r_1, r_2 < n$.

If $r_1 = r_2$, then $a - b = (q_1 - q_2)\,n$ and $a \equiv b \pmod n$ holds.

If $r_1 \neq r_2$, then from the uniqueness of the division theorem, $a - b$ is not divisible by n, so $a \equiv b \pmod n$ does not hold. □

4.2.3 The Relation Modulo n is an Equivalence Relation on $\mathbb{Z}$.

Proposition. Let a, b, and c be integers. Then

1. $a \equiv a \pmod n$ (modulo n is reflexive);
2. if $a \equiv b \pmod n$, then also $b \equiv a \pmod n$ (modulo n is symmetric);
3. if $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$ (modulo n is transitive).

□

The justification is easy, especially if we use 4.2.2.

4.2.4 Properties of the Equivalence Modulo n. The equivalence modulo n also "maintain" operations addition and multiplication of integers. More precisely:

Proposition. Assume that for integers a, b, c, and d it holds that $a \equiv b \pmod n$ and $c \equiv d \pmod n$. Then

$$(a + c) \equiv (b + d) \pmod n \quad \text{a} \quad (a \cdot c) \equiv (b \cdot d) \pmod n.$$

□

Justification. Assume that $a \equiv b \pmod n$ and $c \equiv d \pmod n$. Then $a = b + kn$ and $c = d + rn$ for some $k, r \in \mathbb{Z}$. Therefore, $a + c = b + d + (k + r)n$ and $a \cdot c = (b + kn)(d + rn) = bd + (br + dk + krn)n$. And this is equivalent to $(a + c) \equiv (b + d) \pmod n$ and $(a \cdot c) \equiv (b \cdot d) \pmod n$. □

4.2.5 The 4.2.4 has two special cases. We state them as corollaries.

Corollary. Given two integers a, b such that $a \equiv b \pmod n$. Then

1. $ra \equiv rb \pmod n$ for every integer r;
2. $a^k \equiv b^k \pmod n$ for every natural number k.
3. Moreover, if $a_i \equiv b_i \pmod n$ for every $i = 0, \ldots, k$, a $r_0, \ldots, r_k$ are arbitrary integers, then
$$(r_0\, a_0 + \ldots + r_k\, a_k) \equiv (r_0\, b_0 + \ldots + r_k\, b_k) \pmod n.$$

□

Justification. 1. To prove the first part it suffices to use the above proposition 4.2.4 for the pair $r \equiv r \pmod n$ a $a \equiv b \pmod n$.

2. From the above proposition we know that $a^2 \equiv b^2 \pmod n$ (we have used $a \equiv b \pmod n$ and $a \equiv b \pmod n$). Now, from $a \equiv b \pmod n$ and $a^2 \equiv b^2 \pmod n$ we get $a^3 \equiv b^3 \pmod n$, $a^4 \equiv b^4 \pmod n$, etc.

To make the argument more accurate we can use mathematical induction over k. □

4.2.6 We can ask whether the first part of the corollary is still valid if we reverse the implication. More precisely, if from $ra \equiv rb \bmod n$ it follows that $a \equiv b \bmod n$. A simple example shows that this is not the case. Indeed, we have $6 \equiv 10 \bmod 4$, but $3 \not\equiv 5 \bmod 4$. The following proposition states what can be deduced form $r\,a \equiv r\,b \bmod n$.

Proposition. Let r, a, b be integers and n a natural number $n > 1$ such that $ra \equiv rb \pmod n$. Then
$$a \equiv b \left(\bmod \frac{n}{\gcd(n, r)}\right). \tag{4.2}$$

□

Justification. We know that $ra - rb = kn$ for an integer $k \in \mathbb{Z}$. Hence $r(a - b) = kn$. Denote $d = \gcd(r, n)$. Then $r = s \cdot d$, $n = m \cdot d$, and the integers s and m are relatively prime. Substituting into $r(a - b) = kn$ and get

$$s\,d\,(a - b) = k\,m\,d, \quad \text{and} \quad s\,(a - b) = k\,m.$$

Since the numbers s and m are relatively prime, and s divides the product $k\,m$, the number s must divide k. Therefore, $s\,(a - b) = s\,j\,m$ and $a - b = j\,m$. We have shown that $a \equiv b \pmod m$, in other words $a \equiv b \pmod{\frac{n}{\gcd(n,r)}}$. □

4.2.7 Solving $(a + x) \equiv b \bmod n$. Given integers a, b and a natural number $n > 1$. Find all integers x for which
$$(a + x) \equiv b \pmod n. \tag{4.3}$$
This problem has got always a solution which is any $x \in \mathbb{Z}$ for which $x \equiv (b - a) \pmod n$.

4.2.8 Solving $(a \cdot x) \equiv b \bmod n$. Given two integers a, b and a natural number $n > 1$. Find all integers x for which
$$a\,x \equiv b \pmod n. \tag{4.4}$$
Such x does not always exist. For example, there is no integer x for which $2x \equiv 3 \pmod 4$. We will use Diophantic equations and their solutions to find a necessary and sufficient condition on a, b, and n for which $x \in Z$ satisfying the relation 4.4 exists.

4.2.9 Proposition. Equation 4.4 has got a solution if and only if the number b is a multiple of $\gcd(a, n)$.

In this case all integers x satisfying 4.4 are solutions of the following Diophantic equation

$$a\,x + n\,y = b.$$

□

Justification. We know that $a\,x \equiv b \pmod{n}$ means $a\,x - b = k\,n$ for an integer $k \in \mathbb{Z}$, and this is equivalent to $a\,x - k\,n = b$. If we substitute $y := -k$, we get the Diophantic equation 4.2 which has a solution if and only if b is divisible by $\gcd(a, n)$. □

4.2.10 Let us mention another property that the equivalences modulo have got.

Proposition. Let $n > 1$, $m > 1$ be two relatively prime natural number. And let for some $a, b \in \mathbb{Z}$ it holds that $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$

Then also $a \equiv b \pmod{nm}$. □

Justification. We know that $a - b = kn$ and $a - b = jm$ for some $k, j \in \mathbb{Z}$. Hence $kn = jm$. Since n and m are relatively prime and n divides the product jm, we know that n divides j. So $a - b = jm = r\,nm$ for some $r \in \mathbb{Z}$. We have shown that $a \equiv b \pmod{nm}$. □

4.2.11 Remark. A stronger proposition can be proved than 4.2.10, namely: Assume that $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$. Let $n_1 = \frac{n}{\gcd(n,m)}$ and $m_1 = \frac{m}{\gcd(n,m)}$. Then

$$a \equiv b \pmod{n_1 m_1}.$$

The justification is analogous to 4.2.10; indeed, the equation $kn = jm$ must be first divided by $\gcd(n, m)$.

4.2.12 Small Fermat Theorem. We will end this part concerning the equivalence modulo n by the small Fermat theorem which is a basis of the RSA public-key cryptosystem. (In literature, the Small Fermat Theorem is sometimes called Fermat Little Theorem.)

Theorem. Let p be a prime and a an integer relatively prime to p. Then

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

□

Justification. One of the proofs of the small Fermat theorem uses basic properties of groups and we will give it later. There is also a proof which uses only elementary mathematics. In fact, we will first show that for every integer a it holds that $a^p \equiv a \bmod p$ by mathematical induction on a

1. Basic step: Let $a = 0$ or $a = 1$. Then $a^p = a$, hence $a^p \equiv a \pmod{p}$.

2. Induction step: Assume that $a^p \equiv a \pmod{p}$, and calculate $(a+1)^p - (a+1)$. By the binomial theorem we have

$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + 1 - (a+1) =$$

$$= a^p - a + \binom{p}{1}a^{p-1} + \ldots + \binom{p}{p-1}a.$$

We know by the induction hypothesis that $a^p - a$ is divisible by p. Hence, if we show that $\binom{p}{i}$ is divisible by p for every i, $0 < i < p$, we will know that so is $(a+1)^p - (a+1)$. And this means that $(a+1)^p \equiv (a+1) \bmod p$.

We know that

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!}.$$

Hence

$$i!\,(p-i)!\binom{p}{i} = p!.$$

Moreover, p divides neither $i!$ $(i < p)$ nor $(p-i)!$ $(0 < i)$. Hence, p must divide $\binom{p}{i}$.

Now, assume that a and p are relatively prime. We have $a^p - a = k\,p$ for some $k \in \mathbb{Z}$. Thus $a\,(a^{p-1} - 1) = k\,p$. Since a and p are relatively prime, a divides k and $a^{p-1} - 1 = j\,p$ which proves that $a^{p-1} \equiv 1 \pmod p$. □

4.3 Residue Classes Modulo n

We know that the relation modulo n is an equivalence relation on the set $\mathbb{Z}$, see 4.2.3. An equivalence class of the equivalence modulo n containing a number $i \in \mathbb{Z}$ is called the *residue class containing* i and is denoted by $[i]_n$. We know that

$$[i]_n = \{j \mid j = i + kn \text{ for some } k \in \mathbb{Z}\}. \tag{4.5}$$

The name residue classes comes from the fact that an integer j belongs to $[i]_n$ if and only if i and j have the same remainders when divided by n.

4.3.1 The Set $\mathbb{Z}_n$. There are n distinct residue classes modulo n; indeed, they are the residue classes corresponding to the numbers (remainders) $0, 1, \ldots, n-1$. The set of all residue classes is denoted by $\mathbb{Z}_n$, so

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

4.3.2 Calculations in $\mathbb{Z}_n$. It is clear from the proposition 4.2.4 that the equivalence modulo n is compatible with operations $+$ and $\cdot$. Indeed, if $i \equiv j \pmod n$ and $k \equiv l \pmod n$ then $i + k \equiv j + l \pmod n$ and $i \cdot k \equiv j \cdot l \pmod n$. These properties can be reformulate as follows:

If we choose any $a \in [i]_n$ and any $b \in [j]_n$ then the number $a + b$ belongs to $[i + j]_n$, and the number $a \cdot b$ belongs to $[i \cdot j]_n$. This allows us to define operations addition $\oplus$ and multiplication $\odot$ on the set $\mathbb{Z}_n$ as follows:

$$[i]_n \oplus [j]_n = [i + j]_n, \qquad [i]_n \odot [j]_n = [i \cdot j]_n. \tag{4.6}$$

4.3.3 Properties of the Operation $\oplus$.

- $\oplus$ is associative, i.e. for any three integers i, j, k we have:

$$([i]_n \oplus [j]_n) \oplus [k]_n = [i]_n \oplus ([j]_n \oplus [k]_n).$$

- $\oplus$ is commutative, i.e. for any two integers i, j we have:

$$[i]_n \oplus [j]_n = [j]_n \oplus [i]_n.$$

- The class $[0]_n$ plays the role of "zero", more precisely, for any integer i we have:

$$[0]_n \oplus [i]_n = [i]_n.$$

- We can "subtract", more precisely for any integer $[i]_n$ there exists class $-[i]_n$ such that

$$[i]_n \oplus (-[i]_n) = [0]_n.$$

□

Justification. Verification of the above properties is straightforward and it is left to the reader.

4.3.4 Properties of the Operation $\odot$.

- $\odot$ is associative, i.e for any three integers i, j, k we have:
$$([i]_n \odot [j]_n) \odot [k]_n = [i]_n \odot ([j]_n \odot [k]_n).$$
- $\odot$ is commutative, i.e. for any two integers i, j we have:
$$[i]_n \odot [j]_n = [j]_n \odot [i]_n.$$
- The class $[1]_n$ plays the role of "identity", More precisely, for any integer i we have:
$$[1]_n \odot [i]_n = [i]_n.$$

□

Justification. Verification of the above properties is straightforward and it is left to the reader.

4.3.5 Remark. In the above properties there is no one which means something as "cancellation" or "division" for $\odot$. More precisely, we have not stated any general condition under which for a given integer i there exists an integer j such that $[i]_n \odot [j]_n = [1]_n$. The reason is that no every equation of the form $[i]_n \odot [x]_n = [1]_n$ has a solution. The following proposition characterizes i and n for which such x exists.

4.3.6 Properties of the Operation $\odot$.

- $\odot$ is associative, i.e for any three integers i, j, k we have:
$$([i]_n \odot [j]_n) \odot [k]_n = [i]_n \odot ([j]_n \odot [k]_n).$$
- $\odot$ is commutative, i.e. for any two integers i, j we have:
$$[i]_n \odot [j]_n = [j]_n \odot [i]_n.$$
- The class $[1]_n$ plays the role of "identity", More precisely, for any integer i we have:
$$[1]_n \odot [i]_n = [i]_n.$$

□

Justification. $[i]_n \odot [x]_n = [j]_n$ can be rewritten as $[i \cdot x]_n = [j]_n$ and hence

$$i \cdot x \equiv j \bmod n.$$

And this leads to

$$i\,x - j = k\,n, \text{ so we have } i\,x - k\,n = j.$$

And the last equation is in fact a Diophantic equation $i\,x + n\,y = j$ which has a solution if and only if j is a multiple of $\gcd(i, n)$.

From **??** we know that all integers $x \in \mathbb{Z}$ satisfying $i\,x + n\,y = j$ are of the form $x_0 + k\,n_1$ where x_0 is one solution of the non-homogeneous equation, and $i_1 = \frac{i}{d}$ and $n_1 = \frac{n}{d}$. It can be shown that for $x_k = x_0 + k\,n_1$ it holds that $[x_k]_n$ are distinct elements of $\mathbb{Z}_n$ for which **??** holds. □

4.3.7 A special case of **??** is the following:

Corollary. For a residue class $[i]_n$ there is a residue class $[x]_n$ such that

$$[i]_n \odot [x]_n = [1]_n \tag{4.7}$$

if and only if the numbers i and n are relatively prime. □

The class $[x]_n$ satisfying 4.7 is called the *inverse* of $[i]_n$ and we denote it $[i]_n^{-1}$.

4.3.8 Distributivity Law for $\oplus$ and $\odot$. For any three integers i, j, k it holds that

$$[i]_n \odot ([j]_n \oplus [k]_n) = ([i]_n \odot [j]_n) \oplus ([i]_n \odot [k]_n).$$

4.3.9 Remark. If p is a prime number then the set $\mathbb{Z}_p$ satisfies all the properties that addition and multiplication of real numbers have got.

If n is a composite number (not a prime) then the situation is different. For example if $n = r \cdot s$, $0 < r < n$ and $0 < s < n$, then $[r]_n \odot [s]_n = [0]_n$ even though the classes $[r]_n$ and $[s]_n$ are non-zero. (It means that we cannot "divide" by such elements.)

4.3.10 Convention. Later on, when there is not fear of misunderstanding we will write $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ instead of $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ and the operations $\oplus$, $\odot$ will be denoted by an "ordinary signs", i.e. simply by $+$ and $\cdot$.

Note that we can write that in $\mathbb{Z}_n$ for every $i, j \in \mathbb{Z}_n$

$$i + j = k, \text{ where } k \text{ is the remainder when } i + j \text{ is divided by } n;$$

$$i \cdot j = l, \text{ where } l \text{ is the remainder when } i\,j \text{ is divided by } n.$$