2. Congruences. Chinese Remainder Theorem

2.1. Definition. Let $m \in \mathbb{Z}$. Two integers x, y are called *congruent modulo* m, in symbols

$$x \equiv y \bmod m,$$

if m divides the difference $x - y$, i.e. $x - y \in m\mathbb{Z}$.

Examples. $20 \equiv 0 \bmod 5$, $3 \equiv 10 \bmod 7$, $-4 \equiv 10 \bmod 7$.
$x \equiv 0 \bmod 2$ is equivalent to "x is even",
$x \equiv 1 \bmod 2$ is equivalent to "x is odd".

Remarks. a) x, y are congruent modulo m iff they are congruent modulo $-m$.
b) $x \equiv y \bmod 0$ iff $x = y$.
c) $x \equiv y \bmod 1$ for all $x, y \in \mathbb{Z}$.
Therefore the only interesting case is $m \geq 2$.

2.2. Proposition. *The congruence modulo m is an equivalence relation, i.e. the following properties hold:*

i) *(Reflexivity)* $x \equiv x \bmod m$ *for all* $x \in \mathbb{Z}$
ii) *(Symmetry)* $x \equiv y \bmod m \implies y \equiv x \bmod m$.
iii) *(Transitivity)* $(x \equiv y \bmod m) \wedge (y \equiv z \bmod m) \implies x \equiv z \bmod m$.

2.3. Lemma (Division with rest). *Let $x, m \in \mathbb{Z}$, $m \geq 2$. Then there exist uniquely determined integers q, r satisfying*

$$x = qm + r, \quad 0 \leq r < m.$$

Remark. The equation $x = qm + r$ implies that $x \equiv r \bmod m$. Therefore every integer $x \in \mathbb{Z}$ is equivalent modulo m to one and only one element of

$$\{0, 1, \ldots, m-1\}.$$

2.4. Definition. Let m be a positive integer. The set of all equivalence classes of $\mathbb{Z}$ modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$ or briefly by $\mathbb{Z}/m$.

From the above remark we see that

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$

where $\overline{x} = x \bmod m$ is the equivalence class of x modulo m. If there is no danger of confusion, we will often write simply x instead of $\overline{x}$.

Equivalence modulo m is compatible with addition and multiplication, i.e.

$$x \equiv x' \bmod m \quad \text{and} \quad y \equiv y' \bmod m \implies$$
$$x + y \equiv x' + y' \bmod m \quad \text{and} \quad xy \equiv x'y' \bmod m.$$

Therefore addition and multiplication in $\mathbb{Z}$ induces an addition and multiplication in $\mathbb{Z}/m$ such that $\mathbb{Z}/m$ becomes a commutative ring and the canonical surjection

$$\mathbb{Z} \longrightarrow \mathbb{Z}/m, \quad x \mapsto x \bmod m,$$

is a ring homomorphism.

Example. In $\mathbb{Z}/7$ one has

$$\overline{3} + \overline{4} = \overline{7} = \overline{0}, \quad \overline{3} + \overline{5} = \overline{8} = \overline{1}, \quad \overline{3} \cdot \overline{5} = \overline{15} = \overline{1}.$$

The following are the complete addition and multiplication tables of $\mathbb{Z}/7$.

+	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

×	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	2	2
6	0	6	5	4	3	2	1

2.5. Theorem. *Let m be a positive integer. An element $\overline{x} \in \mathbb{Z}/m$ is invertible iff* $\gcd(x, m) = 1$.

Proof. "$\Leftarrow$" Suppose $\gcd(x, m) = 1$. By theorem 1.6 there exist integers ξ, μ such that

$$\xi x + \mu m = 1.$$

This implies $\xi x \equiv 1 \bmod m$, hence $\overline{\xi}$ is an inverse of $\overline{x}$ in $\mathbb{Z}/m$.

"$\Rightarrow$" Suppose that $\overline{x}$ is invertible, i.e. $\overline{x} \cdot \overline{y} = \overline{1}$ for some $\overline{y} \in \mathbb{Z}/m$. Then $xy \equiv 1 \bmod m$, hence there exists an integer k such that $xy - 1 = km$. Therefore $yx - km = 1$, which means by theorem 1.6 that x and m are coprime, q.e.d.

2.6. Corollary. *Let m be a positive integer. The ring $\mathbb{Z}/m$ is a field iff m is a prime.*

Notation. If p is a prime, the field $\mathbb{Z}/p$ is also denoted by $\mathbb{F}_p$.

For any ring A with unit element we denote its multiplicative group of invertible elements by A^*. In particular we use the notations $(\mathbb{Z}/m)^*$ and $\mathbb{F}_p^*$.

Example. For $p = 7$ we have the field $\mathbb{F}_7 = \mathbb{Z}/7$ with 7 elements. From the above multiplication table we can read off the inverses of the elements of $\mathbb{F}_7^* = \mathbb{F}_7 \smallsetminus \{0\}$.

x	1	2	3	4	5	6
x^{-1}	1	4	5	2	3	6

2.7. *Direct Products.* For two rings (resp. groups) A_1 and A_2, the cartesian product $A_1 \times A_2$ becomes a ring (resp. a group) with component-wise defined operations:

$$(x_1, x_2) + (y_1, y_2) := (x_1 + y_1, x_2 + y_2)$$
$$(x_1, x_2) \cdot (y_1, y_2) := (x_1 y_1, x_2 y_2).$$

If A_1, A_2 are two rings with unit element, then $(0, 0)$ is the zero element and $(1, 1)$ the unit element of $A_1 \times A_2$. For the group of invertible elements the following equation holds:

$$(A_1 \times A_2)^* = A_1^* \times A_2^*.$$

Note that if A_1 and A_2 are fields, the direct product $A_1 \times A_2$ is a ring, but not a field, since there are zero divisors:

$$(1, 0) \cdot (0, 1) = (0, 0).$$

2.8. Theorem (Chinese remainder theorem). *Let m_1, m_2 be two positive coprime integers. Then the map*

$$\phi : \mathbb{Z}/m_1 m_2 \longrightarrow \mathbb{Z}/m_1 \times \mathbb{Z}/m_2, \quad \overline{x} \mapsto (x \bmod m_1, x \bmod m_2)$$

is an isomorphism of rings.

Proof. It is clear that ϕ is a ring homomorphism. Since $\mathbb{Z}/m_1 m_2$ and $\mathbb{Z}/m_1 \times \mathbb{Z}/m_2$ have the same number of elements (namely $m_1 m_2$), it suffices to prove that ϕ is injective.

Suppose $\phi(\overline{x}) = 0$. This means that $x \equiv 0 \bmod m_1$ and $x \equiv 0 \bmod m_1$, i.e. $m_1 \mid x$ and $m_2 \mid x$. Since m_1 and m_2 are coprime, it follows that $m_1 m_2 \mid x$, hence $\overline{x} = 0$ in $\mathbb{Z}/m_1 m_2$, q.e.d.

Remark. The classical formulation of the Chinese remainder theorem is the following (which is contained in theorem 2.8):

Let m_1, m_2 be two positive coprime integers. Then for every pair a_1, a_2 of integers there exists an integer a such that

$$a \equiv a_i \bmod m_i \quad \text{for } i = 1, 2.$$

This integer a is uniquely determined modulo $m_1 m_2$.

2.9. Definition (Euler phi function). Let m be a positive integer. Then $\varphi(m)$ is defined as the number of integers $k \in \{0, 1, \ldots, m-1\}$ which are coprime to m. Using theorem 2.5, this can also be expressed as

$$\varphi(m) := \#(\mathbb{Z}/m)^*,$$

where $\#S$ denotes the number of elements of a set S.

For small m, the φ-function takes the following values

m	1	2	3	4	5	6	7	8	9	10
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4

It is obvious that for a prime p one has $\varphi(p) = p-1$. More generally, for a prime power p^k it is easy to see that

$$\varphi(p^k) = p^k - p^{k-1} = p^k\Big(1 - \frac{1}{p}\Big).$$

If m and n are coprime, it follows from theorem 2.8 that

$$(\mathbb{Z}/mn)^* \cong (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*,$$

hence $\varphi(mn) = \varphi(n)\varphi(m)$. Using this, we can derive

2.10. Theorem. *For every positive integer n the following formula holds:*

$$\varphi(n) = n\prod_{p|n}\Big(1 - \frac{1}{p}\Big),$$

where the product is extended over all prime divisors p of n.

Proof. Let $n = \prod_{i=1}^r p_i^{e_i}$ be the canonical prime decomposition of n. Then

$$\varphi(n) = \prod_{i=1}^r \varphi(p_i^{e_i}) = \prod_{i=1}^r p_i^{e_i}\Big(1 - \frac{1}{p_i}\Big) = n\prod_{i=1}^r\Big(1 - \frac{1}{p_i}\Big), \qquad \text{q.e.d.}$$

2.11. Theorem (Euler). *Let m be an integer ≥ 2 and a an integer with* $\gcd(a, m) = 1$. *Then*

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Proof. We use some notions and elementary facts from group theory. Let G be a finite group, written multiplicatively, with unit element e. The order of an element $a \in G$ is defined as

$$\operatorname{ord}(a) := \min\{k \in \mathbb{N}_1 : a^k = e\}.$$

The order of the group is defined as the number of its elements,

$$\operatorname{ord}(G) := \#G.$$

Then, as a special case of a theorem of Lagrange, one has

$$\operatorname{ord}(a) \mid \operatorname{ord}(G) \quad \text{for all } a \in G.$$

We apply this to the group $G = (\mathbb{Z}/m)^*$. By definition $\operatorname{ord}((\mathbb{Z}/m)^*) = \varphi(m)$. Let r be the order of $\overline{a} \in (\mathbb{Z}/m)^*$. Then $\varphi(m) = rs$ with an integer s and we have in $(\mathbb{Z}/m)^*$

$$\overline{a}^{\varphi(m)} = \overline{a}^{rs} = (\overline{a}^r)^s = \overline{1}^s = \overline{1}, \quad \text{q.e.d.}$$

2.12. Corollary (Little Theorem of Fermat). *Let p be a prime and a an integer with $p \nmid a$. Then*

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