COURSE 6

Quotient ring. Modular arithmetic. The Chinese Remainder Theorem

Let $(R,+,\cdot)$ be a commutative ring and let I be an ideal of $(R,+,\cdot)$. The relation

$$x\rho_I y \ \Leftrightarrow \ y-x\in I \ \Leftrightarrow \ y\in x+I$$

is an equivalence relation on R, called **the equivalence relation induced by** (or **modulo**) I.

The set of all the elements of R which are equivalet modulo I to $x\in R$, i.e. the equivalence class of x, is $\rho_I\langle x\rangle = x+I$, and the corresponding quotient set is

$$R/I=\{x+I \mid x\in R\}=\{I, x+I, y+I,\dots\}.$$

Theorem 1. Let $(R,+,\cdot)$ be a commutative ring and let I be an ideal of $(R,+,\cdot)$.
1) The operations

$$(x+I)+(y+I)=(x+y)+I \text{ şi } (x+I)(y+I)=xy+I \tag{1}$$

are well-defined on R/I.
2) $(R/I,+,\cdot)$ is a commutative ring with respect to $+$ and $\cdot$ defined by (1).
3) The canonical projection $p_I : R\to R/I$, $p_I(x)=x+I$ is a unital ring homomorphism from $(R,+,\cdot)$ onto $(R/I,+,\cdot)$.

Definition 2. Let $(R,+,\cdot)$ be a commutative ring and let I be an ideal of $(R,+,\cdot)$. The ring $(R/I,+,\cdot)$ introduced by the previous theorem is called **the quotient (factor) ring of** $(R,+,\cdot)$ **determined by** (or **modulo**) I.

Example 3. The quotient rings of $(\mathbb{Z},+,\cdot)$.
As we saw in the 4th course, $(\mathbb{Z},+,\cdot)$ is a PID and the set of its ideals is $\{n\mathbb{Z}=(n) \mid n\in\mathbb{N}\}$. So, the quotient rings of $(\mathbb{Z},+,\cdot)$ are $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$ with $n\in\mathbb{N}$. More precisely, $\mathbb{Z}_0=\{\{k\} \mid k\in\mathbb{Z}\}$, $\mathbb{Z}_1=\{\mathbb{Z}\}$ are (isomorphic to) $\mathbb{Z}$ and the zero ring, respectively, and for $n\geq 2$, the rings $(\mathbb{Z}_n,+,\cdot)$ are exactly the residue class rings modulo n. Indeed, in $\mathbb{Z}_0$ the operations defined by (1) are

$$\{k\}+\{k'\}=\{k+k'\},\ \{k\}\{k'\}=\{kk'\}$$

and $p_{0\mathbb{Z}}$ is an isomorphism, i.e. $(\mathbb{Z},+,\cdot)\simeq(\mathbb{Z}_0,+,\cdot)$, and in $\mathbb{Z}_1$ the operations defined by (1) are

$$\mathbb{Z}+\mathbb{Z}=\mathbb{Z} \text{ and } \mathbb{Z}\cdot\mathbb{Z}=\mathbb{Z}.$$

For any $n\in\mathbb{N}$, $n\geq 2$,

$$x\rho_{n\mathbb{Z}}y \ \Leftrightarrow \ y-x\in n\mathbb{Z} \ \Leftrightarrow \ n\mid y-x \ \Leftrightarrow \ x\equiv y\,(\mathrm{mod}\, n),$$

therefore $\mathbb{Z}/n\mathbb{Z}=\{\widehat{0},\widehat{1},\dots,\widehat{n-1}\}=\mathbb{Z}_n$, with $\widehat{i}=i+n\mathbb{Z}$, and the operations defined by (1) are exactly the operations from example 3 f) of Course 4:

$$\widehat{i}+\widehat{j}=\widehat{i+j} \text{ and } \widehat{i}\cdot\widehat{j}=\widehat{i\cdot j}.$$

They determine a commutative ring structure on $\mathbb{Z}_n$. The additive identity element of $\mathbb{Z}_n$ is $\widehat{0}$, and the multiplicative identity element is $\widehat{1}$. If $n\geq 2$ is a prime number then (and only then) the ring $\mathbb{Z}_n$ is a field.

Let us remind some of the properties of the congruence relation:

Proposition 4. Let $n \in \mathbb{N}$, $n \geq 2$ and a, b, c, $d \in \mathbb{Z}$. Then:
1) $a \equiv b \,(\mathrm{mod}\, n)$ and $c \equiv d \,(\mathrm{mod}\, n) \Rightarrow a + c \equiv b + d \,(\mathrm{mod}\, n)$ and $ac \equiv bd \,(\mathrm{mod}\, n)$;
2) if $a \equiv b \,(\mathrm{mod}\, n)$ and $k \in \mathbb{N}$ then $a^k \equiv b^k \,(\mathrm{mod}\, n)$, $a + c \equiv b + c \,(\mathrm{mod}\, n)$ and $ac \equiv bc \,(\mathrm{mod}\, n)$;
3) $ac \equiv bc \,(\mathrm{mod}\, nc) \Rightarrow a \equiv b \,(\mathrm{mod}\, n)$;
4) $ac \equiv bc \,(\mathrm{mod}\, n)$ and $(c, n) = 1 \Rightarrow a \equiv b \,(\mathrm{mod}\, n)$.

Remark 5. The above implication 1) states that the operations (1) are well-defined, and 4) means that in the ring $\mathbb{Z}_n$ one can simplify by any class $\widehat{c}$ whose representative c is coprime with n (fact already proved in Course 4).

We will add this list some known properties on integers which involve congruence relations and which can be seen as applications for the corresponding quotient ring properties.

Let us remind that for any ring homomorphism $f : R \to R'$, $\mathrm{Ker} f = \{x \in R \mid f(x) = 0\}$ is an ideal of R and $f(R)$ is a subring of R', and **the ring homomorphism theorem** states that *the quotient ring $R/Kerf$ is isomorphic to $f(R)$.*

Theorem 6. If R is a PID and $a, b \in R$ are coprime, i.e. $(a, b) = 1$, then $R/(ab)$ and $R/(a) \times R/(b)$ are isomorphic rings.

Remark 7. The ring isomorphism provided by the homomorphism theorem is

$$\overline{f} : R/(ab) \to R/(a) \times R/(b),\ \overline{f}(x + (ab)) = (x + (a), x + (b)).$$

Corollary 8. Let $a, b \in \mathbb{N}^* \setminus \{1\}$ and $(a, b) = 1$. For any $c, d \in \mathbb{Z}$, the system

$$\begin{cases} x \equiv c \pmod{a} \\ x \equiv d \pmod{b} \end{cases} \tag{2}$$

has a solution $x_0 \in \mathbb{Z}$ which is unique modulo ab, i.e. $x_0' \equiv x_0 \pmod{ab}$ for any solution x_0' of (2).

Corolary 8 is a particular case of the famous:

Corollary 9. (**The Chinese Remainder Theorem**) Let $n_1, \ldots, n_k \in \mathbb{N}$ a family of natural numbers mutually coprime with $n_i \geq 2$ for all $i \in \{1, \ldots, k\}$. For any $a_1, \ldots, a_k \in \mathbb{Z}$, the system

$$\begin{cases} x \equiv a_1 \,(\mathrm{mod}\, n_1) \\ x \equiv a_2 \,(\mathrm{mod}\, n_2) \\ \vdots \\ x \equiv a_k \,(\mathrm{mod}\, n_k) \end{cases}$$

has a unique solution modulo $n_1 n_2 \ldots n_k$.

We previously saw that the ring multiplication determines a multiplicative group on the set of the units of the ring. Since for the **Euler's totient function** $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n)$ is the number of $i \in \mathbb{N}$ with $i < n$ and $(i, n) = 1$, and the units of $\mathbb{Z}_n$ are the classes $\widehat{i}$ with $(i, n) = 1$, it follows that $|U(\mathbb{Z}_n)| = \varphi(n)$. From theorem 6 we also deduce that:

Corollary 10. If $m, n \in \mathbb{N}^*$ and $(m, n) = 1$ then

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Corollary 11. If $n \in \mathbb{N}$, $n \geq 2$ and

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k},\ p_1, \dots, p_k \text{ mutually different primes},\ \alpha_1, \dots, \alpha_k \in \mathbb{N}^*$$

is the prime number factorization of n then

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1).$$

We remind that from **Lagrange Theorem** (*the order of any subgroup of a finite group G is finite and it divides $|G|$*) one deduces that $a^{|G|} = 1$ for any $a \in G$. Thus, we have the following:

Theorem 12. (**Euler Theorem**) If $a \in \mathbb{Z}$ and $(a, n) = 1$ then

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

Corollary 13. (**Fermat Theorem**) If $p \in \mathbb{N}^*$ is a prime, $a \in \mathbb{Z}$ and $p \nmid a$ then

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

Remark 14. The conclusion of Fermat Theorem is equivalent to

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

and this congruence is also valid for the case $p \mid a$.

Theorem 15. (**Wilson Theorem**) If $p \in \mathbb{N}$ is a prime number then

$$(p-1)! + 1 \equiv 0 \pmod{p}. \tag{9}$$