Introduction to Remainders

This year's fourth autumn series revolves around the topic of remainders which are essential in Olympiad number theory problems. In this text, we will introduce standard notation and present some useful theorems, which will help you solve problems not only from this series.

Divisibility and modulo

If there exist integers a, b, and k such that $a = kb$, we say a is *divisible* by b. In mathematical notation we use the symbol $\mid$ – symbolically, we can write $b \mid a$. Divisibility has many nice properties, some of them are listed below.

Exercise. Show why the statements below hold for integers a, b, c and d.

(1) $1 \mid a$ and $a \mid 0$.
(2) If $ab \mid c$, then $a \mid c$.
(3) If $a \mid b$, then $a \mid bc$.
(4) If $a \mid b$ and $a \mid c$, then $a \mid b + c$.
(5) If $a \mid b$ and $b \mid c$, then $a \mid c$. (And we can shorten the statement to $a \mid b \mid c$.)
(6) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
(7) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

Congruences

As you know, integers can be divided into two classes: even and odd numbers. Congruences generalize this idea by dividing the integers into classes according to their remainders after division by n.

Definition. We say that integers a and b are congruent modulo $n \in \mathbb{N}$ if $n \mid b-a$. In mathematical notation we write $a \equiv b \pmod{n}$.

Exercise. Show why the statements below hold for integers a, b, c, d and $n \in \mathbb{N}$.

(1) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
(2) If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$.
(3) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
(4) If $a \equiv b \pmod{n}$, then $a^c \equiv b^c \pmod{n}$.
(5) If $a^2 \equiv b \pmod{n}$, then $(-a)^2 \equiv b \pmod{n}$.
(6) If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.
(7) In general, if $ac \equiv bc \pmod{n}$, then $a \equiv b \left(\mathrm{mod}\ \frac{n}{\gcd(c,n)}\right)$.

Using this notation, we now state some more advanced theorems. You can use these in your solutions without proof.

Theorem. (Fermat's little theorem) Let p be a prime and a an integer. Then

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

Theorem. (Wilson's theorem) Let p be a prime number. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

Euler's function

Euler's totient function, also known as Euler's phi function, counts the positive integers up to a given integer n that are coprime to n. It is denoted by the Greek letter phi, so we write $\varphi(n)$. By definition, it is clear that for any prime p, one has $\varphi(p) = p - 1$. Furthermore, the function is multiplicative, meaning $\varphi(mn) = \varphi(m)\varphi(n)$ for coprime m, n.

Fermat's little theorem can be generalized using Euler's function.

Theorem. (Euler's theorem) Let n be a positive integer and a be an integer coprime to n. Then

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

Quadratic residues

If you square the first few natural numbers, you may notice that each square is either divisible by 3 or leaves a remainder of 1 after division by 3. This property holds for all natural numbers. Every natural number can be written in the form $3k, 3k+1$ or $3k+2$. Squaring each number and noticing that all terms containing k vanish (are divisible by 3), we get $(3k)^2 \equiv 0 \pmod 3$, $(3k+1)^2 \equiv 1 \pmod 3$ and $(3k+2)^2 \equiv (-1)^2 \equiv 1 \pmod 3$. There are at most $\frac{n}{2}$ quadratic residues modulo n, because squaring a number and its opposite modulo n gives the same residue.

There are other useful moduli, which greatly restrict the number of possible quadratic residues. Choosing suitable moduli can, for example, help you show the nonexistence of solutions to some Diophantine equations. The most important ones are:

(1) $a^2 \equiv 0, 1 \pmod 3$,
(2) $a^2 \equiv 0, 1, 4 \pmod 5$,
(3) $a^2 \equiv 0, 1, 4 \pmod 8$.

The Legendre symbol

For any odd prime p, there is a special function called the Legendre symbol, which outputs whether an integer a is a quadratic residue modulo p.

Definition. Let p be an odd prime and a an integer. Then we define

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod p. \end{cases}$$

This function may not seem that useful at first, but it has many interesting properties. One of them is that Legendre symbol is a multiplicative function in its top argument:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

There is also a law which gives us the relation between Legendre symbol of two distinct odd primes p and q and the reciprocal.

Theorem. (Law of quadratic reciprocity) For any two distinct odd primes p and q:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Think about how two properties mentioned above help you calculate whether x is a quadratic residue modulo n for specific values of x and n.

We wish you the best of luck when solving the 4th Autumn series! If you want to know more about this topic, you can for example read this lecture from our library: *https://prase.cz/library/KvadratickeZbytkyMD/KvadratickeZbytkyMD.pdf*