Introduction to Integers

Dear friend,

this short text summarizes some basic facts about integers which may be helpful in the fourth autumn series. Also, we would like to provide you with some basic vocabulary so that you can get inspired for writing down your solutions.

The first thing you may wonder now is "What is an integer?" Well, an integer, sometimes called a "whole number", is a number that doesn't have a fractional part. For example 0, 1, 7 and -46 are all integers, while[1] 1.5, $-\frac{8}{7}$ and $\sqrt{2}$ are not.

Probably the main concept concerning integers is *divisibility*. For integers a, b we say that a *divides* b, or that b *is divisible* by a, if there is an integer c such that $ac = b$. We denote this by $a \mid b$. If a doesn't divide b, we write $a \nmid b$.

For example, $2 \mid 6$, $17 \mid -17$, $8 \nmid -4$, 0 is divisible by everything, 1 divides everything and the only integer divisible by 0 is 0.

A lot of problems concerning integers deal with *primes*. Integer p is a *prime*, if it is positive and there exist exactly two positive divisors of p: 1 and p. The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Another concept closely related to divisibility and integers is *congruence modulo*. We say that two integers a, b are *congruent modulo* m (where m is a positive integer), if both a and b give the same remainder after division by m. We denote this by $a \equiv b \pmod{m}$. An equivalent (and more practical) definition is, that a and b are congruent modulo m if and only if $m \mid a - b$.

For example, 14 and 8 are congruent modulo 3, either because they both give a remainder of 2 after division by 3, or because $3 \mid 14 - 8$.

Congruences work quite similiarly as regular equations, meaning that for all integers a, b, c, d and all positive integers m:

(1) $a \equiv 0 \pmod{m}$ if and only if $m \mid a$.
(2) If $a \equiv b \pmod{m}$, then $a + k \equiv b + k \pmod{m}$ and $ak \equiv bk \pmod{m}$ for any integer k.
(3) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
(4) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

[1] In English, decimal point is written as a dot (.), rather than a comma (,) as in Czech. So the number "one and a half" is written as 1,5 in Czech and as 1.5 in English.

(5) If $a \equiv b \pmod{m}$ and n is a positive integer, then $a^n \equiv b^n \pmod{m}$.

Problem. For which integers z is $\frac{z^3-25}{z-3}$ an integer?

Solution. Let $y = z - 3$. Obviously $y \mid z - 3$, so $z \equiv 3 \pmod{y}$. That means $z^3 \equiv 3^3 = 27 \pmod{y}$. But since $\frac{z^3-25}{z-3}$ is an integer, we have $y \mid z^3 - 25$ or $z^3 \equiv 25 \pmod{y}$. By subtracting this from $z^3 \equiv 27 \pmod{y}$, we get $0 \equiv 2 \pmod{y}$, or $y \mid 2$. So $y \in \{-2, -1, 1, 2\}$, or $z \in \{1, 2, 4, 5\}$. We can easily see that all of these work (or that we can reverse all the operations).

Problem. Let n be a positive integer and $h(n)$ an integer created by alternately adding and subtracting digits of n (the last digit has the plus sign). For example, $h(10659) = 1 - 0 + 6 - 5 + 9 = 11$ and $h(7524) = -7 + 5 - 2 + 4 = 0$. Prove that n is divisible by 11 if and only if $h(n)$ is divisible by 11.

Solution. Consider the decimal representation $a_0 + 10a_1 + 10^2a_2 + \cdots + 10^ka_k$ of n, where a_k are the digits of n. Then, since $10 \equiv -1 \pmod{11}$, we have

$$\begin{aligned} n &= a_0 + 10a_1 + 10^2a_2 + \cdots + 10^ka_k \\ &\equiv a_0 - a_1 + a_2 - \cdots + (-1)^ka_k \pmod{11} \\ &= h(n) \pmod{11} \end{aligned}$$

So $n \equiv h(n) \pmod{11}$, and therefore one of them is divisible by 11 if and only if the other one is.

But be careful! Even though you can add and multiply congruences however you wish, you can't always divide without consequences. For example, $0 \cdot 2 \equiv 3 \cdot 2 \pmod{6}$, but $0 \not\equiv 3 \pmod{6}$. How did that happen? Well, $0 \cdot 2 \equiv 3 \cdot 2 \pmod{6}$ means, in other words, $6 \mid 0 \cdot 4 - 3 \cdot 4 = (0 - 3) \cdot 4$. Dividing by 4 basically means that we change $6 \mid (0 - 3) \cdot 4$ into $6 \mid (0 - 3)$ and we cannot do that. But notice that this is caused by the fact that 4 has common factor with 6, specifically 2. We can generalize this observation:

We will say that integers a and b are *coprime*, if there is no prime number dividing both a and b. Which means that if $ac \equiv ad \pmod{b}$, then $b \mid a(c-d)$ and since a and b are coprime, we get $b \mid c-d$ or $c \equiv d \pmod{b}$. Therefore we can divide congruences by integers coprime with the modulus of the congruence. Note that in these cases we are able to divide two integers and get another integer, even if normally they are not divisible, as the following problem shows.

Problem. Let x and m be coprime integers. Then there exists an integer y, such that $xy \equiv 1 \pmod{m}$.

Solution. Consider the integers x^0, x^1, x^2, $\ldots$, x^m. Since there are $m + 1$ of them, there must exist numbers ℓ, k such that $\ell < k$ and $x^\ell \equiv x^k \pmod{m}$. Since x^ℓ is definitely coprime with m, we can divide both sides by x^ℓ and get $x^{k-\ell} \equiv 1 \pmod{m}$. We can then choose $y = x^{k-\ell-1}$ and we are done.