Bardo, październik 2019

IV UNIWERSYTECKI OBÓZ OLIMPIADY MATEMATYCZNEJ

Teoria Liczb - Fakty i definicje

Fakt 1. dzielenie z resztą. Każdy x rzeczywisty ma dla każdego y rzeczywistego(bez zera) dokładnie jeden zapis w postaci $x = yk + r$ gdzie k jest pewną liczbą całkowitą i $r \in [0, 1)$.

Od tego momentu będziemy operować tylko na liczbach całkowitych. (zawsze $c \neq 0$)

Definicja 1. przystawanie modulo. a przystaje do b modulo c wtedy i tylko wtedy gdy c dzieli $a - b$.
Zapisujemy

$$a \equiv b \,(mod\ c) \ \text{ lub } \ a \equiv_c b$$

Równoważnie, jeżeli $a = ck_a + r_a$ i $b = ck_b + r_b$, to

$$a \equiv b \,(mod\ c) \iff r_a = r_b$$

Ponadto oznaczmy $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ oraz $\mathbb{Z}_n^* = \{1, 2, ..., n-1\}$

Fakt 2. własności przystawania modulo. Przystawanie modulo jest zwrotne ($a \equiv_c a$),symetryczne (jeśli $a \equiv_c b$, to $b \equiv_c a$) i przechodnie (jeśli $a \equiv_c b$ i $b \equiv_c d$, to $a \equiv_c d$)

Fakt 3. arytmetyka modulo. Dla a, b, c takich, że $a \equiv b \,(mod\ c)$ zachodza następujące własności:

$$a + d \equiv b + d \,(mod\ c)$$
$$ad \equiv bd \,(mod\ c)$$
$$a^k \equiv b^k \,(mod\ c)$$

dla każdych $d \in \mathbb{Z}$ i $k \in \mathbb{N}_+$

Wniosek. Kongruencje(przystawania) z tym samym modulusem(sic!) można dodawać i mnożyć ze sobą stronami.

Fakt 4. Dla a, b, c, d takich, że $c \perp d$ (c względnie pierwsze z b, $NWD(c, d) = 1$)

$$ad \equiv bd \,(mod\ c) \Rightarrow a \equiv b \,(mod\ c)$$

Fakt 5. Dla każdego $q|c$ dla $a \equiv b \,(mod\ c)$

$$q|a \iff q|c$$

Wniosek. Dla $a \equiv b \,(mod\ c)$

$$NWD(a, c) = NWD(b, c)$$

Algorytm Euklidesa. Skoro dla każdego a $NWD(a, 0) = a$, to stosując wielokrotnie $NWD(a, b) = NWD(b, a\ mod\ b)$ do momentu gdy $b = 0$, możemy policzyć $NWD(a, b)$.

Twierdzenie 1. (generator addytywny). Dla $a \perp c$ zbiór reszt modulo c liczb ze zbioru $\{a, 2a, 3a, ..., (p-1)a\}$ jest zbiorem $\{1, 2, 3, ...(p-1)\}$ ($\mathbb{Z}_p^*$).

Definicja 2. odwrotność modularna. Przez odwrotność modulaną a modulo c rozumiemy taką liczbę a^{-1}, że

$$aa^{-1} \equiv 1 \,(mod\ c)$$

Twierdzenie 2. Odwrotność modularna a modulo c istnieje wtedy i tylko wtedy gdy $a \perp c$.

Twierdzenie 3. Małe Twierdzenie Fermata
. Dla liczby pierwszej p, dla każdego a zachodzi:

$$a^p \equiv a \,(mod\, p)$$

Alternatywnie dla każdego $a \perp p$ zachodzi:

$$a^{p-1} \equiv 1 \,(mod\, p)$$

Materiały przygotował: Adam Morawski.