Kongruencje i ich zastosowania

Bartosz Chojnowski, I Liceum Ogólnokształcące w Ełku

Definicja kongruencji.
Niech $m \in \boldsymbol{N}$ i $a, b \in \boldsymbol{C}$.
Mówimy, że liczba a przystaje do liczby b modulo m, jeśli $m|(a-b)$, to znaczy jeśli m jest dzielnikiem liczby $a-b$. Powyższą relację przystawania nazywamy relacją kongruencji, a liczbę m modułem kongruencji i zapisujemy

$$a = b(mod\, m) \text{ lub } a \equiv b(mod\, m).$$

Oczywiście, dwie liczby a i b przystają do siebie modulo m wtedy i tylko wtedy, gdy dają taką samą resztę z dzielenia przez m.

Podstawowe własności:

1. zwrotność $a = a\ (mod\, m)$,

2. symetria $a = b(mod\, m)$, to $b = a(mod\, m)$,

3. przechodniość $a = b(mod\, m)$ i $b = c(mod\, m)$, to $a = c(mod\, m)$

4. kongruencje można stronami dodawać, odejmować, mnożyć i potęgować, tzn.

jeśli $a = b(mod\, m)$ i $c = d(mod\, m)$, to

$$a + c = b + d(mod\, m),$$
$$a - c = b - d(mod\, m),$$
$$ac = bd(mod\, m) \text{ oraz } a^n = b^n(mod\, m) \text{ dla } n \in \boldsymbol{N}.$$

Przykłady:

$7 = 2(mod\ 5)$ i $8 = 3(mod\ 5)$, wtedy $7^5 = 2^5(mod\ 5)$, $7^5 \cdot 8 = 2^5 \cdot 3(mod\ 5)$

Można łatwo udowodnić własność dodawania kongruencji.

Jeśli $a = b(mod\, m)$ i $c = d(mod\, m)$, to $a - b = km$ i $c - d = lm$, dla pewnych całkowitych liczb l i m. Stąd otrzymujemy $a = km + b$ i $c = lm + d$.
Wtedy

$$(a + c) - (b + d) = (km + b + lm + d) - (b + d) = km + lm = (k + l)m$$

dzieli się przez m , czyli $a + c = b + d\ (mod\, m)$.

W zadaniach należy pamiętać, że relacja kongruencji informuje nas o podzielności różnicy dwóch liczb całkowitych.

Przykładowo wykażemy, że jeśli $n = 2k + 1$, $k \in \boldsymbol{N}$, to $16^n + 1$ jest podzielne przez 17.

$16 = -1(mod\ 17)$, bo różnica $16 - (-1) = 17$ jest podzielna przez 17.

Z własności potęgowania kongruencji otrzymujemy $16^n = (-1)^n(mod\ 17)$, czyli

$16^n = -1(mod\ 17)$, ponieważ $n = 2k + 1$ jest liczbą nieparzystą. Oznacza to, że

$$16^n - (-1) = 17m \text{ dla } k \in \boldsymbol{N} \text{ i ostatecznie } 16^n+1=17m.$$

Zadania do ćwiczeń.

Udowodnij wszystkie podane własności kongruencji.