KONGRUENCJE

Dla $a, b, m \in \mathbb{Z}$ mówimy, że *liczba a przystaje do liczby b modulo m*

$$a \equiv b \ (mod\ m) \Leftrightarrow m|(a-b)$$

($a \equiv b \ (mod\ m)$ można też zapisać jako: $a = km + b,\ k \in \mathbb{Z}$).
Liczbę m nazywamy *modułem kongruencji*.

Własności:

1. - $a \equiv a \ (mod\ m)$
   - $a \equiv b \ (mod\ m) \Leftrightarrow b \equiv a \ (mod\ m)$
   - $a \equiv b \ (mod\ m) \wedge b \equiv c \ (mod\ m) \Rightarrow a \equiv c \ (mod\ m)$

   Zatem relacja kongruencji jest relacją równoważności.

2. $a \equiv b \ (mod\ m) \wedge c \equiv d \ (mod\ m) \Rightarrow$
   $\Rightarrow a \pm c \equiv b \pm d \ (mod\ m) \wedge ac \equiv bd \ (mod\ m)$

3. $a \equiv b \ (mod\ m) \Rightarrow a \equiv b \ (mod\ d)$, gdzie $d|m$

4. $a \equiv b \ (mod\ m) \wedge a \equiv b \ (mod\ n) \wedge m, n -$ względnie pierwsze $\Rightarrow$
   $\Rightarrow a \equiv b \ (mod\ mn)$
   Dowód:
   Założenia:
   $$\begin{cases} a = km + b \\ a = ln + b \end{cases} \qquad NWD(m,n) = 1$$
   Teza:
   $$a = xmn + b, \quad k, l, x \in \mathbb{Z}$$
   Mamy:
   $$\begin{cases} a - b = km \\ a - b = ln \end{cases} \Rightarrow km = ln \overset{NWD(m,n)=1}{\Longrightarrow} k = xn \text{ (i oczywiście } l = xm), \ x \in \mathbb{Z}$$
   Zatem $a - b = nxm \Rightarrow a = xmn + b \Rightarrow a \equiv b \ (mod\ mn)$

Przykłady:

1.
$$\begin{cases} 68 \equiv 3 \ (mod\ 5) \\ 11 \equiv 1 \ (mod\ 5) \end{cases} \Longrightarrow 79 \equiv 4 \ (mod\ 5)$$

2.
$$\begin{cases} 13 \equiv 1 \ (mod\ 3) \\ 13 \equiv 1 \ (mod\ 4) \end{cases} \Longrightarrow 13 \equiv 1 \ (mod\ 12)$$

3. Ale
$$\begin{cases} 29 \equiv 5 \ (mod\ 6) \\ 29 \equiv 5 \ (mod\ 8) \end{cases} \stackrel{?}{\Longrightarrow} 29 \equiv 5 \ (mod\ 48)$$
Taka zależność nie zachodzi, bo $NWD(6,8) \neq 1$. Jak to poprawić? Otóż:
$$\begin{cases} a \equiv b \ (mod\ m) \\ a \equiv b \ (mod\ n) \end{cases} \Longrightarrow a \equiv b \ (mod\ NWW(m,n))$$
Mamy więc:
$$\begin{cases} 29 \equiv 5 \ (mod\ 6) \\ 29 \equiv 5 \ (mod\ 8) \end{cases} \Longrightarrow 29 \equiv 5 \ (mod\ 24)$$

Zadanie 1. Udowodnij, że $53^{53} - 33^{33}$ jest podzielne przez 10.
Rozwiązanie:

$$10|(53^{53} - 33^{33}) \Leftrightarrow 53^{53} - 33^{33} \equiv 0 \ (mod\ 10)$$

$$53 \equiv 3 \ (mod\ 10) \Rightarrow 53^{53} \equiv 3^{53} \ (mod\ 10)$$

Mamy:
$$3 \equiv 3 \ (mod\ 10)$$
$$3^2 \equiv -1 \ (mod\ 10)$$
$$3^4 \equiv 1 \ (mod\ 10)$$

Ale:
$$3^{53} = 3^{4 \cdot 13+1} = 3 \cdot 3^{4 \cdot 13} \equiv 3 \cdot 1 \ (mod\ 10) \equiv 3 \ (mod\ 10)$$

Podobnie:
$$33 \equiv 3 \ (mod\ 10) \Rightarrow 33^{33} \equiv 3^{33} \ (mod\ 10)$$

Więc:

$$3^{33} = 3^{4\cdot 8+1} = 3 \cdot 3^{4\cdot 8} \equiv 3 \cdot 1 \ (mod\ 10) \equiv 3 \ (mod\ 10)$$

Zatem:

$$53^{53} - 33^{33} \equiv 3 - 3 \ (mod\ 10) \equiv 0 \ (mod\ 10)$$

Zadanie 2. (znana zasada podzielności przez 3 i 9)
Udowodnij, że liczba zapisana w systemie dziesiętnym dzieli się przez 3 (9) $\Leftrightarrow$ suma jej cyfr dzieli się przez 3 (9).
Rozwiązanie: Weźmy dowolną liczbę postaci

$$a_n a_{n-1} \ldots a_2 a_1 a_0$$

Możemy ją zapisać jako:

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

Teraz zauważmy, że

$$10 \equiv 1 \ (mod\ 3)$$

więc

$$10^n \equiv 1 \ (mod\ 3)$$

A stąd:

$$a_n \cdot 10^n + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_n + \ldots + a_2 + a_1 + a_0 \ (mod\ 3)$$

więc

$$3 | a_n a_{n-1} \ldots a_2 a_1 a_0 \Leftrightarrow 3 | (a_n + \ldots + a_2 + a_1 + a_0)$$

Analogicznie dla podzielności przez 9.

Wyraz odwrotny
Wiemy, że gdy rozważamy liczby rzeczywiste wyrazem odwrotnym do 3 jest $\frac{1}{3}$, do $\frac{7}{8}$ jest $\frac{8}{7}$. Dlaczego? Bo $3 \cdot \frac{1}{3} = 1$, $\frac{7}{8} \cdot \frac{8}{7} = 1$. Podobnie definiuje się wyraz odwrotny w zbiorach reszt modulo p, tzn. w zbiorach $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, gdzie p jest liczbą pierwszą (elementami takich zbiorów są reszty z dzielenia przez p).Mianowicie:
a^{-1} jest *wyrazem odwrotnym* do a względem $p \Leftrightarrow a \cdot a^{-1} \equiv 1 \ (mod\ p)$, np. dla $p = 7$ mamy:

$$2^{-1} = 4, \text{ bo } 2 \cdot 4 = 8 \equiv 1 \ (mod\ 7)$$

$$3^{-1} = 5, \text{ bo } 3 \cdot 5 = 15 \equiv 1 \ (mod\ 7)$$

Zadanie 3. Znajdź wyrazy odwrotne w zbiorze $\mathbb{Z}_{11}$ do 2, 3, 4, 5, 6, 7, 8, 9, 10.
Odpowiedzi: $2^{-1} = 6, \quad 3^{-1} = 4, \quad 4^{-1} = 3, \quad 5^{-1} = 9, \quad 6^{-1} = 2,$
$7^{-1} = 8, \quad 8^{-1} = 7, \quad 9^{-1} = 5, \quad 10^{-1} = 10$
Przykład rozwiązania: $10 \equiv -1 \ (mod\ 11) \Rightarrow 10^2 \equiv 1 \ (mod\ 11)$, czyli $10 \cdot 10 \equiv 1 \ (mod\ 11)$, więc $10^{-1} = 10$.

Dlaczego wyrazy odwrotne możemy rozważać w $\mathbb{Z}_p$ tylko wtedy, gdy p jest liczbą pierwszą?
Przypuśćmy, że p nie jest pierwsza, tzn. $p = kl$, gdzie $1 < k \leqslant l < p$.
A zatem $k, l \in \mathbb{Z}_p$. To zaś prowadzi do tego, że nie istnieją k^{-1} i l^{-1}, bo gdyby było $xk \equiv 1 \ (mod\ p)$ dla pewnego $x \in \mathbb{Z}$, to wówczas $xk = ps + 1$, $(s \in \mathbb{Z})$ i $x = \frac{ps+1}{k} \in \mathbb{Z}$. Ale $k|p$, więc musiałoby być: $k|1$, co jest niemożliwe.
Oczywiście, jeśli p nie jest pierwsza, ale $NWD(a, p) = 1$ (tzn. a, p są względnie pierwsze) dla pewnego $a < p$, to istnieje a^{-1}, np. dla $p = 8$: $3^{-1} = 3$, ale już 6^{-1} nie istnieje!

Chińskie twierdzenie o resztach
Przypuśćmy, że chcemy rozwiązać układ kongruencji o różnych modułach:

$$\begin{cases} x \equiv a_1 & (mod\ m_1) \\ x \equiv a_2 & (mod\ m_2) \\ \quad \vdots & \quad \vdots \\ x \equiv a_r & (mod\ m_r) \end{cases}$$

Przypuśćmy następnie, że każde dwa moduły są względnie pierwsze, tzn. $NWD(a_i, a_j) = 1$ dla $i \neq j$. Wtedy istnieje wspólne rozwiązanie x wszystkich tych kongruencji i każde dwa rozwiązania przystają do siebie modulo $M = m_1 \cdot m_2 \cdot \ldots \cdot m_r$.
Dowód:
Udowodnimy najpierw jednoznaczność modulo M (ostatnie zdanie). Przypuśćmy, że x' i x'' są dwoma rozwiązaniami. Niech $x = x' - x''$. Wtedy x musi przystawać do 0 względem każdego modułu m_i, $i \in \{1, 2, \ldots, r\}$, a więc i modulo M (por. własność 4.).
Następnie pokażemy, jak skonstruować rozwiązanie x.
Niech $M_i = \frac{M}{m_i}$ będzie iloczynem wszystkich modułów z wyjątkiem i-tego. Oczywiście $NWD(m_i, M_i) = 1$, a więc istnieje taka liczba N_i, że
$M_i \cdot N_i \equiv 1 \ (mod\ m_i)$. Przyjmijmy teraz $x = \sum_i a_i M_i N_i$. Wtedy dla każdego

i wszystkie składniki sumy poza i-tym są podzielne przez m_i, gdyż $m_i|M_i$ dla $i \neq j$. Zatem dla każdego i mamy: $x \equiv a_i M_i N_i \equiv a_i \ (mod\ m_i)$.

Zadanie 4. Znajdź najmniejsze nieujemne rozwiązania następujących układów kongruencji:

1. $$\begin{cases} x \equiv 3 & (mod\ 7) \\ 2x \equiv 5 & (mod\ 11) \\ 3x \equiv 2 & (mod\ 5) \end{cases}$$ Odpowiedź: $x = 129$

2. $$\begin{cases} 7x \equiv 6 & (mod\ 9) \\ 9x \equiv 12 & (mod\ 21) \end{cases}$$ Odpowiedź: $x = 6$

   Podpowiedź: Zauważyć, że druga z tych kongruencji jest równoważna kongruencji $3x \equiv 4\ (mod\ 21)$ i skorzystać z własności 2. i 3.

3. $$\begin{cases} 7x \equiv 5 & (mod\ 11) \\ 5x \equiv 4 & (mod\ 6) \\ x \equiv 3 & (mod\ 7) \end{cases}$$ Odpowiedź: $x = 290$

Zadanie 5. Jakie są dwie ostatnie cyfry liczby $99^{99} - 51^{51}$?
Rozwiązanie:

$$99 \equiv -1\ (mod\ 100)$$

$$99^2 \equiv 1\ (mod\ 100)$$

oraz

$$51 \equiv 51\ (mod\ 100)$$

$$51^2 \equiv (50+1)^2 = 2500 + 100 + 1 \equiv 1\ (mod\ 100)$$

Zatem

$$99^{99} \equiv -1\ (mod\ 100) \quad \text{i} \quad 51^{51} \equiv 51\ (mod\ 100)$$

A stąd:

$$99^{99} - 51^{51} \equiv -1 - 51\ (mod\ 100) \equiv 48\ (mod\ 100)$$

Problem

N - niezwykle duża, tajna liczba całkowita (używana do uruchamiania systemu rakiet bojowych)

Mamy do dyspozycji generała głównodowodzącego (który zna liczbę N) oraz n generałów niższych stopni. Chcemy, by dowolnych trzech generałów niższych stopni (ale nie dwóch) było w stanie w razie niesubordynacji (śmierci, nieobecności) generała głównodowodzącego wspólnie uruchomić system. Jak tego dokonać?

$\rightarrow$ Niech $p_1, \ldots, p_n$ będą różnymi liczbami pierwszymi takimi, że:
$\sqrt[3]{N} < p_i << \sqrt{N}$, $i \in \{1, \ldots, n\}$

Generałowie niższych stopni otrzymają liczbę p_i oraz resztę z dzielenia N przez p_i. (patrz: chińskie twierdzenie o resztach)

Wniosek

Dla k generałów (nie $k-1$) ($k \geqslant 2$), którzy mogą odpalić rakiety:
$\sqrt[k]{N} < p_i << \sqrt[k-1]{N}$.

Takie rozwiązanie nazywa się *k-progowym systemem dzielenia się tajemnicą.*