Kongruencje i ich zastosowania

Andrzej Sładek
sladek@ux2.math.us.edu.pl

Instytut Matematyki, Uniwersytet Śląski w Katowicach

Jufenalia w I Liceum w Rybniku, 13 marca 2018

Poznamy nowe fakty matematyczne, które pozwolą nam w łatwy sposób rozwiązać poniższe zadania.

Zadanie 1.

W szkole uczniowie poznają cechę podzielności przez 3 oraz przez 9. Znajdź cechę podzielności przez inne liczby jak np. 7, 11, 13.

Zadanie 2.

Liczba kostek w bardzo dużej czekoladzie równa jest x. Jeśli podzielić czekoladę na 3 części, to zostanie 1 kostka. Przy podziale na 5 części zostaną 3 kostki, a w przypadku podziału na 7 części zostaną 2 kostki. Ile kostek ma czekolada, jeśli wiadomo, że kostek jest mniej niż 100?

Zadanie 3.

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Definicja

Niech n będzie liczbą naturalną oraz niech a oraz b będą liczbami całkowitymi. Mówimy, że a **przystaje do** b **modulo** n, jeśli n dzieli $a - b$.

$$a \equiv b \pmod{n} \iff a - b = t \cdot n \quad \text{dla pewnej liczby całkowitej } t$$

Uwaga

Dwie liczby całkowite przystają do siebie modulo n wtedy i tylko wtedy, gdy dają tą samą resztę z dzielenia przez n.

Które z poniższych kongruencji są prawdziwe?

$$10 \equiv 1 \pmod{9}, \qquad -1 \equiv 113 \pmod{6}, \qquad -12 \equiv 13 \pmod{5},$$

$$-5 \equiv 31 \pmod{7}, \qquad -26 \equiv 44 \pmod{10}, \qquad 23 \equiv 71 \pmod{11}$$

Własności kongruencji

1. Kongruencja $\equiv \pmod n$ ma podobne własności jak zwykła równość $=$, tzn.
   - $a \equiv a \pmod n$,
   - $a \equiv b \pmod n \;\Rightarrow\; b \equiv a \pmod n$,
   - $a \equiv b \pmod n,\ \ b \equiv c \pmod n \;\Rightarrow\; a \equiv c \pmod n$.
2. Kongruencje można stronami dodawać, odejmować i mnożyć, tzn.

$$a \equiv b \pmod n,\quad c \equiv d \pmod n$$

$$\Downarrow$$

$$a + c \equiv b + d \pmod n,\quad a - c \equiv b - d \pmod n,\quad ac \equiv bd \pmod n$$

Oznacza to, że na kongruencjach można wykonywać podobne rachunki jak w przypadku równości. Zobaczmy to na przykładzie.
Rozwiąż następującą kongruencję:

$$3X+12 \equiv 16 \pmod{26} \to 3X \equiv 4 \pmod{26} \to 27X \equiv 36 \pmod{26} \to X \equiv 10 \pmod{26}$$

Zauważmy, że jeśli $a \equiv b \pmod{n}$, to dla dowolnych liczb całkowitych $a_0, \ldots, a_m$ mamy

$$\begin{aligned} a_0 &\equiv a_0 \pmod{n} \\ a_1 a &\equiv a_1 b \pmod{n} \\ a_2 a^2 &\equiv a_2 b^2 \pmod{n} \\ &\vdots \\ a_m a^m &\equiv a_m b^m \pmod{n} \end{aligned}$$

$$a_m a^m + \ldots + a_1 a + a_0 \equiv a_m b^m + \ldots + a_1 b + a_0 \pmod{n},$$

tzn. $f(a) \equiv f(b) \pmod{n}$, gdzie $f(X) = a_m X^m + \ldots + a_1 X + a_0$

Zatem

$$a \equiv b \pmod{n} \implies f(a) \equiv f(b) \pmod{n}$$

Jak skonstruowany jest system dziesiętny?

$$4326 = 4 \cdot 1000 + 3 \cdot 100 + 2 \cdot 10 + 6 \cdot 1 = 4 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10^1 + 6$$

Ogólniej, liczbę naturalną N w systemie dziesiętnym można zapisać następująco:

$$N = (c_1 c_2 ... c_n)_{10} = c_1 10^{n-1} + c_2 10^{n-2} + ... + c_{n-1} 10^1 + c_n.$$

i wtedy

$$N = f(10), \text{ jeśli } f(X) = c_1 X^{n-1} + c_2 X^{n-2} + ... + c_{n-1} X^1 + c_n.$$

$$f(X) = c_1X^{n-1} + c_2X^{n-2} + \ldots + c_{n-1}X^1 + c_n$$

$$f(10) = (c_1c_2\ldots c_n)_{10} \quad f(1) = c_1 + c_2 + \ldots c_{n-1} + c_n$$

$$10 \equiv 1 \pmod 3$$
$$\Downarrow$$
$$f(10) \equiv f(1) \pmod 3$$
$$\Downarrow$$
$$(c_1c_2\ldots c_n)_{10} = f(10) \equiv f(1) = c_1 + c_2 + \ldots + c_{n-1} + c_n \pmod 3$$

tzn. 3 dzieli $(c_1c_2\ldots c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli sumę jej cyfr.

Czy wiesz jak udowodnić cechę podzielności przez 9 oraz przez 11?

$$10 \equiv -1 \pmod{11}$$
$$\Downarrow$$
$$N = f(10) \equiv f(-1) = (-1)^{n-1}c_1 + (-1)^{n-2}c_2 + \ldots - c_{n-1} + c_n \pmod{11}$$

tzn. 11 dzieli liczbę $N = (c_1 c_2 \ldots c_n)_{10}$ wtedy i tylko wtedy, gdy dzieli

naprzemienną sumę jej cyfr.

Przykład

Aby sprawdzić podzielność liczby 123456789060704 przez 11 obliczamy sumę naprzemienną cyfr

$$4 - 0 + 7 - 0 + 6 - 0 + 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 22,$$

która jest podzielna przez 11. Zatem 11 dzieli 123456789060704.

Cechy podzielności przez inne liczby są bardziej skomplikowane. Przyjrzyjmy się cesze podzielności przez 7 oraz przez 13.

Liczbę naturalną

$$N = (c_1 c_2 ... c_n)_{10} = c_1 10^{n-1} + c_2 10^{n-2} + ... + c_{n-1} 10^1 + c_n$$

możemy zapisać w postaci

$$N = ... + 1000^1 (c_{n-5} c_{n-4} c_{n-3})_{10} + (c_{n-2} c_{n-1} c_n)_{10}.$$

Zauważ, że jeśli

$$g(X) = ... + X(c_{n-5} c_{n-4} c_{n-3})_{10} + (c_{n-2} c_{n-1} c_n)_{10},$$

to

$$N = g(1000).$$

$$1000 \equiv -1 \pmod{7,13} \quad (\text{bo } 1001 = 7 \cdot 11 \cdot 13)$$

$$\Downarrow$$

$$N = g(1000) \equiv g(-1) \pmod{7,13}$$

$$g(-1) = \ldots + (-1)^1 (c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-2}c_{n-1}c_n)_{10}$$

Stąd 7 (tak samo 13) dzieli liczbę N wtedy i tylko wtedy, gdy dzieli

"naprzemienną sumę" liczb powstałych z podziału liczby N na trójki.

Przykład

7 dzieli 23697678872, bo $872 - 678 + 697 - 23 = 868 = 7 \cdot 124$

Zadanie 2

Liczba kostek w bardzo dużej czekoladzie równa jest x. Jeśli podzielić czekoladę na 3 cześci, to zostanie 1 kostka. Przy podziale na 5 części zostaną 3 kostki, a w przypadku podziału na 7 części zostaną 2 kostki. Ile kostek ma czekolada, jeśli wiadomo, że kostek jest mniej niż 100?

Czy wiesz jak rozwiązać zadanie 2?

Należy rozwiązać układ kongruencji

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

Twierdzenie (chińskie o resztach)

Jeśli $n_1, \ldots, n_k$ są parami względnie pierwsze oraz $r_1, \ldots, r_k$ są liczbami całkowitymi, to istnieje liczba całkowita x taka, że

$$\begin{cases} x \equiv & r_1 \pmod{n_1} \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\ x \equiv & r_k \pmod{n_k} \end{cases}$$

Liczba x jest wyznaczona jednoznacznie modulo $n_1 \cdot \ldots \cdot n_k$.

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13.$

Wstawiamy to do trzeciej kongruencji i wyliczamy u.
$15u + 13 \equiv 2 \pmod 7 \implies u - 1 \equiv 2 \pmod 7 \implies u \equiv 3 \pmod 7 \implies u = 7s + 3$
Ostatecznie $x = 15(7s + 3) + 13 = 105s + 58.$

Odp. Liczba kostek czekolady równa jest 58.

Zadanie 3

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Do rozwiązania potrzebować będziemy tzw. funkcji Eulera.

Nazwa tej funkcji pochodzi od nazwiska szwajcarskiego matematyka L. Eulera, który żył w latach 1707-1783.

Funkcja Eulera

Funkcja $\varphi : N \longrightarrow N$ jest jednoznacznie określona poprzez swoje własności:

(1) Jeśli NWD$(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

(2) Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.
W szczególności $\varphi(p) = p - 1$.

Twierdzenie Eulera

Jeśli $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Przykład

$\varphi(200) = \varphi(2^3 5^2) = \varphi(2^3)\varphi(5^2) = 2^2(2-1)5^1(5-1) = 80$

Zatem

$3^{80} \equiv 1 \pmod{200}$.

Zadanie 3

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Rozwiązanie.
Należy znaleźć resztę z dzielenia liczby 3^{14404} przez 1000.
Obliczmy $\varphi(1000) = \varphi(2^3 5^3) = \varphi(2^3)\varphi(5^3) = 400$.
Zatem

$$3^{14404} = 3^{400 \cdot 36 + 4} = (3^{400})^{36} 3^4 \equiv 3^4 \pmod{1000},$$

bo $3^{400} \equiv 1 \pmod{1000}$ na podstawie twierdzenia Eulera.

Ponieważ $3^4 = 81$, więc
ostatnie trzy cyfry liczby 3^{14404} to 081.

1. Rozwiąż kongruencje
   - $3X + 31 \equiv 15 \pmod{47}$
   - $3X \equiv 8 \pmod{13}$
   - $14X \equiv 22 \pmod{36}$
2. Znajdź i uzasadnij cechę podzielności przez 101.
   Wsk. $100 \equiv -1 \pmod{101}$.
3. Wykorzystując kongruencję $1000 \equiv 1 \pmod{27, 37}$ wyprowadź cechy podzielności przez 27 oraz 37.
4. Wykorzystując kongruencję $100 \equiv -2 \pmod{51}$ wyprowadź cechę podzielności przez 51.
5. W sadzie zebrano jabłka, których nie było więcej niż 1000. Gdyby podzielić jabłka równo do 7 koszy, to zostanie 1 jabłko. Gdyby podzielić jabłka równo do 13 koszy, to zostanie 6 jabłek. Można jednak podzielić jabłka równo na 11 części. Ile zebrano jabłek?
6. Znajdź ostatnie dwie cyfry następujących liczb 7^{6042}, 289^{289}, 7^{9^9}.
   Wsk. Oblicz $\varphi(100)$.

1. N.Koblitz, *Wykład z teorii liczb i kryptografii*, WNT, Warszawa 1995.
2. P.Ribenboim, *Mała księga wielkich liczb pierwszych*, WNT, Warszawa 1997.
3. W.Sierpiński, *Wstęp do teorii liczb*, Biblioteczka Matematyczna 25, PZWS, Warszawa 1965.
4. L.A.Steen (redaktor), *Matematyka Współczesna, Dwanaście esejów*, WNT, Warszawa 1983.

I to już koniec!

♡♡♡

Dziękuję za uwagę