Kongruencje — pierwsze kroki

Kongruencje — wykład 1

Definicja

Niech n będzie dodatnią liczbą całkowitą, natomiast a i b – dowolnymi liczbami całkowitymi. Liczby a i b nazywamy *przystającymi (kongruentnymi) modulo* n i piszemy

$$a \equiv b \pmod{n},$$

jeżeli różnica $a - b$ jest podzielna przez n:

$$a - b = kn, \quad (k \text{ – całkowite}).$$

Na przykład:

$$3 \equiv 24 \pmod{7}; \quad -31 \equiv 11 \pmod{7}; \quad -15 \equiv -64 \pmod{7},$$

bo mamy:

$$3-24 = 21 = 3\cdot 7; \quad -31-11 = -42 = -6\cdot 7; \quad -15-(-64) = 49 = 7\cdot 7.$$

Analogicznie, mamy liczby, które *nie są przystające* modulo n

$$a \not\equiv b \pmod{n}.$$

Na przykład: $25 \not\equiv 12 \pmod{7}$, bo $25 - 12 = 13$ – liczbie, która nie jest podzielna przez 7.

Podstawowe własności

Z definicji natychmiast wynika oczywiste...

...twierdzenie

Warunkiem koniecznym i wystarczającym aby $a \equiv b \pmod{n}$ jest aby reszty z dzielenia a i b przez n były równe.

Dowód

$a \equiv b \pmod{n} \rightarrow a = b + kn = \ldots$
przy dzieleniu b przez n zostaje reszta r; tak więc $b = qn + r$
$\ldots = (qn + r) + kn = (q + k)n + r \rightarrow -$ przy dzieleniu a przez n zostanie też reszta r.
W drugą stronę – reszty takie same: $a = q_1 n + r$ i $b = q_2 n + r$.
odejmując stronami $a - b = (q_1 - q_2)n \rightarrow a \equiv b \pmod{n}$.

Na przykład:

$$\begin{aligned} -56 &\equiv -11 \pmod{9} \rightarrow \\ -56 &= (-7) \cdot 9 + 7 \\ -11 &= (-2) \cdot 9 + 7 \end{aligned}$$

Podstawowe własności,c.d.

Kongruencja albo *przystawanie* liczb całkowitych okazuje się mieć podobne własności w stosunku do operacji dodawania, mnożenia i potęgowania jak zwykła relacja równości.

1. $a \equiv a \pmod{n}$;
2. $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
3. $\{a \equiv b \pmod{n} \text{ i } b \equiv c \pmod{n}\} \rightarrow a \equiv c \pmod{n}$;
4. $\{a \equiv b \pmod{n} \text{ i } c \equiv d \pmod{n}\}$
   $\rightarrow a + c \equiv (b + d) \pmod{n}$ oraz $a \cdot c \equiv b \cdot d \pmod{n}$
5. $a \equiv b \pmod{n} \rightarrow \{(a + c) \equiv (b + c) \pmod{n}$ oraz $(a \cdot c) \equiv (b \cdot c) \pmod{n}\}$;
6. $a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$

$a - a = 0 = 0 \cdot n \rightarrow a \equiv a \pmod{n}$

Podstawowe własności,c.d.

Kongruencja albo *przystawanie* liczb całkowitych okazuje się mieć podobne własności w stosunku do operacji dodawania, mnożenia i potęgowania jak zwykła relacja równości.

1. $a \equiv a \pmod{n}$;
2. $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
3. $\{a \equiv b \pmod{n} \text{ i } b \equiv c \pmod{n}\} \rightarrow a \equiv c \pmod{n}$;
4. $\{a \equiv b \pmod{n} \text{ i } c \equiv d \pmod{n}\}$
   $\rightarrow a + c \equiv (b + d) \pmod{n}$ oraz $a \cdot c \equiv b \cdot d \pmod{n}$
5. $a \equiv b \pmod{n} \rightarrow \{(a + c) \equiv (b + c) \pmod{n}$ oraz $(a \cdot c) \equiv (b \cdot c) \pmod{n}\}$;
6. $a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$

$a \equiv b \pmod{n} \rightarrow a - b = kn \rightarrow b - a = -kn \rightarrow b \equiv a \pmod{n}$

Podstawowe własności,c.d.

Kongruencja albo *przystawanie* liczb całkowitych okazuje się mieć podobne własności w stosunku do operacji dodawania, mnożenia i potęgowania jak zwykła relacja równości.

1. $a \equiv a \pmod{n}$;
2. $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
3. $\{a \equiv b \pmod{n} \text{ i } b \equiv c \pmod{n}\} \rightarrow a \equiv c \pmod{n}$;
4. $\{a \equiv b \pmod{n} \text{ i } c \equiv d \pmod{n}\}$
   $\rightarrow a + c \equiv (b + d) \pmod{n}$ oraz $a \cdot c \equiv b \cdot d \pmod{n}$
5. $a \equiv b \pmod{n} \rightarrow \{(a + c) \equiv (b + c) \pmod{n}$ oraz $(a \cdot c) \equiv (b \cdot c) \pmod{n}\}$;
6. $a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$

$\{a \equiv b \pmod{n} \text{ i } b \equiv c \pmod{n}\} \rightarrow \{a - b = hn \text{ oraz } c - d = gn\}$ a więc $a - c = (h + g)n \rightarrow a \equiv c \pmod{n}$;

Podstawowe własności,c.d.

Kongruencja albo *przystawanie* liczb całkowitych okazuje się mieć podobne własności w stosunku do operacji dodawania, mnożenia i potęgowania jak zwykła relacja równości.

1. $a \equiv a \pmod{n}$;
2. $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
3. $\{a \equiv b \pmod{n} \text{ i } b \equiv c \pmod{n}\} \rightarrow a \equiv c \pmod{n}$;
4. $\{a \equiv b \pmod{n} \text{ i } c \equiv d \pmod{n}\}$
   $\rightarrow a + c \equiv (b + d) \pmod{n}$ oraz $a \cdot c \equiv b \cdot d \pmod{n}$
5. $a \equiv b \pmod{n} \rightarrow \{(a + c) \equiv (b + c) \pmod{n}$ oraz $(a \cdot c) \equiv (b \cdot c) \pmod{n}\}$;
6. $a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$

$\{a \equiv b \pmod{n} \text{ i } c \equiv d \pmod{n}\} \rightarrow \{a - b = hn \text{ oraz } c - d = gn\}$
$(a+c)-(b+d) = (a-b)+(c-d) = (h+g)n \rightarrow a+c \equiv b+d \pmod{n}$
dla $a \cdot c \equiv b \cdot d \pmod{n}$ dowód analogiczny.

Podstawowe własności,c.d.

Kongruencja albo *przystawanie* liczb całkowitych okazuje się mieć podobne własności w stosunku do operacji dodawania, mnożenia i potęgowania jak zwykła relacja równości.

1. $a \equiv a \pmod{n}$;
2. $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
3. $\{a \equiv b \pmod{n} \text{ i } b \equiv c \pmod{n}\} \rightarrow a \equiv c \pmod{n}$;
4. $\{a \equiv b \pmod{n} \text{ i } c \equiv d \pmod{n}\}$
   $\rightarrow a + c \equiv (b + d) \pmod{n}$ oraz $a \cdot c \equiv b \cdot d \pmod{n}$
5. $a \equiv b \pmod{n} \rightarrow \{(a + c) \equiv (b + c) \pmod{n}$ oraz $(a \cdot c) \equiv (b \cdot c) \pmod{n}\}$;
6. $a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$

dowód jak (4) z uwzględnieniem (1) – $c \equiv c \pmod{n}$

Podstawowe własności,c.d.

Kongruencja albo *przystawanie* liczb całkowitych okazuje się mieć podobne własności w stosunku do operacji dodawania, mnożenia i potęgowania jak zwykła relacja równości.

1. $a \equiv a \pmod{n}$;
2. $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
3. $\{a \equiv b \pmod{n} \text{ i } b \equiv c \pmod{n}\} \rightarrow a \equiv c \pmod{n}$;
4. $\{a \equiv b \pmod{n} \text{ i } c \equiv d \pmod{n}\}$
   $\rightarrow a + c \equiv (b + d) \pmod{n}$ oraz $a \cdot c \equiv b \cdot d \pmod{n}$
5. $a \equiv b \pmod{n} \rightarrow \{(a + c) \equiv (b + c) \pmod{n}$ oraz $(a \cdot c) \equiv (b \cdot c) \pmod{n}\}$;
6. $a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$

Dowód indukcyjny. Teza spełniona jest dla $k = 1$.
Zakładamy jej prawdziwość dla pewnego k. Mamy więc:
$a \equiv b \pmod{n}$ oraz $a^k \equiv b^k \pmod{n}$. Mnożymy dwie kongruencje stronami i wykorzystujemy własność (4).
$aa^k \equiv bb^k \pmod{n}$ czyli $a^{k+1} \equiv b^{k+1} \pmod{n}$, co kończy dowód indukcyjny.

Przykłady

Jean Pierre Fermat miał pomysł (jeden z wielu !), że *wszystkie* liczby o postaci $2^{2^k}+1$ są liczbami pierwszymi (n.b., dla liczb p *naprawdę* pierwszych o tej postaci, Gauss udowodnił możliwość „Euklidesowej" konstrukcji regularnego p-kąta).
Dla $k = 0, 1, 2, 3$ i 4 wszystko jest OK, ale już Euler (ca. 1735) zauważył, że $2^{2^5}+1$ dzieli się przez 641. Wykazanie tego, korzystając z kongruencji, jest szybkie, łatwe i przyjemne.
W języku „przystawania" mamy wykazać, że:

$$2^{2^5}+1 = 2^{32}+1 \equiv 0 \pmod{641}.$$

W tym celu musimy w liczbie 641 doszukać się podobnej struktury, jak w $2^{32}+1$. Dość oczywisty pomysł (ważne są potęgi dwójki!), to:

$$641 = 640+1 = 5\cdot 128+1 = 5\cdot 2^7+1.$$

A więc

$$5\cdot 2^7 \equiv -1 \pmod{641}.$$

Przykłady, c.d

Wykorzystajmy teraz własność (6) – $k = 4$:

$$5^4 \cdot (2^7)^4 \equiv (-1)^4 \pmod{641} \text{ albo}$$

$$5^4 \cdot 2^{28} \equiv 1 \pmod{641}.$$

W naszej $2^{2^5} + 1$ mamy jednak tylko potęgę (32-gą) dwójki, a nie uświadczysz w niej potęgi piątki. Musimy znaleźć jakąś kongruencją (modulo 641) która zachodzi między potęgami dwójki i piątki. Każdy widzi, że 5^4 to 625, które odległe jest od 641 o $16 = 2^4$. Jesteśmy w domu:

$$5^4 \equiv -16 = -(2^4) \pmod{641}.$$

I już możemy wykazać, że *nie* jest możliwa euklidesowa konstrukcja $2^{2^5} + 1$-kąta foremnego:

$$2^{32} + 1 = 2^4 \cdot 2^{28} + 1 \equiv -(5^4) \cdot 2^{28} + 1 \equiv -1 + 1 = 0 \text{ (modulo 641)}.$$

Przykłady, c.d

Liczba Mersenne'a $2^{83}-1$ (postulowana przez M. M. jako kandydatka na liczbę pierwszą) dzieli się przez 167 (jak pokazał Euler).

Tutaj dwójka występuję w potędze przeszło dwa i pół raza większej niż w poprzednim przykładzie. Trzeba pobawić się w podnoszenie do kwadratu i szukać partnerów kongruentnych (modulo 167) dla kolejnych potęg:

$$\begin{aligned} 2^8 &= 256 \equiv 89 \pmod{167}, \\ 2^{16} &\equiv 89^2 = 7921 \equiv 72 \pmod{167}, \\ 2^{32} &\equiv 72^2 = 5184 \equiv 7 \pmod{167}, \\ 2^{64} &\equiv 7^2 = 49 \equiv 49 \pmod{167} \end{aligned}$$

Pozostało inteligentne rozpisanie 83-ej potęgi dwójki. $83 = 16 + 67$.
A 67 nie jest dalekie od 64:

$$2^{67} = 2^3 \cdot 2^{64} \equiv 8 \cdot 49 \pmod{167} = 392 \pmod{167} \equiv 58 \pmod{167}.$$

Jesteśmy w domu:

$$2^{83}-1 = 2^{67} \cdot 2^{16} - 1 \equiv 58 \cdot 72 \pmod{167} - 1 = 4176 - 1 = 4175 \equiv 0 \pmod{167}.$$

Kilka nie za trudnych i sympatycznych problemików:

- Udowodnij:

$$\begin{array}{lrcl} (1) & a^2 & \equiv & 0 \text{ lub } 1 \pmod 3 \\ (2) & a^3 & \equiv & 0 \text{ lub } 1 \text{ lub } -1 \pmod 7 \\ (3) & a^4 & \equiv & 0 \text{ lub } 1 \pmod 5 \end{array}$$

- Czy $5^{36} - 1$ dzieli się przez 13? A $10^{49} + 5^3$ przez 7?
- Jaką resztę otrzymasz z dzielenia sumy:

$$1! + 2! + 3! + 4! + \ldots + 100!$$

przez 12? (Na wszelki przypadek, pozwalam sobie zauważyć, że $2 \cdot 12$ to $4!$)

- Jaką resztę otrzymamy dzieląc 37^{13} przez 17?

Klasy reszt modulo m

Kiedy liczba całkowita a zostaje podzielona przez inną liczbę całkowitą m mamy

$$a = km + r, \quad \text{gdzie} \quad 0 \leqslant r < m,$$

a zatem każda liczba całkowita przystaje modulo m do jednej z liczb $0, 1, \ldots, m-1$. Żadne dwie liczby tego zbioru nie przystają do siebie modulo m. Mówimy, że ...

Definicja

...zbiór $0, 1, \ldots, m-1$ tworzy pełny układ reszt modulo m.
Liczby, które przy dzieleniu przez m dają tą samą resztę r tworzą *daną klasę reszt modulo* m. Klas takich jest m.
Dla danej reszty r klasa reszt do której ta należy składa się z liczb

$$r,\ r \pm m,\ r \pm 2m, \ldots$$

Nowa definicja kongruencji:
$a \equiv b \pmod{m}$ oznacza, że a i b należą do tej samej klasy reszt modulo m.

Klasy reszt modulo m, c.d.

wniosek:

$a \equiv b \pmod{m} \quad \Longleftrightarrow \quad (a, m) = (b, m)$

Dowód oparty jest na lemacie:

$$a = qb + r \quad \Longleftrightarrow \quad (a, b) = (b, r).$$

Oznaczmy $d = (a, b)$. Mamy $d \mid a$ i y $d \mid b \quad \Rightarrow \quad d \mid a - qb$, tak więc $d \mid (b, r) = c$. //Z drugiej strony mamy $c \mid b$ i $c \mid r \quad \Rightarrow c = (b, r) \quad \Rightarrow \quad c \mid qb + r = a, \quad \Rightarrow \quad c \mid d$. Tak więc $d = c$.

Konsekwencje (niektóre) przystawania

Każde wyrażenie algebraiczne, w konstrukcji którego są użyte operacje dodawania, odejmowania i mnożenia, musi dać „ten sam” (w sensie przystawania) wynik, jeżeli podstawimy za zmienną wartości kongruentne.
Na przykład wielomian $W(x) = x^3 - 8x + 6$ da wartości kongruentne modulo 5 jeżeli za x postawić $x = -2$ i $x = 3$, bo $-2 \equiv 3 \pmod 5$.
Rzeczywiście

$$W(-2) = 14 \equiv 9 = W(3) \pmod 5.$$

Podobnie, dwa wielomiany, których współczynniki sa przystające modulo m dadzą te same wartości dla kongruentnych (modulo m) wartości zmiennej x. Na przykład wielomiany

$$W_1(x) = x^3 - 8x + 6; \qquad W_2(x) = 4x^3 - 3x^2 - 2x - 3$$

mają współczynniki przystające modulo 3:
$1 \equiv 4$, $0 \equiv -3$, $-8 \equiv -2$, $6 \equiv -3$
a więc $W_1(-2) = 14 \equiv -4 = W_2(1) \pmod 3$, bo $-2 \equiv 1 \pmod 3$.

Konsekwencje (dalsze) przystawania

stwierdzenie

$$a \equiv b \pmod{m} \iff a \equiv b \pmod{d},$$

gdzie d jest dowolnym dzielnikiem modułu m.

stwierdzenie

$$a \equiv b \pmod{m_1} \text{ i } a \equiv b \pmod{m_2} \iff a \equiv b \pmod{M},$$

gdzie $M = [m_1, m_2]$.

Konsekwencje (dalsze) przystawania

Naturalnym uogólnieniem tego stwierdzenia będzie kolejne

stwierdzenie

$$a \equiv b \pmod{m_i} \quad i = 1, 2, \ldots, k,$$

i moduły m_i są liczbami parami względnie pierwszymi to

$$a \equiv b \pmod{m_i} \iff a \equiv b \pmod{m_1 m_2 \ldots m_k}.$$

— przypomnijmy, że dla takich m_i ich NWW $[m_1, m_2, \ldots, m_k] = m_1 m_2 \ldots m_k$.

Tak więc jeżeli mamy rozkład kanoniczny liczby $m = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \ldots {p_k}^{\alpha_k}$ to mamy
$a \equiv b \pmod{m} \iff a \equiv b \pmod{{p_i}^{\alpha_i}}$, dla każdego $i = 1, 2, \ldots, k$.

Dzielenie kongruencji przez liczbę

Rozpatrzmy kongruencję $36 \equiv 92 \pmod 8$. „Automatyczne” podzielenie stronami przez 4 daje $9 \equiv 23 \pmod 8$ – ????

Dzielenie obu stron kongruencji przez (wspólny) czynnik

$ak \equiv bk \pmod m \iff (a-b)k = hm$. Oznaczmy $d = (k, m)$. Mamy

$$(a-b)\frac{k}{d} = h\frac{m}{d} \iff a \equiv b \pmod{\frac{m}{d}},$$

bo $k/d \perp m/d$ i jeżeli lewa strona jest podzielna przez m/d to jest to konsekwencją podzielności przez m/d różnicy $a - b$!

Mamy więc

Twierdzenie

w kongruencji $ak \equiv bk \pmod m$ wspólny czynnik k może zostać wydzielony, pod warunkiem, że jednocześnie dzielimy moduł kongruencji m przez $d = (k, m)$.

Dzielenie kongruencji przez liczbę, cd

Rozpatrzmy ponownie kongruencję $36 \equiv 92 \pmod 8$.
Stosując poznany przed chwilą poprawny schemat dostajemy $9 \equiv 23 \pmod{8/4}$.
Podobnie możemy „uprościć” kongruencję $220 \equiv 1\,180 \pmod{96}$: $k = 20$ oraz $d = (20, 96) = 4$, a więc: $11 \equiv 59 \pmod{96/4} \quad \rightarrow \quad 11 \equiv 59 \pmod{24}$.

Twierdzenie

w kongruencji $ak \equiv bk \pmod m$ wspólny czynnik k może zostać wydzielony jeżeli $k \perp m$. Daje to kongruencje $a \equiv b \pmod m$.

Na przykład $27 \equiv 102 \pmod{25} \quad \rightarrow \quad 9 \equiv 34 \pmod{25}$. I jeszcze

Twierdzenie

Jeżeli wszystkie trzy liczby w kongruencji $a \equiv b \pmod m$ są podzielne przez liczbę d to zachodzi

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$