Kongruencje – skromne pożytki praktyczne

Kongruencje – Wykład 2

Weryfikacja niektórych obliczeń algebraicznych

Już sam wielki Karl Friedrich Gauss w swoich słynnych *Disquisitiones aritmeticae* pokazuje jak można zastosować rachunek kongruencji
do takich praktycznych celów jak sprawdzanie podzielności liczby przez 3 lub 9,
a także wychwytywanie ewentualnych błędów w prostych i mniej prostych obliczeniach.

Takie „sztuczki” znane były od niepamiętnych czasów i można je znaleźć – ale bez właściwego „naukowego” uzasadnienia
np. w podręcznikach arabskich (Al-Chowarizmi, Al-Karkhi).

Podzielność przez ...

W układzie dziesiętnym zapisujemy

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

Widzimy, że

- $2 \mid N \iff 2 \mid a_0$ (bo 2 dzieli 10 i wszystkie potęgi dziesiątki). W języku kongruencji:

$$N \equiv a_0 \pmod 2.$$

- $4 \mid N \iff 4 \mid a_0 + a_1 \cdot 10$. W języku kongruencji:

$$N \equiv a_0 + a_1 \cdot 10 \pmod 4.$$

- $5 \mid N \iff 5 \mid a_0$. W języku kongruencji:

$$N \equiv a_0 \pmod 5.$$

To dość banalne. Ale mamy też

- $10 \equiv 1 \pmod 9 \quad \rightarrow \quad 10^n \equiv 1 \pmod 9$
  $\rightarrow \quad N \equiv a_0 + a_1 + a_2 + \ldots + a_{n-1} + a_n \pmod 9.$
- $10 \equiv 1 \pmod 3 \quad \rightarrow \quad 10^n \equiv 1 \pmod 3$
  $\rightarrow \quad N \equiv a_0 + a_1 + a_2 + \ldots + a_{n-1} + a_n \pmod 3.$
  (obie reguły dobrze nam znane). A także
- $10 \equiv -1 \pmod{11} \quad 10^2 \equiv 1 \pmod{11} \quad 10^3 \equiv -1 \pmod{11}, \ldots$
  a jeżeli tak to ...

$$N \equiv a_0 - a_1 + a_2 - a_3 + \ldots \pmod{11}.$$

Leonardo Fibonacci w *Liber abaci* podaje też regułę podzielności przez 7; ponieważ

$$10 \equiv 3, \quad 10^2 \equiv 2, \quad 10^3 \equiv -1, \quad 10^4 \equiv -3,$$
$$10^5 \equiv -2, \quad 10^6 \equiv 1, \quad 10^7 \equiv 3 \pmod 7$$

$$N \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + \ldots \pmod 7.$$

kongruencje a poprawność operacji arytmetycznych. . .

Każda *poprawna* operacja typu dodawanie, mnożenie lub odejmowanie musi być także poprawna w języku kongruencji.
Na przykład z $c = ab$ wynika $c \equiv ab \pmod{m}$, gdzie moduł m może być dowolną liczbą.
Tak zwane *odrzucenie dziewiątek* (ang. *casting out nines*, franc. *preuve par neuf*) polega na użyciu modułu $m = 9$.

Na przykład $a = 8\,297$, $b = 3\,583$ a wynik mnożenia $c = 29\,728\,151$. Mamy

$$\left.\begin{aligned} a &\equiv 8 + 2 + 9 + 7 = 26 \equiv -1, \\ b &\equiv 3 + 5 + 8 + 3 = 19 \equiv 1, \\ c &\equiv \ldots \equiv 35 \end{aligned}\right\} \pmod{9}$$

Tak więc $ab \equiv -1, \quad c \equiv -1 \pmod{9}$. Dla modułu $m = 11$ sprawdzenie jest prawie tak samo łatwe

$$\left.\begin{aligned} a &\equiv -8 + 2 - 9 + 7 = 26 \equiv 3, \\ b &\equiv -3 + 5 - 8 + 3 = 19 \equiv -3, \\ c &\equiv \ldots \equiv 2 \end{aligned}\right\} \pmod{11}$$

więc $ab \equiv 3(-3) \equiv 2, \quad c \equiv 2 \pmod{11}$.

Nie jest to oczywiście dowód, że obliczenia są OK, ale prawdopodobieństwo błędu jest wyraźnie zmniejszone.

przykład

zweryfikuj wynik mnożenia $c = ab$ dla $a = 7\,342$ i $b = 2\,591$ oraz $c = 19\,032\,122$. jakie stąd wnioski?

kongruencje a poprawność operacji arytmetycznych, c.d

Dla dzielenia (z resztą) weryfikacja za pomocą kongruencji jest też sympatyczna:
Relacja $a = qb + r$ musi być spełniona także w języku kongruencji, dla dowolnego modułu.

Na przykład $a = 76\,638\,123$, $b = 37\,547$ a wynik dzielenia daje $q = 2\,041$ i $r = 4\,696$.
Odrzucamy dziewiątki: $a \equiv 0, \quad b \equiv -1, \quad q \equiv -2, \quad r \equiv -2 \pmod 9$ – sprawdzamy $qb + r \equiv (-2)(-1) - 2 \equiv 0 \pmod 9$.
Dla jedenastek: $a \equiv 1, \quad b \equiv 4, \quad q \equiv -5, \quad r \equiv -1 \pmod{11}$ – sprawdzamy $qb + r \equiv (4)(-5) - 1 \equiv 1 \pmod{11}$.
Dla dużych wartości liczb używa się dużych modułów, poręcznie wybranych – $m = 99$ albo $m = 101$. Parzyste potęgi 10 przystają do jedynki modulo 99, a więc dla

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

zachodzi

$$N \equiv a_0 + 10a_1 + a_2 + 10a_3 + \ldots \pmod{99}.$$