ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE III (1959)

wmptm 1897

Ministerstwo Nauki i Szkolnictwa Wyższego

K. TATARKIEWICZ (Lublin)

Ogólne kryterium podzielności liczb

1. Podręczniki teorii liczb podają kryteria podzielności przez niektóre, niezbyt wielkie liczby (na przykład Sierpiński, [3], str. 46-48, podaje, explicite lub implicite, kryteria podzielności przez wszystkie liczby mniejsze od 16, a także przez 27 i 37). Nie wspomina się natomiast o kryteriach słusznych dla wszystkich liczb naturalnych.

Ostatnio Grünbaum [1] podał metodę badania podzielności przez dowolną liczbę naturalną. Wyniki jego pracy sformułował w postaci twierdzenia (kryterium) Niven [2]. Kryterium Grünbauma-Nivena opiera się na rozwinięciach dziesiętnych i uogólnia znane kryteria podzielności przez 3 i przez 9.

Praca niniejsza ma na celu podanie prostszego dowodu kryterium Grünbauma-Nivena oraz jego uogólnienie na rozwinięcia przy dowolnej zasadzie.

2. Niech $(g, m) = 1$, to jest niech g i m będą względnie pierwsze. Wtedy — jak wiadomo — rozwinięcie $1:m$ przy zasadzie g ma okres czysty ([3], str. 222, twierdzenie 6), czyli że przed powtarzającymi się okresowo grupami liczb stoją same zera. Przypuśćmy, że długością tego okresu jest $s = s(m)$. Wtedy

$$1/m = p \sum_{\nu=0}^{\infty} g^{-s\nu} = p/(1-g^{-s}) = g^s p/(g^s - 1).$$

Skąd $g^s - 1 = g^s pm$, a więc

$$g^s \equiv 1 \pmod{m}. \tag{1}$$

Jest to podstawowa kongruencja teorii(1).

(1) Wynika ona zresztą natychmiast z cytowanego wyżej twierdzenia. Z twierdzenia tego wynika ponadto coś więcej, mianowicie że s jest wykładnikiem, do którego należy g według modułu m. Ta ostatnia uwaga może ułatwić w wielu przypadkach wyznaczenie s.

Niech

$$f(x) = \sum_{\nu=0}^{k} a_\nu x^\nu,$$

gdzie $a_0, a_1, \ldots, a_k$ są liczbami naturalnymi. Jak wiadomo, jeśli $a \equiv b \pmod m$, to $f(a) \equiv f(b) \pmod m$. A więc z (1) wynika, że

$$f(g^s) \equiv f(1) \pmod m. \tag{2}$$

Niech

$$N = \sum_{\nu=0}^{k} a_\nu g^{s\nu}, \qquad n = \sum_{\nu=0}^{k} a_\nu,$$

to znaczy że n jest sumą „cyfr" rozwinięcia liczby N przy zasadzie g^s. Oczywiście $N = f(g^s)$, $n = f(1)$, więc z (2) wynika, że

$$N \equiv n \pmod m.$$

Udowodniliśmy więc następujące

TWIERDZENIE. *Jeżeli* $(g, m) = 1$ *i* s *jest długością rozwinięcia* $1:m$ *przy zasadzie* g, *to*

$$m \mid N = \sum_{\nu=0}^{k} a_\nu g^{s\nu}$$

wtedy i tylko wtedy, gdy

$$m \mid n = \sum_{\nu=0}^{k} a_\nu.$$

Liczby N i n można napisać nieco inaczej. Mianowicie, niech $b_0, b_1, \ldots, b_{sk+s-1}$ będą cyframi rozwinięcia liczby N przy zasadzie g, to jest niech

$$N = \sum_{\nu=0}^{sk+s-1} b_\nu g^\nu.$$

Wtedy na to, by — przy wymienionych wyżej założeniach — było $m \mid N$, potrzeba i wystarcza, aby

$$m \mid n = \sum_{\nu=0}^{k} (b_{s\nu} + g b_{s\nu+1} + \ldots + g^{s-1} b_{s\nu+(s-1)}). \tag{3}$$

3. Kryterium to nie rozstrzyga przypadku, gdy $(g, m) = m_1 > 1$. Ale wtedy $m_1 \mid g$ i badanie podzielności N przez m rozpada się na — bardzo proste — badanie podzielności N przez m_1 oraz na badanie podzielności N przez $m_2 = m:m_1$.

Oczywiście najważniejszym przypadkiem szczególnym kryterium jest $g = 10$. Trzeba wszakże pamiętać, iż dla małych m i dla $g = 10$ znane skądinąd kryteria szczegółowe mogą być wygodniejsze w stosowaniu. Na przykład weźmy $m = 11$, $g = 10$, $N = \sum_{\nu=0}^{2k+1} b_\nu 10^\nu$. Wtedy znane kryterium podzielności przez 11 wymaga dzielenia sumy liczb jednocyfrowych $\sum_{\nu=0}^{2k+1} (-1)^\nu b_\nu$ przez 11, natomiast kryterium Grünbauma-Nivena zgodnie z wzorem (3) wymaga dzielenia sumy liczb dwucyfrowych $\sum_{\nu=0}^{k} (b_{2\nu} + 10 b_{2\nu+1})$ przez 11.

Warto zauważyć, że dla niektórych m wartość kryterium Grünbauma-Nivena może być iluzoryczna. Jak wiadomo, może być $s(m) = s-1$. Na przykład dla $m = 1913$, $g = 10$ mamy $s = 1912$ ([3], str. 223), a więc kryterium ustępu 2 dla podzielności przez 1913 nic nie daje, o ile dzielna ma mniej niż 1913 cyfr.

Mimo tych zastrzeżeń kryterium Grünbauma-Nivena może znaleźć zastosowanie praktyczne nawet dla względnie dużych dzielników. Na przykład dla $m = 2439$ i $g = 10$ mamy $s = 5$ ([1]), a więc wzór (3) warto stosować dla badania podzielności przez 2439 wszystkich liczb co najmniej 6-cyfrowych (w układzie dziesiętnym).

Prace cytowane

[1] H. Grünbaum, *On divisibility of numbers*, Scripta Math. 21 (1955), str. 204-207.

[2] I. Niven, *Recenzja pracy H. Grünbauma „On divisibility of numbers"*, Math. Rev. 17 (1956), str. 459.

[3] W. Sierpiński, *Teoria liczb*, Warszawa 1950.