Dowód. Niech p będzie liczbą pierwszą; wykładnikami, z jakimi p wchodzi do rozwinięcia liczb $a_1, a_2, ..., a_m$, niech będą odpowiednio liczby $\alpha_1, \alpha_2, ..., \alpha_m$. Do rozwinięcia $[a_1, a_2, ..., a_m]$ liczba p wchodzi oczywiście z wykładnikiem $\max(\alpha_1, \alpha_2, ..., \alpha_m)$, do rozwinięcia $(a_1, a_2, ..., a_m)$ — z wykładnikiem $\min(\alpha_1, \alpha_2, ..., \alpha_m)$, do rozwinięcia $\left(\frac{a_1 a_2 ... a_m}{a_1}, \frac{a_1 a_2 ... a_m}{a_2}, ..., \frac{a_1 a_2 ... a_m}{a_m}\right)$ — z wykładnikiem $\min(\sigma-\alpha_1, \sigma-\alpha_2, ..., \sigma-\alpha_m)$. gdzie $\sigma = \alpha_1+\alpha_2+...+\alpha_m$; wreszcie do rozwinięcia $\left[\frac{a_1 a_2 ... a_m}{a_1}, \frac{a_1 a_2 ... a_m}{a_2}, ..., \frac{a_1 a_2 ... a_m}{a_m}\right]$ liczba p wchodzi z wykładnikiem $\max(\sigma-\alpha_1, \sigma-\alpha_2, ..., \sigma-\alpha_m)$ i do rozwinięcia $a_1 a_2 ... a_m$ — z wykładnikiem σ. Lecz jak łatwo widzieć:

$$\max(\alpha_1, \alpha_2, ..., \alpha_m)+\min(\sigma-\alpha_1, \sigma-\alpha_2, ..., \sigma-\alpha_m) = \sigma,$$

$$\min(\alpha_1, \alpha_2, ..., \alpha_m)+\max(\sigma-\alpha_1, \sigma-\alpha_2, ..., \sigma-\alpha_m) = \sigma,$$

skąd prawdziwość wzorów (21).

Inny dowód. Niech $N=[a_1, a_2, ..., a_n]$ i $P=a_1 a_2 ... a_n$. Największy wspólny dzielnik liczb

$$\frac{NP}{a_1}, \quad \frac{NP}{a_2}, \quad ..., \quad \frac{NP}{a_m}$$

jest oczywiście równy N-krotnemu największemu wspólnemu dzielnikowi liczb

$$\frac{P}{a_1}, \quad \frac{P}{a_2}, \quad ..., \quad \frac{P}{a_m},$$

jakoteż P-krotnemu największemu wspólnemu dzielnikowi liczb

$$\frac{N}{a_1}, \quad \frac{N}{a_2}, \quad ..., \quad \frac{N}{a_m};$$

lecz ten ostatni jest równy 1, gdyby bowiem był równy $d>1$, to — jak łatwo widzieć — liczba $N:d$ byłaby wspólną wielokrotnością liczb $a_1, a_2, ..., a_m$ wbrew określeniu liczby N, która jest większa niż $N:d$. Jest więc $N\cdot\left(\frac{P}{a_1}, \frac{P}{a_2}, ..., \frac{P}{a_m}\right)=P$, c. b. d. o.

ROZDZIAŁ III

ZASADNICZE WŁASNOŚCI KONGRUENCJI KONGRUENCJE 1-go STOPNIA O MODULE PIERWSZYM

§ 1. Kongruencje i ich ważniejsze własności. O dwu danych liczbach całkowitych a i b mówimy, że *przystają do siebie według modułu* m, jeżeli różnica tych liczb jest podzielna przez m. Wyrażamy to na piśmie w ten sposób:

$$a \equiv b \pmod m$$

i wzór ten nazywamy *kongruencją* [1]).

Jasne jest, że dwie liczby przystające do siebie według danego modułu naturalnego m dają przy dzieleniu przez ten moduł jednakowe reszty i na odwrót.

Kongruencje mają wiele własności przypominających analogiczne własności *równości* (co też usprawiedliwia używanie symbolu $\equiv$ przypominającego znak równości). Ważniejszymi z nich są:

I. Prawo tożsamości, które polega na tym, że każda liczba przystaje sama do siebie według każdego modułu:

$$a \equiv a \pmod m$$

przy wszelkim całkowitym a i naturalnym m. Dla dowodu wystarczy zauważyć, że liczba $a-a=0$ jest podzielna przez każde naturalne m.

II. Prawo symetrii, polegające na tym, że kongruencja

$$a \equiv b \pmod m$$

równoważna jest zawsze kongruencji

$$b \equiv a \pmod m.$$

Dla dowodu wystarczy zauważyć, że liczby $a-b$ i $b-a$ są zawsze jednocześnie podzielne lub jednocześnie niepodzielne przez m.

---

[1]) Znakowanie to wprowadził Karol Fryderyk Gauss.

III. Prawo przechodniości, według którego z kongruencji

$$a \equiv b \pmod m \quad \text{i} \quad b \equiv c \pmod m$$

wynika zawsze kongruencja

$$a \equiv c \pmod m.$$

Dla dowodu wystarczy oprzeć się na tożsamości

$$a - c = (a - b) + (b - c).$$

Równie łatwo dowiedziemy kilku innych własności kongruencji.

Okażemy, że *kongruencje o tym samym module można dodawać i odejmować stronami.*

Niech

$$a \equiv b \pmod m \qquad \text{i} \qquad c \equiv d \pmod m.$$

Aby dowieść, że

$$a + c \equiv b + d \pmod m \qquad \text{i} \qquad a - c \equiv b - d \pmod m,$$

wystarczy oprzeć się na tożsamościach

$$(a + c) - (b + d) = (a - b) + (c - d),$$
$$(a - c) - (b - d) = (a - b) - (c - d).$$

Podobnie, opierając się na tożsamości

$$ac - bd = (a - b)c + (c - d)b,$$

dowodzimy kongruencji

$$ac \equiv bd \pmod m.$$

Zatem *kongruencje o tym samym module można mnożyć stronami.*

Twierdzenia te o dodawaniu i mnożeniu dwu kongruencji uogólniamy natychmiast na dowolną skończoną liczbę kongruencji.

Z twierdzenia o dodawaniu kongruencji wynika natychmiast (podobnie jak dla równań), że *można przenosić wyrazy z jednej strony kongruencji na drugą, zmieniając ich znaki.*

Jest to bowiem równoważne odejmowaniu przenoszonego wyrazu od obu stron kongruencji.

Z twierdzenia o mnożeniu kongruencji wynika w szczególności, że *obie strony kongruencji można mnożyć przez jedną i tę samą liczbę całkowitą* oraz *że obie strony kongruencji można podnosić do jednej i tej samej potęgi* (o naturalnym wykładniku).

Nie mamy jednak na ogół prawa dzielić kongruencji stronami; np. z kongruencji $48 \equiv 18 \pmod{10}$ i $12 \equiv 2 \pmod{10}$, nie wynika kongruencja $4 \equiv 9 \pmod{10}$.

Z twierdzenia, że dzielnik dzielnika danej liczby jest znowu dzielnikiem tejże liczby, wnosimy natychmiast, że *jeżeli* $d \mid m$, *to z kongruencji* $a \equiv b \pmod m$ *wynika kongruencja* $a \equiv b \pmod d$.

Z prawa przechodniości w połączeniu z twierdzeniami o dodawaniu i mnożeniu kongruencji wynika, że *w kongruencji mamy zawsze prawo zastąpić dany składnik i czynnik przez inny, przystający do niego według modułu kongruencji.*

Reguły tej jednak nie mamy prawa stosować względem wykładników; np. kongruencji $2^6 \equiv 4 \pmod 5$ nie mamy prawa zastąpić przez kongruencję $2^1 \equiv 4 \pmod 5$, pomimo że $6 \equiv 1 \pmod 5$.

ĆWICZENIA. 1. Obliczyć ostatnią cyfrę liczby 2^{1000}.

Rozwiązanie. Jest $6^2 \equiv 6 \pmod{10}$, więc przez łatwą indukcję dowodzimy, że $6^k \equiv 6 \pmod{10}$ dla naturalnych k; nadto $2^4 \equiv 6 \pmod{10}$, a więc $2^{1000} \equiv 6^{250} \equiv 6 \pmod{10}$. Ostatnią cyfrą liczby 2^{1000} jest zatem 6.

2. Obliczyć resztę z dzielenia liczby 2^{100} przez 3.

Rozwiązanie. $2^2 \equiv 1 \pmod 3$, skąd $2^{100} \equiv 1^{50} \pmod 3$ czyli $2^{100} \equiv 1 \pmod 3$. Resztą z dzielenia liczby 2^{100} przez 3 jest więc 1.

3. Obliczyć dwie ostatnie cyfry liczby 2^{1000}.

Rozwiązanie. Jest $2^{10} \equiv 24 \pmod{100}$, skąd $2^{20} \equiv 24^2 \equiv 76 \pmod{100}$. Lecz $76^2 \equiv 76 \pmod{100}$, skąd (przez indukcję) $76^k \equiv 76 \pmod{100}$ dla naturalnych k. Zatem $2^{1000} \equiv 2^{20 \cdot 50} \equiv 76^{50} \equiv 76 \pmod{100}$. Ostatnimi dwiema cyframi liczby 2^{1000} są więc 7 i 6.

Uwaga. Przy pomocy logarytmów można też z łatwością obliczyć pierwszą cyfrę liczby 2^{1000}. Istotnie mamy

$$2^{1000} = 10^{1000 \cdot \lg 2} = 10^{301{,}03\ldots} = 10^{301} \cdot 10^{0{,}03\ldots}.$$

Lecz $1 < 10^{0{,}03\ldots} < 10^{1/4} < 2$, zatem $1 \cdot 10^{301} < 2^{1000} < 2 \cdot 10^{301}$, skąd wnosimy, że pierwszą cyfrą liczby 2^{1000} jest 1. Czytelnik zechce się zastanowić nad tym, jakby można obliczyć drugą cyfrę liczby 2^{1000}.

4. Znaleźć najmniejszy dzielnik pierwszy liczby $2^{82} + 1$.

Rozwiązanie. 2 nie jest dzielnikiem tej liczby, gdyż jest ona niepar zytą. Sprawdzamy, czy nie jest nim liczba 3. W tym celu badamy, do jakie liczby przystaje dana liczba modulo 3. Jest $2^2 \equiv 1 \pmod 3$, zatem $2^{82} \equiv 1 \pmod 3$, skąd $2^{82} + 1 \equiv 2 \pmod 3$. Dana liczba nie jest więc podzielna przez 3. Badamy dalej, do jakiej liczby przystaje dana liczba modulo 5. Jest $2^2 \equiv -1 \pmod 5$, zatem $2^{82} \equiv (-1)^{41} \pmod 5$, czyli $2^{82} \equiv -1 \pmod 5$, skąd $2^{82} + 1 \equiv 0 \pmod 5$, czyli $5 \mid 2^{82} + 1$. Najmniejszym dzielnikiem pierwszym liczby $2^{82} + 1$ jest więc liczba 5.

5. Jaki jest najmniejszy dzielnik pierwszy liczby $2^{99} - 1$?

Odpowiedź: 7.

6. Jaki jest najmniejszy dzielnik pierwszy liczby $2^{76} + 1$?

Odpowiedź: 17.

7. Obliczyć dwie ostatnie cyfry liczby 9^{9^9}.

Rozwiązanie. Z łatwością stwierdzamy, że modulo 100:

$9^2 \equiv 81$, $9^4 \equiv 81^2 \equiv 61$, $9^8 \equiv 61^2 \equiv 21$, $9^9 \equiv 21 \cdot 9 \equiv 89$, $9^{10} \equiv 89 \cdot 9 \equiv 1$.

Jest więc $9^9 \equiv 9 \pmod{10}$, zatem $9^9 = 10k+9$, skąd wobec $9^{10} \equiv 1 \pmod{100}$ znajdujemy $9^{9^9} = 9^{10k+9} = 9^{10k} \cdot 9^9 \equiv 9^9 \equiv 89 \pmod{100}$. Ostatnimi dwiema cyframi liczby 9^{9^9} są więc 8 i 9.

Uwagi. Jak łatwo obliczyć, jest $9^9 > 10^8$, skąd $9^{9^9} > 9^{10^8} = 9^{10 \cdot 10^7} > 10^{8 \cdot 10^7}$, co dowodzi, że liczba 9^{9^9} ma miliony cyfr (dokładniej: więcej niż 369 milionów cyfr). Obliczono też 30 pierwszych cyfr tej liczby [1]). Pierwsze pięć są następujące: 4, 2, 8, 1 i 2.

8. Obliczyć dwie ostatnie cyfry liczby $9^{9^{9^9}}$.

Rozwiązanie. Jak obliczyliśmy w ćwiczeniu 7, jest $9^{9^9} \equiv 9 \pmod{10}$, zatem $9^{9^9} = 10k+9$, skąd $9^{9^{9^9}} = 9^{10k+9} \equiv 9^9 \equiv 89 \pmod{100}$. Ostatnimi dwiema cyframi danej liczby są więc 8 i 9.

Uwaga. Jak podaje Lietzmann [2]), liczba cyfr tej liczby ma więcej niż ćwierć miliarda cyfr. Ponoć Gauss nazwał tę liczbę „mierzalną nieskończonością".

9. Znaleźć wszystkie rozwiązania równania $2^m - 3^n = 1$ w liczbach naturalnych m i n.

Odpowiedź. Równanie to ma tylko jedno rozwiązanie w liczbach naturalnych: $m=2$, $n=1$. Istotnie, $3^2 \equiv 1 \pmod 8$, skąd dla k naturalnych $3^{2k}+1 \equiv 2 \pmod 8$ i $3^{2k-1}+1 \equiv 4 \pmod 8$; dowodzi to, że przy naturalnym n liczba 3^n+1 nie jest podzielna przez 8, tym bardziej więc przez 2^m dla naturalnych $m \geqslant 3$. Jeżeli zatem przy naturalnych m i n jest $3^n+1 = 2^m$, to musi być $m \leqslant 2$, a więc albo $3^n+1=2$ albo $3^n+1=2^2$. Pierwsza z tych równości daje $3^n=1$, co przy naturalnym n jest niemożliwe, a druga daje $3^n=3$, skąd $n=1$. Mamy więc $m=2$ i $n=1$, c. b. d. o.

10. Dowieść, że każde dwie różne liczby ciągu $2^{2^n}+1$ ($n=0, 1, 2, \ldots$) są względnie pierwsze.

Dowód. Jeżeli p jest dzielnikiem pierwszym liczby $2^{2^k}+1$ (gdzie k jest liczbą całkowitą nieujemną), to p musi być liczbą nieparzystą i mamy $2^{2^k} \equiv -1 \pmod p$, skąd wynika, że $2^{2^{k+l}} \equiv 1 \pmod p$ dla naturalnych l, zatem $2^{2^{k+l}}+1 \equiv 2 \pmod p$ i liczba $2^{2^{k+l}}+1$ nie jest podzielna przez liczbę (nieparzystą) p. Stąd łatwy wniosek, że żadne dwa różne wyrazy danego ciągu nie mają wspólnego dzielnika pierwszego, są zatem względnie pierwsze, c. b. d. o.

Uwaga. Oznaczmy przez q_n najmniejszy dzielnik pierwszy liczby $2^{2^n}+1$. Liczby $q_0, q_1, \ldots, q_{n-1}$ są więc wszystkie pierwsze i nie większe od $2^{2^{n-1}}+1 < 2^{2^n}$.

[1]) W. Lietzmann, *Riesen und Zwerge im Zahlenreich*, Mathematische Bibliothek von W. Lietzmann und A. Witting Nr. 25, Lipsk-Berlin 1916, str. 33.

[2]) W. Lietzmann, *Lustiges und merkwürdiges von Zahlen und Formen*, wyd. 4-e, Wrocław 1930, str. 118.

Istnieje więc co najmniej n liczb pierwszych mniejszych od 2^{2^n} (Pólya i Szegö), a przeto $p_n < 2^{2^n}$ dla $n=1, 2, \ldots$ (gdzie p_n jest n-tą z kolei liczbą pierwszą).

11. Dowieść, że przy wszelkim naturalnym n liczba $3^{2n-1}+2^{n+1}$ jest podzielna przez 7. (Wolstenholme).

Dowód. Jest $3 \equiv -2^2 \pmod 7$, skąd

$$3^{2n-1}+2^{n+1} \equiv -2^{4n-2}+2^{n+1} \equiv 2^{n+1}(-2^{3(n-1)}+1) \equiv 0 \pmod 7,$$

gdyż $2^{3(n-1)} = 8^{n-1} \equiv 1 \pmod 7$.

12. Dowieść, że $2^{70}+3^{70} \equiv 0 \pmod{13}$. (Kraïtchik).

13. Dowieść, że $10^{50}+1 \equiv 0 \pmod{7019801}$. (Kraïtchik).

14. Dowieść, że $(2^8+1) \mid (2^{120}+1)$ i $97 \mid (2^{120}+1)$.

15. Zbadać, czy liczba 10^8+1 jest pierwszą.

Odpowiedź: Nie, gdyż jest podzielna przez 17. Mamy bowiem $10 \equiv -7 \pmod{17}$, skąd $10^2 \equiv 49 \equiv -2 \pmod{17}$, $10^4 \equiv 4 \pmod{17}$, $10^8 \equiv 16 \pmod{17}$, zatem $10^8+1 \equiv 0 \pmod{17}$ czyli $17 \mid (10^8+1)$.

16. Dowieść, że dla naturalnych $n \geqslant 3$ jest przy wszelkim naturalnym k

$$(2k-1)^{2^{n-2}} \equiv 1 \pmod{2^n}. \tag{*}$$

Dowód. Wzór (*) jest prawdziwy dla $n=3$, gdyż kwadrat liczby nieparzystej przy dzieleniu przez 8 daje zawsze resztę 1. Niech więc n będzie liczbą naturalną większą od 3. Załóżmy, że wzór (*) zachodzi dla liczby $n-1$, mianowicie, że (dla wszelkich naturalnych k)

$$(2k-1)^{2^{n-3}} \equiv 1 \pmod{2^{n-1}}.$$

Jest więc $2^{n-1} \mid (2k-1)^{2^{n-3}} - 1$. Lecz oczywiście $2 \mid (2k-1)^{2^{n-3}}+1$, a zatem

$$2^n = 2^{n-1} \cdot 2 \mid [(2k-1)^{2^{n-3}}-1][(2k-1)^{2^{n-3}}+1] = (2k-1)^{2^{n-2}}-1,$$

skąd wynika od razu wzór (*). Wzór ten został więc dla naturalnych $n \geqslant 3$ udowodniony przez indukcję.

Tak np.:

$(2k-1)^2 \equiv 1 \pmod 8$, $(2k-1)^4 \equiv 1 \pmod{16}$, $(2k-1)^8 \equiv 1 \pmod{32}$.

Dla $n=2$ i $k=2$ wzór (*) jest fałszywy.

17. Dowieść, że dla każdej liczby naturalnej $n \geqslant 3$ istnieje taka liczba naturalna k, iż

$$(2k-1)^{2^{n-2}-1} \not\equiv 1 \pmod{2^n}.$$

Dowód wynika z uwagi, że dla $n \geqslant 3$ liczba $2^{n-2}-1$ jest nieparzysta i że $(2^n-1)^{2^{n-2}-1} \equiv -1 \pmod{2^n}$.

18 Dowieść, że dla każdej liczby naturalnej $n \geqslant 3$ istnieje taka liczba naturalna k, iż

$$(2k-1)^{2^{n-3}} \not\equiv 1 \pmod{2^n}.$$

Dowód wynika z uwagi, że $3 \not\equiv 1 \pmod 8$ i $3^{2^{n-3}} \equiv 2^{n-1}+1 \pmod{2^n}$ dla $n \geqslant 4$, czego z łatwością dowodzi się przez indukcję.

19. Dowieść, że

$$5\,2^{n-3} \equiv 2^{n-1}+1 \pmod{2^n} \text{ dla } n \geqslant 3,$$

natomiast

$$7\,2^{n-3} \equiv 1 \pmod{2^n} \text{ dla } n \geqslant 4.$$

20 Dowieść, że równanie $x^2-2y^2=3$ nie posiada rozwiązań w liczbach całkowitych x, y.

Dowód, Dla $y=2k$ byłoby $x^2=8k^2+3$, a dla $y=2k+1$ byłoby $x^2 \equiv 5 \pmod 8$, gdy tymczasem x jest nieparzyste i przeto $x^2 \equiv 1 \pmod 8$.

21. Dowieść, że równanie $x^2-2y^2=8z+3$ nie posiada rozwiązań w liczbach całkowitych x, y, z.

22. Dowieść, że równanie $x^2-3y^2=3z+2$ nie posiada rozwiązań w liczbach całkowitych x, y, z.

Dowód. Jeżeli $x^2=3y^2+3z+2$, to liczba x nie może być podzielna przez 3. Jest więc $x=3k\pm 1$, skąd $x^2 \equiv 1 \pmod 3$, gdy tymczasem

$$3y^2+3z+2 \equiv 2 \pmod 3.$$

23. Dowieść, że z równań $x^2-2y=3$ i $x^2-3y=2$ pierwsze jest, a drugie nie jest rozwiązalne w liczbach całkowitych x, y.

§ 2. Zastosowanie kongruencji do otrzymania cech podzielności przez 9, 11, 7, 13, 27 i 37.

Niech

$$A_0x^n+A_1x^{n-1}+A_2x^{n-2}+\ldots.+A_{n-1}x+A_n \tag{1}$$

będzie wielomianem całkowitym n-tego stopnia o spółczynnikach całkowitych; wielomian ten oznaczymy dla krótkości przez $f(x)$.

Niech dalej m będzie danym modułem, a a i b liczbami całkowitymi przystającymi według modułu m. W myśl twierdzeń o potęgowaniu i mnożeniu kongruencji, możemy wypisać ciąg kongruencji:

$$\begin{gathered} A_0a^n \equiv A_0b^n \pmod m, \\ A_1a^{n-1} \equiv A_1b^{n-1} \pmod m, \\ \cdots\cdots\cdots \\ A_{n-1}a \equiv A_{n-1}b \pmod m, \\ A_n \equiv A_n \pmod m. \end{gathered}$$

Dodając te kongruencje stronami, otrzymujemy

$$\begin{gathered} A_0a^n+A_1a^{n-1}+\ldots.+A_{n-1}a+A_n \equiv \\ \equiv A_0b^n+A_1b^{n-1}+\ldots.+A_{n-1}b+A_n \pmod m, \end{gathered}$$

czyli w przyjętym znakowaniu

$$f(a) \equiv f(b) \pmod m.$$

Mamy zatem następujące

Twierdzenie 1. *Jeżeli $f(x)$ jest wielomianem całkowitym względem x o spółczynnikach całkowitych, to kongruencja*

$$a \equiv b \pmod m$$

pociąga za sobą kongruencję

$$f(a) \equiv f(b) \pmod m.$$

Podamy teraz zastosowania twierdzenia 1.

Niech N będzie liczbą naturalną, a $c_1, c_2, c_3, \ldots. c_n$ jej kolejnymi cyframi w układzie dziesiętnym. Oczywiście

$$N=c_1\,10^{n-1}+c_2\,10^{n-2}+\ldots.+c_{n-1}\,10+c_n.$$

Niech

$$f(x)=c_1x^{n-1}+c_2x^{n-2}+\ldots.+c_{n-1}x+c_n. \tag{2}$$

Jest to więc wielomian całkowity o spółczynnikach całkowitych i

$$f(10)=N. \tag{3}$$

W myśl twierdzenia 1 i wobec kongruencji $10 \equiv 1 \pmod 9$ jest

$$f(10) \equiv f(1) \pmod 9. \tag{4}$$

Lecz na mocy (2) mamy

$$f(1)=c_1+c_2+\ldots.+c_{n-1}+c_n;$$

zatem wobec (3) i (4)

$$N \equiv c_1+c_2+c_3+\ldots.+c_{n-1}+c_n \pmod 9,$$

co dowodzi, że każda liczba naturalna przystaje według modułu 9 do sumy swoich cyfr.

Wynika stąd natychmiast, że *dla podzielności liczby N przez 9 potrzeba i wystarcza, by suma jej cyfr była podzielna przez 9.*

Oznaczając ogólnie przez s_n sumę cyfr liczby n (w układzie dziesiętnym), będziemy mieli dla liczb całkowitych n i n':

$$n \equiv s_n \pmod 9, \qquad n' \equiv s_{n'} \pmod 9,$$

skąd $nn' \equiv s_n s_{n'} \pmod 9$, a że $nn' \equiv s_{nn'} \pmod 9$, więc ostatecznie

$$s_{nn'} \equiv s_n s_{n'} \pmod 9.$$

Na tym związku między sumami cyfr czynników i iloczynu opiera się znana *próba mnożenia za pomocą liczby 9.*

Wobec wzoru (2) oraz kongruencji $10 \equiv -1 \pmod{11}$, mamy

$$f(10) \equiv f(-1) \pmod{11}$$

czyli

$$N \equiv c_1 - c_2 + c_3 - c_4 + c_5 - \ldots \pmod{11};$$

wynika stąd znana *cecha podzielności przez* 11.

Wyprowadzimy jeszcze cechy podzielności przez 7 i przez 13. Będziemy oznaczali symbolem

$$(c_1 c_2 \ldots c_n)_{10}$$

liczbę naturalną, której kolejnymi cyframi w układzie dziesiętnym są $c_1, c_2, c_3, \ldots, c_n$; znakowanie takie wprowadzamy dla odróżnienia od iloczynu $c_1 c_2 c_3 \ldots c_n$.

Każdą liczbę naturalną $N=(c_1 c_2 \ldots c_n)_{10}$ możemy oczywiście przedstawić w postaci

$$N=(c_{n-2}c_{n-1}c_n)_{10}+(c_{n-5}c_{n-4}c_{n-3})_{10}\cdot 1000+(c_{n-8}c_{n-7}c_{n-6})_{10}\cdot 1000^2+\ldots$$

Wobec kongruencji $1000 \equiv -1 \pmod 7$ i $\pmod{13}$ mamy stąd

$$N \equiv (c_{n-2}c_{n-1}c_n)_{10} - (c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-8}c_{n-7}c_{n-6})_{10} - \ldots \pmod 7$$

i taką samą kongruencję według modułu 13.

Z kongruencji tych wynikają od razu cechy podzielności przez 7 i przez 13. Więc np.

$$N = 8\,589\,879\,056 \equiv 56 - 879 + 589 - 8 \pmod 7 \text{ i } \pmod{13},$$

a że prawa strona tych kongruencji, wynosząca -242, nie jest podzielna ani przez 7, ani przez 13, więc i liczba N nie jest podzielna ani przez 7, ani przez 13.

Opierając się na kongruencjach

$$1000 \equiv 1 \pmod{27} \quad \text{i} \quad \pmod{37},$$

wyprowadza się w podobny sposób cechy podzielności przez 27 i przez 37. Więc np.:

$$n = 24540509 \equiv 509 + 540 + 24 \pmod{27} \quad \text{i} \quad \pmod{37}.$$

Prawa strona tej kongruencji wynosi 1073. Możemy jednak znowu napisać

$$1073 \equiv 73 + 1 \pmod{27} \quad \text{i} \quad \pmod{37},$$

a że 74 jest podzielne przez 37, lecz nie podzielne przez 27, więc tak samo jest z liczbą n.

§ 3. Pierwiastki kongruencji. Reszty według danego modułu. Niech $f(x)$ będzie wielomianem (1) całkowitym n-tego stopnia o spółczynnikach całkowitych, a m — danym modułem. Każdą liczbę $x=a$, dla której

$$f(a) \equiv 0 \pmod m,$$

nazywamy *pierwiastkiem kongruencji*

$$f(x) \equiv 0 \pmod m. \tag{5}$$

Z twierdzenia 1 wynika, że jeżeli a jest pierwiastkiem kongruencji (5), to każda liczba przystająca do a według modułu m również jest pierwiastkiem tej kongruencji. Całą taką klasę liczb przystających według modułu m i spełniających daną kongruencję będziemy uważali za jeden jej pierwiastek. Pierwiastek ten może być reprezentowany przez dowolną liczbę tej klasy.

Każda liczba całkowita przystaje według modułu m do jednej i tylko jednej z liczb ciągu

$$0, 1, 2, 3, \ldots, m-1. \tag{6}$$

Rzeczywiście, niech a będzie liczbą całkowitą. Oznaczmy (według Legendre'a) symbolem $\mathrm{E}(x)$ największą liczbę całkowitą nie większą od x; jest to tak zwana z francuska funkcja liczbowa *Entier* z x. Niech

$$r = a - m\,\mathrm{E}\left(\frac{a}{m}\right). \tag{7}$$

Jest to oczywiście pewna liczba całkowita. Z definicji symbolu $\mathrm{E}(x)$ wynika, iż $\mathrm{E}\left(\frac{a}{m}\right) \leqslant \frac{a}{m}$, lecz już $\mathrm{E}\left(\frac{a}{m}\right)+1 > \frac{a}{m}$. Jest zatem

$$\frac{a}{m} - 1 < \mathrm{E}\left(\frac{a}{m}\right) \leqslant \frac{a}{m},$$

skąd wobec (7)

$$0 \leqslant r < m.$$

Liczba r jest więc jednym z wyrazów ciągu (6). Z drugiej strony, ze wzoru (7) wnosimy, że zachodzi kongruencja

$$r \equiv a \pmod m.$$

Każda liczba całkowita a przystaje więc według modułu m co najmniej do jednej z liczb (6). Ponieważ z drugiej strony, żadne dwa wyrazy ciągu (6), jako dające przy dzieleniu przez m różne reszty, nie przystają do siebie, więc wnosimy, że każda liczba całkowita a przystaje tylko do jednej z liczb (6).

Liczbę tę nazywamy *resztą* liczby a modulo m.

Wszystkie liczby całkowite, mające tę samą resztę r według modułu m, są oczywiście postaci

$$mk+r,$$

gdzie k jest liczbą całkowitą ($k=0, \pm 1, \pm 2, \pm 3, \ldots$). Dla rozwiązania danej kongruencji (5) n-tego stopnia wystarczy więc oczywiście badać tylko liczby ciągu (6).

PRZYKŁAD. Rozwiążemy kongruencję

$$x^5-3x^2+2\equiv 0 \pmod 7. \tag{8}$$

Mamy tu więc zbadać tylko liczby 0, 1, 2, 3, 4, 5, 6.

Przez bezpośrednie podstawienie sprawdzamy, że 0 nie jest, natomiast 1 jest pierwiastkiem kongruencji (8). Z łatwością sprawdzamy też, że 2 nie spełnia tej kongruencji. Badanie liczby 3 możemy sobie ułatwić w ten sposób: $3^2\equiv 2 \pmod 7$; podnosząc obie strony do kwadratu, dostajemy $3^4\equiv 4 \pmod 7$, mnożąc zaś przez 3 ostatnią kongruencję, znajdujemy $3^5\equiv 12\equiv 5 \pmod 7$. Jest więc

$$3^5-3\cdot 3^2+2\equiv 5-6+2\equiv 1 \pmod 7.$$

Dla liczby 4 jest $4\equiv -3 \pmod 7$; stąd $4^5\equiv(-3)^5\equiv -5 \pmod 7$. i przeto

$$4^5-3\cdot 4^2+2\equiv -5-6+2\equiv 5 \pmod 7.$$

Dla liczby 5 mamy $5\equiv -2 \pmod 7$, skąd $5^5\equiv(-2)^5\equiv 3 \pmod 7$ i przeto

$$5^5-3\cdot 5^2+2\equiv 3-5+2\equiv 0 \pmod 7.$$

Liczba 5 jest więc pierwiastkiem kongruencji (8).

Dla liczby 6 mamy $6\equiv -1 \pmod 7$, skąd wnosimy z łatwością, że 6 nie spełnia kongruencji (8).

Kongruencja (8) ma więc dwa pierwiastki: 1 i 5. Każda liczba całkowita, spełniająca tę kongruencję, musi być zatem jednej z dwu postaci:

$$7k+1, \qquad 7k+5.$$

§ 4. Związek między kongruencjami a pewną klasą równań nieoznaczonych. Kongruencje tożsamościowe i kongruencje sprzeczne. Istnieje ścisły związek między kongruencjami a pewnymi równaniami nieoznaczonymi, mianowicie tymi, w których jedna ze zmiennych występuje liniowo. Na to bowiem, by liczba x spełniała kongruencję (5), potrzeba i wystarcza, żeby było

$f(x)=my$, gdzie y jest liczbą całkowitą. Kongruencja (5) jest więc równoważna równaniu nieoznaczonemu

$$f(x)-my=0.$$

Tak np. kongruencja (8) jest równoważna równaniu nieoznaczonemu

$$x^5-3x^2+2-7y=0.$$

Kongruencję, którą spełnia każda liczba całkowita, nazywamy *tożsamościową*.

Np. kongruencja

$$x^2+x\equiv 0 \pmod 2$$

jest tożsamościowa. Wynika to stąd, że liczby x i x^2 są zawsze albo obie parzyste, albo obie nieparzyste, tak że suma ich jest zawsze parzysta.

Przytoczony przykład dowodzi zarazem, że w kongruencji tożsamościowej niekoniecznie wszystkie spółczynniki muszą być podzielne przez moduł.

Kongruencję nazywamy *sprzeczną*, jeżeli nie ma ona żadnego pierwiastka.

Np. kongruencja

$$x^3\equiv 2 \pmod 4$$

jest sprzeczna, gdyż w razie x nieparzystego x^3 jest również nieparzyste (a więc przystające do 1 lub do 3 według modułu 4), w razie zaś x parzystego x^3 jest oczywiście podzielne przez 8, a więc przystające do $0 \pmod 4$.

§ 5. Kongruencje 1-go stopnia o module pierwszym. Każdą kongruencję 1-go stopnia możemy oczywiście sprowadzić do postaci

$$ax\equiv b \pmod m.$$

Załóżmy więc, że $m=p$, gdzie p jest liczbą pierwszą, i zbadajmy kongruencję

$$ax\equiv b \pmod p. \tag{9}$$

Rozróżnimy trzy przypadki:

1° Liczby a i b są obie podzielne przez p. Jasne jest, że w tym przypadku kongruencja (9) jest tożsamościowa.

2° Liczba a jest podzielna przez p, a b nie jest podzielna przez p. W tym przypadku mamy oczywiście przy wszelkim x całkowitym, $ax\equiv 0 \pmod p$ i kongruencja (9) jest sprzeczna.

3⁰ Liczba a nie jest podzielna przez p. W tym przypadku mamy $(a,p)=1$ wobec założenia, że p jest liczbą pierwszą. Możemy więc (ob. Rozdział II, § 2) wyznaczyć takie dwie liczby całkowite ξ i η, iż

$$a\xi+p\eta=1;$$

pisząc $x_0=b\xi$, będziemy mieli $ax_0=ab\xi=b-bp\eta\equiv b\pmod p$ czyli

$$ax_0\equiv b\pmod p. \tag{9}$$

Kongruencja (9) ma więc w tym przypadku co najmniej jeden pierwiastek. Załóżmy, że liczba x_1 jest również pierwiastkiem kongruencji (9). Mielibyśmy $ax_1\equiv ax_0\pmod p$, skąd wnosilibyśmy, że różnica $a(x_1-x_0)$ jest podzielna przez p.

Lecz wobec $(a,p)=1$ musiałoby x_1-x_0 być wtedy podzielne przez p, czyli

$$x_1\equiv x_0\pmod p.$$

Liczby x_0 i x_1 przedstawiają więc ten sam pierwiastek kongruencji (9). Udowodniliśmy zatem

Twierdzenie 2. *Jeżeli a jest liczbą niepodzielną przez liczbę pierwszą p, to kongruencja*

$$ax\equiv b\pmod p$$

ma jeden i tylko jeden pierwiastek.

Zauważmy na zakończenie, że liczenie pierwiastków kongruencji $f(x)\equiv 0\pmod m$, jakie stosujemy w przypadku, gdy $f(x)$ jest wielomianem całkowitym o spółczynnikach całkowitych, nie daje się zastosować w innych przypadkach, np. do kongruencji wykładniczej $2^x\equiv 1\pmod 7$, gdyż np. liczba 10, choć przystaje według modułu 7 do pierwiastka 3 tej kongruencji, nie jest jej pierwiastkiem (por. str. 43).

ROZDZIAŁ IV

TWIERDZENIA WILSONA, EULERA I FERMATA TWIERDZENIA O ROZKŁADACH NA SUMĘ KWADRATÓW

§ 1. Reszty i niereszty kwadratowe. Dowód twierdzeń Wilsona, Eulera i małego twierdzenia Fermata. Symbol Legendre'a. Niech p oznacza liczbę pierwszą nieparzystą, D zaś liczbę całkowitą niepodzielną przez p.

Będziemy nazywać liczbami *odpowiednimi* każde dwie liczby m i n z ciągu

$$1,\ 2,\ \ldots,\ p-1, \tag{1}$$

dla których zachodzi kongruencja

$$mn\equiv D\pmod p. \tag{2}$$

Z definicji tej wynika bezpośrednio, że jeżeli n jest liczbą odpowiednią dla m, to i na odwrót, m jest liczbą odpowiednią dla n.

Udowodnimy, że każda z liczb ciągu (1) ma jedną i przy tym tylko jedną liczbę odpowiednią.

Istotnie, niech m będzie liczbą z ciągu (1). Na to, żeby liczba x z ciągu (1) była odpowiednią dla m, potrzeba i wystarcza, by zachodziła kongruencja

$$mx\equiv D\pmod p. \tag{3}$$

Jest to kongruencja 1-go stopnia o module pierwszym i spółczynnik m przy niewiadomej jest niepodzielny przez moduł, gdyż — jak zakładamy — m jest jednym z wyrazów ciągu (1). Kongruencja (3) ma zatem jeden i tylko jeden pierwiastek. W ciągu wszystkich reszt według modułu p, tj. w ciągu

$$0,\ 1,\ 2,\ \ldots,\ p-1, \tag{4}$$

jest więc jedna i tylko jedna liczba, spełniająca kongruencję (3). Liczbą tą nie może być 0, gdyż prawa strona kongruencji (3),