Kongruencje

Sławomir Cynk

Instytut Matematyki Uniwersytetu Jagiellońskiego

24 września 2008

Nowy Sącz

Przykłady

W. Sierpiński, *250 zadań z elementarnej teorii liczb*, Biblioteczka Matematyczna 17.

Zadanie 3. Pokazać, że jeżeli $7 \mid a^2 + b^2$ to $7 \mid a$ i $7 \mid b$.

Przykłady

W. Sierpiński, *250 zadań z elementarnej teorii liczb*, Biblioteczka Matematyczna 17.

Zadanie 3. Pokazać, że jeżeli $7 \mid a^2 + b^2$ to $7 \mid a$ i $7 \mid b$.

Rozwiązanie (z książki:) Kwadrat liczby niepodzielnej przez 7 daje resztę z dzielenia przez 7 równą 1, 2, 4. Suma takich dwóch kwadratów daje więc 2, 3, 4, 5, 6 czyli liczbę niepodzielną przez 7.

Przykłady

W. Sierpiński, *250 zadań z elementarnej teorii liczb*, Biblioteczka Matematyczna 17.

Zadanie 3. Pokazać, że jeżeli $7 \mid a^2 + b^2$ to $7 \mid a$ i $7 \mid b$.

Rozwiązanie (z książki:) Kwadrat liczby niepodzielnej przez 7 daje resztę z dzielenia przez 7 równą 1, 2, 4. Suma takich dwóch kwadratów daje więc 2, 3, 4, 5, 6 czyli liczbę niepodzielną przez 7.

	0	1	2	3	4	5	6
0	0	1	4	2	2	4	1
1	1	2	5	3	3	5	2
2	4	5	1	6	6	1	5
3	2	3	6	4	4	6	3
4	2	3	6	4	4	6	3
5	4	5	1	6	6	1	5
6	1	2	5	3	3	5	2

Działania na resztach

Reszta dodawania, odejmowania lub mnożenia w dzieleniu przez daną liczbę n zależy wyłącznie od reszt z dzielenia przez n składników, odjemnej i djemnika lub czynników.

Działania na resztach

Reszta dodawania, odejmowania lub mnożenia w dzieleniu przez daną liczbę n zależy wyłącznie od reszt z dzielenia przez n składników, odjemnej i djemnika lub czynników. Można mówić o działaniach na resztach z dzielenia przez liczbę n. Np. dla $n = 5$

0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

0	0	1	2	3	4
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Kongruencje

Mówimy, że a przystaje do b modulo n, zapisujemy

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

jeśli a i b dają tę samą resztę z dzielenia przez n.

Kongruencje

Mówimy, że a przystaje do b modulo n, zapisujemy

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

jeśli a i b dają tę samą resztę z dzielenia przez n.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

Kongruencje

Mówimy, że a przystaje do b modulo n, zapisujemy

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

jeśli a i b dają tę samą resztę z dzielenia przez n.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

Relacja przystawania ma następujące własności
Zwrotność: $a \equiv a \pmod{n}$,

Kongruencje

Mówimy, że a przystaje do b modulo n, zapisujemy

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

jeśli a i b dają tę samą resztę z dzielenia przez n.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

Relacja przystawania ma następujące własności
Zwrotność: $a \equiv a \pmod{n}$,
Symetryczność: $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$,

Kongruencje

Mówimy, że a przystaje do b modulo n, zapisujemy

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

jeśli a i b dają tę samą resztę z dzielenia przez n.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

Relacja przystawania ma następujące własności
Zwrotność: $a \equiv a \pmod{n}$,
Symetryczność: $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$,
Przechodniość: $a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

Kongruencje

Mówimy, że a przystaje do b modulo n, zapisujemy

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

jeśli a i b dają tę samą resztę z dzielenia przez n.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

Relacja przystawania ma następujące własności
Zwrotność: $a \equiv a \pmod{n}$,
Symetryczność: $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$,
Przechodniość: $a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$
Jest to relacja równoważności.

Działania na kongruencjach

Dodawanie: kongruencje można dodawać stronami:
Jeżeli

$$a \equiv b \pmod{n}$$
$$c \equiv d \pmod{n}$$

to

$$a + c \equiv b + d \pmod{n}.$$

Mnożenie: kongruencje można mnożyć stronami:
Jeżeli

$$a \equiv b \pmod{n}$$
$$c \equiv d \pmod{n}$$

to

$$ac \equiv bd \pmod{n}.$$

Przykład

Twierdzenie M. Kraitchika: $13 \mid 2^{70} + 3^{70}$

Przykład

Twierdzenie M. Kraitchika: $13 \mid 2^{70} + 3^{70}$

Komputer:

$$2^{70} + 3^{70} = 2503155504994422192936289397389273 =$$

$$13 \times 192550423461109399456637645953021$$

Przykład

Twierdzenie M. Kraitchika: $13 \mid 2^{70} + 3^{70}$
Komputer:

$$2^{70} + 3^{70} = 2503155504994422192936289397389273 =$$

$$13 \times 192550423461109399456637645953021$$

Inaczej: $2^6 \equiv -1 \pmod{13}$ gdyż
$2^6 - (-1) = 64 + 1 = 65 = 5 \times 13.$

Przykład

Twierdzenie M. Kraitchika: $13 \mid 2^{70} + 3^{70}$
Komputer:

$$2^{70} + 3^{70} = 2503155504994422192936289397389273 =$$

$$13 \times 192550423461109399456637645953021$$

Inaczej: $2^6 \equiv -1 \pmod{13}$ gdyż
$2^6 - (-1) = 64 + 1 = 65 = 5 \times 13$.Mnożąc tę kongruencje przez siebie 11 razy otrzymujemy $2^{66} \equiv (-1)^{11} \pmod{13}$. Ponieważ $2^4 = 16 \equiv 3 \pmod{13}$, więc mnożąć te kongruencje przez siebie stronami otrzymujemy $2^{70} \equiv -3 \pmod{13}$.

Przykład

Twierdzenie M. Kraitchika: $13 \mid 2^{70} + 3^{70}$
Komputer:

$$2^{70} + 3^{70} = 2503155504994422192936289397389273 =$$

$$13 \times 192550423461109399456637645953021$$

Inaczej: $2^6 \equiv -1 \pmod{13}$ gdyż
$2^6 - (-1) = 64 + 1 = 65 = 5 \times 13$.Mnożąc tę kongruencje przez siebie 11 razy otrzymujemy $2^{66} \equiv (-1)^{11} \pmod{13}$. Ponieważ $2^4 = 16 \equiv 3 \pmod{13}$, więc mnożąć te kongruencje przez siebie stronami otrzymujemy $2^{70} \equiv -3 \pmod{13}$.
Podobnie $3^3 = 27 \equiv 1 \pmod{13}$, więć $3^{69} \equiv 1 \pmod{13}$, a stąd $3^{70} \equiv 3 \pmod{13}$.

Przykład

Twierdzenie M. Kraitchika: $13 \mid 2^{70} + 3^{70}$
Komputer:

$$2^{70} + 3^{70} = 2503155504994422192936289397389273 =$$

$$13 \times 192550423461109399456637645953021$$

Inaczej: $2^6 \equiv -1 \pmod{13}$ gdyż
$2^6 - (-1) = 64 + 1 = 65 = 5 \times 13$.Mnożąc tę kongruencje przez siebie 11 razy otrzymujemy $2^{66} \equiv (-1)^{11} \pmod{13}$. Ponieważ $2^4 = 16 \equiv 3 \pmod{13}$, więc mnożąć te kongruencje przez siebie stronami otrzymujemy $2^{70} \equiv -3 \pmod{13}$.
Podobnie $3^3 = 27 \equiv 1 \pmod{13}$, więć $3^{69} \equiv 1 \pmod{13}$, a stąd $3^{70} \equiv 3 \pmod{13}$.
Dodając stronami dwie osttnie kongruencje otrzymujemy

$$2^{70} + 3^{70} \equiv 0 \pmod{13}$$

czyli

$$13 \mid 2^{70} + 3^{70}.$$

Dzielenie Kongruencji

Zauważmy, że $3 \times 3 \equiv 3 \times 5 \pmod 6$, ale $3 \not\equiv 5 \pmod 6$. Oznacza to, że w zbiorze reszt modulo 6 nie ma sensu dzielenie przez 3 (jest niejednoznaczne). Poza tym, iloczyn liczby dającej resztę 3 z dzielenia przez 6 przez dowolną resztę daje resztę 0 lub 3.

Dzielenie Kongruencji

Zauważmy, że $3 \times 3 \equiv 3 \times 5 \pmod 6$, ale $3 \not\equiv 5 \pmod 6$. Oznacza to, że w zbiorze reszt modulo 6 nie ma sensu dzielenie przez 3 (jest niejednoznaczne). Poza tym, iloczyn liczby dającej resztę 3 z dzielenia przez 6 przez dowolną resztę daje resztę 0 lub 3. Dzieje się tak dlatego, że $6 \mid (5-3)3 = 6$. Można jednoznacznie dzielić wyłącznie przez reszty, które są względnie pierwsze z modułem 6, czyli przez 1 i 5 (przez 2, 3, 4 nie zawsze się da, a jeśli sie da to wynik będzie niejednoznaczny).

Dzielenie Kongruencji

Zauważmy, że $3 \times 3 \equiv 3 \times 5 \pmod 6$, ale $3 \not\equiv 5 \pmod 6$. Oznacza to, że w zbiorze reszt modulo 6 nie ma sensu dzielenie przez 3 (jest niejednoznaczne). Poza tym, iloczyn liczby dającej resztę 3 z dzielenia przez 6 przez dowolną resztę daje resztę 0 lub 3. Dzieje się tak dlatego, że $6 \mid (5-3)3 = 6$. Można jednoznacznie dzielić wyłącznie przez reszty, które są względnie pierwsze z modułem 6, czyli przez 1 i 5 (przez 2, 3, 4 nie zawsze się da, a jeśli sie da to wynik będzie niejednoznaczny).
Zbiór reszt z dzielenia przez n oznacza się $\mathbb{Z}_n$. W ziorze $\mathbb{Z}_n$ wykonalne są działania dodawania i mnożenia, a jeśli n jest liczbą pierwszą, to również dzielenia przez elementy różne od zera.

ustawianie żołnierzyków

Chłopiec bawi się swoimi żołnierzykami, jeśli ustawia ich czwórkami, to zostaje mu trzech, a jeśli trójkami – to dwóch. Ilu żołnierzyków zostanie, gdy ustawi ich szóstkami?

ustawianie żołnierzyków

Chłopiec bawi się swoimi żołnierzykami, jeśli ustawia ich czwórkami, to zostaje mu trzech, a jeśli trójkami – to dwóch. Ilu żołnierzyków zostanie, gdy ustawi ich szóstkami?

n	czwórkami	trójkami	szóstkami
1	1	1	1
2	2	2	2
3	3	0	3
4	0	1	4
5	1	2	5
6	2	0	0
7	3	1	1
8	0	2	2
9	1	0	3
10	2	1	4
11	3	2	5
12	0	0	0

ustawianie żołnierzyków

Chłopiec bawi się swoimi żołnierzykami, jeśli ustawia ich czwórkami, to zostaje mu trzech, a jeśli trójkami – to dwóch. Ilu żołnierzyków zostanie, gdy ustawi ich szóstkami?

n	czwórkami	trójkami	szóstkami
1	1	1	1
2	2	2	2
3	3	0	3
4	0	1	4
5	1	2	5
6	2	0	0
7	3	1	1
8	0	2	2
9	1	0	3
10	2	1	4
11	3	2	**5**
12	0	0	0

Twierdzenie chińskie o resztach

Twierdzenie

Niech $n_1, \ldots, n_r$ *będą liczbami parami względnie pierwszymi.* $k_1, \ldots, k_r$ *dowolnymi liczbami naturalnymi. Układ kongruencji*

$$\begin{cases} N \equiv k_1 \pmod{n_1} \\ N \equiv k_2 \pmod{n_2} \\ \ldots \\ N \equiv k_r \pmod{n_r} \end{cases}$$

ma rozwiązanie N*. Dowolna liczba naturalna* M *jest również rozwiązaniem tego układu konkurencji wtedy i tylko wtedy gdy* $M \equiv N \pmod{\mathrm{NWW}(n_1, \ldots, n_r)}$

Niech $m = n_1 \dots n_r$, $m_i = \frac{m}{n_i}$. Ponieważ n_1, m_1 są względnie pierwsze więc istnieją u_i, v_i takie, że $n_i | u_i$, $m_i | v_i$ oraz $u_i + v_i = 1$. Rozwiązaniem układu kongruencji jest

$$N = n_1 v_1 + \dots + n_r v_r$$

Przykład: Wyznaczyć wszystkie rozwiązania układu kongruencji $n \equiv 2 \mod 4$, $n \equiv 1 \mod 3$, $n \equiv 3 \mod 7$.
W naszym przypadku $n_1 = 4, n_2 = 3, n_3 = 7$,
$m = 3 \cdot 3 \cdot 7 = 84$,$m_1 = 21$, $m_2 = 28$ oraz $m_3 = 12$.
Ponieważ $-5 \cdot 4 + 21 = 1, -9 \cdot 2 + 28 = 1, -5 \cdot 7 + 3 \cdot 21 = 1$,
więc możemy przyjąć $v_1 = 21, v_2 = 28, v_3 = 36$.
Rozwiązaniem układu kongruencji jest liczba
$2 \cdot 21 + 28 + 3 \cdot 36 = 178 = 10 + 2 \cdot 84$. Czyli N spełnia rozważany układ kongruencji wtedy i tylko wtedy gdy $N \equiv 10 \mod 84$.