Chińskie Twierdzenie o Resztach

Antoni Łuczak

26 lipca 2024

Twierdzenie 1 (CRT)**.** Dane są liczby całkowite $a_1, \ldots, a_n$ oraz parami względnie pierwsze liczby naturalne $m_1, \ldots m_n$. Wtedy istnieje dokładnie jedna liczba naturalna x spełniająca układ kongruencji

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

oraz nierówność $x < m_1 m_2 \ldots m_n$.

Jeżeli ustalimy $M = m_1 m_2 \ldots m_n$, to łatwo zauważyć, że wszystkie liczby postaci $x + kM$ dla k całkowitego również są rozwiązaniami powyższego układu. W szczególności jesteśmy w stanie konstruować dowolnie duże rozwiązania takiego układu.

Zadanie 1. Udowodnij, że dla dowolnej liczby naturalnej n istnieją takie liczby całkowite a, b, że liczba

$$4a^2 + 9b^2 - 1$$

jest podzielna przez n.

Zadanie 2. Udowodnij, że istnieją 2024 kolejne liczby naturalne, z których każda jest podzielna przez kwadrat pewnej liczby całkowitej większej niż 1.

Zadanie 3. Niech a, b, c będą parami różnymi liczbami naturalnymi. Udowodnij, że istnieje taka liczba naturalna n, że liczby $a + n,\ b + n,\ c + n$ są parami względnie pierwsze.

Zadanie 4. Udowodnij, że istnieje 2137 kolejnych liczb naturalnych, z których żadna nie jest potęgą liczby całkowitej o wykładniku większym niż 1.

Zadanie 5. Wyznacz liczbę liczb x ze zbioru $\{1, \ldots, 2024\}$, dla których $x^2 \equiv x \pmod{2024}$.

Zadanie 6. Udowodnij, że dla dowolnej liczby naturalnej n istnieje taka liczba całkowita a, że liczby

$$a,\ 2a,\ 3a\ \ldots\ na$$

są potęgami liczb całkowitych o wykładnikach większych niż 1.

Zadanie 7. Udowodnij, że dla dowolnych liczb naturalnych $a_1, \ldots a_{2024}$ istnieje taka liczba naturalna b, że liczby $ba_1, \ldots ba_{2024}$ są potęgami liczb całkowitych o wykładnikach większych niż 1.

Rozwiązania

1. Niech $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Jeżeli uda nam się znaleźć takie liczby całkowite $a_1, \dots, a_k$ oraz $b_1, \dots b_k$, że liczba

$$4a_i^2 + 9b_i^2 - 1$$

jest podzielna przez $p_i^{\alpha_i}$ dla $i = 1, \dots, k$, to na mocy CRT istnieją takie liczby całkowite a, b, że

$$\begin{cases} a \equiv a_1 \pmod{p_1^{\alpha_1}} \\ \vdots \\ a \equiv a_k \pmod{p_k^{\alpha_k}} \end{cases} \qquad \begin{cases} b \equiv b_1 \pmod{p_1^{\alpha_1}} \\ \vdots \\ b \equiv b_k \pmod{p_k^{\alpha_k}} \end{cases}$$

Wtedy dla dowolnego indeksu i mamy

$$4a^2 + 9b^2 - 1 \equiv 4a_i^2 + 9b_i^2 - 1 \equiv 0 \pmod{p_i^{\alpha_i}},$$

zatem liczba $4a^2 + 9b^2 - 1$ będzie podzielna przez n. Weźmy dowolny indeks i. jeżeli $p_i = 2$, to ustalmy

$$a_i = 0,\ b_i \equiv 3^{-1} \pmod{p_i^{\alpha_i}},$$

gdzie 3^{-1} to odwrotność 3 modulo $p_i^{\alpha_i}$. Wtedy

$$4a_i^2 + 9b_i^2 - 1 \equiv 9 \cdot 3^{-2} - 1 \equiv 1 - 1 \equiv 0 \pmod{p_i^{\alpha_1}}.$$

Jeżeli $p_i > 2$, to ustalmy

$$a_i \equiv 2^{-1} \pmod{p_i^{\alpha_i}},\ b_i = 0.$$

Wtedy

$$4a_i^2 + 9b_i^2 - 1 \equiv 4 \cdot 2^{-2} - 1 \equiv 1 - 1 \equiv 0 \pmod{p_i^{\alpha_i}}.$$

2. Rozważmy układ kongruencji

$$\begin{cases} x \equiv 0 \pmod{a_1^2} \\ x \equiv -1 \pmod{a_2^2} \\ \vdots \\ x \equiv -2023 \pmod{a_{2024}^2} \end{cases}$$

gdzie $a_1, \dots, a_{2024}$ są parami różnymi liczbami. Na podstawie CRT ma on rozwiązanie naturalne. Wtedy liczby

$$x,\ x+1, \dots, x+2023$$

są podzielne odpowiednio przez $a_1^2, \dots, a_{2024}^2$.

3. Zauważmy, że

$$\mathrm{NWD}(a+n, b+n) \mid a-b,\ \mathrm{NWD}(b+n, c+n) \mid b-c,\ \mathrm{NWD}(c+n, a+n) \mid c-a.$$

Wystarczy zatem dobrać tak n, żeby liczby $a+n$, $b+n$, $c+n$ były względnie pierwsze odpowiednio z $a-b$, $b-c$ oraz $c-a$. Jednak ostatnie 3 liczby posiadają skończenie wiele dzielników pierwszych, więc na mocy CRT damy radę dobrać takie n (szczegóły pozostawiam czytelnikowi).

4. Rozważmy układ kongruencji

$$\begin{cases} x \equiv p_1 \pmod{p_1^2} \\ x \equiv p_2 - 1 \pmod{p_2^2} \\ \vdots \\ x \equiv p_{2137} - 2136 \pmod{p_{2137}^2} \end{cases}$$

gdzie $p_1, \ldots, p_{2137}$ są parami różnymi liczbami pierwszymi. Na podstawie CRT ma on rozwiązanie naturalne. Wtedy liczby

$$x,\ x+1, \ldots, x+2136$$

są podzielne odpowiednio przez $p_1, \ldots, p_{2137}$, ale nie przez $p_1^2, \ldots, p_{2137}^2$, zatem nie mogą być potęgami o wykładnikach większych od 1.

5. Rozważmy kongruencję

$$x^2 \equiv x \pmod{p^\alpha} \iff p^\alpha \mid x(x-1).$$

Skoro x oraz $x-1$ są względnie pierwsze, to

$$p^\alpha \mid x \text{ albo } p^\alpha \mid x-1.$$

Łatwo sprawdzić, że $2024 = 2^3 \cdot 11 \cdot 23$. Dla każdej z liczb 8, 11, 23 możemy wybrać na 2 sposoby, czy liczba x daje resztę 0 czy 1 z dzielenia przez tą liczbę. W takim razie możemy wybrać reszty z dzielenia x przez 8, 11, 23 na 8 sposobów, co na mocy CRT odpowiada 8 rozwiązaniom ze zbioru $\{1, \ldots, 2024\}$.

6. Niech $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, gdzie $p_1, \ldots, p_n$ to pierwsze n liczb pierwszych. Chcemy, żeby

$$a_1 \mid \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n,$$

$$a_2 \mid \alpha_1 + 1,\ \alpha_2,\ \ldots,\ \alpha_n,$$

$$a_3 \mid \alpha_1,\ \alpha_2 + 1\ \ldots,\ \alpha_n,$$

$$a_4 \mid \alpha_1 + 2,\ \alpha_2\ \ldots,\ \alpha_n,$$

i tak dalej, gdzie $a_1, \ldots, a_{n+1}$ są pewnymi liczbami całkowitymi większymi od 1. Jest to jednak układ $n(n+1)$ kongruencji, więc jeśli wybierzemy parami względnie pierwsze $a_1, \ldots, a_{n+1}$, to na mocy CRT będzie on miał rozwiązanie.

7. Postępujemy podobnie jak w poprzednim zadaniu. Niech

$$b = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

oraz

$$a_i = p_1^{\alpha_{i,1}} \cdots p_k^{\alpha_{i,k}}.$$

Wybierzmy parami względnie pierwsze liczby $x_1, \ldots, x_k$. Chcemy dobrać tak $\beta_1, \ldots, \beta_k$, aby

$$x_i \mid \alpha_{i,j} + \beta_j$$

dla $i = 1, \ldots, 2024$ oraz $j = 1, \ldots, k$. Jest to układ $2024k$ kongruencji, który na mocy CRT ma rozwiązanie.