Chińskie Twierdzenie o Resztach

1. Dowódca kazał ustawić się oddziałowi piątkami oraz siódemkami. Bez piątki pozostał 1 żołnierz, bez siódemki – dwóch. Ilu żołnierzy może mieć oddział, wiedząc że jest ich więcej niż 70 oraz mniej niż 100?

2. Rozwiąż układy kongruencji:

   (a) $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 4 \pmod 6 \end{cases}$

   (b) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \end{cases}$

   (c) $\begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$.

3. Poproś kogoś, żeby wybrał liczbę naturalną mniejszą od 60 i wykonał następujące czynności:

   (a) podzielił ją przez 3 i podał resztę. Niech tą resztą będzie a,

   (b) podzielił ją przez 4 i podał resztę. Niech tą resztą będzie b,

   (c) podzielił ją przez 5 i podał resztę. Niech tą resztą będzie c.

   Wybrana liczba jest resztą otrzymaną z dzielenia liczby $40a + 45b + 36c$ przez 60. Wytłumacz.

4. Niech p, q będą różnymi liczbami pierwszymi.

   (a) Ile rozwiązań ma kongruencja $x^2 \equiv 1 \pmod p$?

   (b) Ile rozwiązań ma kongruencja $x^2 \equiv 1 \pmod{pq}$?

   (c) Znajdź wszystkie rozwiązania kongruencji $x^2 \equiv 1 \pmod{15}$.

5. Znajdź najmniejszą liczbę dodatnią, która daje resztę 1 przy dzieleniu przez 11, resztę 2 przy dzieleniu przez 12 i resztę 3 przy dzieleniu przez 13.

6. Znajdź liczbę trzycyfrową (w systemie dziesiętnym), która daję resztę 4 przy dzieleniu przez 7, 9 i 11.

7. Oblicz, ile jest liczb naturalnych mniejszych od 2000, które przy dzieleniu przez 11 dają resztę 1, a przy dzieleniu przez 4 dają resztę 3.

8. Wykaż, że układ kongruencji

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

   ma rozwiązanie x wtedy i tylko wtedy, gdy $a \equiv b \pmod{NWD(m,n)}$.

9. * Czy istnieją parami różne liczby pierwsze p, q, r takie, że $p|rq - 1$, $q|pr - 1$, $r|pq - 1$?

   (*Wsk. rozwiąż układ kongruencji*

$$\begin{cases} x \equiv pq \pmod r \\ x \equiv qr \pmod p \\ x \equiv rp \pmod q. \end{cases}$$

   Zauważ, że 1 *spełnia ten układ i wykaż na tej podstawie, że* $A := \frac{1}{p} + \frac{1}{p} + \frac{1}{p} - \frac{1}{pqr} \in \mathbb{Z}$. *Jak duże może być* A*?*)