KONGRUENCJE
Pasjonaci matematyki
dr Jędrzej Garnek
mail: jgarnek amu.edu.pl
strona: jgarnek.faculty.wmi.amu.edu.pl (Dydaktyka ⇒ Pasjonaci Matematyki)

Podstawowe zadania z kongruencji

1. Wykaż, że:
   a) $5|3^{53}+7^{32}+6^{13}$,
   b) $7|2^{1988}-4$,
   c) $13|3^{1974}+5^{1974}$,
   d) $7|2^{n+2}+3^{2n+1}$ dla każdego $n \in \mathbb{N}$,
   e) $21|2^{4^n}+5$,
   f) $2011^{2^n} \equiv 1 \pmod{2^{n+1}}$ dla każdego $n \in \mathbb{N}$.

2. Załóżmy, że liczby $a_1, a_2, ..., a_{2011} \in \mathbb{Z}$ są nieparzyste. Znajdź resztę, jaką daje suma ich kwadratów przy dzieleniu przez 4.

3. Udowodnij, że 0 jest ostatnią cyfrą liczby $53^{53}-33^{33}$.

4. Wyznacz 2 ostatnie cyfry liczby $99^{99}-49^{49}$.

5. Udowodnij, że jeżeli ostatnią cyfrą liczby n jest 5, to dwie ostatnie cyfry liczby n^2 to 25.

6. Cechy podzielności:
   a) Każda liczba naturalna daje przy dzieleniu przez 3 oraz 9 taka sama resztę, jak jej suma cyfr.
   b) Każda liczba naturalna daje przy dzieleniu przez 11 taka sama resztę, jak suma jej cyfr na pozycjach nieparzystych (licząc od rzędu jedności) minus suma cyfr na pozycjach parzystych.
   c) Każda liczba naturalna daje przy dzieleniu przez 7 taka sama resztę jak liczba, powstała przez skreślenie jej ostatnie trzech cyfr, a następnie przez odjęcie od liczby skreślonej tak powstałej liczby.
   d) Każda liczba naturalna daje przy dzieleniu przez 2^n taka sama resztę jak liczba złożona z n jej ostatnich cyfr.

7. Udowodnij, że jeżeli $x \in \mathbb{Z}$, zaś p jest liczbą pierwszą, taką że
$$x^3 \equiv 2x^2+3x \pmod{p}$$
to co najmniej jedna z liczb $x, x-3, x+1$ dzieli się przez p.

8. Udowodnij, że dla $p \neq 2,3$ zachodzi: $2^{p-2}+3^{p-2}+6^{p-2} \equiv 1 \pmod{p}$.

9. Wykaż, że dla dowolnej liczby pierwszej p: $p|\underbrace{11\ldots1}_{p-1}$.

10. Wykaż, że dla dowolnej liczby pierwszej p oraz $a, b \in \mathbb{Z}$: $p|a^pb-b^pa$.

11. ZADANIE KRYPTOGRAFICZNE.

    Wyślij koledze/koleżance tajną wiadomość w następujący sposób:

    - przeczytaj jego/jej liczby N oraz e,
    - wybierz wiadomość m będącą liczbą mniejszą od N oraz oblicz $c := m^e \pmod{N}$.
      (skorzystaj np. ze strony *wolframalpha.com*)

    Odbiorca odszyfruje wiadomość za pomocą tajnej liczby d, obliczając $c^d \pmod{N}$.
    Możliwe pary (N, e):
    $(874219, 539421)$, $(925003, 300249)$, $(819517, 95969)$, $(616747, 223813)$, $(694151, 94507)$, $(594463, 238933)$.

Zaawansowane zadania z kongruencji

1. Wykaż, że dla dowolnego $n > 1$: $n^n - n^2 + n - 1 \equiv 0 \pmod{(n-1)^2}$.
2. Wykaż, że liczba p jest pierwsza wtw. gdy $(p-1)! \equiv -1 \pmod{p}$.
3. Niech $p > 2$ będzie liczbą pierwszą, która nie jest dzielnikiem żadnej z liczb całkowitych a, b. Liczby $a^2 + b^2$ i $a^3 + b^3$ dają resztę 1 z dzielenia przez p. Dowieść, że liczba $a + b + 2$ dzieli się przez p.
4. Niech a będzie liczbą nieparzystą. Wykaż, że $NWD(a^{2^m} + 2^{2^m}, a^{2^n} + 2^{2^n}) = 1$ dla $m \neq n$.
5. Ile rozwiązań ma kongruencja $x^{67} \equiv 2 \pmod{101}$?

   Wskazówka: skorzystaj z następującego faktu: jeżeli r jest najmniejszą liczbą naturalną taką, że $a^r \equiv 1 \pmod{p}$ oraz $a^n \equiv 1 \pmod{p}$ dla pewnego n, to $r|n$. Jakie własności ma funkcja $f : \mathbb{Z}/101 \to \mathbb{Z}/101$, $f(x) = x^{67}$?
6. Wykaż, że $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ dla dowolnej liczby pierwszej $p > 2$.
7. Wykaż, że mamy następujące równości wielomianów w $\mathbb{F}_p[x, y]$:

$$\sum_{i \in \mathbb{F}_p} (x+i)^{p-1} = 1, \qquad \sum_{i,j \in \mathbb{F}_p} (x + i + j \cdot y)^{p^2-1} = (y^p - y)^{p-1}.$$

Reszty kwadratowe

1. Oblicz, korzystając z prawa wzajemności:
   (a) $\left(\frac{85}{101}\right)$, (c) $\left(\frac{29}{541}\right)$. (e) $\left(\frac{261}{2017}\right)$,
   (b) $\left(\frac{101}{1987}\right)$, (d) $\left(\frac{10}{1009}\right)$, (f) $\left(\frac{-77}{9907}\right)$.
2. Ustal, które z poniższych kongruencji mają rozwiązanie $x \in \mathbb{Z}/p$:
   (a) $x^2 \equiv 5 \pmod{227}$, (c) $x^2 \equiv -5 \pmod{227}$, (e) $x^2 \equiv 150 \pmod{1009}$.
   (b) $x^2 \equiv 5 \pmod{229}$, (d) $x^2 \equiv 7 \pmod{1009}$,
3. Wykaż, że dla $p \in \mathbb{P}$, $p \neq 2$, $a, b, c \in \mathbb{Z}$, $p \nmid a$ kongruencja $ax^2 + bx + c \equiv 0 \pmod{p}$ ma $1 + \left(\frac{b^2-4ac}{p}\right)$ rozwiązań.
4. Wykaż, że jeżeli p jest liczbą pierwszą oraz $p = x^2 + 2y^2$, to $p \equiv 5 \pmod{8}$ lub $p \equiv 7 \pmod{8}$.
5. Udowodnij, że $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Jeżeli $4|p-1$, to ile wynosi "pierwiastek" z -1 modulo p?

   (Wskazówka: $(p-1)! \equiv -1 \pmod{p}$)
6. Wykaż, że jeżeli $p = 4k + 3$ jest liczbą pierwszą, zaś a jest resztą kwadratową modulo p, to "pierwiastkiem" modulo p z a jest a^{k+1}.
7. Jakie dzielniki pierwsze posiadają liczby z ciągu:
   (a) $n^2 + 20$, (b) $n^2 - 5$, (c) $n^2 + 2n - 11$?

   Uwaga: jeżeli $NWD(a, n) = 1$, to istnieje nieskończenie wiele liczb pierwszych $p \equiv a \pmod{n}$.
8. Wykaż, że jeżeli $p \in \mathbb{P}$, $p \nmid a$, $n \in \mathbb{N}$, to kongruencja $x^2 \equiv a \pmod{p^n}$ ma rozwiązanie wtedy i tylko wtedy, gdy $\left(\frac{a}{p}\right) = 1$. Udowodnij, że w tym przypadku istnieją dokładnie dwa rozwiązania $0 < x < p^n$.

   (*Wskazówka: załóżmy, że $x_n^2 \equiv a \pmod{p^n}$. Spróbuj znaleźć y takie, że $x_{n+1} := x_n + y \cdot p^n$ spełnia $x_{n+1}^2 \equiv a \pmod{p^{n+1}}$*).
9. Niech $p \in \mathbb{P}$, $p \neq 2$.
   (a) Znajdź $\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \ldots + \left(\frac{p-1}{p}\right)$.

(b) Niech $a, b \in \mathbb{Z}$, $p \nmid a$. Znajdź $\left(\frac{a+b}{p}\right) + \left(\frac{2a+b}{p}\right) + \ldots + \left(\frac{(p-1)\cdot a+b}{p}\right)$.

10. Znajdź wszystkie liczby pierwsze p dla których kongruencja $x^2 + y^2 \equiv 0 \pmod{p}$ ma rozwiązanie $x, y \in \mathbb{Z}$, $p \nmid x, y$.

11. Wykaż, że jeżeli p jest liczbą pierwszą oraz $p | n^4 - n^2 + 1$, to $p \equiv 1 \pmod{12}$.

12. Niech $p \in \mathbb{P}$, $p \neq 2$. Funkcja $f : \mathbb{Z}/p \setminus \{0\} \to \{-1, 1\}$ spełnia $f(a \cdot b) = f(a) \cdot f(b)$. Wykaż, że f jest funkcją stałą, albo $f(a) = \left(\frac{a}{p}\right)$ dla każdego $a \in \mathbb{Z} \setminus p\mathbb{Z}$.

13. Wykaż, że jeśli a jest liczbą całkowitą różną od zera, p, q liczbami pierwszymi nieparzystymi niedzielącymi a oraz $p \equiv q \pmod{4|a|}$, to $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

14. (a) Udowodnij, że jeżeli $p \in \mathbb{P}$, $p \neq 2$ to:

$$\sum_{j=1}^{p-2} \left(\frac{j \cdot (j+1)}{p}\right) = -1.$$

Wskazówka: zapisz $j \cdot (j+1) = j^2 \cdot (1 + 1/j)$.

(b) Udowodnij, że jeżeli $p \in \mathbb{P}$, $p \geqslant 7$, to istnieją a oraz b takie, że a oraz $a+1$ są resztami kwadratowymi, zaś b oraz $b+1$ są nieresztami kwadratowymi.

15. Ile rozwiązań ma kongruencja $x^2 \equiv 1 \pmod{pq}$ dla liczb pierwszych $p \neq q$?

Wskazówka: skorzystaj z Chińskiego Twierdzenia o Resztach.

16. Niech $p \in \mathbb{P} \setminus \{2\}$; udowodnij, że:

(a) $p \mid x^2 - 2 \Rightarrow p \equiv 1 \pmod{8}$ lub $p \equiv 7 \pmod{8}$,
(b) $p \mid x^2 + 2 \Rightarrow p \equiv 1 \pmod{8}$ lub $p \equiv 3 \pmod{8}$,
(c) $p \mid x^4 + 1 \Rightarrow p \equiv 1 \pmod{8}$.

Korzystając z wykazanych faktów, wykaż, że istnieje nieskończenie wiele liczb pierwszych postaci $8n + 1$, $8n + 3$, $8n + 5$, $8n + 7$.

(*Wskazówka: jeżeli $p_1, \ldots, p_n$ byłyby wszystkimi takimi liczbami, to przyjmij $x := p_1 \cdot \ldots \cdot p_n$ i skorzystaj z powyższych faktów*)

17. Wykaż, że jeżeli $p = 2^{2^n} + 1$ jest liczbą pierwszą, to 3 jest generatorem modulo p.

Wskazówka: skorzystaj z następującego faktu: jeżeli r jest najmniejszą liczbą naturalną taką, że $a^r \equiv 1 \pmod{p}$ oraz $a^n \equiv 1 \pmod{p}$ dla pewnego n, to $r|n$.

18. Wykaż, że jeżeli a jest resztą kwadratową dla wszystkich $p \in \mathbb{P}$, to a jest kwadratem liczby naturalnej.

Wskazówka: jeżeli $NWD(a, n) = 1$, to istnieje nieskończenie wiele liczb pierwszych $p \equiv a \pmod{n}$.