

Matematyka dyskretna

Jan Rodziewicz-Bielewicz, Wydział Informatyki ZUT

May 8, 2023

7 Teoria liczb

ZASTOSOWANIE: Kryptografia.

1. Znaleźć $NWD(a, b)$ wykorzystując algorytm Euklidesa:
 - (a) $a = 27, b = 42$
 - (b) $a = 89, b = 55$
 - (c) $a = 220, b = 28$
 - (d) $a = 546, b = 231$
 - (e) $a = 1001, b = 6235$
 - (f) $a = 10k + 9, b = k + 1, k \in \mathbb{N}$
 - (g) $a = 3k + 1, b = 10k + 3, k \in \mathbb{N}$
2. Wyznaczyć NWD dla podanych liczb a i b , a następnie znaleźć takie x i y , że $ax + by = NWD(a, b)$:
 - (a) $a = 26, b = 19$
 - (b) $a = 187, b = 34$
 - (c) $a = 111, b = 21$
 - (d) $a = 115, b = 25$
 - (e) $a = 841, b = 160$
 - (f) $a = 2613, b = 2127$
3. Rozwiązać w liczbach naturalnych układ równań:

$$\begin{cases} x + y = 96 \\ NWD(x, y) = 12 \end{cases}$$

4. Załóżmy, że ułamek $\frac{a}{b}$ jest nieskracalny. Czy ułamek $\frac{a}{a+b}$ jest nieskracalny?
5. Wiadomo, że $14|784$. Pokazać, że $14|770$ oraz $14|812$.
6. Wiadomo, że $14|784$. Czy $7|784$? Czy $7|817$?
7. Załóżmy, że dla pewnych całkowitych m, a, b zachodzi $m|ab$. Czy m musi wtedy dzielić a lub b ?
8. Udowodnić własności podzielności:
 - (a) Jeżeli $m|a$, to $m|(-a)$
 - (b) Jeżeli $m|a$ i $b \in \mathbb{Z}$, to $m|ab$
 - (c) Jeżeli $m|a$ oraz $m|b$, to $m|a + b$ i $m|a - b$.
 - (d) Jeżeli $m|a$ i $a \neq 0$ to $|m| \leq |a|$
9.  Udowodnić, że podzielność porządkuje częściowo zbiór $\mathbb{N}$ i narysować diagram Hassego. Czy jest to porządek liniowy? Czy relacja podzielności jest relacją równoważności w zbiorze liczb naturalnych?

10. Podać wartość funkcji Eulera (wskazówka: aby czynniki były parami względnie pierwsze wystarczy przedstawić cały iloczyn wykorzystując faktoryzację):
- 1, 1, 4, 7, 10, 13
 - $3^6, 5^8, 11^3, 17^3, 19^2$
 - $3 \cdot 7, 3 \cdot 7 \cdot 11, 13 \cdot 17, 16 \cdot 27 \cdot 49, 24 \cdot 28 \cdot 45$
 - 375, 720, 988, 4320
11. $\varphi(n) = 840$ oraz $n = 3^\alpha \cdot 7^\beta \cdot 11^\gamma$. Wyznaczyć n .
12. $\varphi(a) = 60$ oraz $a = pq$, gdzie $p \neq q \wedge p, q \in \mathbb{P}$ Wyznaczyć a , jeżeli $p - q = 4$.
13. $\varphi(a) = 120$ oraz $a = p^2 q^2$, gdzie $p \neq q \wedge p, q \in \mathbb{P}$ Wyznaczyć a .
14. Wyznaczyć ile jest liczb naturalnych, mniejszych lub równych 1665, takich, że największy wspólny dzielnik tych liczb z liczbą 1665 jest równy 37.
15. Wyznaczyć ile jest liczb naturalnych, mniejszych lub równych 1476, takich, że największy wspólny dzielnik każdej z tych liczb z liczbą 1476 jest równy 41.
16. Udowodnić:
- $\varphi(4n + 2) = \varphi(2n + 1)$
 - $\varphi(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$, gdzie $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, a $p_1, \dots, p_k$ są różnymi liczbami pierwszymi.
17. Dane są liczby 100, 210, 346. Które z tych liczb przystają do 23 modulo 7?
18. Dane są liczby 180, 531, 104. Które z tych liczb przystają do 11 modulo 13?
19. ★ Podać liczby przeciwne modulo:
- $-2 \pmod{7}$
 - $-3 \pmod{7}$
 - $-5 \pmod{11}$
 - $-8 \pmod{12}$
 - $-2 \pmod{9}$
20. ★ Podać liczby odwrotne modulo:
- | | |
|-----------------------|------------------------|
| (a) $2^{-1} \pmod{5}$ | (f) $2^{-1} \pmod{8}$ |
| (b) $2^{-1} \pmod{7}$ | (g) $4^{-1} \pmod{11}$ |
| (c) $3^{-1} \pmod{7}$ | (h) $7^{-1} \pmod{11}$ |
| (d) $4^{-1} \pmod{7}$ | (i) $7^{-1} \pmod{13}$ |
| (e) $6^{-1} \pmod{7}$ | (j) $3^{-1} \pmod{23}$ |
21. Wykonać obliczenia w zbiorze $\mathbb{Z}_n$:
- $\mathbb{Z}_7 : 7 + 2, 4 - 8, 2 \cdot 4$
 - $\mathbb{Z}_{13} : 5 + 11, 1 - 9, 7 \cdot 6$
 - $\mathbb{Z}_{12} : 5 + 4, 3 - 8, 5 \cdot 8$
22. Wykonać obliczenia:
- $324548 - 345 - 34234 \pmod{3}$
 - $12543 \cdot 4321 \pmod{5}$
 - $529 - 121 \pmod{7}$
 - $329 \cdot 988 \pmod{9}$

- (e) $13 \cdot (18 + 23) \pmod{7}$
 (f) $3^7 \pmod{2}$
 (g) $4^4 \pmod{5}$
 (h) $3^5 \pmod{7}$
23. Sprawdzić, czy $5^{18} \equiv 1 \pmod{27}$.
24. Obliczyć w zbiorze $M_3(\mathbb{Z}_7)$: $\begin{bmatrix} 3 & 5 & 4 \\ 2 & 6 & 3 \\ 4 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & -6 & 1 \\ 3 & 4 & 0 \\ 3 & 4 & 2 \end{bmatrix}$
25. Obliczyć w zbiorze $M_2(\mathbb{Z}_7)$: $\begin{bmatrix} 3 & 5 \\ 2 & 6 \end{bmatrix} \cdot \begin{bmatrix} 1 & -6 \\ 3 & 4 \end{bmatrix}$
26. Czy wektory $v_1 = \begin{bmatrix} 3 \\ 2 \\ 0 \end{bmatrix}$, $v_2 = \begin{bmatrix} 3 \\ 4 \\ 1 \end{bmatrix}$, $v_3 = \begin{bmatrix} 2 \\ 2 \\ 2 \end{bmatrix} \in (\mathbb{Z}_5)^3$ są liniowo niezależne?
27. Wyznaczyć odwrotności modulo:
- (a) $67^{-1} \pmod{119}$
 (b) $16^{-1} \pmod{97}$
 (c) $16^{-1} \pmod{113}$
28. Pokazać, że jeśli n jest liczbą nieparzystą, to $n^2 \equiv 1 \pmod{8}$.
29.  Udowodnić, że przystawanie modulo jest relacją równoważności w $\mathbb{Z}$. Wyznaczyć klasy abstrakcji.
30. Rozwiązać równania:
- (a) $2x \equiv 3 \pmod{6}$
 (b) $3x \equiv 4 \pmod{7}$
 (c) $3x \equiv 2 \pmod{5}$
 (d) $3x \equiv 5 \pmod{6}$
 (e) $4x \equiv 8 \pmod{12}$
 (f) $4x \equiv 6 \pmod{7}$
 (g) $3x \equiv 3 \pmod{6}$
 (h) $21x \equiv 5 \pmod{36}$
 (i) $5x \equiv 2 \pmod{10}$
31. Rozwiązać układy kongruencji:
- (a) $\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 7 \pmod{13} \end{cases}$
 (b) $\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 5 \pmod{7} \end{cases}$
 (c) $\begin{cases} x \equiv 23 \pmod{31} \\ x \equiv 7 \pmod{12} \\ x \equiv 12 \pmod{35} \end{cases}$
 (d) $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{16} \end{cases}$

32. Rozwiązać układy kongruencji:

$$\begin{array}{ll} \text{(a)} \begin{cases} 3x \equiv 4 \pmod{5} \\ 2x \equiv 3 \pmod{7} \end{cases} & \text{(d)} \begin{cases} 2x \equiv 7 \pmod{13} \\ 5x \equiv 8 \pmod{17} \\ 3x \equiv 7 \pmod{31} \\ 14x \equiv 35 \pmod{19} \end{cases} \\ \text{(b)} \begin{cases} 2x \equiv 5 \pmod{7} \\ 16x \equiv 4 \pmod{11} \end{cases} & \\ \text{(c)} \begin{cases} 4x \equiv 3 \pmod{7} \\ 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases} & \end{array}$$

33. Udowodnić cechy podzielności przez:

- | | |
|-------|--------|
| (a) 2 | (f) 8 |
| (b) 3 | (g) 9 |
| (c) 4 | (h) 10 |
| (d) 5 | (i) 11 |
| (e) 6 | |

34. Obliczyć, korzystając z odpowiedniego twierdzenia:

- (a) $5^{84} \pmod{3}$
- (b) $4^{47} \pmod{5}$
- (c) $36^{36} \pmod{17}$
- (d) $85^{143} \pmod{11}$

35. Wyznaczyć resztę z dzielenia:

- (a) 4^{47} przez 45
- (b) 383^{169} przez 45
- (c) 109^{345} przez 14
- (d) $3^{80} + 7^{80}$ przez 11
- (e) $3^{100} + 5^{100}$ przez 7

36. Wyznaczyć ostatnią cyfrę liczby:

- (a) 3^{564139} w zbiorze $\mathbb{Z}_7$
- (b) 2^{320119} w zbiorze $\mathbb{Z}_5$

37. Wyznaczyć ostatnie dwie cyfry liczby 7^{43} .

References

- [1] Larisa Dobryakova, *Matematyka dyskretna*. Lulu, 2012.
- [2] Grzegorz Szkibieli, Czesław Wowk, *Zadania z arytmetyki szkolnej i teorii liczb*. Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, 2001.
- [3] Władysław Narkiewicz *Teoria liczb*. Wydawnictwo Naukowe PWN, 2003.
- [4] Kenneth A. Ross, Charles R. B. Wright, *Matematyka dyskretna*. Wydawnictwo Naukowe PWN, 1999.