Matematyka dyskretna

Jakub Rydzewski jr@fizyka.umk.pl

Lista nr 1:
Data: 26/02/21

1. Pewna liczba sześciocyfrowa a kończy się cyfrą 5. Jeśli tę cyfrę przestawimy na miejsce pierwsze ze strony lewej, to otrzymamy nową liczbę cztery razy większą od poprzedniej. Znaleźć liczbę a.
2. Znaleźć liczbę czterocyfrową n^2 będącą kwadratem pewnej liczby naturalnej n, której cyfra tysięcy jest równa cyfrze dziesiątek, a cyfra setek jest o 1 większa of cyfry jedności.
3. Dowieźć, że dla $n \in \mathbb{N}$:
   a) $9|10^n - 1$ b) $3|10^n + 4^n - 2$ c) $30|n^5 - n$ d) $3|\frac{n(n^2+5)}{2}$
4. Dowieźć, że dla $n \in \mathbb{N}$ liczba $(n+1)^n - 1$ jest podzielna przez liczbę n^2.
5. Stosując algorytm Euklidesa znaleźć NWD liczb:
   a) 963 i 657 b) 423 i 198 c) 1109 i 4999 d) 229, 391 i 667
6. Stosując rozszerzony algorytm Euklidesa znaleźć NWD dla przykładów z zadania poprzedniego.
7. Narysować schemat blokowy algorytmu Euklidesa.
8. Zaimplementować algorytm Eukidesa w wersji podstawowej i rozszerzonej w dowolnym języku programowania.
9. Stosując rozkład na czynniki pierwsze, znaleźć NWW następujących liczb:
   a) 360 i 504 b) 187 i 533 c) 9163, 2737 i 9639
10. Największy wspólny dzielnik liczb naturalnych jest równy 24, a największa wspólna wielokrotność tych liczb wynosi 2496. Znaleźć te liczby.

Lista nr 2:
Data: 12/03/21

1. Uzasadnić, że iloczyn trzech kolejnych liczb naturalnych jest podzielny przez sześć.
2. Liczbę 1000 rozłożyć na takie dwa składniki dodatnie, aby pierwszy był wielokrotnością 10, a drugi w dzieleniu przez 13 dawał resztę 3.
3. Pokazać, że jeśli p jest liczbą pierwszą większą od 5, to p^2 przy dzieleniu przez 30 daje resztę równą 1 lub 19.
4. Mamy podaną liczbę pięciocyfrową 3_152, w której cyfrę tysięcy zastąpiono _. Wyznaczyć cyfrę tysięcy tak, aby liczba była podzielna przez szesnaście. Ile rozwiązań ma to zadanie?
5. Obliczyć ostatnią cyfrę liczby 2^{1000}.
6. Pokazać, że $61! \equiv_{71} 63!$
7. Pokazać, że $2^{11 \cdot 31} \equiv_{11 \cdot 31} 2$.
8. Udowodnić, że reszta z dzielenia przez 10 liczby 33^{100} jest taka sama jak reszta z dzielenia przez 10 liczby 3^{100}.
9. Obliczyć resztę z dzielenia 3^{100} przez 100.

10. Obliczyć resztę z dzielenia 2^{70}, 3^{70}, 4^{70}, 5^{70} przez 71.
11. Wykazać, że $13|2^{70} + 3^{70}$.
12. Obliczyć następujące wyrażenia:
    a) $(50 \cdot 51 + 15) \mod 7$
    b) $15 \cdot 36 \mod 7$
    c) $15^3 \cdot 37^3 \mod 7$
    d) $7000 \mod 9$
    e) $2^{39} \mod 5$
    f) $7^{40} \mod 10$

Lista nr 3:
Data: 19/03/21

1. Udowodnić przechodniość relacji kongruencji.
2. Pokazać, że jeżeli $a \equiv_m b$ oraz $c \equiv_m d$, to $a + c \equiv_m b + d$.
3. Pokazać, że jeżeli $a \equiv_m b$ oraz $c \equiv_m d$, to $ac \equiv_m bd$.
4. Pokazać, że liczba $a \in \mathbb{Z}_m$ jest odwracalna wtedy i tylko wtedy, gdy $\text{NWD}(a, m) = 1$.
5. Pokazać, że dla $n > 0$, jeśli $ad \equiv_n bd$ oraz $\text{NWD}(n, d) = 1$, to $a \equiv_n b$.
6. Zapisując wykładnik potęgi binarnie, oblicz następujące wyrażenia:
    a) $7^{12} \mod 10$ b) $5^{81} \mod 7$ c) $3^{51} \mod 13$ d) $12^{53} \mod 7$ e) $77^{19} \mod 6$ f) $121^{36} \mod 7$
7. Znaleźć wartości funkcji Eulera dla następujących liczb:
    a) 375 b) 720 c) 957 d) 988 e) 1440 f) 4320
8. Funkcja Eulera dla argumentu a przyjmuje wartość 120, gdzie $a = pq$ oraz $p - q = 2$, przy czym p oraz q są dwiema liczbami pierwszymi różnymi od siebie. Znaleźć liczbę a.
9. Funkcja Eulera dla argumentu a przyjmuje wartość 11424, gdzie $a = p^2q^2$, przy czym p oraz q są dwiema liczbami pierwszymi różnymi od siebie. Znaleźć liczbę a.
10. Znaleźć x, jeśli funkcja Eulera w x przyjmuje wartość 12.
11. Wykorzystując Małe Twierdzenie Fermata, obliczyć wyrażenie $7^{126} \mod 11$. Ile mnożeń jest potrzebnych, aby je obliczyć?
12. Wykorzystując Twierdzenie Eulera, obliczyć $13^{101} \mod 16$.

Lista nr 4:
Data: 26/03/21

1. Obliczyć reszty z następujących wyrażeń:
    a) $5^{36} \mod 13$
    b) $10^{49} + 5^3 \pmod 7$
    c) $37^{13} \pmod{17}$
    d) $2^{83} - 1 \pmod{167}$
    e) $3^{12} + 5^{10} \pmod{11}$
    f) $15^{61} - 1 \pmod 7$
    g) $5^{13} + 6^{13} \pmod 9$
    h) $10^{30} - 7^8 \pmod{15}$
    i) $6^6 + 14^{14} \pmod{128}$
    j) $6^{102} \mod 25$
2. Jeśli to możliwe, rozwiązać przykłady z zadania 1. za pomocą twierdzenia Eulera.

3. Korzystając z twierdzenia Eulera uprościć, a następnie obliczyć następujące kongruencje:
   a) $2x^5 + x + 1 \equiv_{45} 0$ b) $2x^2 + x + 1 \equiv_5 0$ c) $x^{13} + 7x^{12} + x \equiv_{13} 5$
   d) $x^{19} + 3x^6 - 4x \equiv_7 1$ e) $7x^{21} - 6x^{10} + 5x \equiv_{11} 4$ f) $13^{100}x \equiv_{16} 15^{81}$
4. Korzystając z twierdzenia Eulera, policzyć dwie ostatnie cyfry 3^{1001}.
5. Zastępując wyrażenie $10^{33} + 12^{44} \pmod{15}$ układem kongruencji, znaleźć jego rozwiązanie.
6. Wypisać tabele dodawania i mnożenia dla $\mathbb{Z}_n$, dla n od 2 do 9.
7. Korzystając z utworzonych tabel wyznaczyć wszystkie rozwiązania następujących kongruencji liniowych:
   a) $5x \equiv_7 2$ b) $4x \equiv_7 2$ c) $4x \equiv_7 3$ d) $5x + 2 \equiv_7 3$ e) $3x + 5 \equiv_9 7$
8. Rozwiązać następujące równania w pierścieniu $\mathbb{Z}_8$:
   a) $1 + x = 0$ b) $1 + x = 2$ c) $5 + x = 2$
9. Przedstawić tabliczkę dodawania i mnożenia w ciele $\mathbb{Z}_7$ i podać elementy odwrotne do 2, 5 i 6 w $\mathbb{Z}_7$.

Lista nr 5:
Data: 9/04/21

1. Wykonać dzielenie wielomianów $p(x)/s(x)$ obliczając iloraz $q(x)$ oraz resztę z dzielenia $r(x)$:
   a) $p(x) = 2x^4 + 5x^3 + 3x^2 + 13x - 3$, $s(x) = x^2 + 2$
   b) $p(x) = x^5 - x^4 - x^3 - 3x - 1$, $s(x) = x^2 - x - 2$
   c) $p(x) = 2x^5 + 3x^4 + 8x^2 + 2x - 15$, $s(x) = 2x + 3$
   d) $p(x) = x^6 - 1$, $s(x) = x - 1$
2. Wykonać dzielenie wielomianów $p(x)/s(x)$ obliczając iloraz $q(x)$ oraz resztę z dzielenia $r(x)$. Działania wykonać we wskazanej arytmetyce modularnej:
   a) $p(x) = x^5 + 3x^4 + 4x^3 + x^2 + 1$, $s(x) = 3x^2 + 2 \pmod 5$
   b) $p(x) = 3x^3 + x^2$, $s(x) = 2x + 1 \pmod 5$
   c) $p(x) = x^4$, $s(x) = x + 1 \pmod 2$
   d) $p(x) = x^6 + x^2 + 1$, $s(x) = x^3 + x + 1 \pmod 2$
3. Zastosować algorytm Euklidesa dla wielomianów $p(x)$ i $q(x)$ by wyznaczyć ich NWD.
   a) $p(x) = x^2 + 4x + 3$, $q(x) = x^2 + x - 6$
   b) $p(x) = x^3 - 2x^2 - 13x + 15$, $q(x) = x^2 - 3x - 10$
   c) $p(x) = x^3 + x + 2$, $q(x) = x^2 + 2 \pmod 3$
   d) $p(x) = x^3 - 1$, $q(x) = x^2 + 2x + 2 \pmod 3$
   e) $p(x) = x^4 + x^3 + x$, $q(x) = x^2 + 1 \pmod 2$
4. W $\mathbb{Z}_4$ wykonać następujące działania:
   a) $(x^4 + 2x^2 + 2x + 1) + (x^4 + x^3 + 3x^2 + 2x + 2)$
   b) $(2x^2 + x + 3)(2x^4 + 3x^3 + x^2 + 3x)$
   c) $(2x^3 + 2x^2 + 3) \cdot (3x^2 + x + 2)$
   d) $(2x^4 + 3) \cdot (2x^4 + 1)$

5. Dobrać liczby a, $b \in \mathbb{Z}$, aby wielomian $x^5 - 4x^3 + 2X^2 + ax + b \in \mathbb{Z}[x]$ przy dzieleniu przez $x - 1$ dawał resztę 1, a przy dzieleniu przez $x - 2$ resztę -5.
6. Wielomian o współczynnikach rzeczywistych przy dzieleniu przez $x - 2$ daje resztę 1, zaś przy dzieleniu przez $x - 1$ daje resztę 2. Jaką resztę daje ten wielomian przy dzieleniu przez $(x - 1)(x - 2)$?
7. Dobrać takie liczby całkowite a, b, aby wielomian $x^4 + 5x^3 + ax^2 + bx + 3 \in \mathbb{Z}[x]$ dzielił się przez wielomian $x^2 - 2x - 3$.

Lista nr 6:
Data: 16/04/21

Oznaczenia: $GF(p) = \mathbb{Z}_p$ oraz $GF(p^n) = \mathbb{Z}_p/_{\equiv f}$, gdzie f jest stopnia n. Ciała: $\mathbb{Z}_p$ oraz $GF(p^n) = \mathbb{Z}_p/_{\equiv f}$, gdy f nad $\mathbb{Z}_p$ jest nierozkładalny.

1. Znaleźć wielomiany nierokładalne stopnia 1, 2 i 3 nad $\mathbb{Z}_2$ oraz $\mathbb{Z}_3$.
2. Przedstawić następujące wielomiany w postaci iloczynu wielomianów nierozkładalnych:
   Nad $\mathbb{Z}_2$:
   a) $f(X) = X^4 + X^2 + X + 1$
   b) $f(X) = X^5 + X^3 + X^2 + X$
   c) $f(X) = X^{10} - X$
   d) $f(X) = X^7 + 1$

   Nad $\mathbb{Z}_3$:
   a) $f(X) = X^9 - X$
   b) $f(X) = X^8 + X^7 + 2X^6 + X^2 + X + 2$
3. Wypisać elementy ciał skończonych $GF(4)$ oraz $GF(9)$.
4. Znaleźć wielomian nierozkładalny w $GF(4)$ eliminując wszystkie wielomiany rozkładalne.
5. Czy $GF(9)$ może mieć więcej niż jeden wielomian nierozkładalny? Jeśli tak, jak nazywamy zbiór takich ciał?
6. Czy wielomian $X^3 - X - 1$ jest redukowalny nad $GF(2)$ lub $GF(3)$?
7. Dlaczego dla elementów x oraz y pierścienia przemiennego o charakterystyce $p \in \mathbb{P}$ prawdziwa jest relacja $(x + y)^p = x^p + y^p$?
8. Wyznaczyć tabelki działań $(+, \cdot)$ w następujących pierścieniach wielomianów nad $K_m[X]$, $m \in \mathbb{Z}$. Które z tych pierścieni są ciałami?
   a) $\mathbb{K}_3[X]/_{\equiv X^2+1}$
   b) $\mathbb{K}_4[X]/_{\equiv X^2+1}$
   c) $\mathbb{K}_2[X]/_{\equiv X^2+1}$
   d) $\mathbb{K}_2[X]/_{\equiv X^2+X+1}$
   e) $\mathbb{K}_2[X]/_{\equiv X^3+X+1}$
   f) $\mathbb{K}_3[X]/_{\equiv X^2+X+1}$
   g) $\mathbb{K}_6[X]/_{\equiv X^2-1}$
9. W pierścieniu $\mathbb{Z}[X]/_{\equiv X^2}$, rozwiązać równanie $(1 + 2X + X^2)t = 5 + 9X + X^2$ o niewiadomej t.
10. W pierścieniu $\mathbb{Z}_3[X]/_{\equiv X^3+2X+1}$, rozwiązać równania o niewiadomej t:
    a) $(1 + 2X + 2X^2 + X^3 + 2X + 1)t = 2 + X + 2X^2 + X^3 + 2X + 1$
    b) $(X + X^3 + 2X + 1)t = X^3 + 2X + 1$

Lista nr 7:
Data: 30/04/21

Oznaczenia: Kod liniowy o długości n i wymiarze k to podprzestrzeń liniowa C o wymiarze k przestrzeni wektorowej $\mathbb{F}_q^n$. Dla $q = 2$ kod nazywamy binarnym. Wektory w C to słowa kodowe. Wielkość kodu to ilość słów kodowych w C, q^k. Macierz generująca $\mathbf{G}$ kodu C to każda macierz rzędu k spełniająca $\mathbf{H} \cdot \mathbf{G}^T = 0$, gdzie macierz $\mathbf{H}$ rzędu $n - k$ to macierz kontroli parzystości, dla której każde słowo kodowe $\mathbf{x}$ spełnia warunek $\mathbf{H} \cdot \mathbf{x} = 0$.

1. Tekst zapisany jest za pomocą 26 liter alfabetu łacińskiego: *a, b, . . . , z*. Aby zaszyfrować tekst należy utożsamić zbiór liter z elementami pierścienia $\mathbb{Z}_{26}$, tj. $a = 0$, $b = 1$, . . . , $z = 25$ i wybrać dwie liczby ψ i $\phi \in \mathbb{Z}_{26}$, takie że $NDW(\psi, 26) = 1$ i zaszyfrować litera po literze według wzoru:

   $$C(x) = \psi x + \phi \pmod{26}.$$

   Funkcja deszyfrująca dana jest wzorem:

   $$D(y) = \psi^{-1} y - \psi^{-1}\phi \pmod{26}.$$

   a) Dla $\psi = 23$ i $\phi = 20$ zaszyfruj słowo *matematyka*.
   b) Udowodnić, że funkcja szyfrująca jest $C(x)$ jest wzajemnie jednoznacza, tj. $D(C(x)) = x$.

2. Podać odległość Hamminga dla następujących par słów kodowych:

   a) 01011 i 01110 b) 01 i 00101 c) 01203 i 02101

3. Sprawdzić, czy wielomian $X^7 + X^6 + X^4 + X^3 + 1$ jest słowem kodowym binarnego kodu wielomianowego $\mathbb{Z}[X]/_{\equiv X^4+X^3+X^2+1}$ długości $n = 8$.

4. Zakodować wielomiany należące do $\mathbb{Z}_2[X]/_{\equiv X^3-1}$ przemnażając je przez wielomian $X - 1$. Czy otrzymany kod jest cykliczny?

5. Zakodować wielomiany należące do $\mathbb{Z}_2[X]/_{\equiv X^3-1}$ przemnażając je przez wielomian $X^2 + X + 1$. Czy otrzymany kod jest cykliczny?

6. Korekta t przekłamanych bitów w binarnym kodzie blokowym typu (n, k) jest możliwa, jeżeli n spełnia nierówność:

   $$2^{n-k} \leq \sum_{p=0}^{t} \binom{n}{p}.$$

   Jak duże musi być n, aby przy przesyłaniu $k = 4$ użytkowych bitów możliwa była korekta $t = 1, 2$ bitów lub odpowiednio 3 bitów? Znajdź podobne oszacowanie dla n, gdy $k = 6$.

7. Przesyłamy 32-bitowe słowa kodowe przez zaszumione łącze. Ile bitów użytkowych można zakodować w tych słowach jeżli przewidujemy korektę a) jednego, b) dwóch przekłamanych bitów?

8. Znaleźć macierz generującą binarnego (6,3)-kodu liniowego o macierzy kontroli patrzystości:

   $$\mathbf{H} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

   Odkodować wektory $\mathbf{c}_1 = [1, 1, 0, 0, 1, 0]$, $\mathbf{c}_2 = [0, 1, 1, 1, 0, 0]$ oraz $\mathbf{c}_3 = [1, 0, 1, 0, 1, 1]$.

9. Wektor $\mathbf{c} = [c_1, \ldots, c_7] \in \mathbb{Z}_2^7$ jest słowem kodowym binarnego (7,4)-kodu liniowego wtedy i tylko wtedy, gdy:

   $$c_1 = c_4 + c_5 + c_7,$$
   $$c_2 = c_4 + c_6 + c_7,$$
   $$c_3 = c_4 + c_5 + c_6.$$

   Znaleźć macierz generującą oraz macierz kontroli parzystości kodu. Zakodować wiadomość $\mathbf{u} = [0, 1, 1, 0]$. Sprawdzić, czy wektor $\mathbf{c} = [0, 0, 0, 0, 1, 1, 1]$ należy do tego kodu. Odkodować słowa $\mathbf{c}_1 = [0, 0, 0, 0, 1, 1, 1]$ oraz $\mathbf{c}_2 = [0, 0, 0, 1, 1, 1, 1]$.

Lista nr 8:
Data: 7/05/21

1. Znaleźć rozkład liczby N wykorzystując metodę faktoryzacji Fermata dla:

   a) $N = 187$ b) $N = 255$ c) $N = 5959$ d) $N = 6557$ e) $N = 5005$

2. Znaleźć rozkład liczby N wykorzystując metodę $p - 1$ Pollarda dla:

   a) $N = 533$ b) $N = 299$ c) $N = 1739$ d) $N = 34571$ e) $N = 220459$

3. Znaleźć rozkład liczby N z użyciem metody ρ Pollarda. Za wielomian generujący sekwencję liczb pseudolosowych wziąć $g(x) = (x^2 + 1) \mod N$:

   a) $N = 221$ b) $N = 7171$ c) $N = 8051$ d) $N = 15347$ e) $N = 84923$

4. Wykorzystując test pierwszości Fermata, sprawdzić czy następujące liczby N są liczbami pierwszymi:

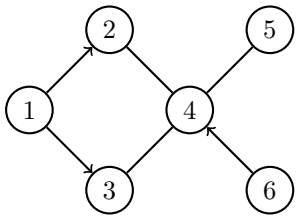
   a) $N = 341$ b) $N = 561$ c) $N = 1001$ d) $N = 1105$ e) $N = 1729$

5. Sprawdzić, czy a jest generatorem w $\mathbb{Z}_n$ dla:

   a) $a = 2$, $n = 11$ b) $a = 2$, $n = 41$ c) $a = 3$, $n = 11$ d) $a = 3$, $n = 41$

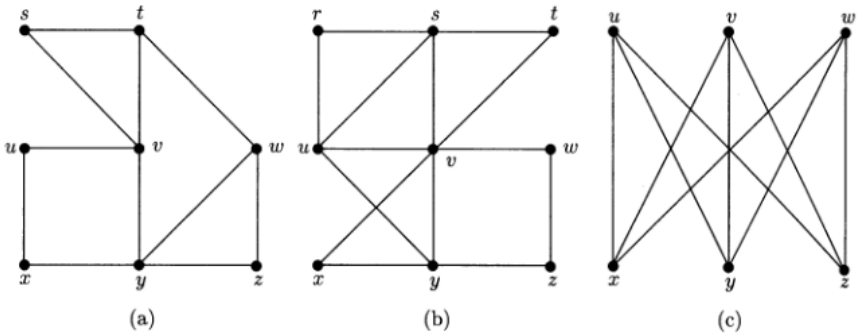
Lista nr 9:
Data: 21/05/21

1. Wyznaczyć macierze sąsiedztwa oraz incydencji dla poniższego grafu:



2. Wykorzystując tw. Cayley'a (tj. istnieje n^{n-2} drzew o n wierzołkach), narysować wszystkie drzewa dla $n = 3$ oraz $n = 4$ i podzielić je na klasy drzew izomorficznych.

3. Który z poniższych grafów ma cykle Eulera? Podać ciąg wierzchołków w cyklu Eulera, jeśli taki istnieje.



4. Wykorzystać algorytm Fleury'ego do znalezienia cyklu Eulera w grafie z 3(b).

5. Zbudować graf mający zbiór wierzchołków $\{0,1\}^3$, w którym wierzchołki v i w są połączone krawiędzią, jeśli ciągi v i w różnią się dokładnie na dwóch współrzędnych. (a) Ile składowych ma taki graf? (b) Ile wierzchołków danego stopnia ma ten graf? Czy ma cykl Eulera?

6. Zbudować graf na podstawie poniższego schematu domu. Czy można obejść cały dom przechodząc przez każde drzwi dokładnie jeden raz?