Rozdział 1

Zadania

1.1 Liczby pierwsze

1. Wykorzystując sito Eratostenesa wyznaczyć wszystkie liczby pierwsze mniejsze niż 200.

2. Wyliczyć największy wspólny dzielnik d liczb n i m oraz znaleźć liczby całkowite p i q takie, że $d = pn + qm$.

(a) $n = 21$, $m = 55$.

(b) $n = 15$, $m = 303$.

(c) $n = 303$, $m = 159$.

(d) $n = 77$, $m = 371$.

(e) $n = 183$, $m = 305$.

3. Udowodnić, że dla dowolnych liczb naturalnych dodatnich a i b mamy $(n^a - 1, n^b - 1) = n^{(a,b)} - 1$, gdzie $n > 1$ jest liczbą naturalną.

4. Znaleźć wzór na największą potęgę liczby pierwszej p dzielącej $n!$.

5. Rozłożyć na czynniki pierwsze liczbę 100!.

6. Iloma zerami zakończone jest rozwinięcie dziesiętne liczby 1000!?

7. Iloma zerami zakończone jest przedstawienie w systemie szesnastkowym liczby 200!?

8. Udowodnić, że

$$S := 1 + \frac{1}{2} + \cdots + \frac{1}{n},$$

nie jest liczbą całkowitą dla $n > 1$.

9. Udowodnić, że

$$S := 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$$

nie jest liczbą całkowitą dla $n > 1$.

10. Niech $a_1, \ldots, a_n$, $n \geq 1$, będą niezerowymi liczbami całkowitymi. Przypuśćmy, że istnieje liczba pierwsza p i dodatnia liczba całkowita k takie, że $p^k \mid a_i$ dla pewnego i oraz $p^k \nmid a_j$ dla $j \neq i$. Udowodnić, że

$$S := \frac{1}{a_1} + \cdots + \frac{1}{a_n}$$

nie jest liczbą całkowitą.

11. Udowodnić, że jeśli n jest liczbą złożoną, to n ma dzielnik pierwszy nie przekraczający $\sqrt{n}$.

12. Udowodnić, że jeśli najmniejsza liczba pierwsza p dzieląca liczbę całkowitą dodatnią n przekracza $\sqrt[3]{n}$, to $\frac{n}{p} = 1$ lub $\frac{n}{p}$ jest liczbą pierwszą.

13. Niech p będzie liczbą pierwszą. Udowodnić, że $\binom{p}{k}$ jest liczbą podzielną przez p, dla $1 \leq k \leq p-1$.

14. Niech p będzie liczbą pierwszą. Udowodnić, że $p \mid \binom{np}{p} - n$ dla każdej liczby naturalnej $n \geq 1$.

15. Niech p_k oznacza k-tą liczbę pierwszą, $k \geq 1$. Udowodnić, że $p_k < 2^{2^k}$.

W s k a z ó w k a. Udowodnić, że $p_k \leq p_1 \cdots p_{k-1} + 1$.

16. Udowodnić, że $\pi(x) \geq \log(\log(x))$ dla $x > 1$.

17. Udowodnić, że $\sqrt{x} \leq 2^{\pi(x)}$ dla $x \geq 2$.

W s k a z ó w k a. Wykorzystać fakt, że każda liczba naturalna może być przedstawiona w postaci mn^2, gdzie m jest liczbą bezkwadratową.

18. Udowodnić, że $\pi(x) \geq \frac{\log x}{2 \log 2}$ dla $x \geq 2$.

19. Udowodnić, że $\pi(x) \leq \frac{9x \log 2}{\log x}$, dla $x \geq 2$.

W s k a z ó w k a. Wykorzystać fakt, że $\prod_{n<p\leq 2n} p \mid \binom{2n}{n}$.

20. Niech a, b będą względnie pierwszymi liczbami naturalnymi takimi, że $ab = n^k$ dla pewnych liczb naturalnych n i k. Pokazać, że istnieją liczby naturalne d i e takie, że $a = c^k$ i $b = d^k$.

21. Udowodnić, że jeśli x, y i z są parami względnie pierwszymi liczbami naturalnymi będącymi rozwiązaniem równania $x^2 + y^2 = z^2$, to istnieją względnie pierwsze liczby naturalne a i b, z których jedna jest parzysta, takie, że $x = a^2 - b^2$, $y = 2ab$ i $z = a^2 + b^2$ (z dokładnością do zamiany miejscami liczb x i y).

22. Udowodnić, że równanie $x^4 + y^4 = z^2$ nie ma nietrywialnych rozwiązań naturalnych.

23. Udowodnić, że równanie $x^4 - y^4 = z^2$ nie ma nietrywialnych rozwiązań naturalnych.

24. Udowodnić, że jeśli f jest wielomianem dodatniego stopnia o współczynnikach całkowitych, to dla nieskończenie wielu liczb pierwszych p istnieje liczba całkowita x o własności $p \mid f(x)$.

25. Niech q będzie liczbą pierwszą. Udowodnić, że istnieje nieskończenie wiele liczb pierwszych o własności $q \mid p - 1$.

26. Niech $F_m := 2^{2^m} + 1$, $m \geq 0$, będzie liczbą Fermata. Pokazać, że $F_m = F_1 \cdots F_{m-1} + 2$, oraz, że każdy dzielnik pierwszy liczby F_m jest postaci $2^{m+1}k + 1$.

1.2 Kongruencje

27. Udowodnić, że liczba $10^6 - 1$ jest podzielna przez 13.

28. Udowodnić, że liczba $10^8 + 1$ jest podzielna przez 17.

29. Udowodnić, że liczba $10^9 + 1$ jest podzielna przez 19.

30. Udowodnić, że jeśli $3 \nmid n$, to $3 \mid n^4 + n^2 + 1$.

31. Udowodnić, że $3 \mid 2^{2n} - 1$ dla każdej liczby naturalnej n.

32. Udowodnić, że $\sum_{j=1}^{n-1} j \equiv 0 \pmod{n}$ wtedy i tylko wtedy, gdy n jest liczbą nieparzystą.

33. Udowodnić, że $\sum_{j=1}^{n-1} j^3 \equiv 0 \pmod{n}$ wtedy i tylko wtedy, gdy $n \not\equiv 2 \pmod{4}$.

34. Rozwiązać następujące kongruencje.
(a) $3x \equiv 4 \pmod{7}$
(b) $27x \equiv 25 \pmod{256}$
(c) $2x \equiv 37 \pmod{21}$
(d) $10x \equiv 15 \pmod{35}$
(e) $3x \equiv 7 \pmod{18}$

35. Rozwiązać następujące układy kongruencji.
(a) $x \equiv 3 \pmod{4}$, $x \equiv 2 \pmod{7}$, $x \equiv 1 \pmod{9}$
(b) $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 1 \pmod{8}$, $x \equiv 9 \pmod{11}$
(c) $2x \equiv 1 \pmod{3}$, $3x \equiv 1 \pmod{4}$, $5x \equiv 4 \pmod{7}$

36. W koszu znajduje się n jajek. Jeśli wyjmujemy z kosza po 2 (3, 4, 5, 6 odpowiednio) jajka, to na koniec zostaje w koszu 1 (2, 3, 4, 5 odpowiednio) jajko. Jeśli wyjmujemy z kosza po 7 jajek, to na koniec nie zostanie nam ani jedno jako. Jaka jest najmniejsza możliwa wartość n?

1.3 Funkcja Eulera

37. Wyliczyć $\varphi(1000)$, $\varphi(125)$, $\varphi(180)$, $\varphi(360)$, $\varphi(1001)$.

38. Znaleźć wszystkie liczby całkowite dodatnie n, dla których $\varphi(n) = m$.
(a) $m = 14$.
(b) $m = 8$.
(c) $m = 12$.

39. Udowodnić, że $\varphi(m^k) = m^{k-1}\varphi(m)$ dla dowolnych liczb całkowitych dodatnich m i k.

40. Udowodnić, że $\varphi(n)$ jest liczbą parzystą dla wszystkich całkowitych $n > 2$.

41. Udowodnić, że jeśli $d = (m, n)$ dla liczb całkowitych dodatnich m i n, to $\varphi(mn) = d\varphi(m)\varphi(n)/\varphi(d)$.

42. Udowodnić, że jeśli $d \mid n$, to $\varphi(d) \mid \varphi(n)$.

43. Udowodnić, że $a^{12} \equiv 1 \pmod 7$ dla każdej liczby całkowitej a spełniającej warunek $(a, 7) = 1$.

44. Udowodnić, że $a^{12} \equiv 1 \pmod{65}$ dla każdej liczby całkowitej n spełniającej warunek $(a, 65) = 1$.

45. Udowodnić, że $n \mid \varphi(a^n - 1)$ dla wszystkich $a > n$.

46. Udowodnić, że $n \nmid 2^n - 1$ dla wszystkich $n > 1$.

47. Udowodnić, że $\frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right)$ interpretując lewą stroną jako prawdopodobieństwo, że losowo wybrana liczbą ze zbioru $\{1, \ldots, n\}$ jest względnie pierwsza z n.

48. Znaleźć dwie ostatnie cyfry liczby 3^{1000}.

49. Znaleźć dwie ostatnie cyfry liczby 2^{1000}.

50. Złamać system kryptograficzny RSA, w którym $n = 9991$, zaś jawnym kluczem szyfrującym jest liczba 37.

1.4 Elementy teorii pierścieni

51. Które z podanych zbiorów są pierścieniami ze względu na zwykłe działania dodawania i mnożenia liczb?

(a) zbiór liczb naturalnych.

(b) zbiór liczb całkowitych podzielnych przez 2 lub 3.

(c) zbiór liczb postaci $a + b\sqrt{2}$, gdzie liczby a i b są całkowite.

(d) zbiór liczb postaci $\frac{a}{2^k}$, gdzie liczby a i k są całkowite, $k \geq 0$.

(e) zbiór liczb postaci $a + b\sqrt[3]{2}$, gdzie liczby a i b są całkowite.

52. Które z podanych zbiorów funkcji określonych w przedziale $[0, 1]$ i przyjmujących wartości rzeczywiste są pierścieniami ze względu na zwykłe działania dodawania i mnożenia funkcji?

(a) zbiór funkcji ciągłych w przedziale $[0, 1]$.

(b) zbiór funkcji wielomianowych, których wyraz wolny jest liczbą całkowitą.

(c) zbiór funkcji f, dla których $f(\frac{1}{2}) = 0$.

(d) zbiór funkcji f, dla których $f(0) = f(1)$.

(e) zbiór funkcji f, dla których istnieje liczba całkowita k o własności $2^k f(0) = f(1)$.

53. Udowodnić, że każdy skończony pierścień bez dzielników zera jest ciałem.

54. Wielomian $f \in \mathbb{R}[X]$ daje przy dzieleniu przez $X - 2$ resztę 1, zaś przy dzieleniu przez $X - 1$ resztę 2. Jaką resztę daje ten wielomian przy dzieleniu przez $(X - 1)(X - 2)$?

55. Wyznaczyć największy wspólny dzielnik d wielomianów $f, g \in \mathbb{R}[X]$ oraz wyznaczyć wielomiany $u, v \in \mathbb{R}[X]$ takie, że $d = uf + vg$.

(a) $f = X^4 + X^2 + 1$, $g = X^2 + 1$.

(b) $f = X^4 - 4X^3 + 6X^2 - 4X + 1$, $g = X^3 - X^2 + X - 1$.

(c) $f = X^4 + 2X^3 - X^2 - 4X - 2$, $g = X^4 + X^3 - X^2 - 2X - 2$.

56. Znaleźć element odwrotny do warstwy wielomianu $1 + X^2$ w pierścieniu $\mathbb{R}[X]/(X^3)$.

1.5 Ciała skończone

57. Wypisać unormowane wielomiany nierozkładalne stopnia nie większego niż 4 nad $\mathbb{F}_2$ i $\mathbb{F}_3$.

58. Przedstawić wielomian f w postaci iloczynu wielomianów nierozkładalnych nad ciałem $\mathbb{F}_p$.

(a) $f = X^{16} - X$, $p = 2$.

(b) $f = X^9 - X$, $p = 3$.

(c) $f = X^{27} - X$, $p = 3$.

59. Wyznaczyć liczbę unormowanych wielomianów nierozkładalnych stopnia nie większego niż 8 nad $\mathbb{F}_2$, $\mathbb{F}_3$ i $\mathbb{F}_5$.

60. Przedstawić wielomian f w postaci iloczynu wielomianów nierozkładalnych nad ciałem $\mathbb{F}_p$.

(a) $f = X^7 + X^4 + X^2 + X + 1$, $p = 2$.

(b) $f = X^8 + X^7 + 2X^6 + X^2 + X + 2$, $p = 3$.

(c) $f = X^9 + 2X^7 + X^6 + 3X^5 + X^4 + 2X^2 + 3X + 3$, $p = 5$.

61. Czy w przedstawieniu wielomianu f w postaci iloczynu wielomianów nierozkładalnych nad $\mathbb{F}_p$ każdy czynnik występuje w potędze 1?

(a) $f = X^6 + X^3 + X^2 + X$, $p = 2$.
(b) $f = X^6 + X^4 + X^2 + X$, $p = 3$.
(c) $f = X^6 + 2X^5 + 3X^4 + 2X^3 + 4X^2 + X + 4$, $p = 5$.

62. W ciele $\mathbb{F}_q$ rozwiązać równanie $f(x) = 0$.
(a) $f = X^2 + 1$, $q = 9$.
(b) $f = X^2 + X + 2$, $q = 9$.
(c) $f = X^2 + 2X + 3$, $q = 25$.

63. Niech p będzie liczbą pierwszą i $\alpha \in \mathbb{F}_{p^2}$ będzie pierwiastkiem wielomianu $X^2 + aX + b$, gdzie $a, b \in \mathbb{F}_p$. Udowodnić, że jeśli $\alpha \notin \mathbb{F}_p$, to $(c\alpha + d)^{p+1} = d^2 - acd + bc^2$. Wykorzystując ten fakt policzyć $(2 + 3i)^{101}$, gdzie i jest pierwiastkiem z -1 w $\mathbb{F}_{19^2}$.

64. Udowodnić, że jeśli $f \in \mathbb{F}_p[X]$, to $f' = 0$ wtedy i tylko wtedy, gdy istnieje wielomian $g \in \mathbb{F}_p[X]$ takie, że $f = g^p$.

1.6 Elementy teorii grup

65. Które z następujących zbiorów są grupami ze względu na dodawanie liczb?
(a) zbiór liczb naturalnych.
(b) zbiór liczb całkowitych.
(c) zbiór liczb rzeczywistych.
(d) zbiór liczb całkowitych podzielnych przez ustaloną liczbę naturalną n.
(e) $\{0, 1, 2, 3, 4\}$.

66. Które z następujących zbiorów są grupami ze względu na mnożenie liczb?
(a) zbiór liczb rzeczywistych.
(b) zbiór liczb rzeczywistych różnych od 0.
(c) zbiór liczb rzeczywistych większych od 0.
(d) zbiór liczb całkowitych.
(e) zbiór liczb zespolonych o module 1.

67. Wyznaczyć rzędy elementów grup $\mathbb{F}_7^*$, $\mathbb{F}_8^*$ i $\mathbb{F}_9^*$.

68. Wyliczyć ilość generatorów grupy $\mathbb{F}_{p^2}^*$. Pokazać, że wielomian X^2+c jest nierozkładalny nad $\mathbb{F}_p$. Niech $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2+c)$ i niech α będzie warstwą X w $\mathbb{F}_{p^2}$. Sprawdzić czy elementy α, $\alpha+1$ i $2\alpha+1$ są generatorami grupy $\mathbb{F}_{p^2}^*$. Przedstawić w postaci $a+b\alpha$ odwrotność elementu $2+3\alpha \in \mathbb{F}_{p^2}$.

(a) $p=3$, $c=1$.

(b) $p=5$, $c=3$.

(c) $p=7$, $c=2$.

69. Udowodnić, że wielomian $X^4+X+1 \in \mathbb{F}_2[X]$ jest nierozkładalny w $\mathbb{F}_2[X]$. Niech $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4+X+1)$ i niech α będzie warstwa jedynki. Ile generatorów ma grupa $\mathbb{F}_{16}^*$? Udowodnić, że $\alpha+1$ jest generatorem tej grupy. Znaleźć liczbę naturalną k o własności $(\alpha+1)^k = \alpha$ i przedstawić w postaci $a+b\alpha+c\alpha^2+d\alpha^3$ odwrotność elementu α.

70. Jakie warunki muszą spełniać liczb p i k, aby każdy element grupy $\mathbb{F}_{p^k}^*$ różny od 1 był jej generatorem?

71. Jakie warunki muszą spełniać liczb p i k, aby każdy element grupy $\mathbb{F}_{p^k}^*$ różny od 1 był jej generatorem lub kwadratem generatora?

72. Wyliczyć rzędy elementów grup $(\mathbb{Z}/8\mathbb{Z})^*$, $(\mathbb{Z}/15\mathbb{Z})^*$ i $(\mathbb{Z}/16\mathbb{Z})^*$.

73. Udowodnić, ze grupa $(\mathbb{Z}/p^k\mathbb{Z})^*$ jest cykliczna dla liczby pierwszej $p>2$ oraz dowolnej liczby naturalnej $k>0$.

W s k a z ó w k a. Niech a będzie liczbą generującą grupę $\mathbb{F}_p^*$. Wtedy jedna z warstw a lub $(p+1)a$ jest generatorem grupy $(\mathbb{Z}/p^k\mathbb{Z})^*$.

74. Wyliczyć podgrupy $\langle 6\rangle$, $\langle 10\rangle$ i $\langle 6,10\rangle$ w $\mathbb{Z}/15\mathbb{Z}$.

1.7 Elementy teorii kodowania

75. Niech $m(n,k)$ oznacza maksymalną możliwą ilość słów w kodzie $C \subset \mathbb{F}_2^n$, którego minimalna odległość jest nie mniejsza niż k. Udowodnić następujące własności symbolu $m(n,k)$.

(a) $m(3k,2k) = 4$.

(b) $m(n+d,d) \geq 2m(n,d)$.

(c) $m(2n,d) \geq (m(n,d))^2$.

(d) $m(n,d) \leq 2m(n-1,d)$.

(e) $(\sum_{i=0}^{k} \binom{n}{i}) m(n,2k+1) \leq 2^n$.

76. Udowodnić, że kod ISBN jest rozpoznaje tzw. „czeski błąd", polegający na przestawieniu dwóch kolejnych znaków.

77. Wyznaczyć minimalną odległość kodu $C \subset \mathbb{F}_2^8$, którego macierz kontroli parzystości H ma postać

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

Zakładając, że przy przesyłaniu ośmiu bitów występuje co najwyżej jeden błąd, określić jaki ciąg był przesyłany, jeśli otrzymano ciąg v.

(a) $v = (1, 0, 0, 0, 1, 0, 1, 0)$.
(b) $v = (0, 1, 0, 1, 1, 1, 0, 0)$.
(c) $v = (0, 0, 0, 1, 1, 1, 0, 1)$.
(d) $v = (0, 1, 1, 1, 1, 1, 1, 1)$.
(e) $v = (0, 0, 1, 0, 1, 1, 0, 0)$.

78. Wyznaczyć minimalną odległość kodu $C \subset \mathbb{F}_2^7$, którego macierz kontroli parzystości H ma postać

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

79. Wyznaczyć minimalną odległość kodu $C \subset \mathbb{F}_2^5$, którego macierz kontroli parzystości H ma postać

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

80. Wyznaczyć minimalna odległość kodu $C \subset \mathbb{F}_3^8$, którego macierz kontroli parzystości H ma postać

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 2 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Znaleźć bazę liniową kodu C nad $\mathbb{F}_3$.

81. Wyznaczyć macierz kontroli parzystości wszystkich kodów cyklicznych długości n nad ciałem $\mathbb{F}_p$.

(a) $p = 2$, $n = 5$.

(b) $p = 2$, $n = 9$.

(c) $p = 3$, $n = 8$.

Rozdział 2

Rozwiązania

2.1 Liczby pierwsze

1. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.

2. (a)**.** $d = 1$, $p = 21$, $q = -8$, gdyż

$$\begin{array}{rclcrcl} 55 &=& 2 \cdot 21 + 13, & & 13 &=& 55 - 2 \cdot 21, \\ 21 &=& 1 \cdot 13 + 8, & & 8 &=& 21 - 13 = -55 + 3 \cdot 21, \\ 13 &=& 1 \cdot 8 + 5, & & 5 &=& 13 - 8 = 2 \cdot 55 - 5 \cdot 21, \\ 8 &=& 1 \cdot 5 + 3, & & 3 &=& 8 - 5 = -3 \cdot 55 + 8 \cdot 21, \\ 5 &=& 1 \cdot 3 + 2, & & 2 &=& 5 - 3 = 5 \cdot 55 - 13 \cdot 21, \\ 3 &=& 1 \cdot 2 + 1, & & 1 &=& 3 - 2 = -8 \cdot 55 + 21 \cdot 21, \\ 2 &=& 2 \cdot 1 + 0. & & & & \end{array}$$

2. (b)**.** $d = 3$, $p = -20$, $q = 1$.

2. (c)**.** $d = 3$, $p = 21$, $q = -40$.

2. (d)**.** $d = 7$, $p = -24$, $q = 5$.

2. (e)**.** $d = 61$, $p = 2$, $q = -1$.

3. Dowód będzie indukcyjny ze względu na $\max(a, b)$. Łatwo zauważyć, że teza jest prawdziwa, gdy $a = b$. W szczególności zachodzi dla $\max(a, b) = 1$. Przypuśćmy zatem, że $\max(a, b) > 1$ oraz, że dla każdej pary liczb naturalnych dodatnich a' i b' o własności $\max(a', b') < \max(a, b)$ mamy $(n^{a'} - 1, n^{b'} - 1) = n^{(a',b')} - 1$. Bez straty ogólności możemy założyć, że $a \geq b$. Ponieważ

przypadek $a = b$ już rozważaliśmy, więc ograniczymy się teraz do sytuacji $a > b$. Wtedy $n^a = n^{a-b}(n^b - 1) + n^{a-b} - 1$, więc korzystając z założenia indukcyjnego oraz własności największego wspólnego dzielnika otrzymujemy, że $(n^a - 1, n^b - 1) = (n^b - 1, n^{a-b} - 1) = n^{(b,a-b)} - 1 = n^{(a,b)} - 1$, gdyż $\max(b, a - b) = \max(a, b)$.

4. $\sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$.

5. W rozkładzie liczby 100! na czynniki pierwsze występują tylko liczby pierwsze mniejsze od 100, które możemy wyznaczyć przy pomocy sita Eratostenesa. Ponadto każda z nich występuje w potędze opisanej przez wzór z zadania 4. W efekcie otrzymujemy

$$100! = 2^{97} \cdot 3^{48} \cdot 5^{24} \cdot 7^{16} \cdot 11^9 \cdot 13^7 \cdot 17^5 \cdot 19^5 \cdot 23^4 \cdot 29^3 \cdot 31^3 \cdot 37^2 \cdot 41^2 \cdot 43^2 \cdot 47^2 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 83 \cdot 89 \cdot 97.$$

6. Liczba zer kończących rozwinięcie dziesiętne liczby 1000! jest równa największej potędze liczby 5 dzielącej 1000!, a więc $200 + 40 + 8 + 1 = 249$.

7. Liczba zer kończący przestawienie w systemie szesnastkowym liczby 200! jest równa części całkowitej ilorazu z dzielenia największej potęgi liczby 2 dzielącej 200! przez 4, a więc 49.

8. Niech k będzie taką liczbą całkowitą, że $2^k \leq n < 2^{k+1}$, zaś m będzie największa wspólną wielokrotnością liczb $1, \ldots, 2^k - 1, 2^{k+1}, \ldots, n$. Gdyby S było liczbą całkowitą, to mS też byłoby liczbą całkowitą. Z drugiej strony $\frac{m}{i}$ jest liczbą całkowitą dla $i = 1, \ldots, n$, $i \neq 2^k$, zaś $\frac{m}{2^k}$ nie jest liczbą całkowitą, co prowadzi do sprzeczności.

9. Wybieramy maksymalną potęgę liczby 3 nie większą niż n i dalej postępujemy podobnie jak zadaniu 8.

10. Niech m będzie najmniejszą wspólną wielokrotnością liczb $a_1, \ldots, a_n$. Wtedy $p \mid m$, zatem gdyby S było liczbą całkowitą, to $\frac{m}{p}S$ też byłoby liczbą całkowitą. Zauważmy jednak, że $\frac{m}{p}a_j$ jest liczbą całkowitą dla $j \neq i$ oraz $\frac{m}{p}a_i$ nie jest liczbą całkowitą, co prowadzi do sprzeczności.

11. Wiemy, że $n = ab$, gdzie $1 < a \leq b < n$. Wtedy $a \leq \sqrt{n}$, więc jeśli p jest liczbą pierwszą dzielącą a, to $p \leq \sqrt{n}$.

12. Gdyby $\frac{n}{p}$ było liczbą złożoną, to na mocy zadania 11 i założeń istniałaby liczba pierwsza q spełniająca warunki $\sqrt[3]{n} < q \leq \sqrt{\frac{n}{p}} < \sqrt[3]{n}$, co jest niemożliwe.

13. Dla $1 \leq k \leq p-1$ liczba pierwsza p nie występuje w rozkładzie liczb $k!$ i $(p-k)!$. Z drugiej strony $p!$ jest podzielne przez p, więc teza wynika ze wzoru na $\binom{p}{k}$.

14. Dowód będzie indukcyjny ze względu na n. Dla $n = 1$ teza jest oczywista. Załóżmy zatem, że $n > 1$ oraz, że $p \mid \binom{np-p}{p} - (n-1)$. Mamy wzór $\binom{np}{p} = \sum_{k=0}^{p} \binom{p}{k}\binom{np-p}{p-k}$, a więc $\binom{np}{p} - n = (\binom{np-p}{p} - (n-1)) + \sum_{k=1}^{p-1} \binom{p}{k}\binom{np-p}{p-k}$. Korzystając z zadania 13 oraz założenia indukcyjnego otrzymujemy tezę.

15. Pokażemy najpierw, że $p_k \leq p_1 \cdots p_{k-1} + 1$ dla $k \geq 2$. Istotnie $p_1 \cdots p_{k-1} + 1$ jest liczbą większą od 1 i $(p_1 \cdots p_{k-1} + 1, p_i) = 1$ dla $i = 1, \ldots, k-1$. Zatem istnieje liczba pierwsza p dzieląca $p_1 \cdots p_{k-1} + 1$ różna od liczb p_i, $i = 1, \ldots, k-1$. Stąd wynika, że $p_k \leq p_1 \cdots p_{k-1} + 1$.

Pokażemy teraz, że $p_k < 2^{2^k}$. Dla $k = 1$ teza jest oczywista. Przypuśćmy zatem, że $k > 1$ oraz że $p_j < 2^{2^j}$ dla $j = 1, \ldots, k-1$. Korzystając z nierówności $p_k \leq p_1 \cdots p_{k-1} + 1$ otrzymujemy wtedy, że $p_k < 2^{2^1} \cdots 2^{2^{k-1}} + 1 \leq 2^{2^k}$, co kończy dowód.

16. Fakt, że $\pi(x) \geq \log(\log(x))$ dla $x \in (1, 3)$ jest łatwy do zweryfikowania. Przypuśćmy zatem, że $x \geq 3$. Niech p będzie najmniejszą liczbą pierwszą większą od x. Wtedy $p < 2^{2^{\pi(x)+1}}$ na mocy zadania 15. Stąd otrzymujemy, że $x < 2^{2^{\pi(x)+1}}$. Ponieważ $\pi(x) \geq 2$ dla $x \geq 3$, więc $2^{2^{\pi(x)+1}} < e^{e^{\pi(x)}}$ zatem $x < e^{e^{\pi(x)}}$ dla $x \geq 3$. Dwukrotnie logarytmując powyższą nierówność otrzymujemy tezę zadania.

17. Dla $x \leq 3$ nierówność można sprawdzić bezpośrednio. Załóżmy zatem, że $x \geq 3$. Niech $p_1, \ldots, p_m$ $(m = \pi(x))$ będą wszystkimi, parami różnymi, liczbami pierwszymi nie większymi niż x. Wtedy każda liczba naturalna $n \leq x$ może być zapisana w postaci $n = p_1^{\varepsilon_1} \cdots p_m^{\varepsilon_m} r^2$, gdzie $\varepsilon_1, \ldots, \varepsilon_m \in \{0, 1\}$ i $r \leq \lfloor \sqrt{x} \rfloor$. Ponadto, $p_1 \cdots p_m (\lfloor \sqrt{x} \rfloor)^2 \geq 6(\lfloor \sqrt{x} \rfloor)^2 > x$ (istotnie, $x \leq (\lfloor \sqrt{x} \rfloor + 1)^2 \leq 4(\lfloor \sqrt{x} \rfloor)^2$). Stąd $\lfloor x \rfloor < 2^{\pi(x)} \sqrt{\lfloor x \rfloor}$. Ponieważ $2^{\pi(x)} \sqrt{\lfloor x \rfloor}$ jest liczbą naturalną, więc otrzymujemy, że $x \leq 2^{\pi(x)} \sqrt{x}$, co kończy dowód.

18. Wystarczy zlogarytmować nierówność z zadania 17.

19. Z faktu, że $\prod_{n<p\leq 2n} p \mid \binom{2n}{n}$ wynika, że $\sum_{n<p\leq 2n} \log p \leq 2n \log 2$, gdyż $\binom{2n}{n} \leq 2^{2n}$. Niech $\theta(n) := \sum_{p \leq n} \log p$. Mamy zatem, że $\theta(2n) - \theta(n) \leq 2n \log 2$, skąd indukcyjnie dowodzimy, że $\theta(2^r) \leq 2^{r+1} \log 2$. Dla $x \geq 2$ wybierzmy r takie, że $2^{r-1} < x \leq 2^r$. Wtedy $\theta(x) \leq \theta(2^r) \leq 2^{r+1} \log 2 \leq 4x \log 2$. W szczególności $\sum_{\sqrt{x}<p\leq x} \log p \leq 4x \log 2$, co prowadzi do wniosku,

że $\pi(x) - \pi(\sqrt{x}) \leq \frac{8x \log 2}{\log x}$. Ponieważ $\pi(\sqrt{x}) \leq \sqrt{x}$ i $\sqrt{x} \leq \frac{x \log 2}{\log x}$ dla $x \geq 16$, więc w tym przypadku dowód nierówności jest zakończony. Dla $x \leq 16$ nierówność można sprawdzić bezpośrednio.

20. Jeśli $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ i $b = q_1^{\beta_1} \cdots q_s^{\beta_s}$ są przedstawieniami liczb a i b w postaci iloczynów potęg parami różnych liczb pierwszych, to z założenia $(a, b) = 1$ wynika, że $p_i \neq q_j$ dla wszystkich par indeksów i, j. W ten sposób otrzymujemy równość $n^k = ab = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$. Z twierdzenia o jednoznaczności przedstawienia liczby naturalnej w postaci iloczynu potęg liczb pierwszych wynika, że w rozkładzie liczby n występują tylko liczby pierwsze $p_1, \ldots, p_r$ i $q_1, \ldots, q_s$. Zatem $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r} q_1^{\theta_1} \cdots q_s^{\gamma_s}$ dla pewnych naturalnych liczb dodatnich $\gamma_1, \ldots, \gamma_r$ i $\theta_1, \ldots, \theta_s$. Z równości $n^k = ab$ i twierdzenia o jednoznaczności przedstawienia liczby naturalnej w postaci iloczynu potęg liczb pierwszych otrzymujemy, że $\alpha_i = k\gamma_i$ dla $i = 1, \ldots, r$ i $\beta_j = k\theta_j$ dla $j = 1, \ldots, s$. Zatem $c = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ i $d = q_1^{\theta_1} \cdots q_s^{\theta_s}$ spełniają warunki zadania.

21. Ponieważ liczby x i y są względnie pierwsze, więc nie mogą być obie jednocześnie parzyste. Gdyby obie były nieparzyste, to $z^2 \equiv 2 \pmod 4$, co jest niemożliwe. Zatem bez straty ogólności możemy założyć, że x jest liczbą parzystą, zaś y nieparzystą. Wtedy także z jest liczbą nieparzystą. Ponadto $(\frac{x}{2})^2 = \frac{z+y}{2} \cdot \frac{z-y}{2}$. Wykorzystując założenie o względnej pierwszości liczb x, y i z wnioskujemy, że $(\frac{z+y}{2}, \frac{z-y}{2}) = 1$, i korzystając z zadania 20 otrzymujemy, że $\frac{z+y}{2} = a^2$ i $\frac{z-y}{2} = b^2$ dla pewnych względnie pierwszych liczb naturalnych a i b. Ostatecznie $x = 2ab$, $y = a^2 - b^2$ i $z = a^2 + b^2$, przy czym jedna z liczb a i b jest parzysta, gdyż y nie jest liczbą parzystą.

22. Przypuśćmy, że równanie $x^4 + y^4 = z^2$ ma nietrywialne rozwiązanie i wybierzmy takie rozwiązanie o najmniejszej wartości z. Wtedy oczywiście liczby x^2, y^2 i z są parami względnie pierwsze, więc z zadania 21 wiemy, że $x^2 = 2ab$, $y^2 = a^2 - b^2$ i $z = a^2 + b^2$ dla pewnych parami względnie pierwszych liczb a i b, z których jedna jest liczbą parzystą. Gdyby a było parzyste, to $y^2 \equiv 3 \pmod 4$, co jest niemożliwe. Zatem b jest liczbą parzystą i $b = 2c$ dla pewnej liczby naturalnej c. Ponieważ $x^2 = 4ac$ i $(a, c) = 1$, więc $a = m^2$ i $c = n^2$ dla pewnych względnie pierwszych liczb naturalnych m i n na mocy zadania 20. Wtedy $(2n^2)^2 + y^2 = (m^2)^2$, przy czym $(2n^2, y) = (y, m^2) = (2n^2, m^2) = 1$. Z zadania 21 wynika zatem, że istnieją parami względnie pierwsze liczby naturalne α i β, z których jedna jest podzielna przez 2, takie, że $n^2 = \alpha\beta$, $y = \beta^2 - \alpha^2$ i $m^2 = \alpha^2 + \beta^2$. Z równości $n^2 = \alpha\beta$ i zadania 20 wnioskujemy, że istnieją liczby naturalne p i q takie, że $\alpha = p^2$ i $\beta = q^2$, co daje nam równości $p^4 + q^4 = m^2$, co przeczy minimalności z.

23. Wybierzmy nietrywialne rozwiązanie równanie $x^4 = z^2 + y^4$ o minimalnej wartości x. Z zadania 21 wynika, że x musi być liczbą nieparzystą. Przypuśćmy najpierw, że także y jest liczbą nieparzystą. Wtedy $z = 2ab$, $y^2 = a^2 - b^2$ i $x^2 = a^2 + b^2$ dla pewnych względnie pierwszych liczb naturalnych a i b. Wtedy $a^4 = (xy)^2 + b^4$ i $a < x$, co przeczy założeniu o minimalności x. Załóżmy teraz, że y jest liczbą parzystą. Wtedy $y^2 = 2ab$, $z = a^2 - b^2$ i $x^2 = a^2 + b^2$, dla względnie pierwszych liczb a i b, z których jedna jest parzysta. Jeśli a jest liczbą parzystą, to na mocy zadania 20 $2a = s^2$ i $b = t^2$ dla pewnych liczb naturalnych s i t. Wtedy s też jest liczbą parzystą, więc $a = 2u^2$. Stąd $x^2 = (2u^2)^2 + (t^2)^2$, więc $2u^2 = 2vw$, $t^2 = v^2 - w^2$, $x = v^2 + w^2$ dla względnie pierwszych liczb naturalnych v i w. Ponadto $v = c^2$ i $w = d^2$ i $c^4 = t^2 + d^4$, przy czym $c < x$, co prowadzi do sprzeczności. Podobnie dochodzimy do sprzeczności przy założeniu, że b jest liczbą parzystą.

24. Jeśli $f(0) = 0$, to teza jest oczywista. Przypuśćmy zatem, że $a = f(0) \neq 0$ i niech $p_1, \ldots, p_k$ będą wszystkimi liczbami pierwszymi p, dla których istnieją rozwiązania kongruencji $f(x) \equiv 0 \pmod{p}$. Niech $m := p_1 \cdots p_k$ i $g(x) := \frac{f(amx)}{a}$. Jeśli istnieje rozwiązanie kongruencji $g(x) \equiv 0 \pmod{p}$ dla pewnej liczby pierwszej p, to $p = p_i$ dla pewnego i. Z drugiej strony $g(x) \equiv 1 \pmod{p_i}$ dla wszystkich $x \in \mathbb{Z}$ i $i = 1, \ldots, k$, skąd wynika, że wielomian g przyjmuje jedynie wartości -1 i 1, co jest niemożliwe.

25. Niech $f(x) := 1 + x + \cdots + x^{q-1}$. Przypuśćmy, że p jest taką liczbą pierwszą, że istnieje liczba całkowita x taka, że $p \mid f(x)$. Jeśli $x \equiv 1 \pmod{p}$, to $p = q$, zaś w przeciwnym wypadku otrzymujemy, że $x^q \equiv 1 \pmod{p}$, więc $q \mid p - 1$, gdyż $x^{p-1} \equiv 1 \pmod{p}$ i q jest liczbą pierwszą. To kończy rozwiązanie na mocy zadania 24.

26. Udowodnienie wzoru $F_m = F_1 \cdots F_{m-1} + 2$ jest prostym ćwiczeniem na indukcję matematyczną. Niech p będzie dzielnikiem pierwszym liczby $2^{2^n} + 1$. Wtedy $2^{2^{n+1}} \equiv 1 \pmod{p}$. Niech l będzie najmniejszą liczbą całkowitą dodatnią taką, że $2^l \equiv 1 \pmod{p}$. Wtedy $l \mid 2^{n+1}$, więc $l = 2^m$ dla pewnej liczby całkowitej dodatniej $m \leq n + 1$. Gdyby $m \leq n$, to $2^{2^n} \equiv 1 \pmod{p}$, co jest sprzeczne z założeniem, że $p \mid 2^{2^n} + 1$. Stąd $l = 2^{n+1}$. Ponieważ z twierdzenia Eulera $2^{p-1} \equiv 1 \pmod{p}$, wynika stąd, że $2^{n+1} \mid p - 1$, co kończy dowód.

2.2 Kongruencje

27. Zauważmy, że $10^2 \equiv 9 \pmod{13}$. Stąd $10^3 \equiv -1 \pmod{13}$, a więc $10^6 \equiv 1 \pmod{13}$.

28. Podobnie jak zadanie 27.

29. Podobnie jak zadanie 27.

30. Ponieważ $3 \nmid n$, więc $n^2 \equiv 1 \pmod 3$ i $n^4 \equiv 1 \pmod 3$, skąd $n^4 + n^2 + 1 \equiv 0 \pmod 3$.

31. Ponieważ $2^2 \equiv 1 \pmod 3$, więc $2^{2n} \equiv 1 \pmod 3$.

32. Wiadomo, że $\sum_{j=1}^{n-1} j = n\frac{n-1}{2}$, zatem $n \mid \sum_{j=1}^{n-1} j$ wtedy i tylko wtedy, gdy $2 \mid n-1$.

33. Wiadomo, że $\sum_{j=1}^{n-1} j^3 = n\frac{n(n-1)^2}{4}$, zatem $n \mid \sum_{j=1}^{n-1} j^3$ wtedy i tylko wtedy, gdy $4 \mid n(n-1)^2$. To jest możliwe tylko, gdy $4 \mid n$ lub $2 \mid n-1$.

34. (a)**.** Wykorzystując algorytm Euklidesa wiemy, że $(3,7) = 1 = 7 - 2 \cdot 3$. Stąd mnożąc stronami wyjściową kongruencję przez -2 otrzymujemy, że $-6x \equiv -8 \pmod 7$. Ponieważ $-6 \equiv 1 \pmod 7$ oraz $-8 \equiv 6 \pmod 7$, więc ostatecznie mamy $x \equiv 6 \pmod 7$.

34. (b)**.** $x \equiv 219 \pmod{256}$.

34. (c)**.** $x \equiv 8 \pmod{21}$.

34. (d)**.** Ponieważ $(10,35) = 5 \mid 15$, więc kongruencja posiada rozwiązanie, które znajdujemy rozwiązując kongruencję $2x \equiv 3 \pmod 7$. Zatem $x \equiv 5 \pmod 7$ (tzn. $x \equiv 5, 12, 19, 26, 33 \pmod{35}$).

34. (e)**.** Ponieważ $(18,3) = 3 \nmid 7$, więc kongruencja nie posiada rozwiązania.

35. (a)**.** Mamy $m_1 := 4$, $m_2 := 7$, $m_3 := 9$, $m := 4 \cdot 7 \cdot 9 = 252$, $n_1 := 7 \cdot 9 = 63$, $n_2 := 4 \cdot 9 = 36$ i $n_3 := 4 \cdot 7 = 28$. Wykorzystując algorytm Euklidesa szukamy liczby e_1 spełniającej warunki $e_1 \equiv 1 \pmod 4$ i $e_1 \equiv 0 \pmod{63}$. Ponieważ $(4,63) = 1 = 16 \cdot 4 - 63$, wiec przyjmujemy $e_1 := -63$. Podobnie wyliczamy $e_2 := 36$ i $e_3 := 28$. Wtedy mamy rozwiązanie postaci $x \equiv 3e_1 + 2e_2 + e_3 \pmod{252}$, skąd wynika, że $x \equiv 163 \pmod{252}$.

35. (b)**.** $x \equiv 713 \pmod{1320}$.

35. (c)**.** Rozważany układ kongruencji można sprowadzić do układu $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$ i $x \equiv 5 \pmod 7$, którego rozwiązaniem są $x \equiv 47 \pmod{84}$.

36. Rozwiązanie tego zadania polega na znalezieniu najmniejszego rozwiązania układu kongruencji $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$, $x \equiv 5 \pmod 6$ i $x \equiv 0 \pmod 7$, skąd wynika, że $n = 119$.

2.3 Funkcja Eulera

37. $\varphi(1000) = \varphi(2^3 \cdot 5^3) = (2-1) \cdot 2^2 \cdot (5-1) \cdot 5^2 = 400$, $\varphi(125) = 100$, $\varphi(180) = 48$, $\varphi(360) = 96$ i $\varphi(1001) = 720$.

38. (a)**.** $x \in \emptyset$.

38. (b)**.** $x = 15, 16, 20, 24, 30$.

38. (c)**.** $x = 13, 21, 26, 28, 36, 42$.

39. Wzór ten jest bezpośrednią konsekwencją wzoru na funkcję Eulera.

40. Jeśli istnieje liczba pierwsza $p > 2$, która dzieli n, to $\varphi(n)$ jest podzielne przez $p-1$, które jest liczbą parzystą. W przeciwnym wypadku $n = 2^m$ i $\varphi(n) = 2^{m-1}$, przy czym $m > 1$.

41. Mamy $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\gamma_1} \cdots q_s^{\gamma_s}$ oraz $n = p_1^{\beta_1} \cdots p_k^{\beta_k} q_{s+1}^{\gamma_{s+1}} \cdots q_{s+r}^{\gamma_{s+r}}$, gdzie $k, r, s \geq 0$, $p_1, \ldots, p_k$, $q_1, \ldots, q_{r+s}$ są parami różnymi liczbami pierwszymi oraz $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_k$, $\gamma_1, \ldots, \gamma_{r+s}$ są dodatnimi liczbami naturalnymi. Ponieważ $d = p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)}$, więc teza jest konsekwencją wzoru na funkcję Eulera.

42. Niech $d = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ będzie przedstawieniem liczby d w postaci iloczynu potęg parami różnych liczb pierwszych. Wtedy $n = p_1^{\beta_1} \cdots p_k^{\beta_k} m$, gdzie $\beta_i \geq \alpha_i$ oraz $p_i \nmid m$ dla $i = 1, \ldots, k$. Zatem $\varphi(n) = \varphi(p_1^{\beta_1} \cdots p_k^{\beta_k})\varphi(m) = \varphi(d) p_1^{\beta_1 - \alpha_1} \cdot p_k^{\beta_k - \alpha_k} \varphi(m)$.

43. Na mocy twierdzenia Eulera $a^6 \equiv 1 \pmod 7$. Podnosząc tę nierówność stronami do kwadratu otrzymujemy tezę.

44. Kongruencja $a^{12} \equiv 1 \pmod{65}$ zachodzi wtedy i tylko wtedy, gdy zachodzą kongruencje $a^{12} \equiv 1 \pmod 5$ i $a^{12} \equiv 1 \pmod{13}$. Korzystając z warunku $(a, 65) = 1$ wnioskujemy, że $(a, 5) = 1$ i $(a, 13) = 1$. Z twierdzenia Eulera wynika, że $a^{12} \equiv 1 \pmod{13}$ i $a^4 \equiv 1 \pmod 5$. Podnosząc drugą z kongruencji stronami do trzeciej potęgi otrzymujemy, że $a^{12} \equiv 1 \pmod 5$, co kończy rozwiązanie.

45. Ponieważ n jest najmniejszą potęgą naturalną k, dla której $a^k \equiv 1 \pmod{(a^n - 1)}$ oraz $a^{\varphi(a^n-1)} \equiv 1 \pmod{(a^n - 1)}$ na mocy twierdzenia Eulera, więc $n \mid \varphi(a^n - 1)$.

46. Przypuśćmy, że n jest najmniejszą liczbą naturalną $n > 1$ taką, że $n \mid 2^n - 1$. Oczywiście $n \mid 2^{\varphi(n)} - 1$. Zatem jeśli $d = (n, \varphi(n))$, to wykorzystując zadanie 3 otrzymujemy, że $n \mid 2^d - 1$. Ponieważ $n > 1$, więc oznacza to w szczególności, że $d > 1$. Ale, to przeczy minimalności liczby n, gdyż $d \mid 2^d - 1$.

47. Poszczególne czynniki występujące po prawej stronie można interpretować jako prawdopodobieństwo, że losowo wybrana liczba spośród liczb $1, \ldots, n$ nie jest podzielna przez p.

48. Z twierdzenia Eulera $3^{40} \equiv 1 \pmod{100}$, więc dwie ostatnie cyfry liczby 3^{1000} to 01.

49. Z twierdzenia Eulera wynika, że $2^{1000} \equiv 1 \pmod{25}$. Oczywiście mamy, też $2^{1000} \equiv 0 \pmod{4}$. Rozwiązując układ kongruencji $x \equiv 1 \pmod{25}$ i $x \equiv 0 \pmod{4}$ otrzymujemy, że $2^{1000} \equiv 76 \pmod{100}$.

50. 5293.

2.4 Elementy teorii pierścieni

51. (a)**.** Nie, gdyż nie jest to zbiór zamknięty ze względu na odejmowanie.

51. (b)**.** Nie, gdyż 1 nie należy do tego zbioru.

51. (c)**.** Tak.

51. (d)**.** Tak.

51. (e)**.** Nie, gdyż nie jest to zbiór zamknięty ze względu na mnożenie.

52. (a)**.** Tak.

52. (b)**.** Tak.

52. (c)**.** Tak. Jedynką w tym pierścieniu jest funkcja f równa 1 dla argumentów równych od $\frac{1}{2}$ i równa 0 dla $\frac{1}{2}$ należy do tego zbioru.

52. (d)**.** Tak.

52. (e)**.** Nie, gdyż nie jest to zbiór zamknięty ze względu na dodawanie funkcji.

53. Niech R będzie skończonym pierścieniem bez dzielników zera. Trzeba pokazać, że dla każdego elementu $a \in R$, $a \neq 0$, istnieje element $b \in R$ o własności $ab = 1$. Ustalmy $a \in R$, $a \neq 0$. Rozważmy funkcję $f : R \to R$ daną wzorem $f(x) = ax$ dla $x \in R$. Wtedy funkcja f jest różnowartościowa. Istotnie, jeśli $f(x_1) = f(x_2)$ dla $x_1, x_2 \in R$, to $a(x_1 - x_2) = ax_1 - ax_2 = f(x_1) - f(x_2) = 0$. Ponieważ w pierścieniu R nie ma dzielników zera i $a \neq 0$, więc $x_1 - x_2 = 0$, co oznacza, że $x_1 = x_2$ i kończy dowód różnowartościowości funkcji f. Wykorzystując założenie, że pierścień R jest skończony, oraz fakt, że każda funkcja różnowartościowa na zbiorze skończonym jest funkcją „na", wnioskujemy, że funkcja f jest „na". W szczególności istnieje element $b \in R$ taki, że $f(b) = 1$, tzn. $ab = 1$.

54. Wiemy, że $f = q(X-1)(X-2) + h$ dla pewnych wielomianów $q, h \in \mathbb{R}[X]$, przy czym $h = aX + b$ dla $a, b \in \mathbb{R}$. Wykorzystując założenia wiemy, że $h(1) = f(1) = 2$ i $h(2) = f(2) = 1$, skąd otrzymujemy układ równań

$$\begin{cases} a + b = 2 \\ 2a + b = 1. \end{cases}$$

Rozwiązując powyższy układ równań dostajemy $a = -1$ i $b = 3$, zatem reszta z dzielenia wielomianu f przez $(X-1)(X-2)$ jest równa $-X + 3$.

55. (a)**.** $d = 1$, $u = 1$, $v = -X^2$.

55. (b)**.** $d = X - 1$, $u = -\frac{1}{4}X + \frac{1}{4}$, $v = \frac{1}{4}X^2 - X + 1$.

55. (c)**.** $d = X^2 - 2$, $u = -X - 1$, $v = X + 2$.

56. Znalezienie odwrotności do warstwy wielomianu $1+X^2$ w $\mathbb{R}[X]/(X^3)$ jest równoważne znalezieniu wielomianu $f \in \mathbb{R}[X]$ spełniającego warunek $f(1 + X^2) = 1 \pmod{X^3}$. Korzystając z algorytmu Euklidesa otrzymujemy, że $(1 + X^2, X^3) = 1$ oraz

$$1 = (1 - X^2)(1 + X^2) + X \cdot X^3,$$

a więc możemy przyjąć $f = 1 - X^2$. Zatem odwrotnością do warstwy wielomianu $1 + X^2$ w $\mathbb{R}[X]/(X^3)$ jest warstwa wielomianu $1 - X^2$.

2.5 Ciała skończone

57. $\mathbb{F}_2$: X, $X + 1$, $X^2 + X + 1$, $X^3 + X + 1$, $X^3 + X^2 + 1$, $X^4 + X + 1$, $X^4 + X^3 + 1$, $X^4 + x^3 + X^2 + X + 1$.

$\mathbb{F}_3$: X, $X+1$, $X+2$, X^2+1, X^2+X+2, X^2+2X+2, X^3+2X+1, X^3+2X+2, X^3+X^2+2, X^3+X^2+X+2, X^3+X^2+2X+1, X^3+2X^2+1, X^3+2X^2+X+1, X^3+2X^2+2X+2, X^4+X+2, X^4+2X+2, X^4+X^2+2, X^4+X^2+2X+1, X^4+2X^2+2, X^4+X^3+2, X^4+X^3+2X+1, $X^4+X^3+X^2+1$, $X^4+X^3+X^2+X+1$, $X^4+X^3+X^2+2X+2$, $X^4+X^3+2X^2+2X+2$, X^4+2X^3+2, X^4+2X^3+X+1, $X^4+2X^3+X^2+1$, $X^4+2X^3+X^2+X+2$, $X^4+2X^3+X^2+2X+1$, $X^4+2X^3+2X^2+X+2$.

58. (a). $X^{16}-X = X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1)$.

58. (b). $X^9-X = X(X+1)(X+2)(X^2+1)(X^2+X+2)(X^2+2X+2)$.

58. (c). $X^{27}-X = X(X+1)(X+2)(X^3+2X+1)(X^3+2X+2)(X^3+X^2+2)(X^3+X^2+X+2)(X^3+X^2+2X+1)(X^3+2X^2+1)(X^3+2X^2+X+1)(X^3+2X^2+2X+2)$.

59. Jeśli $k_{n,p}$ oznacza liczbę unormowanych wielomianów nierozkładalnych stopnia n nad ciałem $\mathbb{F}_p$, to korzystając ze wzoru inwersyjnego Möbiusa mamy $k_{n,p} = \frac{1}{n}\sum_{d|p}\mu(d)p^{\frac{n}{d}}$, gdzie μ jest funkcją Möbiusa. Stąd $k_{1,2}=2$, $k_{2,2}=1$, $k_{3,2}=2$, $k_{4,2}=3$, $k_{5,2}=6$, $k_{6,2}=9$, $k_{7,2}=18$, $k_{8,2}=30$, $k_{1,3}=3$, $k_{2,3}=3$, $k_{3,3}=8$, $k_{4,3}=18$, $k_{5,3}=48$, $k_{6,3}=116$, $k_{7,3}=312$, $k_{8,3}=810$.

60. (a). $(f,f') = X^4+X^2+1 = (X^2+X+1)^2$, więc $f = (X^2+X+1)^2(X^3+X+1)$.

60. (b). $(f,f') = X^6+1 = (X^2+1)^3$, więc $f = (X^2+1)^2(X^2+X+2)$.

60. (c). $(f,f') = X^4+4X^2+4 = (X^2+2)^2$, więc $f = (X^2+2)^3(X^3+X+1)$.

61. (a). Nie, gdyż $(f,f') \neq 1$.

61. (b). Tak, gdyż $(f,f') = 1$.

61. (c). Tak, gdyż $(f,f') = 1$.

62. (a). Ponieważ wielomian x^2+1 nie posiada pierwiastków w ciele $\mathbb{F}_3$, więc $\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+1)$. Oznaczmy przez α warstwę wielomianu X w ciele $\mathbb{F}_9$. Wtedy pierwiastkami wielomianu f są α i 2α.

62. (b). Pierwiastkami wielomianu f są α i $2+2\alpha$, gdzie α jest warstwą wielomianu X w ciele $\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+X+2)$.

62. (c)**.** Pierwiastkami wielomianu f są α i $3+4\alpha$, gdzie α jest warstwą wielomianu X w ciele $\mathbb{F}_{25} := \mathbb{F}_5[X]/(X^2+2X+3)$.

63. Ponieważ $\alpha \notin \mathbb{F}_p$, więc $\alpha^p \neq \alpha$. Z drugiej strony $a^p = a$ i $b^p = b$. Stąd $(\alpha^p)^2 + \alpha^p a + b = (\alpha^2)^p + (\alpha a)^p + b^p = (\alpha^2 + \alpha a + b)^p = 0$, a więc α^p jest drugim pierwiastkiem wielomianu $X^2 + aX + b$, zatem $\alpha + \alpha^p = -a$ i $\alpha^{p+1} = b$. Z powyższych równości wynika, że $(c\alpha+d)^p(c\alpha+d) = (c\alpha^p+d)(c\alpha+d) = c^2\alpha^{p+1} + cd(\alpha^p+\alpha) + d^2 = c^2b - cda + d^2$, co było do udowodnienia. $(2+3i)^{101} = ((2+3i)^{20})^5(2+3i) = 9+4i$.

64. Jeśli $f = g^p$, to $f' = pg^{p-1}g' = 0$. Z drugiej strony, gdy $f = \sum_i a_i X^i$ oraz $f' = 0$, to $a_i \neq 0$ tylko, gdy $p \mid i$. Ponieważ $a^p = a$ dla $a \in \mathbb{F}_p$, więc otrzymujemy w ten sposób, że $f = \sum_j a_{pj}^p X^{pj} = (\sum_j a_{pj} X^j)^p$, co kończy dowód.

2.6 Elementy teorii grup

65. (a)**.** Nie, gdyż nie jest to zbiór zamknięty ze względu na odejmowanie.

65. (b)**.** Tak.

65. (c)**.** Tak.

65. (d)**.** Tak.

65. (e)**.** Nie, gdyż nie jest to zbiór zamknięty ze względu na dodawanie.

66. (a)**.** Nie, gdyż nie istnieje element odwrotny do 0.

66. (b)**.** Tak.

66. (c)**.** Tak.

66. (d)**.** Nie, gdyż nie istnieją liczby całkowite odwrotne do liczb całkowitych różnych od 1 i -1.

66. (e)**.** Tak.

67. $\mathbb{F}_7^*$: $r(1) = 1$, $r(2) = r(4) = r(6) = 2$, $r(3) = r(5) = 6$.
$\mathbb{F}_8^* := \mathbb{F}_2[X]/(X^3+X+1)$, $\alpha :=$ warstwa X: $r(1) = 1$, $r(\alpha) = r(\alpha+1) = r(\alpha^2) = r(\alpha^2+1) = r(\alpha^2+\alpha) = r(\alpha^2+\alpha+1) = 7$.
$\mathbb{F}_9^* := \mathbb{F}_3[X]/(X^2+1)$, $\alpha :=$ warstwa X: $r(1) = 1$, $r(2) = 2$, $r(\alpha) = r(2\alpha) = 4$, $r(\alpha+1) = r(\alpha+2) = r(2\alpha+1) = r(2\alpha+2) = 8$.

68. (a)**.** Ilość generatorów grupy $\mathbb{F}_q^*$ jest równa $\varphi(q-1)$, zatem ilość generatorów grupy $\mathbb{F}_9^*$ jest równa 4. α nie jest generatorem grupy $\mathbb{F}_9^*$, bo $\alpha^4 = 1$, zaś $\alpha+1$, $2\alpha+1$ są generatorami grupy $\mathbb{F}_9^*$. $2^{-1} = 2$.

68. (b)**.** $\varphi(24) = 8$, α, $\alpha+1$ – nie, gdyż $\alpha^8 = 1$ i $(\alpha+1)^{12} = 1$, $2\alpha+1$ – tak. $(2+3\alpha)^{-1} = \frac{1}{2-3\alpha}(2+3\alpha)(2-3\alpha) = 2-3\alpha$.

68. (c)**.** $\varphi(48) = 16$, α, $2\alpha+1$ – nie, gdyż $\alpha^6 = 1$ i $(2\alpha+1)^{24} = 1$, $\alpha+1$ – tak. $(2+3\alpha)^{-1} = 2-3\alpha$.

69. $\varphi(15) = 10$, $(\alpha+1)^3 = \alpha^3+\alpha^2+\alpha+1$ i $(\alpha+1)^5 = \alpha^2+\alpha$, $\alpha = (\alpha+1)^4$, $\alpha^{-1} = (\alpha+1)^{15-4} = (\alpha+1)^{4\cdot 2}(\alpha+1)^3 = \alpha^3+1$.

70. $p = 2$ i $2^k - 1$ liczba pierwsza.

71. $p = 2$ i $2^k - 1$ liczba pierwsza lub $p = 3$ i $\frac{3^p-1}{2}$ liczba pierwsza.

72. $(\mathbb{Z}/8\mathbb{Z})^*$: $r(1) = 1$, $r(3) = r(5) = r(7) = 2$.
$(\mathbb{Z}/15\mathbb{Z})^*$: $r(1) = 1$, $r(4) = r(11) = r(14) = 2$, $r(2) = r(7) = r(8) = r(13) = 4$.
$(\mathbb{Z}/16\mathbb{Z})^*$: $r(1) = 1$, $r(7) = r(9) = r(15) = 2$, $r(3) = r(5) = r(11) = r(13) = 4$.

73. Bez straty ogólności możemy założyć, że $k \geq 2$. Niech a będzie generatorem grupy $\mathbb{F}_p^*$. Przypuśćmy, że $a^{p-1} \equiv 1 \pmod{p^2}$. Wtedy $((p+1)a)^{p-1} \not\equiv 1 \pmod{p^2}$. Zatem istnieje element $b \in (\mathbb{Z}/p^k\mathbb{Z})^*$ o własności $b^{p-1} \not\equiv 1 \pmod{p^2}$. Ponadto $b^{p-1} \not\equiv 1 \pmod{p}$, więc istnieje liczba całkowita c taka, że $b^{p-1} = 1+cp$, przy czym $(c,p) = 1$.

Gdy $b^i \equiv 1 \pmod{p^k}$, to $p-1 \mid i$, gdyż $a \equiv b \pmod{p}$ i a jest generatorem grupy $\mathbb{F}_p^*$. Stąd $i = (p-1)j$ dla pewnego j. Wtedy $(1+cp)^j \equiv 1 \pmod{p^k}$. Niech p^l będzie największą potęgą liczby p dzielącą j. Gdyby $l+2 \leq k$, to $(1+cp)^j \equiv 1 \pmod{p^{l+2}}$. Z drugiej strony $p^{l+2} \mid \binom{j}{m}p^m$ dla $m \geq 2$, skąd $(1+cp)^j \equiv cdp^{l+1}+1 \pmod{p^{l+2}}$, gdzie d jest ilorazem z dzielenia i przez p^l. Ponieważ $(cd,p) = 1$, więc prowadzi to do wniosku, że $p^{l+2} \mid p^{l+1}$, a więc do sprzeczności. Zatem $l+2 > k$, czyli $p^{k-1} \mid j$. Ostatecznie $(p-1)p^{k-1} \mid i$, co kończy dowód.

74. $\langle 6\rangle = \langle (6,15)\rangle = \langle 3\rangle = \{0,3,6,9,12\}$.
$\langle 10\rangle = \langle (10,15)\rangle = \langle 5\rangle = \{0,5,10\}$.
$\langle 6,10\rangle = \langle (6,10,15)\rangle = \langle 1\rangle = \mathbb{Z}/15\mathbb{Z}$.

2.7 Elementy teorii kodowania

75. (b). Niech $C \subset \mathbb{F}_2^n$ będzie kodem o odległości minimalnej nie mniejszej niż d. Definiujemy kod $C' \subset \mathbb{F}_2^{n+d}$ następującym wzorem $C' = C \times \{(0,\ldots,0),(1,\ldots,1)\}$. Wtedy $|C'| = 2|C|$ oraz $d_{\min}(C') =| (d_{\min}(C), d) = d$.

75. (c). Niech $C \subset \mathbb{F}_2^n$ będzie kodem o odległości minimalnej nie mniejszej niż d. Definiujemy kod $C' \subset \mathbb{F}_2^{2n}$ wzorem $C' := C \times C$. Wtedy $|C| = |C'|^2$ oraz $d_{\min}(C) = d_{\min}(C') \geq d$.

75. (d). Niech $C \subset \mathbb{F}_2^n$ będzie kodem o odległości minimalnej nie mniejszej niż d. Definiujemy kody $C_1, C_2 \subset \mathbb{F}_2^{n-1}$ wzorami $C_1 := \{w \in \mathbb{F}_2^{n-1} \mid (w,0) \in C$ oraz $C_2 := \{w \in \mathbb{F}_2^{n-1} \mid (w,1) \in C\}$. Wtedy $d_{\min}(C_1), d_{\min}(C_2) \geq d$ oraz $\min(|C_1|,|C_2|) \geq \frac{|C|}{2}$.

75. (e). Niech $C \subset \mathbb{F}_2^n$ będzie kodem o odległości minimalnej nie mniejszej niż d. Dla każdego ciągu $w \in C$ określamy zbiór $B_w(k)$ wzorem $B_w(k) := \{v \in \mathbb{F}_2^n \mid d(w,v) \leq k\}$. Wtedy $|B_w(k)| = \sum_{i=0}^{k} \binom{k}{i}$ dla każdego $w \in C$ oraz $B_{w_1}(k) \cap B_{w_2}(k) = \emptyset$ dla $w_1 \neq w_2$. Stąd $(\sum_{i=0}^{k} \binom{n}{i})|C| \leq 2^n$, co kończy dowód.

76. Przypuśćmy, że $d = (d_1,\ldots,d_{10})$ jest poprawnym kodem ISBN. Pokażemy, że wtedy $d' = (d_1,\ldots,d_{i-1},d_{i+1},d_i,d_{i+2},\ldots,d_{10})$ jest poprawnym kodem ISBN wtedy i tylko wtedy, gdy $d_{i+1} = d_i$. Mamy $n := 1 \cdot d_1 + \cdots + (i-1)d_{i-1} + id_{i+1} + (i+1)d_{i-1} + (i+2)d_{i+2} + \cdots + 10d_{10} = 1 \cdot d_1 + \cdots 10d_{10} + d_{i+1} - d_i \equiv d_{i+1} - d_i \pmod{11}$. Zatem $n \equiv 0 \pmod{11}$ wtedy i tylko wtedy, gdy $d_i = d_{i+1}$, gdyż $d_i, d_{i+1} \in \{0,\ldots,10\}$.

77. $d_{\min}(C) = 3$.

77. (a). $Hv^{\mathrm{T}} = 0$, więc wysłano v.

77. (b). $Hv^{\mathrm{T}} = 0$, więc wysłano v.

77. (c). $Hv^{\mathrm{T}} = (1,0,0,0)^{\mathrm{T}}$, który jest 5. kolumną macierzy H, a więc błąd wystąpił na 5. miejscu, zatem wysłano $(0,0,0,1,0,1,0,1)$.

77. (d). $Hv^{\mathrm{T}} = (0,1,0,1)^{\mathrm{T}}$, a więc wysłano $(0,1,1,0,1,1,1,1)$.

77. (e). $Hv^{\mathrm{T}} = (1,0,1,0)^{\mathrm{T}}$, a więc wysłano $(0,0,1,1,1,1,0,0)$.

78. $d_{\min}(C) = 3$.

79. $d_{\min}(C) = 5$.

80. $d_{\min}(C) = 3$. Baza liniową kodu C są wektory: $(1,0,0,0,2,0,2,1)$, $(0,1,0,0,0,2,2,0)$, $(0,0,1,0,2,0,2,2)$ i $(0,0,0,1,0,0,2,2)$.

81. (a)**.** $X^5 - 1 = (X+1)(X^4 + X^3 + X^2 + X + 1)$, więc mamy 2 nietrywialne kody cykliczne długości 5 nad $\mathbb{F}_2$ o następujących macierzach kontroli parzystości:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

81. (b)**.** $X^9-1 = (X+1)(X^2+X+1)(X^6+X^3+1)$, więc mamy 6 nietrywialnych kodów cyklicznych długości 9 nad $\mathbb{F}_2$ o następujących macierzach kontroli parzystości:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

81. (c)**.** $X^8 - 1 = (X+1)(X+2)(X^2+1)(X^2+X+2)(X^2+2X+2)$, więc mamy 30 nietrywialnych kodów cyklicznych długości 9 nad $\mathbb{F}_2$ o następujących macierzach kontroli parzystości:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 0 & 2 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 2 & 2 & 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 2 & 2 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 & 2 & 2 & 1 & 2 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 & 0 & 1 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 2 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 1 & 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 2 & 1 & 1 & 0 & 2 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \end{bmatrix}.$$