Wersja z 2022/06/01 o 09:17:06 (E5E335C79A7495544903454955A99270)

1 Magiczne liczby

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, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719

2 Grafy

- Lem. o uściskach dł.: $\sum_{v \in V} deg(v) = 2|E|$;
- H podgrafem indukowanym $G \iff \forall_{u,v \in V[H]} \{ u, v \} \in E[G] \implies \{ u, v \} \in E[H]$;
- Droga nie powtarza krawędzi, a ścieżka wierzchołków;
- G spójny $\iff \forall_{u,v \in V[G]} \exists e_{uv}$;
- G k-reguralny $\iff \forall_v deg(v) = k$;
- G dwudzielny, gdy $V[G] = V_1 \cup V_2, V_1 \cap V_2 = \emptyset$ i każda krawędź ma jeden koniec w V_1, a drugi w V_2;
- $K_{|V|,|U|}$ pełny dwudzielny, gdy $E = \{ \{ v, u \}, v \in V, u \in U \}$;
- v rozcinający, gdy usunięcie v zwiększa l. spójnych s.;
- Tw.: G dwudzielny $\iff$ nie zawiera cykli nieparz. dł.;

2.1 Cykle

- C. E. — krawędzie; C. H. — wierzchołki; Graf h. — graf z c. H.;
- Tw. Eulera: G ma c. E. $\iff \forall_{v \in V[G]} 2|deg(v)$;
- Tw.: Silnie spójny G ma skierowany c. E. $\iff \forall_{v \in V[G]} deg_{in}(v) = deg_{out}(v)$;
- G ma c. H., to po usunięciu dow. k wierz. rozpada się na co najw. k spójnych s.;
- $G = \langle V, U; E \rangle$ dwudzielny ma c. H., to $|V| = |U|$;
- Tw.: Każdy turniej jest półhamilton. (zawiera ś. H.);
- Tw.: Turniej ma c. H. $\iff$ jest silnie spójny;
- Tw.: Turniej spójny, to ma c. H.;
- Tw. (Ore): $n = |V| \geqslant 3$ i $\forall_{\{ v,w \} \notin E} deg(v) + deg(w) \geqslant n$, to G ma c. H.;
- Każdy turniej hamiltonowski jest silnie spójny;
- G silnie spójny $\Rightarrow$ G zawiera skierowany k-cykl;

2.2 Drzewa

- Tw. (Cayley): Jest n^{n-2} etykietowanych drzew n-wierzchołkowych;
- Równoważne są:

G jest drzewem,
każde dwa wierzchołki w G są połączone dokładnie jedną droga,
G jest minimalny spójny,
G jest maksymalny acykliczny,
G jest spójny i $|V| = |E| + 1$

2.3 Planarność

- Wz. Eulera: $n - m + f = 2$, gdzie $m = |E[G]|$;
- Tw.: W grafie plan. z $n \geqslant 3$ mamy $m \leqslant 3n - 6$;
- Mocjiejszym twierdzeniem jest gdy graf nie zawiera trójkątów $m \leqslant 2n - 3$;
- Tw. Kuratowskiego: G nieplan. $\iff$ G zawiera podgraf homeomorficzny z $K_{3,3}$ lub z K_5 (homeomorficzny, czyli izomorficzny po ew. dołożeniu wierzchołków na krawędziach);
- G planarny $\implies \exists_{v \in G[V]} deg(v) \leqslant 5$;

2.4 Kolorowanie wierzchołków

- Kolorowanie G za pomocą k kolorów to $f : V[G] \to \{ 1, \ldots, k \}$ t., że $f(u) \neq f(v)$ dla $\{ u, v \} \in E[G]$. Najm. k t., że $\exists k$-kolorowanie G to liczba chromatyczna $\chi(G)$.
- $\chi(G) \leqslant 2 \Leftrightarrow G$ dwudzielny;
- $\chi(G) \leqslant k \Leftrightarrow \chi(G) \leqslant k$ dla każdej dwuspójnej s. B grafu G;
- Tw. o 4 barwach: G plan. $\implies \chi(G) \leqslant 4$;
- Tw. Brooksa: G spójny, nie cykl nieparz. dł., nie klika, to $\chi(G) \leqslant \Delta$, gdzie Δ to maks. stop. wierz. w G;
- Tw.: $\chi(G) \leqslant \Delta + 1$;
- $f_G(t)$ — wielomian chrom. (liczba kolorowań G za pomocą t kolorów);
- W. ch.: • K_n — $t^{\underline{n}}$, • $\overline{K_n}$ — t^n, • Drzewo$_n$ — $t(t-1)^{n-1}$, • Cykl$_n$ — $(t-1)^n + (-1)^n(t-1)$, • $K_{n,m}$ — $\sum_{a,b} \left\{ {n \atop a} \right\} \left\{ {m \atop b} \right\} t^{\underline{a+b}}$;
- Tw.: $e = \{ v, w \} \notin E[G]$, to $f_G(t) = f_{G \cup e}(t) + f_{G/e}(t)$;

2.5 Kolorowanie krawędzi

- Funkcja $f : E[G] \to \{ 1, \ldots, k \}$ to kolorowanie krawędziowe, jeśli kraw. incydentne mają różne kolory. Indeks chromatyczny $\chi_e(G)$ to najmniejsze k, dla którego istnieje k-kolorowanie kraw.;
- Tw. Vizinga: $\forall_G \chi_e(G) \leqslant \Delta(G) + 1$;
- Tw. (König): G dwudzielny, to $\chi_e(G) = \Delta(G)$;

2.6 Systemy różnych reprezentantów

- SSR dla rodziny zbiorów $\langle A_i \rangle_{i \in I}$, to ciąg elem. $\langle a_i \rangle_{i \in I}$ t., że $\forall_{i \in I} a_i \in A_i$ oraz $a_i \neq a_j$ (skojarzenia w g. dwudzielnym);
- Tw. (Hall): SRR dla skończonej r. zb. skończonych $\langle A_i \rangle_{i=1}^n$, istnieje $\iff \forall_{J \subseteq \{ 1, \ldots, n \}} |\bigcup_{j \in J} A_j| \geqslant |J|$;
- G dwudzielny r-regularny $\Rightarrow$ r-kolorowalny kraw.;
- G dwudzielny, regularny ma pełne skojarzenie;
- G $(n - m)$-regularny $\Rightarrow \exists$ pełne skojarzenie;
- Tw.: Podziały $\mathcal{A}$ i $\mathcal{B}$ mają wspólny SRR $\Leftrightarrow \forall_{J \subseteq I} |\bigcup_{j \in J} g(A_j)| \geqslant |J|$, gdzie $g(C) = \{ j \mid C \cap B_j \neq \emptyset \}$;
- $A_1 \cup \cdots \cup A_n = B_1 \cup \cdots \cup B_n$ i $\forall_{1 \leqslant i \leqslant n} |A_i| = |B_i| = r \Rightarrow \mathcal{A}$ i $\mathcal{B}$ mają SRR;

3 Teoria liczb

- $NWD(a, b) = min_+ \{ ax + by \mid x, y \in \mathbb{Z} \}$; • $a \perp b \Leftrightarrow NWD(a, b) = 1$;
- Alg. Euklidesa: $NWD(a, b) = ax + by$. Jeśli $b = 0$, to $\langle x, y \rangle \langle 1, 0 \rangle$, wpp $NWD(a, b) = NWD(b, a \mod b) = bx' + (a \mod b)y'$ ($\langle x, y \rangle \leftarrow \left\langle y', x' - y' \cdot \lfloor a/b \rfloor \right\rangle$);
- $$\begin{array}{cccc} 20 & 56 & 3 & -1 \\ 16 & 20 & -1 & 1 \\ 4 & 16 & 1 & 0 \\ 0 & 4 & 0 & 1 \end{array}$$
- $a = \prod_{i=1}^m p_i$;
- $a|bc \wedge a \perp b \Rightarrow a|c$
- $NWW(a, b) = ab/NWD(a, b) = \prod_{i=1}^k p_i^{max(\alpha_i, \beta_i)}$;
- $a \equiv_n b$ oraz $c \equiv_n d \implies a + c \equiv_n b + d$ oraz $a \cdot c \equiv_n b \cdot d$;
- $d \perp n \wedge ad \equiv bd \pmod{n} \Rightarrow a \equiv b \pmod{n}$;
- $ad \equiv bd \pmod{nd} \Leftrightarrow a \equiv b \pmod{n}$;
- $b = a^{-1} \pmod{n} \Leftrightarrow ab \equiv 1 \pmod{n}$;
- $n \perp m \implies \big(a \equiv b \pmod{n} \wedge a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{nm}\big)$ (uogólnia się na dow. liczbę parami wzgl. pierwszych modułów $n_1, \ldots, n_k$);
- $a \perp n \Rightarrow a^x = a^{x \mod \phi(n)} \mod n$;

- CRT: $n = n_1 \ldots n_k, n_i \perp n_j$, to $\forall_{a_1, \ldots, a_k} \exists a \in \{ 0, \ldots, n-1 \}$ t., że $a \equiv a_i \pmod{n_i}$ dla $i = 1, \ldots, k$;
- 1 $x \equiv_3 2$, $x \equiv_{10} 7$, $x \equiv_{11} 10$, $x \equiv_7 1$; 2 Warunki CRT: $\forall_{n_i, n_j, n_i \neq n_j} NWD(n_i, n_j) = 1$ 3 $n = 3 \cdot 7 \cdot 10 \cdot 11 = 2310$, $m_1 = \frac{2310}{3} = 770$, $m_2 = \ldots = 231$, $m_3 = \ldots = 210$, $m_4 = \ldots = 330$; 4 $m_1^{-1} \mod n_1 = 1$, $\ldots$ oraz $x_1 = m_1(m_1^{-1} \mod n_1)$, $\ldots$ 5 R. alg. Eukl.: $NWD(3, 770) = 1 = 257 \cdot 3 - 1 \cdot 770 \Rightarrow x_1 = -1 \equiv_3 2$, $NWD(10, 231) = \ldots \Rightarrow x_2 = 1$, $NWD(11, 210) = \ldots \Rightarrow x_3 = 1$, $NWD(7, 330) = \ldots \Rightarrow x_4 = 1$; 6 $x = 2 \cdot 2 \cdot 770 + 7 \cdot 1 \cdot 231 + 10 \cdot 1 \cdot 210 + 1 \cdot 1 \cdot 330$;
- Ogólniej: $a^{\phi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}}$, $a^{\phi(p_2^{\alpha_2})} \equiv 1 \pmod{p_2^{\alpha_2}} \Rightarrow a^{NWW(\phi(p_1^{\alpha_1}), \phi(p_2^{\alpha_2}))} \equiv 1 \pmod{n}$, gdzie $n = p_1^{\alpha_1} p_2^{\alpha_2}$;
- $x^{118} \equiv 113 \pmod{1001}$; 1 $x^{118} \equiv_7 1$, $\ldots \equiv_{11} 3$, $\ldots \equiv_{13} 9$ są $\perp$, więc tw. Eulera; 2 $x^2 \equiv_7 1^{-1}$, $x^2 \equiv_{11} 3^{-1}$, $x^2 \equiv_{13} 9^{-1}$ 3 $x^2 \equiv_7 1$, $x^2 \equiv_{11} 4$, $x^2 \equiv_{13} 3$ 4 $x \equiv_7 \pm 1$, $x \equiv_{11} \pm 2$, $x \equiv_{13} \pm 4$ 5 Teraz z CRT: $\ldots$: $c_1 = 5 \cdot 143$, $c_2 = 4 \cdot 91$, $c_3 = 12 \cdot 77$;

- MTF: $p \in \mathbb{P} \wedge p \not| a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$, inaczej $a^p \equiv a \pmod{p}$;
- F. Eulera: $\phi : \mathbb{N} \to \mathbb{N}$ t., że $\phi(n) = |\mathbb{Z}_n^*| = |\{ 1 \leqslant k \leqslant n : k \perp n \}|$;
- $p \in \mathbb{P} \Rightarrow \phi(p^k) = p^k - p^{k-1}$;
- $m \perp n \Rightarrow \phi(mn) = \phi(m)\phi(n)$, np.: $\phi(2016) = \phi(2^3)\phi(3^2)\phi(7) = 2016(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7})$;
- $\phi(n) = n \prod_{\mathbb{P} \ni p | n} (1 - 1/p)$;
- $\sum_{d|m} \phi(d) = m$;
- Tw. Eulera: $a \perp n \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$;
- Tw. Wilsona: $p \in \mathbb{P} \Leftrightarrow (p-1)! \equiv -1 \pmod{p}$;
- Alg. RSA: $n = pq, e, M, e \perp \phi(n)$. Wtedy $E(M) = M^e \mod n$, $d = e^{-1}$

$\bmod \phi(n)$, $D(C) = C^d \mod n$. Działa, bo $(M^e)^d \mod n =$ z tw. Eulera $= M^{ed \mod n} = M^1 \mod n$;

• Test Millera-Rabina: $\exists_{0<a<n} a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow n \notin \mathbb{P}$ (słaby, bo liczby Carmichaela);