Velká čísla

RADEK ERBAN — 6. PROSINCE 2000

Užitečné poznatky z teorie čísel

1) Nechť a, b jsou přirozená čísla, $p_1, \ldots, p_n$ po dvou různá prvočísla a nechť platí

$$a = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdot \ldots \cdot p_n^{q_n}, \qquad b = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdot \ldots \cdot p_n^{r_n},$$

kde $q_1, \ldots, q_n, r_1, \ldots, r_n$ jsou nezáporná celá čísla. Pak:
(a) $a \mid b$ právě tehdy, pokud $q_i \leq r_i$ pro všechna $i = 1, 2, \ldots, n$;
(b) a je k-tou mocninou přirozeného čísla právě tehdy, pokud $k \mid q_i$ pro všechna $i = 1, 2, \ldots, n$;
(c) $(a, b) = p_1^{\min(q_1, r_1)} \cdot p_2^{\min(q_2, r_2)} \cdot p_3^{\min(q_3, r_3)} \cdot \ldots \cdot p_n^{\min(q_n, r_n)}$.

2) Pro přirozené číslo a označíme symbolem $\varphi(a)$ počet čísel z množiny $\{0, 1, 2, \ldots, a-1\}$ nesoudělných s číslem a. Funkce φ, která každému a přiřazuje $\varphi(a)$, se nazývá *Eulerova funkce.* Pokud má přirozené číslo $a \geq 2$ prvočíselný rozklad $a = p_1^{q_1} \cdot p_2^{q_2} \cdot \ldots \cdot p_n^{q_n}$, kde $p_1, \ldots, p_n$ jsou po dvou různá prvočísla a $q_1, \ldots, q_n \in \mathbb{N}$, pak platí

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right).$$

Pro každá dvě nesoudělná čísla $a, b \in \mathbb{N}$ platí $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,

3) Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Řekneme, že *a je kongruentní s b podle modulu m*, a píšeme $a \equiv b \pmod{m}$, pokud $m \mid (b-a)$. V tomto případě se m nazývá modul a číslo b zbytek od a při modulu m. Zápis $a \equiv b \pmod{m}$ nazýváme *kongruencí.* Kongruence splňují:
(a) Pokud $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, pak $a + c \equiv b + d \pmod{m}$ a $ac \equiv bd \pmod{m}$;
(b) Pokud $a \equiv b \pmod{m}$ a $d \mid m$, pak $a \equiv b \pmod{d}$;
(c) Pokud $a \equiv b \pmod{m}$, $a = a_0 d$, $b = b_0 d$ a $(d, m) = 1$, pak $a_0 \equiv b_0 \pmod{m}$.

4) (*Eulerova věta*) Pokud $(a, m) = 1$, pak $a^{\varphi(m)} \equiv 1 \pmod{m}$.

5) (*Malá Fermatova věta*) Je-li p prvočíslo, pak $a^p \equiv a \pmod{p}$.

6) (*Lagrangeova věta*) Nechť f je polynom stupně n proměnné x, p prvočíslo, pak kongruence $f(x) \equiv 0 \pmod{p}$ má maximálně n řešení z množiny $\{0, 1, \ldots, p-1\}$, nebo jsou všechny koeficienty polynomu f kongruentní s nulou podle modulu p.

7) (*Wilsonova věta*) Pokud p je prvočíslo, pak $(p-1)! \equiv -1 \pmod{p}$.

8) Pro každé $n \in \mathbb{N}, n \geq 2$ platí

$$n! = \prod_{p \leq n} p^{q_p}, \quad \text{kde} \qquad q_p = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor$$

pro všechna p (p probíhá prvočísla nepřesahující n).

9) Stirlingův vzorec: $\quad n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$

Tabulka prvních tří set prvočísel

2	101	233	383	547	701	877	1049	1229	1429	1597	1783
3	103	239	389	557	709	881	1051	1231	1433	1601	1787
5	107	241	397	563	719	883	1061	1237	1439	1607	1789
7	109	251	401	569	727	887	1063	1249	1447	1609	1801
11	113	257	409	571	733	907	1069	1259	1451	1613	1811
13	127	263	419	577	739	911	1087	1277	1453	1619	1823
17	131	269	421	587	743	919	1091	1279	1459	1621	1831
19	137	271	431	593	751	929	1093	1283	1471	1627	1847
23	139	277	433	599	757	937	1097	1289	1481	1637	1861
29	149	281	439	601	761	941	1103	1291	1483	1657	1867
31	151	283	443	607	769	947	1109	1297	1487	1663	1871
37	157	293	449	613	773	953	1117	1301	1489	1667	1873
41	163	307	457	617	787	967	1123	1303	1493	1669	1877
43	167	311	461	619	797	971	1129	1307	1499	1693	1879
47	173	313	463	631	809	977	1151	1319	1511	1697	1889
53	179	317	467	641	811	983	1153	1321	1523	1699	1901
59	181	331	479	643	821	991	1163	1327	1531	1709	1907
61	191	337	487	647	823	997	1171	1361	1543	1721	1913
67	193	347	491	653	827	1009	1181	1367	1549	1723	1931
71	197	349	499	659	829	1013	1187	1373	1553	1733	1933
73	199	353	503	661	839	1019	1193	1381	1559	1741	1949
79	211	359	509	673	853	1021	1201	1399	1567	1747	1951
83	223	367	521	677	857	1031	1213	1409	1571	1753	1973
89	227	373	523	683	859	1033	1217	1423	1579	1759	1979
97	229	379	541	691	863	1039	1223	1427	1583	1777	1987

Příklady

1. příklad Dokažte, číslo $53^{103} + 103^{53}$ je dělitelné číslem 78.

2. příklad Seřaďte podle velikosti čísla: $\left(11^{11}\right)!$, $\quad (11!)^{11^{11}}$, $\quad (11!)^{(11!)}$, $\quad (11^{11})^{(11^{11})}$.

3. příklad Dokažte, že rovnice $10^{10^{10}}x^2 + 11^{11^{11}}x - 9^{9^9} = 0$ má dva různé reálné iracionální kořeny.

4. příklad Ukažte, že číslo

$$77777777^{7777^{77^{7}}} + 1$$

má alespoň miliardu prvočíselných dělitelů.

5. příklad Porovnejte čísla A_n a B_n (v závislosti na n), kde

$$A_n = \left. 2^{3^{2^{\cdot^{\cdot^{\cdot}}}}} \right\} n \text{ pater}, \qquad B_n = \left. 3^{2^{3^{\cdot^{\cdot^{\cdot}}}}} \right\} n \text{ pater}.$$

6. příklad Najděte všechna přirozená čísla n, pro která platí vztah: $1995!n^{666n} > 1995^{1995}$.

7. příklad Určete poslední číslici čísla $7^{4567890}$.

8. příklad Které z čísel

$$\varphi\left(10^{10^{10}}\right), \qquad \varphi\left(10^{10^{10}} + 1\right)$$

je větší? Písmenem φ označujeme Eulerovu funkci.

9. příklad Ukažte, že číslo $3^{105} + 4^{105}$ je dělitelné čísly 13, 49, 181 a 379, ale není dělitelné pěti ani jedenácti.

10. příklad Určete poslední číslici čísla $(3 + \sqrt{7})^{k_{1995}}$ před desetinnou čárkou, kde $k_1 = 1995$ a platí rekurentní vztah $k_{i+1} = 1995^{k_i}$.

11. příklad Kolik z čísel 9^k, kde $k = 1, 2, \ldots 4000$, začíná číslicí 9 ?

12. příklad Definujme posloupnost: $r_1 = 2$, $r_{i+1} = 2^{r_i}$. Dokažte, že pak platí

$$\exists n \in \mathbb{N} : \forall k \geq n : r_n \equiv r_k \pmod{2000}.$$

13. příklad Ukažte, že číslo 100101102103104 ... 998999 není mocninou žádného přirozeného čísla.

14. příklad Ukažte, že číslo $5^{2001} + 4^{2002} + 3^{2000}$ je dělitelné číslem 11.

15. příklad Porovnejte čísla A_n a B_n (v závislosti na n), kde

$$A_n = n^{n^{n^{n^2}}}, \qquad B_n = 2^{2^{2^{2^n}}}.$$

16. příklad Je celá část čísla $(\sqrt{2} + 1)^{2001}$ sudá nebo lichá?

17. příklad Ukažte, že číslo $10^{10^{10}} + 1$ nemá prvočíselný dělitel menší než 24 000.

18. příklad Určete poslední číslici čísla $17^{15^{13^{11}}}$.

19. příklad Zjistěte kolikrát se číslo $10^{10^{10}}$ nachází v Pascalově trojúhelníku.

20. příklad Dokažte, že dekadický zápis některé mocniny čísla

$$A = 1993^{1994^{1995^{1996^{1997}}}}$$

končí skupinou právě A nul a cifrou 1.

21. příklad Dokažte, že rovnice $7!! \cdot x^3 + 8!! \cdot x^2 + 9!! \cdot x + 10!! = 0$ má právě jeden reálný iracionální kořen.

22. příklad Určete posledních šest číslic čísla $5^{678^{901^{234}}}$.

23. příklad Vyřešte nerovnici $(n!)! < 10^{10^{10}}$.

24. příklad Určete tři číslice před a tři číslice za desetinnou čárkou čísla $\left(\sqrt{2} + \sqrt{3}\right)^{1000}$.

25. příklad Dokažte, že číslo $9^{9^9} + 10^{10^{10}}$ je dělitelné číslem 73.

26. příklad Porovnejte čísla A_n a B_n (v závislosti na n), kde

$$A_n = 2^{3^{4^{5^{\cdot^{\cdot^{\cdot^{n}}}}}}}, \qquad B_n = (n+1)^{n^{\cdot^{\cdot^{\cdot^{4^{3^2}}}}}}$$

27. příklad Určete poslední trojčíslí čísla $11^{11^{11}}$.

28. příklad Dokažte, že trojice komplexních kořenů rovnice

$$7^{7^7} \cdot x^3 + 8^{8^8} \cdot x^2 + 9^{9^9} \cdot x + 10^{10^{10}} = 0$$

netvoří v komplexní rovině rovnostranný trojúhelník.

29. příklad Určete dvě číslice před a dvě číslice za desetinnou čárkou čísla $\sqrt{9^{603} + 9^{306}}$.

30. příklad Ukažte, že číslo $18^{17^{19}} + 18^{19^{17}}$ není mocninou žádného přirozeného čísla.