

Eulerova veta

Jozef Rajník, KMS zimné sústreďenie BETA 2016, Juskova voľa

Číslo a je deliteľné číslom d , ak existuje také celé číslo k , že $a = k \cdot d$. V prípade, že a nie je deliteľné d môžeme hovoriť všeobecnejšie, že a dáva po delení d zvyšok z . Formálne to môžeme zapísať tak, že pre ľubovoľné celé čísla a , d existujú čísla k , z také, že $a = k \cdot d + z$. Pritom číslo z volíme čo najmenšie, najčastejšie z množiny $\{0, 1, \dots, d-1\}$. Pripomeňme si niekoľko pravidiel ako sa správa deliteľnosť.

- Ak $d \mid a$ a zároveň $d \mid b$, tak $d \mid (a \pm b)$.
- Ak p je prvočíslo a $p \mid ab$, tak $p \mid a$ alebo $p \mid b$.
- Ak d , a sú nesúdeliteľné a $d \mid ab$ tak $d \mid b$.

Číslo 4247 dáva po delení 9-timi zvyšok 8 a číslo 212 dáva zvyšok 5. Aký zvyšok budú dávať po delení 9-timi číslo $4247 + 212$? Ľahko zistíme, že $4247 + 212 \equiv 4$ a to aj bez toho aby sme tie čísla sčítali. Stačí nám totižto sčítať zvyšky, čo si vieme ľahko dokázať. Rovnako zistíme, že $4247 - 212 \equiv 3$ a $4247 \cdot 212 \equiv 4$. Ako sa zvyšky správajú pri umocňovaní? Ak číslo $a \equiv z \pmod{d}$, tak podobne vieme dokázať, že $a^n \equiv z^n \pmod{d}$. Ale ak chceme zistiť zvyšok 212^{10} po delení 9-timi, počítať 5^{10} nie je zrovna výhrou. Ale môžeme zvyšky mocnín počítať postupne.

$$\begin{array}{lll} 212^1 \equiv 5^1 \equiv 5 & 212^2 \equiv 5^2 \equiv 7 & 212^3 \equiv 5^3 \equiv 8 \\ 212^4 \equiv 5^4 \equiv 4 & 212^5 \equiv 5^5 \equiv 2 & 212^6 \equiv 5^6 \equiv 1 \\ 212^7 \equiv 5^7 \equiv 5 & 212^8 \equiv 5^8 \equiv 7 & 212^9 \equiv 5^9 \equiv 8 \end{array}$$

A nakoniec $212^{10} \equiv 5^{10} \equiv 4$. Isto ste si všimli, že sa tie zvyšky začali opakovať. Potom by už bolo jednoduché zistiť, že číslo 212^{2016} dáva zvyšok 1. Prečo sa to opakuje. A bude sa to takto opakovať vždy? Ak chceme zistiť zvyšok a^n po delení d , tak zoberieme zvyšok čísla a^n a vynásobíme ho zvyškom a . Keďže zvyškov po delení d je konečne veľa, musí sa nám nejaký opakovať. Vtedy sa dostaneme do rovnakej pozície, v akej sme už raz boli a keďže zvyšky ďalších mocnín počítame rovnakým postupom, ktorý závisí len od zvyšku poslednej mocniny, budeme dostávať tie isté výsledky ako na začiatku, teda sa nám začnú opakovať.

Ale čo všetko vieme povedať o tomto opakovaní sa zvyškov? Aká bude perióda opakovania? Vieme ju nejako zistiť v závislosti od čísel a , d ? Aké zvyšky sa budú opakovať? Na tieto otázky sa pokúsime nájsť odpoveď. Na začiatok sa skúsime pozrieť, ako sa zvyšky opakujú pri delení číslami 9, 10 a 11.

a^1	1	2	3	4	5	6	7	8
a^2	1	4	0	7	7	0	4	1
a^3	1	8	0	1	8	0	1	8
a^4	1	7	0	4	4	0	7	1
a^5	1	5	0	7	2	0	4	8
a^6	1	1	0	1	1	0	1	1
a^7	1	2	0	4	5	0	7	8

Na týchto tabuľkách si môžeme všimnúť niekoľko zaujímavých vecí. Prvou je, že v poslednom stĺpci sa striedajú zvyšky $d-1$ a 1. Je to preto, lebo zvyšok $d-1$ je vlastne ten istý ako -1 : $44 = 4 \cdot 9 + 8$ ale aj $44 = 5 \cdot 9 - 1$. A keď umocňujeme -1 , tak sa nám strieda -1 a $+1$. Podobne si môžeme každý zvyšok $d-x$ zapísať ako $-x$ (pri delení 9-timi môžeme 5, 6, 7, 8 zapísať ako -4, -3, -2, -1). Z toho vidíme ďalšiu peknú vec, že tieto opačné zvyšky majú párne mocniny rovnaké a