Lehká teorie čísel na brutalitách

Franta Konopecký

Úvod

Tato přednáška je přepracovanou verzí Víťovy přednášky před dvěma lety doplněná o příklady, které mi přišly ke zvolenému tématu zajímavé, názorné a ne úplně jednoduché. Přednáška je nenáročná na předchozí znalosti, z hlediska příkladů, které na ní vyřešíme, bude však patřit k těžším. Takže kdo chcete s minimálními znalostmi řešit drsné úlohy, je vám přednášky brána otevřená.

Zavedeme si na úvod jeden důležitý pojem, ať máme odborné termíny z krku, a to pojem **kongruence**.

Kongruence

Definice. *Mějme celá čísla a a b a přirozené číslo n. Pokud $n|(a-b)$, řekneme, že čísla a a b jsou kongruentní podle modulu n (případně kongruentní modulo n), a píšeme $a \equiv b \pmod{n}$.*

Poznámka. Jednoduše bychom řekli, že čísla a, b jsou kongruentní modulo n, pokud dávají stejné zbytky po dělení číslem n.

S kongruencemi se dá pracovat skoro stejně jako s rovnicemi. K oběma stranám kongruence můžeme přičíst (nebo odečíst) libovolné celé číslo a můžeme je vynásobit jakýmkoli nenulovým číslem. Dělit je ale možné jen čísly nesoudělnými s modulem (tak se říká tomu číslu n z předchozí definice). Také můžeme sečíst, odečíst nebo vynásobit libovolné dvě kongruence podle stejného modulu.

O kongruencích platí několik zajímavých tvrzení, která si na přednášce pořádně vysvětlíme:

Věta. (malá Fermatova) *Mějme přirozené číslo a a prvočíslo p, které nedělí a. Potom platí $a^{p-1} \equiv 1 \pmod{p}$.*

Věta. (Bezoutova) *Nechť jsou a a b celá čísla, jejich největšího společného dělitele značme $d = (a, b)$. Potom existují celá čísla x a y taková, že $ax + by = d$. Speciálně pokud jsou a a b nesoudělná, existují čísla x, y taková, že $ax + by = 1$*

Věta. *Buď p libovolné prvočíslo p a a číslo s ním nesoudělné. Potom existuje mezi čísly 1, 2, ..., $p-1$ právě jedno číslo b, pro které $ab \equiv 1 \pmod{p}$.*

Eulerova funkce a Eulerova věta

Definice. (Eulerova funkce) *Ať je n přirozené číslo. Počet všech s n nesoudělných přirozených čísel, jež jsou menší nebo rovna n, značíme $\varphi(n)$. Této funkci říkáme Eulerova.*

Věta. *Ať je n přirozené číslo větší než 1 a ať je $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}$ jeho rozklad na součin prvočísel (p_1, p_2, …, p_k jsou po dvou různá prvočísla, α_1, α_2, …, α_k jsou přirozená čísla). Potom platí $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$.*

Věta. (Eulerova) *Buďte a celé číslo a m přirozené číslo nesoudělné s a. Potom platí $a^{\varphi(m)} \equiv 1 \pmod m$.*

Příklady

Nejdřív něco na kongruence:

Příklad 1. Dokažte, že druhá mocnina přirozeného čísla dává po dělení čtyřmi jen zbytky 0 a 1.

Příklad 2. (Kanada 1973) Ukažte, že jestliže jsou čísla p a $p+2$ obě prvočísla, tak potom buď $p = 3$ nebo $6|(p+1)$.

Příklad 3. Transformací čísla budeme rozumět jeho nahrazení vlastním ciferným součtem. Začněme s 2007^{2007} a udělejme čtyři transformace. Jaký dostaneme výsledek? (Kanada 1989)

Příklad 4. (Brazílie 1989) n je přirozené číslo takové, že $\frac{n(n+1)}{3}$ je čtverec. Ukažte, že pak n je násobek tří a čísla $n+1$ a $\frac{n}{3}$ jsou též čtverce.

Příklad 5. (Prasátko, 24. ročník, 5. série) Buď p dané prvočíslo. Najděte všechna celá čísla a, b splňující $a^2 \equiv b^3 \pmod p$.

Tady už hledejte použití malé Fermatovy a Eulerovy věty:

Příklad 6. (Irsko 2000) Definujme $f(n) = 5n^{13} + 13n^5 + 9kn$. Najděte nejmenší přirozené číslo k takové, že je $f(n)$ dělitelné 65 pro všechna n.

Příklad 7. (Irsko 1996) Ukažte, že číslo $2^p + 3^p$ nemůže být n-tá mocnina ($n > 1$) pro p prvočíslo.

Příklad 8. Ukažte, že pro každé prvočíslo p můžeme najít nekonečně mnoho přirozených čísel n takových, že p dělí výraz $2^n - n$. (Kanada 1983)

Příklad 9. Existuje přirozené číslo N dělitelné přesně 2007 různými prvočísly (prvočísla mohou vystupovat v N v různých mocninách) takové, že N dělí $2^N - 2$?

(když vám to k něčemu bude, můžete předpokládat, že prvočísel ve tvaru $4k + 3$ je aspoň 3000).

Příklad 10. (Prasátko, 24. ročník, 5.série) Nechť n je přirozené číslo a p prvočíslo takové, že $p|n^2 + n + 1$. Dokažte, že $p \equiv 1 \pmod 6$ nebo $p = 3$.

Příklad 11. Uvažujme posloupnost $a_1, a_2, \ldots$ definovanou vztahem $a_n = 2^n + {} + 3^n + 6^n - 1$. Určete všechna přirozená čísla, která jsou nesoudělná s každým členem této posloupnosti. Nápověda: jediné nesoudělné číslo se všemi členy posloupnosti je číslo 1. (IMO 2005)

Příklad 12. Číslo nazvěme pruhované, pokud jsou jeho číslice střídavě liché a sudé. Ukažte, že všechna čísla n nesoudělná s 10 mají nějaký pruhovaný násobek. Upgrade: ukažte, že všechna čísla nedělitelná dvaceti mají pruhovaný násobek. (IMO 2004)

Příklad 13. (Brazílie 1992) Dokažte, že existuje přirozené číslo n takové, že prvních 1992 číslic z n^{1992} jsou jedničky.

Příklad 14. (IMO 2000) Můžeme najít číslo N dělitelné právě 2000 různými prvočísly (v libovolných mocninách) takové, že N dělí $2^N + 1$?