Diofantické rovnice

Víťa Kala

Na přednášce se budeme snažit vyřešit nějaké diofantické rovnice. Copak jsou zač? Diofantická rovnice je prostě nějaká rovnice, kterou se snažíme vyřešit v oboru celých (občas ale také přirozených nebo racionálních) čísel. Takovou asi nejslavnější diofantickou rovnicí vůbec je Fermatova diofantická rovnice $x^n + y^n = z^n$. Velká Fermatova věta, kterou asi před deseti lety dokázal Andrew Wiles, říká, že tato rovnice pro $n \geq 3$ nemá žádné nenulové řešení. Tuto větu si na přednášce bohužel nedokážeme (a ani to neumím), ale vyřešíme spoustu jiných rovnic, které jsou taky zajímavé. A ještě se pro úsporu místa domluvme, že pokud nenapíšu jinak, budou všechna písmenka v zadání rovnic značit celá čísla.

Několik základních metod řešení diofantických rovnic

Nejjednodušší situace, která může nastat, je, když máme pouze lineární rovnici, tedy něco takovéhoto:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

kde $n \geq 2$, a_i jsou nenulové parametry, b je taky nějaké dané číslo a x_i jsou neznámé, které se snažíme vypočíst. V této situaci pomocí kongruencí snadno zjistíme, že rovnice má řešení právě tehdy, když největší společný dělitel čísel a_i dělí číslo b.

Trochu složitějším případem je, když rovnice, kterou chceme vyřešit, není lineární úplně, ale je aspoň lineární vzhledem k jedné z neznámých (několik příkladů takových rovnic si můžeš prohlédnout v příkladu 4). Potom není nic lehčího, než tuto neznámou vyjádřit (dostaneme něco jako $ax =$blablabla, kde a je nějaký nenulový parametr, x hledáme a blablabla značí pravou stranu rovnice). Pak už ubohému číslu a nezbývá nic jiného než dělit pravou stranu, takže rychle vyřešíme odpovídající kongruenci a máme vyhráno.

No a dost podobně se dá vyřešit i diofantická rovnice, která není vyloženě lineární vůči nějaké z neznámých, ale z níž se dá jedna z neznámých jednoduše vyjádřit.

Trikem, který ti dost často může výrazně usnadnit práci, je zkusit použít nerovností. Vysvětlovat to byť jen trošku teoreticky by byl nesmysl, tak počkej na přednášku … To jediné, co sem napíšu, bude fakt, že pokud dostaneš nerovnost tvaru $a^n < b^n < (a+1)^n$, byla by to velká haluz, kdyby rovnice měla řešení. (:

Další z fint, které naťukneme, bude zkusit rozložit jednu ze stran rovnice na součin nejlépe navzájem nesoudělných čísel a využít toho, že druhá strana půjde rozložit jen několika málo způsoby. To takto teoreticky určitě zase zní úplně hrozně, ale při počítání příkladů je to úplně jasné …

A to by z těch jednoduchých postupů už pomalu snad mohlo stačit, stejně je všechny na přednášce nestihneme … Občas se taky dá dokázat, že rovnice nemá řešení, často pomocí kongruencí – třeba přesně tak jako v 2. úloze 5. série letošního ročníku PraSátka.

A teď ty drsné způsoby, k nimž se (doufám) dostaneme na druhé a třetí přednášce

Půjde v podstatě o (nejvýše) dva triky, jejichž podstatu zde jen zlehka naznačím – psát je pořádně by bylo vskutku únavné jak pro čtenáře, tak (a to především (:) pro mě.

Ten první bude spočívat v tom, že si nakreslíme obrázek … Například řešení rovnice $a^2 + 2b^2 = 3c^2$ napřed převedeme na hledání racionálních řešení rovnice $x^2 + 2y^2 = 3$. Body o souřadnicích (x, y), které splňují tuto rovnici, leží na nějaké elipse. A když chytře spojíme bod $(1, 1)$, odpovídající jednomu z řešení rovnice, se skoro jakýmkoli bodem o racionálních souřadnicích, protne vzniklá přímka elipsu v bodě, který je taky racionálním řešením. Nevěříš? Tak přijď na přednášku a já tě o tom přesvědčím (a když se ti to nebude líbit, klidně zvolím i nějaký násilnější přesvědčovací prostředek než jen důkaz (:).

A druhá finta je ještě vyfintěnější. Navazuje totiž na ideu o rozkládání na součin. Člověku by se na první pohled mohlo zdát, že třeba v rovnici $y^2+2 = x^3$ se toho moc rozložit nedá … Ale chyba lávky! Proč jednoduše nepsat, že $y^2+2 = (y+\sqrt{-2})(y-\sqrt{-2})$, a tedy $(y+\sqrt{-2})(y-\sqrt{-2}) = x^3$? A světe div se, ono se s tím fakt dá celkem rozumně pracovat a zmíněnou rovnici tak vyřešit. Tak k tomu se třeba taky někdy dostaneme (a když ne na tomto, tak na nějakém příštím soustředku).

Příklad 1. Zkus si rozmyslet, že každou soustavu diofantických rovnic jde nahradit jedinou diofantickou rovnicí o stejném počtu neznámých, která je s původní soustavou ekvivalentní (tedy má přesně ta řešení jako původní soustava). To znamená, že z teoretického hlediska se vůbec nemusíme zajímat o řešení soustav diofantických rovnic, že si vždy vystačíme s jedinou rovnicí.

Příklad 2. A zkus si taky uvědomit, že libovolnou diofantickou rovnici jde převést na ekvivalentní rovnici stupně nejvýše čtyři (k tomu ale můžeš potřebovat přidat nějaké nové neznámé).

Příklad 3. Zvládneš vyřešit následující diofantické rovnice?
a) $11x + 7y = 13$
b) $84x - 42y = 35$
c) $21a + 51b - 18c + 84d = 100$

Příklad 4. A co říkáš na tyto rovnice?
a) $x^2 - 11y - 4 = 0$
b) $x^2 - 11y - 6 = 0$
c) $(x^2 + 2)x = 125y - 2$
d) $x^3 - 13x^2 - 13y = 2$
e) $2^x = 3 + 13y$
f) $2xy + 3y^2 = 24$
g) $x^2 + y^2 = (x - y)^3$

Příklad 5. Nemohly by se tady hodit nějaké nerovnosti (pro tentokrát budou písmena v druhé půlce abecedy označovat přirozená čísla)?
a) $x + y + z = xyz$
b) $x^x + y^y = 2x + y$
c) $a^2 - ab + b^2 = a + b$
d) $x^2 = 1 + y + y^2 + y^3 + y^4$
e) $(i + 2)^4 = i^4 + j^3$
f) $c^8 + 2c^6 + 2c^4 + 2c^2 + 1 = d^2$
g) $a^2 + a = b^4 + b^3 + b^2 + b$
h) $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$

Příklad 6. I tyto rovnice je potřeba vyřešit! (:
a) $x^3 - y^3 = 91$
b) $x^4 + 2x^7y - x^14 - y^2 = 7$
c) $xy = x + y$
d) $2^{x-1} + 1 = y^{z+1}$, kde neznámé jsou přirozená čísla
e) $x + y + z = 3, x^3 + y^3 + z^3 = 3$

Příklad 7. Kdyby se někomu snad ještě chtělo počítat ...
a) $x^2 + 2y^2 = z^2, 2x^2 + y^2 = t^2$
b) $x^2 + 5 = y^3$
c) $2^x + 5^y = 19^z$

Příklad 8. Příklady na ty drsnější metody sem asi psát nebudu, těch si každý zvládne vymyslet habaděj (třeba $5a^2 + 2b^2 = c^2$ nebo $y^2 + 1 = x^p$, kde p je prvočíslo).