Factoring lemma

Háňa Bendová

Abstrakt. Factoring lemma je jednoduché, ale užitečné lemma, s jehož pomocí se dají snadno vyřešit některé diofantické rovnice i jiné číselně teoretické úlohy. Příspěvek obsahuje lemma samotné, několik řešených úloh a několik úloh na procvičení.

Motivační příklad. Buďte a, b, c, d přirozená čísla taková, že $ab = cd$. Dokažte, že $a + b + c + d$ je složené.

Lemma. (Factoring lemma) *Nechť a, b, c, d jsou přirozená čísla taková, že platí $ab = cd$. Pak existují přirozená čísla m, n, p, q taková, že* $\gcd(n, p) = 1$ a

$$a = mn, \quad b = pq, \quad c = mp, \quad d = nq.$$

Důkaz. Podmínku $ab = cd$ můžeme přepsat jako

$$\frac{a}{c} = \frac{d}{b}.$$

Oba zlomky se dají reprezentovat stejným zlomkem $\frac{n}{p}$ v základním tvaru. Položme

$$m = \frac{a}{n} = \frac{c}{p}, \quad q = \frac{b}{p} = \frac{d}{n}.$$

Zřejmě m a q jsou přirozená a čísla m, n, p, q mají požadované vlastnosti.

Řešení příkladu. Najdeme přirozená čísla m, n, p, q jako v lemmatu. Pak

$$a + b + c + d = mn + pq + mp + nq = (m + q)(n + p),$$

z čehož vidíme, že $a + b + c + d$ je složené číslo.

Klíčová slova. factoring lemma, nesoudělnost, pythagorejské trojice, diofantické rovnice

Diofantické rovnice

Příklad 1. Po dvou nesoudělná celá čísla splňují $a^2 + b^2 = c^2$. Jestliže a je liché, existují celá čísla u, v tak, že $a = u^2 - v^2$ a $b = 2uv$.

Řešení. Přepíšeme podmínku jako

$$b^2 = (c - a)(c + a).$$

Podle lemmatu existují m, n, p, q tak, že $b = mn = pq$, $c - a = mp$, $c + a = nq$. Opět podle lemmatu existují x, y, z, w tak, že $m = xy$, $n = zw$, $p = xz$, $q = yw$. Tedy

$$b = xzyw, \quad a = \frac{nq - mp}{2} = \frac{yz}{2}(w^2 - x^2).$$

Protože w^2 a x^2 dávají po dělení čtyřmi pouze zbytky 0 nebo 1 a a je liché, musí platit $2 \mid yz$. Na druhou stranu číslo yz dělí jak b, tak $2a$, tedy $yz = 2$. Tím je důkaz hotov.

Příklad 2. Po dvou nesoudělná přirozená čísla a, b, c splňují $a^2+b^2 = 2c^2$. Dokažte, že existují celá čísla t, u, v tak, že

$$\begin{aligned} a &= \frac{t}{4}(u^2 - v^2 + 2uv), \\ b &= \frac{t}{4}(v^2 - u^2 + 2uv), \\ c &= \frac{t}{4}(u^2 + v^2). \end{aligned}$$

Řešení. Protože $(a - c)(a + c) = (c - b)(c + b)$, existují podle lemmatu celá čísla m, n, p, q tak, že

$$a - c = mn, \quad a + c = pq, \quad c - b = mp, \quad c + b = nq.$$

Odtud $pq - mn = mp + nq$, tedy $p(q - m) = n(q + m)$. Opět podle lemmatu existují celá čísla x, y, z, w taková, že

$$p = xy, \quad q - m = zw, \quad n = xz, \quad q + m = yw.$$

Platí

$$\begin{aligned} a &= \frac{1}{2}(mn + pq) = \frac{1}{2}\left(\frac{yw - zw}{2}xz + \frac{zw + yw}{2}xy\right) = \frac{xw}{4}(y^2 + 2yz - z^2), \\ b &= \frac{1}{2}(nq - mp) = \frac{1}{2}\left(\frac{zw + yw}{2}xz + \frac{yw - zw}{2}xy\right) = \frac{xw}{4}(-y^2 + 2yz + z^2). \end{aligned}$$

Nyní stačí položit $t = uv$, $u = y$, $v = z$.

Příklad 3. Buďte (a, b) a (c, d) dvě různé neuspořádané dvojice celých čísel takové, že $a^2 + b^2 = c^2 + d^2 = k$. Dokažte, že k je složené.

Řešení. Bez újmy na obecnosti $a > c$ (kdyby $a = c$, pak $b = d$ a dvojice by nebyly různé). Úpravou dostaneme

$$(a - c)(a + c) = (d - b)(d + b).$$

Vidíme, že $d > b$, tedy $a + c$, $a - c$, $d + b$, $d - b$ jsou přirozená čísla a podle lemmatu najdeme přirozená čísla m, n, p, q tak, že

$$a + c = mn, \quad a - c = pq, \quad d + b = mp, \quad d - b = nq.$$

Potom

$$a = \frac{mn + pq}{2}, \quad b = \frac{mp - nq}{2}$$

a platí

$$\begin{aligned} 4k = 4(a^2 + b^2) &= (mn + pq)^2 + (nq - mp)^2 \\ &= m^2n^2 + p^2q^2 + n^2q^2 + m^2p^2 = (m^2 + q^2)(n^2 + p^2). \end{aligned}$$

Předpokládejme, že k je prvočíslo. Pak bez újmy na obecnosti $k \mid m^2 + q^2$. Tedy buď $n^2 + p^2 = 4$, nebo $n^2 + p^2 = 2$. První případ nemůže nastat, neboť číslo 4 se nedá napsat jako součet dvou čtverců. Ve druhém případě $n = p = 1$, z čehož plyne $a = c$, $b = d$, což jsme v zadání zamítli. Číslo k tedy musí být složené.

V řešení posledního příkladu jsme po cestě dokázali i následující lemma.

Lemma. *Jsou-li a, b, c, d celá čísla a $a^2 + b^2 = c^2 + d^2$, pak existují celá čísla m, n, p, q taková, že*

$$2a = mn + pq, \quad 2b = mp - nq, \quad 2c = mp + nq, \quad 2d = mn - pq.$$

Další příklady

Příklad 1. Najdi všechna celočíselná řešení rovnice $x^2 + 3y^2 = z^2$.

Příklad 2. Najdi všechna celočíselná řešení rovnice $x^2 + y^2 = 5z^2$.

Příklad 3. Dokažte, že je-li $N = a^2 + 2b^2 = c^2 + 2d^2$ a $\{a, b\} \neq \{c, d\}$, pak N je složené.

Příklad 4. Dokažte, že jsou-li a, b, c, d přirozená čísla a $ab = cd$, pak $a^n + b^n + c^n + d^n$ je složené.

Literatura a zdroje

[1] Iurie Boreico, Roman Teleuca, *A Factoring Lemma*, Mathematical reflections, 2007.
[2] Herman, Šimša, Kučera, *Metody řešení matematických úloh I*, Brno, 2001