1. Axiómy celých čísel

Uvažujme množinu $\mathbb{Z}$ celých čísel s operáciami sčítania a násobenia. Pre každé $x, y, z \in \mathbb{Z}$ platí:

(1) $x + y = y + x$;
(2) $x + (y + z) = (x + y) + z$;
(3) $x + 0 = x$;
(4) $x + (-x) = 0$;
(5) $x(yz) = (xy)z$;
(6) $x(y + z) = xy + xz$, $(y + z)x = yx + zx$;
(7) $xy = yx$;
(8) $1 \cdot x = x$;
(9) ak $xy = 0$ tak $x = 0$ alebo $y = 0$.

Splnenie podmienok (1)-(6) znamená, že $(\mathbb{Z}, +, \cdot)$ je *okruh*, podmienky (1)-(9) hovoria, že je to *obor integrity*.

Z horeuvedených podmienok sa dajú odvodiť aj ďalšie známe vlastnosti, napríklad $x \cdot 0 = 0$.

Na množine $\mathbb{Z}$ máme aj prirodzené usporiadanie $\leq$, ktoré má nasledujúce vlastnosti (pre každé x, y, z).

(1) $x \leq x$;
(2) ak $x \leq y$ a $y \leq x$, tak $x = y$;
(3) ak $x \leq y$ a $y \leq z$, tak $x \leq z$;
(4) ak $x \leq y$, tak $x + z \leq y + z$;
(5) ak $x \leq y$ a $z \geq 0$, tak $xz \leq yz$;

Ďalšia dôležitá vlastnosť sa nazýva *Princíp dobrého usporiadania*: Každá neprázdna, zdola ohraničená podmnožina množiny $\mathbb{Z}$ má najmenší prvok.

Význam uvedeného princípu spočíva hlavne v tom, že umožňuje robiť dôkazy *matematickou indukciou*.

Všetky vlastnosti uvedené v tomto odstavci budeme považovať za známe a nebudeme ich dokazovať. (Dajú sa dokázať v rámci teórie množín.)

2. Deliteľnosť

Nech a, b sú celé čísla. Hovoríme, že a je deliteľné b (a píšeme $b|a$) ak existuje $c \in \mathbb{Z}$ tak, že $a = bc$.

Vzťah $b|a$ opisujeme tiež slovnými spojeniami "b delí a", "b je deliteľom a", "a je násobkom b".

Ľahko sa dokážu nasledujúce vlastnosti relácie deliteľnosti:

(1) $a|a$ pre každé a;
(2) $1|a$ pre každé a;
(3) $a|0$ pre každé a;
(4) $0|a$ práve vtedy, keď $a = 0$;
(5) ak $a|b$ a $b|c$, tak $a|c$;
(6) ak $a|b$ a $a|c$, tak $a|(b + c)$;
(7) ak $a|b$, tak $a|bc$ pre každé c;
(8) ak $a|b$, tak $b = 0$ alebo $|a| \leq |b|$.

Symboly $|a|, |b|$ v (8) znamenajú absolútnu hodnotu. Všimnime si, že podľa (4) číslo 0 *je* deliteľné 0. (A žiadne iné číslo nulou deliteľné nie je.)

Nasledujúce dôležité tvrdenie je známe ako *Veta o delení so zvyškom*.

Veta 2.1. *Nech $a, b \in \mathbb{Z}$, $b \neq 0$. Potom existujú $p, z \in \mathbb{Z}$ tak, že*

$$a = bp + z$$

a $0 \leq z \leq |b|$. Naviac, čísla p a z sú určené jednoznačne.

D ô k a z. Uvažujme najprv prípad $b > 0$ a postupnosť

$$\cdots < -4b < -3b < -2b < -b < 0 < b < 2b < 3b < 4b < 5b < \ldots$$

Je zrejmé, že číslo a musí padnúť do niektorého z intervalov $\langle pb, (p+1)b)$, teda $pb \leq a < (p+1)b$. Položme $z = a - pb$. Potom zrejme $a = pb + z$ a $z \geq 0$. V nerovnosti $a < (p+1)b$ odčítame od oboch strán pb a dostaneme

$$z = a - pb < (p+1)b - pb = b = |b|.$$

Ak by bolo $b < 0$, tak potom $c = -b > 0$ a podľa predchádzajúcej úvahy existujú p, z tak, že $a = cp + z$ a $0 \leq z < c$. Potom $a = b(-p) + z$ a $z < |b| = c$.

Tým sme dokázali existenciu čísel p a z. Ostáva ukázať jednoznačnosť. Predpokladajme, že $a = bp_1 + z_1 = bp_2 + z_2$. Potom

$$bp_1 - bp_2 = z_2 - z_1,$$

takže

$$b(p_1 - p_2) = z_2 - z_1.$$

To znamená, že b delí $z_2 - z_1$. Pritom ale $|z_2 - z_1| < |b|$ (prečo?), takže podľa (8) musí byť $z_2 - z_1 = 0$, teda $z_2 = z_1$ a z rovnosti $b(p_1 - p_2) = 0$ dostávame $p_1 = p_2$. ∎

Čísla p a z v predošlej vete sa nazývajú *podiel* a *zvyšok*. Samozrejme, $z = 0$ práve vtedy, keď $b|a$.

3. Najväčší spoločný deliteľ

Pojem deliteľa už poznáme z predošlej kapitoly. Symbolom $D(a)$ označme množinu všetkých deliteľov čísla a. Napríklad $D(6) = \{1, -1, 2, -2, 3, -3, 6, -6\}$. Ďalej, nech $D(a, b)$ označuje množinu spoločných deliteľov čísel a, b, t.j. čísel, ktoré súčasne delia a aj b. Napríklad $D(6, 8) = \{1, -1, 2, -2\}$.

Definícia 3.1. *Číslo d sa nazýva najväčším spoločným deliteľom (NSD) čísel a, b ak*

(i) *$d \in D(a, b)$;*
(ii) *pre každé $x \in D(a, b)$ platí $x|d$.*

Teda spoločné delitele neporovnávame reláciou $\leq$, ale reláciou $|$: najväčší spoločný deliteľ je taký, že je deliteľný všetkými ostatnými spoločnými deliteľmi. Dôsledkom toho je, že najväčšie spoločné delitele sú dva. Napríklad NSD čísel 6 a 8 sú čísla 2 ale aj -2. (Jediná výnimka je prípad $a = b = 0$, kedy jediný NSD je 0.)

Definícia samozrejme nezaručuje existenciu nejakých NSD. Tú dostaneme až z nasledujúcej vety.

Veta 3.2. *Pre každé dve celé čísla a, b existuje ich NSD. Ten je určený jednoznačne až na znamienko a dá sa vyjadriť v tvare $d = au + bv$ pre nejaké $u, v \in \mathbb{Z}$.*

D ô k a z. Prípad $a = b = 0$ je triviálny. Predpokladajme, že aspoň jedno z čísel a, b je nenulové. Uvažujme množinu

$$A = \{x \in \mathbb{Z} \mid 0 < x = au + bv \text{ pre nejaké } u, v \in \mathbb{Z}\}.$$

Pretože aspoň jedno z čísel a, b je nenulové, množina A je neprázdna. Okrem toho je zdola ohraničená (číslom 0). Podľa princípu dobrého usporiadania množina A má najmenší prvok. Tento najmenší prvok označme d. Ukážeme, že d spĺňa podmienky (i), (ii).

Pretože $d \in A$, d sa dá vyjadriť v tvare $d = au + bv$ pre nejaké $u, v \in \mathbb{Z}$. Deľme číslo a číslom d. Podľa vety o delení so zvyškom existujú $p, z \in \mathbb{Z}$ tak, že $a = dp + z$ a $0 \leq z < d$. Potom

$$z = a - dp = a - (au + bv)p = a(1 - up) + b(-vp).$$

Keby bolo $z > 0$, bol by to prvok množiny A. To ale nie je možné, lebo $z < d$ a d bol najmenší prvok v A. Preto musí byť $z = 0$, čo znamená, že $d|a$.

Podobne by sa dokázalo $d|b$, takže $d \in D(a, b)$, podmienka (i) je dokázaná.

Dôkaz (ii) je ešte jednoduchší. Ak $e \in D(a, b)$, tak $a = ep$, $b = eq$ pre nejaké $p, q \in \mathbb{Z}$. Potom

$$d = au + bv = epu + eqv = e(pu + qv),$$

čo znamená $e|d$.

K jednoznačnosti: ak d_1 aj d_2 sú NSD čísel a, b, tak podľa (ii) platí $d_1|d_2$ aj $d_2|d_1$. To znamená, že $|d_1| \leq |d_2|$ aj $|d_2| \leq |d_1|$, takže d_1 a d_2 majú rovnakú absolútnu hodnotu a môžu sa líšiť len znamienkom. ∎

Označenie: Nezáporný NSD čísel a a b budeme označovať (a, b).

V prípade, že $(a, b) = 1$ hovoríme, že a a b sú *nesúdeliteľné*.

Dôkaz predošlej vety je tzv. existenčný, čo znamená, že nedáva návod ako NSD dvoch čísel nájsť. Na taký výpočet však existuje dobre známa metóda, ktorá sa nazýva *Euklidov algoritmus*. Zakladá sa na nasledujúcom tvrdení.

Lema 3.3. *Ak $a = bp + z$ $(a, b, p, z \in \mathbb{Z})$, tak $D(a, b) = D(b, z)$. Následne, NSD čísel a a b je taký istý, ako NSD čísel b a z.*

D ô k a z. Ak $x \in D(a, b)$, tak x delí a aj b. Potom ale x delí aj $z = a - bp$, takže $x \in D(b, z)$.

Opačne, ak $y \in D(b, z)$, tak y delí b aj z. Potom ale y delí aj $a = bp + z$, teda $y \in D(a, b)$. ∎

Popis algoritmu: Predpokladajme, že $a \geq b$. Podľa Vety o delení so zvyškom nájdeme $p, z \in \mathbb{Z}$ tak, že $a = bp + z$, kde $0 \leq z < |b|$. Ak $z = 0$, tak NSD je b. Ak $z \neq 0$, tak hľadáme NSD čísel b a z. Výpočet sa nakoniec musí skončiť, lebo zvyšky stále klesajú.

Poznámka: Euklidov algoritmus sa dá využiť aj na vyjadrenie NSD v tvare $d = au + bv$.

NSD môžeme definovať nielen pre dve čísla, ale pre ľubovoľný počet. Nech $D(a_1, \ldots, a_n)$ označuje množinu všetkých spoločných deliteľov čísel a_1,..., a_n.

Definícia 3.4. *Číslo d sa nazýva najväčším spoločným deliteľom (NSD) čísel a_1,...,a_n ak*

(i) $d \in D(a_1, \ldots, a_n)$;

(ii) *pre každé* $x \in D(a_1, \ldots, a_n)$ *platí* $x|d$.

Podobne ako v prípade dvoch čísel sa dá dokázať, že NSD vždy existuje a je určený jednoznačne až na znamienko. Na jeho výpočet môžeme využiť nasledujúce tvrdenie.

Lema 3.5. *Nech d je NSD čísel* a_1,...,a_n. *Nech e je NSD čísel d a* a_{n+1}. *Potom e je NSD čísel* a_1,...,a_{n+1}.

Na základe uvedenej lemy môžeme postupne vypočítať NSD 2 čísel, 3 čísel, 4 čísel, atď.

Nakoniec tejto kapitoly si niečo povieme o *najmenšom spoločnom násobku*, čo je pojem duálny ku NSD.

Definícia 3.6. *Číslo n sa nazýva najmenším spoločným násobkom (NSN) čísel a, b ak*

(i) $a|n$, $b|n$;
(ii) *pre každé x také, že* $a|x$, $b|x$ *platí* $n|x$.

Na výpočet NSN nám slúži nasledujúce tvrdenie.

Veta 3.7. *Ak* $(a, b) \neq 0$, *tak číslo*

$$n = \frac{ab}{(a, b)}$$

je NSN čísel a a b.

D ô k a z. Podmienky $a|n$, $b|n$ vyplývajú z rovností

$$n = a \cdot \frac{b}{(a, b)} = b \cdot \frac{a}{(a, b)}.$$

Na dôkaz (ii) predpokladajme $x = ap = bq$ a použijeme vyjadrenie

$$(a, b) = au + bv.$$

Túto rovnosť vynásobíme x a dostaneme

$$x(a, b) = xau + xbv = bqau + apbv = ab(qu + pv),$$

odkiaľ po vydelení (a, b) vyplýva

$$x = \frac{ab}{(a, b)}(qu + pv) = n(qu + pv),$$

takže $n|x$. ∎

4. Prvočísla a veta o rozklade

Definícia 4.1. *Celé číslo* $p > 1$ *sa nazýva prvočíslo, ak je deliteľné* **len** *číslami* $1, -1, p$ *a* $-p$.

Ekvivalentne, $p > 1$ je prvočíslo, ak nie je súčinom dvoch menších kladných čísel. Ak $p > 1$ nie je prvočíslo, tak p sa nazýva *zložené*.

Lema 4.2. *Nech* $p, a_1, \ldots, a_n \in \mathbb{Z}$.

(i) *Ak* $p|a_1a_2$ *a* $(p, a_1) = 1$, *tak* $p|a_2$;
(ii) *Ak* $p|a_1a_2 \ldots a_n$ *a p je prvočíslo, tak* $p|a_k$ *pre niektoré k.*

D ô k a z. (i) Vychádzame z rovností $a_1a_2 = px$, $1 = pu + a_1v$ $(x, u, v \in \mathbb{Z})$. Druhú z týchto rovností vynásobíme číslom a_2 a dostaneme

$$a_2 = a_2pu + a_2a_1v = a_2pu + pxv = p(a_2u + xv),$$

čo sme chceli dokázať.

(ii) Tvrdenie dokážeme pre $n = 2$. (Na všeobecný prípad sa to ľahko prenesie matematickou indukciou.) Ak p je prvočíslo a $p|a_1a_2$, tak sú 2 možnosti: $(p, a_1) = p$ alebo $(p, a_1) = 1$ (keďže p nemá iné kladné delitele). Prvá možnosť znamená $p|a_1$, druhá (na základe (i)) $p|a_2$. ∎

Teraz môžeme dokázať tvrdenie o rozklade, ktoré sa tiež nazýva *Hlavná veta aritmetiky.*

Veta 4.3. *Každé celé číslo $n > 1$ sa dá rozložiť na súčin prvočísel, a to jednoznačne až na poradie činiteľov.*

D ô k a z. Formulácia "súčin prvočísel" zahŕňa aj prípad, že n je prvočíslo, t.j. "súčin" jedného prvočísla.

Existenciu rozkladu dokážeme matematickou indukciou. Pre $n = 2$ tvrdenie platí. Predpokladajme, že $n > 2$ a že tvrdenie platí pre všetky $m < n$. Rozlíšime 2 prípady. Ak n je prvočíslo, tak tvrdenie pre n zrejme platí. Ak n je zložené, tak $n = uv$ pre nejaké $1 < u, v < n$. Podľa indukčného predpokladu máme $u = p_1 \dots p_k$, $v = q_1 \dots q_l$, kde všetky p_i aj q_i sú prvočísla. Potom

$$n = p_1 \dots p_k \cdot q_1 \dots q_l$$

je hľadaný rozklad čísla n.

Ostáva dokázať jednoznačnosť. Predpokladajme, že

$$n = p_1 \dots p_k = q_1 \dots q_l,$$

kde všetky p_i aj q_i sú prvočísla. Potom podľa (ii) z predchádzajúcej lemy $p_1|q_j$ pre nejaké j. Keďže p_1 aj q_j sú prvočísla, musí platiť $p_1 = q_j$. Teraz vyškrtneme čísla p_1, q_j z horeuvedenej rovnosti a úvahu opakujeme postupne pre p_2, p_3,..., p_n. Tak každé p_i "spárujeme" s niektorým q_j, takže uvedené rozklady sa môžu líšiť len poradím činiteľov. ∎

Poznámka Dôkaz Základnej vety aritmetiky má opäť existenčný charakter a nedáva návod ako rozložiť dané celé číslo (iný než vyskúšanie všetkých možností). Pre malé čísla to nie je problém. Pre veľké čísla však nie sú známe žiadne efektívne metódy rozkladu (faktorizácie). Na tomto fakte sa zakladajú viaceré šifrovacie algoritmy.

Na rozklad malých čísel používame známe kritériá deliteľnosti a tiež nasledujúce jednoduché tvrdenie.

Lema 4.4. *Každé zložené n má deliteľa $1 < k \leq \sqrt{n}$.*

D ô k a z. Máme $n = ab$, kde $1 < a$, $1 < b$. Predpokladajme $a \leq b$. Potom $n = ab \geq a^2$, takže $a \leq \sqrt{n}$. ∎

Existuje množstvo zaujímavých tvrdení o prvočíslach. My uveďme aspoň nasledujúce.

Veta 4.5. *Existuje nekonečne veľa prvočísel.*

D ô k a z. Urobíme dôkaz sporom. Predpokladajme, že prvočísel je konečne veľa, označme ich $p_1, \ldots, p_n$. Potom ich môžeme všetky vynásobiť a uvažovať o čísle $x = p_1 \ldots p_n + 1$. To je potom číslo, ktoré nie je deliteľné žiadnym prvočíslom (po delení každým z nich dáva zvyšok 1). Dostávame tak spor s vetou o rozklade. ∎

Znalosť prvočíselného rozkladu možno využiť pri hľadaní NSD a NSN. Konkrétne, nech čísla a a b majú rozklady

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n},$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},$$

kde $p_1, \ldots, p_n$ sú rôzne prvočísla. (Pripúšťame, že niektoré exponenty α_i a β_j môžu byť 0, čo by znamenalo, že príslušné prvočíslo sa v rozklade nenachádza.) Potom NSD čísel a, b má rozklad

$$p_1^{\min\{\alpha_1,\beta_1\}} \ldots p_n^{\min\{\alpha_n,\beta_n\}}$$

a NSN

$$p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_n^{\max\{\alpha_n,\beta_n\}}.$$

V špeciálnych prípadoch táto metóda môže byť rýchlejšia než Euklidov algoritmus. Vo všeobecnosti je ale nájdenie prvočíselného rozkladu výpočtovo podstatne zložitejšie než výpočet NSD.

5. Kongruencie

Nech $a, b, m \in \mathbb{Z}$, $m \geq 0$. Hovoríme, že a je *kongruentné* s b *modulo* m, a píšeme

$$a \equiv b \ (\mod m),$$

ak m delí $a - b$.

Pri $m \neq 0$ je to ekvivalentné s podmienkou, že čísla a a b dávajú pri delení m rovnaký zvyšok. Skutočne, podľa Vety o delení so zvyškom máme

$$a = mp_1 + z_1, \quad b = ap_2 + z_2,$$

odkiaľ

$$a - b = m(p_1 - p_2) + (z_1 - z_2),$$

takže $a - b$ je deliteľné m práve vtedy, keď $z_1 - z_2$ je deliteľné m, a to je práve vtedy keď $z_1 - z_2 = 0$, lebo $-(m-1) \leq z_1 - z_2 \leq m - 1$.

Kongruencia modulo m je pre každé m reláciou ekvivalencie, čo znamená, že je

a) reflexívna: $a \equiv a \ (\mod m)$ pre každé $a \in \mathbb{Z}$;
b) symetrická: ak $a \equiv b \ (\mod m)$, tak $b \equiv a \ (\mod m)$;
c) tranzitívna: ak $a \equiv b \ (\mod m)$ a $b \equiv c \ (\mod m)$, tak $a \equiv c \ (\mod m)$.

Prakticky si to treba predstavovať tak, že kongruencia modulo $m \neq 0$ rozdelí množinu $\mathbb{Z}$ na m častí, podľa toho, ktoré čísla dávajú pri delení m aký zvyšok. Čísla, ktoré patria do tej istej skupiny, sú navzájom kongruentné. (Samozrejme, rôzne m rozdelia $\mathbb{Z}$ rôznym spôsobom.)

Kongruencie modulo 0 a 1 sú podľa definície prípustné, ale nie veľmi zaujímavé: $a \equiv b \ (\mod 1)$ platí vždy (všetky čísla sú v 1 skupine), zatiaľ čo $a \equiv b \ (\mod 0)$ platí len pre $a = b$ (každé číslo je v inej "skupine").

Samozrejme, $a \equiv 0 \ (\mod m)$ práve vtedy, keď $m|a$.

Pravidlá pre počítanie s kongruenciami sú zhrnuté v nasledujúcom tvrdení.

Veta 5.1. *Pre každé $a, b, c, d, n, m \in \mathbb{Z}$, $m, n \geq 0$ platí:*

(i) *ak* $a \equiv b \pmod m$ *a* $c \equiv d \pmod m$, *tak* $a + c \equiv b + d \pmod m$;
(ii) *ak* $a \equiv b \pmod m$, *tak* $a + c \equiv b + c \pmod m$;
(iii) $a \equiv b \pmod m$ *a* $c \equiv d \pmod m$, *tak* $ac \equiv bd \pmod m$;
(iv) *ak* $a \equiv b \pmod m$, *tak* $ac \equiv bc \pmod m$;
(v) *ak* $a \equiv b \pmod m$, *tak* $a^n \equiv b^n \pmod m$.

D ô k a z. (i) Ak m delí $a - b$ aj $c - d$, tak potom delí aj $(a + c) - (b + d) = (a - b) + (c - d)$.

(ii) To je špeciálny prípad (i), lebo $c \equiv c \pmod m$.

(iii) Platí

$$ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d).$$

Preto keď m delí $a - b$ aj $c - d$, tak delí celú pravú stranu, a teda aj $ac - bd$.

(iv) To je špeciálny prípad (iii), lebo $c \equiv c \pmod m$.

(v) Toto vyplýva z (iii) pomocou matematickej indukcie. (Kongruenciu $a \equiv b \pmod m$ násobíme n-krát samú so sebou.) ∎

Uvedené pravidlá možno využit napríklad na tzv. *modulárne umocňovanie*.

Príklad Vypočítame zvyšok po delení čísla 5^{222} číslom 11. Použijeme kongruenciu modulo 11 a dostávame

$$5^{222} = (5^2)^{111} = 25^{111} \equiv 3^{111} = (3^3)^{37} = 27^{37} \equiv 5^{37} =$$
$$= 25^{18} \cdot 5 \equiv 3^{18} \cdot 5 = 27^6 \cdot 5 \equiv 5^6 \cdot 5 = 25^3 \cdot 5 \equiv 3^3 \cdot 5 =$$
$$= 27 \cdot 5 \equiv 5 \cdot 5 = 25 \equiv 3,$$

takže hľadaný zvyšok je 3.

Teraz si ukážme pravidlá pre krátenie kongruencií.

Veta 5.2. *Nech $a, b, c, m \in \mathbb{Z}$, $c \neq 0$, $m \geq 0$.*

(i) *Ak* $ac \equiv bc \pmod{mc}$, *tak* $a \equiv b \pmod m$.
(ii) *Ak* $ac \equiv bc \pmod m$ *a* $(m, c) = 1$, *tak* $a \equiv b \pmod m$.

D ô k a z. (i) Ak $ac - bc$ je deliteľné mc, tak $ac - bc = mcx$ pre nejaké $x \in \mathbb{Z}$, potom $a - b = mx$, takže $a \equiv b \pmod m$.

(ii) Z podmienky $(m, c) = 1$ dostávame, že $1 = mu + cv$ pre nejaké $u, v \in \mathbb{Z}$. Ďalej máme predpoklad $ac - bc = mx$ pre nejaké $x \in \mathbb{Z}$. Prvú rovnosť vynásobíme $a - b$ a dostaneme

$$a - b = (a - b)(mu + cv) = amu - bmu + acv - bcv = amu - bmu + (ac - bc)v =$$
$$= amu - bmu + mxv = m(au - bu + xv),$$

takže m delí $(a - b)$. ∎

Nasledujúce tvrdenie je známe ako *Malá veta Fermatova* (MVF).

Veta 5.3. *Pre každé prvočíslo p a každé $n \in \mathbb{Z}$ platí*

$$n^p \equiv n \pmod p.$$

Naviac, keď $(p, n) = 1$, tak

$$n^{p-1} \equiv 1 \pmod n.$$

D ô k a z. Druhá kongruencia vyplýva z prvej po vykrátení n. Prvá sa ľahko dokáže pre $p = 2$, lebo $n^2 - n = n(n-1)$ je súčin dvoch za sebou idúcich celých čísel, a teda musí byť deliteľný 2.

Predpokladajme teraz $p \neq 2$, takže p je nepárne. Kongruenciu $n^p \equiv n \pmod{p}$ stačí dokážať pre nezáporné n, lebo $(-n)^p - (-n) = -(n^p - n)$. (Tu treba nepárnosť p.)

Použijeme matematickú indukciu podľa n. Pre $n = 0$ je tvrdenie zrejmé. Predpokladajme teraz, že tvrdenie platí pre $n = k$, teda že

$$k^p - k \quad \text{je deliteľné } p.$$

Chceme dokázať, že

$$(k+1)^p - (k+1) \quad \text{je deliteľné } p.$$

Podľa binomickej vety máme

$$(k+1)^p = k^p + \binom{p}{1} k^{p-1} + \binom{p}{2} k^{p-2} + \cdots + \binom{p}{p-1} k + 1.$$

Binomický koeficient je definovaný ako

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Teraz prichádza najdôležitejší myšlienkový krok. Pretože p je prvočíslo, nemôže sa v horeuvedenom zlomku vykrátiť (v menovateli sú len čísla od 1 do $p-1$), takže všetky tie binomické koeficienty ($i = 1, \ldots, p-1$) sú deliteľné p. Preto

$$(k+1)^p = k^p + px + 1$$

pre nejaké $x \in \mathbb{Z}$ a potom

$$(k+1)^p - (k+1) = k^p + px + 1 - k - 1 = (k^p - k) + px,$$

čo je deliteľné p, lebo podľa indukčného predpokladu je $k^p - k$ deliteľné p. ∎

Spolu s technikou modulárneho umocňovania poskytuje Malá veta Fermatova možnosť efektívneho testovania prvočíselnosti. Pre veľké čísla p (povedzme rádu 10^{100}) priame testovanie prvočíselnosti (delením) presahuje možnosti aj najrýchlejších počítačov. Efektívne však vieme zistiť, či pre zvolené n platí $n^p \equiv n \pmod{p}$. Ak taká kongruencia neplatí, máme istotu, že p je zložené. (Ale nezistíme tým jeho rozklad!) Ak kongruencia platí, máme aspoň 50% pravdepodobnosť, že p je prvočíslo. (Pre niektoré p tento odhad celkom neplatí a treba použiť trochu zložitejšie metódy.). Opakovaním tohoto testu sa môže istota prvočíselnosti priblížiť ľubovoľne blízko k 100%.

Tieto okolnosti uvádzame preto, lebo majú praktický význam. Veľké prvočísla sa často využívajú v šifrovacích algoritmoch a počítačovej bezpečnosti.

Z druhej strany, ak *vieme*, že modul je prvočíslo, Malá veta Fermatova urýchli modulárne umocňovanie. Zopakujme výpočet 5^{222} modulo 11. Pre $p = 11$, $n = 5$ nám MVF dáva

$$5^{10} \equiv 1 \pmod{11}.$$

Po umocnení na 22 dostávame

$$5^{220} \equiv 1^{20} = 1 \pmod{11},$$

takže

$$5^{222} = 5^{220} \cdot 5^2 \equiv 1 \cdot 25 = 25 \equiv 3,$$

čím sme dospeli k rovnakému výsledku ako predtým.

6. Lineárne kongruencie a Diofantické rovnice

Lineárna kongruencia je vzťah

$$ax \equiv b \ (\mod m)$$

s neznámou x a danými $a, b, m \in \mathbb{Z}$. Celé čísla x, ktoré vyhovujú tejto kongruencii nazývame riešeniami.

Veta 6.1. *Kongruencia $ax \equiv b \ (\mod m)$ má riešenie práve vtedy, keď $d = (a, m)$ delí b. Riešením sú práve tie $x \in \mathbb{Z}$, ktoré spĺňajú podmienku*

$$x \equiv \frac{b}{d}u \ (\mod \frac{m}{d}),$$

kde $d = au + mv$ $(u, v \in \mathbb{Z})$.

D ô k a z. Predpokladajme, že x je riešenie, teda

$$ax - b = my$$

pre nejaké $y \in \mathbb{Z}$. Potom

$$\frac{b}{d} = \frac{a}{d}x - \frac{m}{d}y$$

je celé číslo, teda d delí b. Ďalej, rovnosť $ax - b = my$ vynásobíme číslom u a dosadíme $au = d - mv$:

$$aux - bu = myu$$
$$(d - mv)x - bu = myu$$
$$dx - bu = m(vx - yu).$$

Vydelíme d:

$$x - \frac{b}{d}u = \frac{m}{d}(vx - yu).$$

Zistili sme, že $x - \frac{b}{d}u$ je deliteľné $\frac{m}{d}$, teda platí

$$x \equiv \frac{b}{d}u \ (\mod \frac{m}{d}).$$

Opačným smerom, predpokladajme, že $d|b$ a $x \equiv \frac{b}{d}u \ (\mod \frac{m}{d})$. Chceme dokázať, že $ax \equiv b \ (\mod m)$. Máme

$$x - \frac{b}{d}u = \frac{m}{d}y$$

pre nejaké $y \in \mathbb{Z}$. Potom

$$ax - b = a(\frac{b}{d}u + \frac{m}{d}y) - b = \frac{b}{d}(d - mv) + \frac{m}{d}ay - b = \frac{b}{d}(-mv) + \frac{m}{d}ay = m\frac{ay - bv}{d}.$$

(Opäť sme dosadili $au = d - mv$.) Pretože $\frac{ay-bv}{d}$ je celé číslo (a aj b sú deliteľné d), je $ax - b$ deliteľné m, čo sme mali dokázať. ∎

Riešenie lineárnych kongruencií ilustrujeme na príklade

$$15x \equiv 7 \ (\mod 37).$$

Platí $(15, 37) = 1$, Euklidovým algoritmom dostaneme $1 = 15 \cdot 5 - 37 \cdot 2$, teda $u = 5$ a kongruencia má riešenie

$$x \equiv 7 \cdot u = 35 \ (\mod 37).$$

Veta o delení so zvyškom dovoľuje zapísať riešenie aj v parametrickom tvare

$$x = 37k + 35, \quad k \in \mathbb{Z}.$$

Ako príklad lineárnej kongruencie, ktorá nemá riešenie uveďme

$$21x \equiv 16 \ (\mod 33).$$

Skutočne, $(21, 33) = 3$ a 3 nedelí 16.

Diofantické rovnice sú vo všeobecnosti rovnice s viacerými neznámymi, kde hľadáme celočíselné riešenia. My sa budeme venovať iba najjednoduchšiemu typu, a to sú lineárne rovnice s dvoma neznámymi. Pri riešení takých rovníc sa uplatnia lineárne kongruencie. Postup ukážeme na príklade.

Hľadajme celočíselné riešenia rovnice

$$18x - 23y = 10.$$

Vyjadríme

$$x = \frac{23y + 10}{18}.$$

Pretože x má byť celé číslo, musí $23y + 10$ byť deliteľné 18, čo sa dá vyjadriť kongruenciou

$$23y \equiv -10 \ (\mod 18),$$

ktorá má riešenie

$$y \equiv 16 \ (\mod 18).$$

Parametrický tvar $y = 18k + 16$ nám teraz dovoľuje dopočítať x:

$$x = \frac{23(18k + 16) + 10}{18} = \frac{23 \cdot 18k + 378}{18} = 23k + 21.$$

Takže riešením pôvodnej rovnice sú všetky dvojice tvaru $[23k + 21, 18k + 16]$, kde $k \in \mathbb{Z}$. Napríklad pre $k = 0$ máme riešenie $x = 21$, $y = 16$, voľba $k = -1$ dáva $x = -2$, $y = -2$.

7. Polia

Pole je množina F, na ktorej sú definované binárne operácie $\oplus$ a $\odot$ (sčítanie a násobenie), pričom platí:

(1) $x \oplus y = y \oplus x$ pre každé $x, y \in F$;
(2) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ pre každé $x, y, z \in F$;
(3) existuje $o \in F$ také, že $x \oplus o = x$ pre každé $x \in F$;
(4) pre každé $x \in F$ existuje $y \in F$ také, že $x \oplus y = o$;
(5) $x \odot (y \odot z) = (x \odot y) \odot z$ pre každé $x, y, z \in F$;
(6) $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$, $(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$ pre každé $x, y, z \in F$;
(7) $x \odot y = y \odot x$ pre každé $x, y \in F$;
(8) existuje $j \in F$ také, že $j \odot x = x$ pre každé $x \in F$;
(9) pre každé $x \in F \setminus \{o\}$ existuje $y \in F$ také,že $x \odot y = j$.

Prvok o z axiómy (3) sa nazýva *nulový prvok* a vo väčšine prípadov (vtedy keď $\oplus$ a $\odot$ sú obvyklé sčítanie a násobenie) to bude číslo 0. Podobne, prvok j z axiómy (8) sa nazýva *jednotkový prvok* a vo väčšine prípadov to bude číslo 1. Prvok y z axiómy (4) sa nazýva *opačný ku* x a označuje $-x$. Pomocou opačných prvkov sa v poli definuje odčítanie. Prvok y z axiómy (9) sa nazýva *inverzný ku* x a označuje x^{-1}. Pomocou inverzných prvkov sa v poli definuje delenie. Všimnime si, že (9) žiada existenciu inverzného prvku len ku nenulovým x. (Nulou sa nedá deliť!)

Axiómy (1),(2),(5), (6), (7) majú svoje pomenovania známe zo školskej matematiky.

Veta 7.1. *Množina $\mathbb{Q}$ racionálnych čísel s obvyklými operáciami sčítania a násobenia tvorí pole.*

D ô k a z. Na ukážku dokážeme distributívny zákon, ostatné ponecháme ako cvičenie. Využívame vlastnosti celých čísel, uvedené v 1. kapitole. Takže nech

$$x = \frac{p}{q}, \quad y = \frac{r}{s}, \quad z = \frac{t}{u}$$

sú racionálne čísla, t.j. $p, q, r, s, t, u \in \mathbb{Z}$. Potom

$$x(y+z) = \frac{p}{q}\frac{ru+st}{su} = \frac{pru+pst}{qsu},$$

$$xy + xz = \frac{pr}{qs} + \frac{pt}{qu} = \frac{pru+pst}{qsu},$$

teda $x(y+z) = xy + xz$. ∎

Veta 7.2. *Množina $\mathbb{R}$ reálnych čísel s obvyklými operáciami sčítania a násobenia tvorí pole.*

Dôkaz uvedenej vety si vyžaduje precíznu definíciu reálnych čísel, ktorá patrí skôr do matematickej analýzy než algebry, preto ho neuvádzame. Na druhej strane, pomocou tejto vety môžeme dokázať nasledujúcu.

Veta 7.3. *Množina $\mathbb{C}$ komplexných čísel s obvyklými operáciami sčítania a násobenia tvorí pole.*

D ô k a z. Opäť na ukážku dokážeme platnosť asociatívneho zákona pre násobenie a zákona o inverzných prvkoch.

Nech $x = a+bi$, $y = c+di$, $z = e+fi$ sú komplexné čísla, teda $a, b, c, d, e, f \in \mathbb{R}$. Pri nasledujúcich úpravách využívame fakt, že reálne čísla tvoria pole a teda spĺňajú príslušné zákony:

$$x(yz) = (a+bi)(ce-df+cfi+dei) = ace-adf-bcf-bde+(acf+ade+bce-bdf)i,$$
$$(xy)z = (ac-bd+adi+bci)(e+fi) = ace-bde-adf-bcf+(acf-bdf+ade+bce)i,$$

takže $x(yz) = (xy)z$.

Ďalej,

$$\frac{1}{a+bi} = \frac{1}{a+bi}\cdot\frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2},$$

takže komplexné číslo

$$\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$$

je inverzné ku $a + bi$. ∎

Existuje nekonečne veľa ďalších príkladov číselných polí. Uveďme z nich aspoň nasledujúci.

Nech $\mathbb{Q}(\sqrt{2})$ je množina všetkých reálnych čísel, ktoré sa dajú zapísať v tvare $a + b\sqrt{2}$, kde $a, b \in \mathbb{Q}$. Ľahko možno overiť, že $\mathbb{Q}(\sqrt{2})$ s obvyklým sčítaním a násobením je pole. (Využitím faktu, že $\mathbb{Q}$ je pole. Zákon o inverzných prvkoch sa dokáže podobne ako pre komplexné čísla.)

Prejdeme teraz k dôležitému príkladu, ktorým je pole zvyškových tried. Pre $n > 0$ a $0 \leq k < n$ nech k_n označuje množinu všetkých celých čísel, ktoré pri delení číslom n dávajú zvyšok k. Teda

$$k_n = \{nz + k \mid z \in \mathbb{Z}\}.$$

Napríklad

$$3_5 = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}.$$

Množina

$$\mathbb{Z}_n = \{0_n, 1_n, 2_n, \ldots, (n-1)_n\}$$

sa nazýva *množinou zvyškových tried modulo n*. Je to teda n-prvková množina, ktorej prvkami sú množiny 0_n,...,$(n-1)_n$ - tým hovoríme zvyškové triedy.

Na množine $\mathbb{Z}_n$ definujeme operácie sčítania a násobenia pomocou reprezentantov. Triedy k_n a l_n sčítame tak, že z nich vyberieme reprezentantov $x \in k_n$, $y \in l_n$, a zistíme, do ktorej zvyškovej triedy patrí súčet $x+y$ (t.j. nájdeme zvyšok po delení čísla $x + y$ číslom n). Zo základných vlastností kongruencií vyplýva, že výsledok nezávisí na výbere reprezentantov. Najjednoduchšie je zvoliť $x = k$ a $y = l$, ale nutné to nie je.

Podobne postupujeme pri definícii súčinu. Súčinom $k_n \cdot l_n$ bude tá zvyšková trieda, do ktorej patrí xy.

Na ilustráciu uveďme tabuľky pre násobenie v $\mathbb{Z}_5$. Kvôli prehľadnosti v nich vynechávame index 5 v označení zvyškových tried.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Veta 7.4. *Množina $\mathbb{Z}_n$ s uvedenými operáciami spĺňa podmienky (1)-(8) z definície poľa, pre každé $n > 1$. Podmienka (9) je splnená v $\mathbb{Z}_n$ práve vtedy, keď n je prvočíslo.*

D ô k a z. Platnosť podmienok (1)-(8) v $\mathbb{Z}_n$ vyplýva z platnosti týchto podmienok v $\mathbb{Z}$. Napríklad $k_n + l_n = l_n + k_n$ platí preto, lebo $k + l = l + k$, takže čísla $k + l$ a $l + k$ patria do tej istej zvyškovej triedy.

Pozrime sa podrobnejšie na podmienku (9). (Tá totiž v $\mathbb{Z}$ neplatí!) Máme zvyškovú triedu $a_n \in \mathbb{Z}_n$, $a_n \neq 0_n$. Hľadáme zvyškovú triedu y_n tak, aby $a_n \cdot y_n = 1_n$. To znamená, že chceme, aby číslo ay dávalo pri delení n zvyšok 1. To jest, máme kongruenciu

$$ay \equiv 1 \ (\mod n).$$

A teraz: ak n je prvočíslo, tak $(a, n) = 1$ (lebo $a \in \{1, \ldots, n-1\}$) a podľa Vety 6.1 má horeuvedená kongruencia riešenie - existuje inverzný prvok. Naopak, ak n nie je prvočíslo, tak môžeme zvoliť a tak, aby $(a, n) \neq 1$, a vtedy kongruencia nemá riešenie - ku takému a_n nebude existovať inverzný prvok. ∎

Takže ak n je prvočíslo, $\mathbb{Z}_n$ je pole. Dáva nám to nekonečne veľa nových príkladov polí (tentoraz s konečným počtom prvkov).

Ak n nie je prvočíslo, tak $\mathbb{Z}_n$ nie je pole. Splnenie (1)-(8) však znamená, že $\mathbb{Z}_n$ je *okruh* (presnejšie, *komutatívny okruh s jednotkou*).

8. Sústavy lineárnych rovníc

Pod sústavou lineárnych rovníc (SLR) nad poľom F rozumieme systém rovníc tvaru

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \cdots + a_{2n}x_n &= b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 + \cdots + a_{3n}x_n &= b_3 \\ &\ldots \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \cdots + a_{mn}x_n &= b_m, \end{aligned} \tag{1}$$

kde $a_{ij}, b_i \in F$ voláme *koeficienty* sústavy, a $x_1, \ldots, x_n$ sú symboly označujúce neznáme.

Všimnime si, že počet rovníc a počet neznámych nemusí byť rovnaký.

Za riešenie takejto sústavy považujeme každú n-ticu $(t_1, \ldots, t_n)$ prvkov z F, ktoré po dosadení $x_i = t_i$, $i = 1, \ldots, n$ spĺňajú uvedené rovnice. Takých n-tíc môže existovať aj viac, alebo nemusí existovať žiadna, preto hovoríme o množine riešení.

Uvedenú SLR budeme riešiť pomocou algoritmu, ktorý sa nazýva *Gaussova eliminačná metóda*. Myšlienkou tejto metódy je, že pomocou vhodných úprav budeme znižovať počet neznámych v rovniciach, až nakoniec (v ideálnom prípade) dostaneme rovnicu s jednou neznámou.

Budeme používať nasledujúce úpravy:

(U1) výmena poradia rovníc;
(U2) vynásobenie rovnice nenulovou konštantou;
(U3) pripočítanie ľubovoľného násobku niektorého riadku k inému riadku;
(U4) vynechanie nulovej rovnice (t.j. takej, ktorej všetky koeficienty sú 0).

Tieto úpravy voláme *ekvivalentné*, pretože platí

Veta 8.1. *Úpravy typov (U1)-(U4) nemenia množinu riešení sústavy.*

D ô k a z. Pre (U1) a (U4) je tvrdenie triviálne. Dokážeme tvrdenie pre (U3). ((U2) sa dokáže podobne.) Predpokladajme, že máme SLR v podobe ako na

začiatku tejto kapitoly. Teraz ku k-tej rovnici pripočítajme c-násobok j-tej ($k \neq j$). Dostaneme tým novú SLR, v ktorej sa pôvodná k-tá rovnica

$$a_{k1}x_1 + a_{k2}x_2 + a_{k3}x_3 + \cdots + a_{kn}x_n = b_k$$

zmenila na

$$(a_{k1} + ca_{j1})x_1 + (a_{k2} + ca_{j2})x_2 + \cdots + (a_{kn} + ca_{jn})x_n = b_k + cb_j.$$

Ostatné rovnice sa nezmenili. (j-tú sme násobili c iba "v duchu".) Nech teraz $(t_1, \ldots, t_n)$ je riešenie pôvodnej SLR. Táto n-tica teda spĺňa j-tú aj k-tú rovnicu pôvodnej SLR, takže

$$a_{j1}t_1 + a_{j2}t_2 + a_{j3}t_3 + \cdots + a_{jn}t_n = b_j$$
$$a_{k1}t_1 + a_{k2}x_2 + a_{k3}x_3 + \cdots + a_{kn}x_n = b_k.$$

Keď prvú z týchto dvoch rovností vynásobíme c a pripočítame ku druhej, dostaneme

$$(a_{k1} + ca_{j1})t_1 + (a_{k2} + ca_{j2})t_2 + \cdots + (a_{kn} + ca_{jn})t_n = b_k + cb_j,$$

čo znamená, že $(t_1, \ldots, t_n)$ vyhovuje aj zmenenej k-tej rovnici.

Tým sme ukázali, že pri úprave typu (U3) sa žiadne riešenia nestratia. Nemôžu ale ani pribudnúť. To vyplýva napríklad z toho, že úprava typu (U3) je vratná: od novej SLR sa môžeme vrátiť ku pôvodnej zase použitím úpravy typu (U3) (len treba zobrať $-c$ namiesto c). A pri tom návrate sa tiež žiadne riešenia nestratia. ∎

Kvôli prehľadnosti je obvyklé namiesto SLR v podobe ako na začiatku tejto kapitoly pracovať s obdĺžnikovou tabuľkou

$$\left(\begin{array}{ccccc|c} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} & b_2 \\ a_{31} & a_{32} & a_{33} & \ldots & a_{3n} & b_3 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} & b_m \end{array}\right)$$

ktorú voláme *rozšírená matica sústavy*, a po vynechaní posledného stĺpca *matica sústavy*. Ekvivalentné úpravy SLR teraz zodpovedajú operáciám s riadkami tejto matice. A tieto úpravy budeme robiť tak, aby sme maticu upravili na tzv. *Gaussov tvar* v zmysle nasledujúcej definície.

Definícia 8.2. Pivotom *riadku matice rozumieme prvý nenulový prvok tohoto riadku. (Nulové riadky pivot nemajú.) Hovoríme, že matica je v Gaussovom tvare, ak platí*

(i) *matica nemá nulový riadok;*
(ii) *ak a_{jp} je pivot j-tého riadku a a_{kq} je pivot k-tého riadku, pričom $j < k$, tak $p < q$.*

Názorne, podmienka (ii) znamená, že rovnica, ktorá je nižšie, musí mať pivot viac napravo. Špeciálne, žiadne dva pivoty nesmú byť pod sebou.

Veta 8.3. *Každá matica sa pomocou ekvivalentných úprav upraviť na Gaussov tvar.*

Dôkazom uvedenej vety je algoritmus, ktorý teraz popíšeme. Jeho myšlienka je, že "robíme poriadok po stĺpcoch".

1. Zistíme, či nejaký riadok má pivot v prvom stĺpci. Ak áno, tak výmenou dosiahneme, aby to bol prvý riadok. Potom použitím (U3) dosiahneme, aby všetky

ďalšie riadky mali v prvom stĺpci 0. Konkrétne, ku k-tému riadku pripočítame $(-\frac{a_{k1}}{a_{11}})$-násobok prvého.

2. Ak by v prvom stĺpci nebol žiaden pivot (t.j. sú tam samé nuly), nemusíme robiť nič - stĺpec je v poriadku.

3. Po vykonaní horeuvedených krokov urobíme tú istú procedúru s druhým stĺpcom, následne s tretím a ďalšími, až dostaneme Gaussov tvar. Ak sa v priebehu výpočtu vyskytne nulový riadok, tak ho vynecháme.

Celý postup si predvedieme na príklade. Uvažujme SLR nad $\mathbb{R}$ s maticou

$$\left(\begin{array}{cccc|c} 0 & 0 & -1 & 1 & 2 \\ 1 & -2 & -4 & 1 & 0 \\ 2 & -4 & 0 & -3 & -10 \\ 3 & -6 & -5 & -1 & -8 \end{array}\right)$$

Vymeníme prvé dva riadky.

$$\left(\begin{array}{cccc|c} 1 & -2 & -4 & 1 & 0 \\ 0 & 0 & -1 & 1 & 2 \\ 2 & -4 & 0 & -3 & -10 \\ 3 & -6 & -5 & -1 & -8 \end{array}\right)$$

Pomocou pivota prvého riadku teraz vynulujeme pivotov ostatných riadkov. Preto

a) (-2)-násobok prvého riadku pripočítame ku tretiemu;
b) (-3)-násobok prvého riadku pripočítame ku štvrtému.

Všimnime si, že prvý riadok sa pri týchto úpravách nezmení.

$$\left(\begin{array}{cccc|c} 1 & -2 & -4 & 1 & 0 \\ 0 & 0 & -1 & 1 & 2 \\ 0 & 0 & 8 & -5 & -10 \\ 0 & 0 & 7 & -4 & -8 \end{array}\right)$$

Teraz by sme mali podobným spôsobom spracovať druhý stĺpec. Nastal však zvláštny prípad, že v tomto stĺpci nie je žiaden pivot. Preto prejdeme ku tretiemu stĺpcu. Tam sú až tri pivoty, zostať môže iba jeden. Preto

a) 8-násobok druhého riadku pripočítame ku tretiemu;
b) 7-násobok druhého riadku pripočítame ku štvrtému.

$$\left(\begin{array}{cccc|c} 1 & -2 & -4 & 1 & 0 \\ 0 & 0 & -1 & 1 & 2 \\ 0 & 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 3 & 6 \end{array}\right)$$

Zostali nám ešte dva pivoty vo štvrtom stĺpci, jeden treba vynulovať. Preto (-1)-násobok tretieho riadku pripočítame ku štvrtému. Tým sa ale štvrtý riadok úplne vynuluje, takže ho vynecháme. Dostali sme maticu v Gaussovom tvare

$$\left(\begin{array}{cccc|c} 1 & -2 & -4 & 1 & 0 \\ 0 & 0 & -1 & 1 & 2 \\ 0 & 0 & 0 & 3 & 6 \end{array}\right)$$

Po úprave na Gaussov tvar už vieme popísať množinu riešení SLR. Môžu nastať nasledujúce prípady.

1. SLR obsahuje sporný riadok, t.j. taký, ktorý má pivot na pravej strane. Taký riadok zodpovedá rovnici

$$0x_1 + 0x_2 + \cdots + 0x_n = b \neq 0.$$

Taká rovnica zrejme nemôže byť splnená pre žiadne $x_1, \ldots, x_n$, takže SLR nemá riešenie.

2. SLR nebsahuje sporný riadok a počet riadkov sa rovná počtu neznámych. Takémuto Gaussovnu tvaru hovoríme *trojuholníkový tvar*. SLR má vtedy jediné riešenie $(t_1, t_2, \ldots, t_n)$, ktoré nájdeme "odzadu": z poslednej rovnice vypočítame t_n, z predposlednej potom t_{n-1}, atď.

3. SLR neobsahuje sporný riadok a počet riadkov je menší ako počet neznámych. Počet riešení teraz závisí od rozdielu medzi počtom riadkov a neznámych, a tiež od poľa F. (Nad konečným poľom musí byť počet riešení konečný.) Množinu riešení môžeme popísať pomocou parametrov. Tie stĺpce, v ktorých nie je pivot, zodpovedajú tzv. voľným neznámym - môžeme ich voliť ľubovoľne. Hodnoty ostatných premenných potom dopočítame podobne ako v bode 2.

Vráťme sa teraz k nášmu prípadu. Dostali sme Gaussov tvar, v ktorom nie je sporná rovnica, a kde sú 3 riadky a 4 neznáme. Nastal teda prípad 3. Neznáma x_2 je voľná, môže nadobudnúť akúkoľvek hodnotu $x_2 = t \in \mathbb{R}$. Z tretej rovnice teraz dostaneme $x_4 = 2$, z druhej potom $x_3 = 0$ a z prvej $x_1 = 2t - 2$. Množina riešení SLR je

$$\{(2t - 2, t, 0, 2) \mid t \in \mathbb{R}\}.$$

9. Permutácie

Permutácia na množine A je bijektívne zobrazenie $A \to A$. My sa budeme zaoberať prípadom $A = \{1, 2, \ldots, n\}$. Množinu všetkých permutácii na $\{1, \ldots, n\}$ označujeme S_n. Táto množina má $n!$ prvkov.

Z rozsiahlej teórie permutácií sa budeme venovať iba jednej otázke: párnosti.

Definícia 9.1. *Dvojica $i < j$ sa nazýva* inverzia *permuácie $\varphi \in S_n$, ak $\varphi(i) > \varphi(j)$. Permuácia φ sa nazýva párna, ak má párny počet inverzií; v opačnom prípade sa nazýva nepárna.*

Počet inverzií permutácie φ budeme označovať $i(\varphi)$.

Permutácie budeme zapisovať ako matice s dvomi riadkami. V prvom riadku sú čísla od 1 do n, v druhom sú postupne dodnoty $\varphi(1)$, $\varphi(2), \ldots, \varphi(n)$. Napríklad

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

popisuje permutáciu $\pi \in S_5$ takú, že $\pi(1) = 5$, $\pi(2) = 1$, $\pi(3) = 3$, $\pi(4) = 2$, $\pi(5) = 4$. Jej inverzie sú $1 < 2, 1 < 3, 1 < 4, 1 < 5, 3 < 4$, teda $i(\pi) = 5$, ide teda o permutáciu nepárnu.

Často je užitočná aj ekvivalentná charakterizácia párnosti, ktorá sa zakladá na skladaní transpozícií. *Transpozícia* je permuácia, ktorá mení dva prvky a všetky ostatné necháva na mieste. Napríklad

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

je transpozícia, ktorá mení 2 a 4.

Permutácie sú funkcie, takže ich môžeme skladať. Zloženie dvoch permutácií znamená, že množina $\{1,\dots,n\}$ sa najprv permutuje (premieša) jednou permutáciou, potom druhou. Ľahko sa ukáže, že každá permutácia je zložením transpozícií. Napríklad vyššie uvedená permutácia π je zložením 3 transpozícií. najprv vymeníme prvky 1 a 5. To je transpozícia

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$

Potom vymeníme 1 a 2, dostaneme

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$$

Nakoniec vymeníme 2 a 4 a dostaneme permutáciu π.

Každá transpozícia je nepárna permutácia. Ak transpozícia mení j a k ($j<k$), tak jej inverziami sú dvojice $(j,j+1),(j+1,k),(j,j+2),(j+2,k),\dots,(j,k-1),(k-1,k)$ a ešte (j,k). Spolu je to $2(k-j-1)+1$ inverzií, čo je nepárne číslo.

Podobnou úvahou (detailný dôkaz vynecháme) sa dá dokázať nasledujúce tvrdenie.

Lema 9.2. *Zloženie ľubovoľnej permutácie φ s ľubovoľnou transpozíciou mení párnosť permutácie φ.*

Ako dôsledok teraz dostávame

Veta 9.3. (i) *Permutácia je párna práve vtedy, keď je zložením párneho počtu transpozícií.*

(ii) *Zloženie dvoch permutácií rovnakej párnosti (t.j. dvoch párnych alebo dvoch nepárnych) je párne.*

(iii) *Zloženie dvoch permutácií opačnej párnosti je nepárne.*

D ô k a z. Z predošlej lemy vyplýva, že zloženie párneho počtu transpozícií je párne a nepárneho počtu nepárne. Takže platí (i). Ďalej, nech π je zložením transpozícií $\sigma_1,\dots,\sigma_k$, a φ zložením $\tau_1,\dots,\tau_l$. Potom $\pi\varphi$ je zložením $\sigma_1,\dots,\sigma_k,\tau_1,\dots,\tau_l$, a to je párne práve vtedy, keď číslo $k+l$ je párne, čiže keď k a l majú rovnakú párnosť. ∎

Medzi permutácie zahŕňame aj identické zobrazenie

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix},$$

t.j. $\iota(k)=k$ pre každé k. Táto permutácia nemá žiadne inverzie, takže je párna. Ďalej, táto permutácia je neutrálnym prvkom vzhľadom na skladanie, t.j. $\pi\iota=\iota\pi=\pi$ pre každé $\pi\in S_n$.

Ku každej permutácii π existuje inverzná π^{-1}, ktorú definujeme predpisom

$$\pi^{-1}(j)=k \quad \text{práve vtedy keď} \quad \pi(k)=j$$

(všetko pošleme naspäť). Napríklad ku

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

bude inverzná

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

Z vety 9.3 vyplýva, že π a π^{-1} majú rovnakú párnosť: ich zložením je totiž párna permutácia ι.

10. Determinanty

Nech A je matica

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

s prvkami z poľa F. Je to teda štvorcová matica $n \times n$, ktorej prvok v j-tom stĺpci a k-tom riadku označíme a_{jk}. *Determinantom* takejto matice nazývame číslo (prvok F)

$$|A| = \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} a_{2\varphi(2)} \dots a_{n\varphi(n)}.$$

Tento vzorec znamená, že

(1) pre každú permutáciu φ nájdeme v matici prvky $a_{1\varphi(1)}, \dots, a_{n\varphi(n)}$;
(2) tieto prvky vynásobíme;
(3) ak permutácia je nepárna, tak ten súčin ešte vynásobíme (-1);
(4) takto získané čísla (pre všetky permutácie) spočítame.

Všimnime si, že medzi prvkami $a_{1\varphi(1)}, \dots, a_{n\varphi(n)}$ je presne jedno z každého riadku a presne jedno z každého stĺpca. V skutočnosti to platí aj naopak: každý výber n prvkov s touto vlastnosťou zodpovedá nejakej permutácii.

Pri maticiach malých rozmerov môžeme definíciu determinantu rozpísať explicitne. Pre $n = 1$ je

$$|A| = a_{11},$$

pre $n = 2$ máme

$$|A| = a_{11}a_{22} - a_{12}a_{21},$$

a pre $n = 3$ (tzv. *Sarusovo pravidlo*)

$$|A| = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{31} - a_{12}a_{21}a_{33}.$$

Pre matice vyšších rozmerov počet sčítancov rýchlo rastie a výpočet priamo z definície sa stáva neefektívny. Takéto determinanty možno počítať pomocou úpravy na trojuholníkový tvar. Výpočet sa zakladá na niekoľkých nasledujúcich tvrdeniach.

Lema 10.1. *Ak matica B vznikne z matice A výmenou dvoch riadkov, tak $|A| = -|B|$.*

D ô k a z. Uvedieme myšlienku dôkazu. V definícii determinantov $|A|$ a $|B|$ vystupujú tie isté súčiny $a_{1\varphi(1)} \dots a_{n\varphi(n)}$. (Lebo to sú všetky také n-tice, kde z každého riadku aj stĺpca je presne jeden prvok, a to sa výmenou riadkov nezmení.) Každý taký súčin však vystupuje v determinantoch $|A|$ a $|B|$ s opačným znamienkom. To je preto, lebo príslušná permutácia sa zložila s transpozíciou (ktorá zodpovedá výmene riadkov), takže zmenila párnosť. ∎

Lema 10.2. *Ak matica obsahuje dva rovnaké riadky, determinant je* 0.

D ô k a z. Keď vymeníme dva rovnaké riadky, matica sa nezmení. Podľa predošlej lemy ale $|A| = -|A|$, takže $|A| = 0$. (Nad poľom, kde $1+1=0$, napríklad $\mathbb{Z}_2$, tento argument nefunguje, treba použiť iný.) ∎

Lema 10.3. *Ak matica B vznikne z A tým, že k-tý riadok vynásobíme konštantou $c \in F$, tak $|B| = c|A|$.*

D ô k a z. Prvky matice B označme b_{ij}. Takže $b_{kj} = ca_{kj}$ a $b_{ij} = a_{ij}$ pre všetky i, j, $i \neq k$. Potom

$$\begin{aligned} |B| &= \sum_{\varphi \in S_n} (-1)^{i(\varphi)} b_{1\varphi(1)} b_{2\varphi(2)} \dots b_{n\varphi(n)} = \\ &= \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} \dots c a_{k\varphi(k)} \dots a_{n\varphi(n)} = \\ &= c \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} \dots a_{k\varphi(k)} \dots a_{n\varphi(n)} = c|A|. \end{aligned}$$

∎

Lema 10.4. *Ak matica B vznikne z A tým, že c-násobok m-tého riadku pripočítame ku k-tému riadku ($k \neq m$), tak $|B| = |A|$.*

D ô k a z. Označme C maticu, ktorá vznikne tak, že v matici A k-tý riadok nahradíme m-tým. Matica C má teda 2 rovnaké riadky, takže $|C| = 0$. Podobne ako v predošlom dôkaze, prvky matice B označíme b_{ij}. Teda $b_{kj} = a_{kj} + ca_{mj}$ a $b_{ij} = a_{ij}$ pre $i \neq k$. Rozpísaním definície a použitím distributívneho zákona dostávame

$$\begin{aligned} |B| &= \sum_{\varphi \in S_n} (-1)^{i(\varphi)} b_{1\varphi(1)} b_{2\varphi(2)} \dots b_{n\varphi(n)} = \\ &= \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} \dots (a_{k\varphi(k)} + ca_{m\varphi(k)}) \dots a_{n\varphi(n)} = \\ &= \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} \dots a_{k\varphi(k)} \dots a_{n\varphi(n)} + \\ &+ c \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} \dots a_{m\varphi(k)} \dots a_{n\varphi(n)} = |A| + c|C| = |A|. \end{aligned}$$

∎

Lema 10.5. *Ak matica obsahuje nulový riadok, determinant je* 0.

D ô k a z. Tvrdenie je zrejmé z definície. Každý súčin obsahuje prvok z každého riadku, čiže každý súčin obsahuje nulu. ∎

Lema 10.6. *Ak A je trojuholníková matica (t.j. $a_{ij} = 0$ pre všetky $i > j$), tak*

$$|A| = a_{11} a_{22} a_{33} \dots a_{nn}.$$

D ô k a z. Sčítanec $a_{11}a_{22}a_{33}\dots a_{nn}$ sa nachádza v definícii determinantu a zodpovedá identickej permutácii. Tá nemá žiadne inverzie, takže tento sčítanec tam je so znamienkom +. Tvrdíme, že všetky ostatné sčítance sú 0. Nech $\varphi \in S_n$, $t = a_{1\varphi(1)}a_{2\varphi(2)}\dots a_{n\varphi(n)}$. Potom:

(1) Ak $\varphi(1) \neq 1$, tak $\varphi(k) = 1$ pre nejaké $k > 1$ a t je súčinom prvkov medzi ktorými je $a_{k1} = 0$, takže $t = 0$.
(2) Ak $\varphi(1) = 1$ a $\varphi(2) \neq 2$, tak $\varphi(k) = 2$ pre nejaké $k > 2$ a súčin pre t obsahuje $a_{k2} = 0$.
(3) Ak $\varphi(1) = 1$, $\varphi(2) = 2$ a $\varphi(3) \neq 3$, tak $\varphi(k) = 3$ pre nejaké $k > 3$ a súčin obsahuje $a_{k3} = 0$.

Pokračovaním tejto úvahy dostaneme, že t môže byť nenulové jedine keď φ je identická permutácia. ∎

Teraz už môžeme popísať metódu výpočtu $|A|$. Maticu A upravujeme pomocou úprav (U1)-(U3) na Gaussov tvar. Ak počas výpočtu vznikne nulový riadok, determinant je 0. Ak nulový riadok nevznikne, dostaneme maticu v trojuholníkovom tvare, ktorej determinant získame vynásobením prvkov na hlavnej diagonále. Determinant pôvodnej matice dostaneme, keď zohľadníme, že pri úpravách typu (U1) sa menilo znamienko a pri úpravách typu (U2) sa hodnota násobila prvkom c.

Transponovanie matice A je preklopenie okolo hlavnej uhlopriečky. To znamená, že matica B transponovaná ku A má prvky $b_{ij} = a_{ji}$. Označujeme to $B = A^T$.

Veta 10.7. $|A| = |A^T|$.

D ô k a z. Uvedieme myšlienku dôkazu. Súčin $a_{1\varphi(1)}a_{2\varphi(2)}\dots a_{n\varphi(n)}$ v definícii $|A|$ je ten istý ako súčin $b_{1\psi(1)}b_{2\psi(2)}\dots b_{n\psi(n)}$ v definícii $|B|$, kde $\psi = \varphi^{-1}$. A pretože inverzné permutácie majú rovnakú párnosť, vystupujú tam tie súčiny s rovnakým znamienkom. ∎

Dôsledkom tejto vety je, že pri výpočte determinantov môžeme používať aj stĺpcové úpravy, ktoré majú na hodnotu determinantu rovnaký vplyv ako analogické riadkové úpravy. (Napríklad výmena 2 stĺpcov mení znamienko.) Totiž stĺpcové úpravy matice A zodpovedajú riadkovým úpravám matice A^T.

11. Rozvoj determinantu a Cramerovo pravidlo

Označme A_{ij} maticu, ktorá vznikne z A vynechaním i-tého riadku a j-tého stĺpca. Determinant tejto matice je $|A_{ij}|$. Ďalej označme $M_{ij} = (-1)^{i+j}|A_{ij}|$. Toto číslo (prvok F) sa nazýva *algebraický doplnok prvku* a_{ij}.

Veta o rozvoji (dôkaz vynecháme) hovorí nasledovné.

Veta 11.1. (i) *Pre každé k platí*

$$|A| = a_{k1}M_{k1} + a_{k2}M_{k2} + a_{k3}M_{k3} + \dots + a_{kn}M_{kn}.$$

(ii) *Pre každé k platí*

$$|A| = a_{1k}M_{1k}a_{2k}M_{2k} + a_{3k}M_{3k} + \dots + a_{nk}M_{nk}.$$

Rozpísanie determinantu podľa (i) sa volá rozvoj podľa k-tého riadku, (ii) je rozvoj podľa k-tého stĺpca. Použitie rozvoja znamená, že namiesto jedného determinantu matice $n \times n$ budeme počítať n determinantov $(n-1) \times (n-1)$. Napríklad

rozvojom determinantu

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$$

podľa druhého riadku dostaneme

$$4(-1)^{2+1}\begin{vmatrix} 2 & 3 \\ 8 & 9 \end{vmatrix} + 5(-1)^{2+2}\begin{vmatrix} 1 & 3 \\ 7 & 9 \end{vmatrix} + 6(-1)^{2+3}\begin{vmatrix} 1 & 2 \\ 7 & 8 \end{vmatrix}$$

Z výpočtového hľadiska je výhodné urobiť rozvoj podľa riadku alebo stĺpca, v ktorom je iba málo nenulových prvkov. Napríklad z

$$\begin{vmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 2 & 0 & 0 & 0 & 1 \end{vmatrix}$$

rozvojom podľa prvého stĺpca dostaneme

$$1 \cdot (-1)^{1+1}\begin{vmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{vmatrix} + 2 \cdot (-1)^{5+1}\begin{vmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{vmatrix}$$

Obe matice sú trojuholníkové (druhá po transponovaní), ich determinanty vypočítame vynásobením prvkov na uhlopriečke. Hodnota pôvodného determinantu teda je

$$1 \cdot 1 + 2 \cdot 16 = 33.$$

Pomocou vety o rozvoji teraz dokážeme Cramerovo pravidlo, ktoré dáva do súvisu determinanty a SLR. Také spojenie naznačoval už fakt, že determinanty môžeme počítať tým istým algoritmom, ktorý sa používa na riešenie SLR. Najprv jedno pomocné tvrdenie.

Lema 11.2. *Ak $j \neq k$, tak*

$$a_{j1}M_{k1} + a_{j2}M_{k2} + \cdots + a_{jn}M_{kn} = 0,$$

$$a_{1j}M_{1k} + a_{2j}M_{2k} + \cdots + a_{nj}M_{nk} = 0.$$

D ô k a z. Máme elegantný argument: $a_{j1}M_{k1} + a_{j2}M_{k2} + \cdots + a_{jn}M_{kn}$ je rozvoj podľa k-tého riadku matice, ktorá vznikne z A, keď k-tý riadok nahradíme j-tým. Taká matica má ale 2 rovnaké riadky, takže jej determinant je 0.

Druhá rovnosť vyplýva z podobnej úvahy pre stĺpce. ∎

Teraz uvažujme SLR s maticou

$$\left(\begin{array}{ccccc|c} a_{11} & a_{12} & a_{13} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} & b_2 \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} & b_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} & b_n \end{array}\right)$$

Nech A je matica tejto sústavy (bez pravej strany). Ďalej, nech B_j je matica, ktorá vznikne z A, keď j-tý stĺpec nahradíme pravou stranou, t.j. stĺpcom $(b_1, b_2, \ldots, b_n)^T$.

Veta 11.3. (Cramerovo pravidlo) *Ak $|A| \neq 0$, tak SLR má jediné riešenie, a to n-ticu $(y_1, \ldots, y_n)$, kde*

$$y_j = \frac{|B_j|}{|A|}$$

$j = 1, \ldots, n$.

D ô k a z. Ak $|A| \neq 0$, tak pri úprave na Gaussov tvar sa nemôže vynulovať žiaden riadok matice A. Preto dostaneme trojuholníkový tvar, čo znameá, že SLR má jediné riešenie. Zostáva len ukázať, že tým riešením je práve n-tica uvedené v našej vete. Teda chceme overiť, že n-tica $(y_1, \ldots, y_n)$ spĺňa všetky rovnice sústavy.

k-tá rovnica má tvar

$$a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n = b_k.$$

Dosaďme do nej $x_j = \frac{|B_j|}{|A|}$ a vynásobme rovnosť $|A|$. Máme teda dokázať, že

$$a_{k1}|B_1| + a_{k2}|B_2| + \cdots + a_{kn}|B_n| = b_k|A|.$$

Každý z determinantov $|B_j|$ rozvinieme podľa j-tého stĺpca, teda

$$|B_j| = b_1M_{1j} + b_2M_{2j} + b_3M_{3j} + \cdots + b_nM_{nj}.$$

(Algebraické doplnky M_{ij} sú tie isté ako pre maticu A.) Všetky tieto rozvoje dosadíme do ľavej strany dokazovanej rovnosti. Po preskupení sčítancov dostávame

$$a_{k1}|B_1| + a_{k2}|B_2| + \cdots + a_{kn}|B_n| = b_1c_1 + b_2c_2 + \cdots + b_nc_n,$$

kde

$$c_j = a_{k1}M_{j1} + a_{k2}M_{j2} + a_{k3}M_{j3} + \cdots + a_{kn}M_{jn}.$$

Podľa predošlej lemy je $c_j = 0$ pre všetky $j \neq k$. Ďalej,

$$c_k = a_{k1}M_{k1} + a_{k2}M_{k2} + a_{k3}M_{k3} + \cdots + a_{kn}M_{kn} = |A|.$$

(Je to rozvoj $|A|$ podľa k-tého riadku.) Preto

$$b_1c_1 + b_2c_2 + \cdots + b_nc_n = b_k|A|,$$

odkiaľ vyplýva dokazovaná rovnosť. ∎

Poznamenajme, že ak $|A| = 0$ (alebo ak matica A nie je štvorcová), tak Cramerovo pravidlo sa nedá použiť a SLR treba riešiť úpravou na Gaussov tvar.