

KALEIDOSKOP

TEORIE

ČÍSEL

(4. kapitola)

Martin Klazar

Vím, že čísla jsou krásná. A jestliže krásná nejsou, pak není krásné nic.

(Paul Erdős, *Sunday Times Magazine*, 27. listopadu 1988.)

Analogicky prožíval pan Š. číslice.

„Pro mne 2, 4, 6, 5 nejsou pouhá čísla. Mají tvar . . .

1 — to je ostré číslo, nezávisle na jeho grafickém vyjádření,
je to něco ukončeného, tvrdého.

2 — to je plošší, čtverhranné, bělavé, bývá trochu našedlé . . .

3 — to je zaostřený úlomek a točí se.

4 — to je opět čtvercové, tupé, podobné 2, ale mohutnější, tlusté . . .

5 — plné zakončení v podobě kužele, věže, masívní.

6 — to následuje první za „5“, je bělavé.

8 — to je nevinné, modravě mléčné, podobné vápnu.“

(A. R. Lurija, *Malá knížka o velké paměti*.)

Toto je předběžný text 4. kapitoly (kongruence) skript k mé přednášce *Úvod do teorie čísel*, kterou jsem konal na MFF UK v Praze v zimních semestrech školních roků 1996/97, 1998/99 a 1999/00. Zatím v preprintové řadě KAM-DIMATIA Series vyšly kapitoly 1 (základní pojmy a obraty), 2 (diofantické aproximace) a 3 (diofantické rovnice) a budou v ní postupně vydány zbylé kapitoly 5 (prvočísla), 6 (geometrie čísel), 7 (číselné rozklady), 8 (medailony matematiků) a 9 (návody k řešení úloh). Obtížnost úloh je bodována 0 (nejlehčí) až 5 (nejtěžší).

červenec 2000

Martin Klazar

Obsah

4	Zbytky čísel	1
4.1	Konečná pole	3
4.2	Chevalley–Warningova věta a kombinatorika	11
4.3	Zlatá věta	14
4.4	Weilova věta pro $F = \mathbf{Z}_p$	25
	4.4.1 Paleyho turnaje	27
	4.4.2 První část důkazu	32
	4.4.3 Druhá část důkazu	37
	4.4.4 Třetí část důkazu	44
4.5	Poznámky	47
4.6	Úlohy	51
	Literatura	55

Kapitola 4

Zbytky čísel

Zákon reciprocity kvadratických zbytků, věta 106, patří mezi nejkrásnější výsledky elementární teorie čísel. Poprvé ho formuloval v jazyku kvadratických forem už Leonard Euler ve spisu *Theoremata circa divisores numerorum in hac forma $pa^2 \pm qb^2$ contentorum* (1744/46). (Na to upozornil Leopold Kronecker v roce 1875.) Explicitně ho ve tvaru blízkém dnešnímu Euler uveřejnil znovu v *Observationes circa divisionem quadratorum per numeros primos* (publikováno v *Opuscula Analytica* posmrtně v r. 1783). Termín „reciprocita“ v názvu zákona razil Adrien-Marie Legendre, který se jím zabýval v pracích *Recherches d'Analyse Indéterminée* (1785/88) a *Essai sur la Théorie des Nombres* (1798). *Essai . . .* je vůbec první kniha věnovaná výhradně teorii čísel.

Legendre byl první, kdo podal alespoň částečný důkaz zákona reciprocity. Z osmi případů odpovídajících možnostem $p, q \equiv \pm 1 \pmod{4}$ a $\left(\frac{p}{q}\right) = \pm 1$ uměl dokázat v úplnosti dva: $p \equiv -q \equiv 1 \pmod{4}$ & $\left(\frac{p}{q}\right) = -1$ a $p \equiv q \equiv -1 \pmod{4}$ & $\left(\frac{p}{q}\right) = 1$. V důkazu zbylých šesti případů se odvolával na tvrzení, jehož důkaz tehdy nebyl znám a které dokázal Peter Dirichlet až v r. 1837, že v jisté zbytkové třídě leží vždy alespoň jedno prvočíslo.

V polovině devadesátých let vstoupil na scénu německý mladík, který byl synem nádeníka v Braunschweigu a jehož zázračný talent zachránilo mecenášství brunšvicko-wolfenbüttelského vévody. Carl Friedrich Gauss (nebo Gauß podle staršího pravopisu) experimentoval s kvadratickými zbytky už od roku 1792. Na začátku roku 1795 znovuobjevil nejprve 1. doplněk zákona reciprocity, relaci $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, a v březnu téhož roku zákon sám. 8. dubna 1796, podle záznamu v deníku, Gauss našel jeho důkaz. Důkaz rozlišuje osm Legendreových případů, je založen na indukci a je zcela elementární,

ale složitý. Gaussovi bylo bez několika dní 19 let. Svým objevem se po zásluze pyšnil a zákon reciprocity nazýval *Theorema Fundamentale* či dokonce *Theorema Aureum* (zlatá věta). 22. června 1796 našel druhý důkaz, založený na rodu kvadratických forem, a na podzim 1796 další dva důkazy. Monografie *Disquisitiones Arithmeticae*, jejíž vydání čtyřiatvacetiletým Gaussem v roce 1801 se považuje za počátek letopočtu moderní teorie čísel, obsahuje první dva důkazy. Gauss jich v průběhu života publikoval celkem šest a další dva byly nalezeny v jeho pozůstalosti.

My se v oddílu 4.3 spokojíme se dvěma. První, asi nejelementárnější ze známých důkazů, je založen na identitě mezi počty mřížových bodů v jistých rovinných útvech. Druhý užívá vlastností exponenciální funkce a náleží Gaussovu žáku Ferdinandu Eisensteinovi.

Nicméně naším hlavním tématem v kapitole 4 nebudou kvadratické zbytky, ale konečná pole. V 4.1 odvodíme jejich základní vlastnosti (shrnujeme je v tvrzení 92). Existence konečného pole vyplyne z enumerace polynomů: V Gaussově větě 89 dokážeme, že v $\mathbf{Z}_p[x]$ je $\frac{1}{n} \sum_{d \mid n} p^d \mu(n/d)$ monických ireducibilních polynomů stupně n . V důkazu Erdősovy a Chowlovy věty 94 uvidíme, jak lze pomocí konečných polí sestrojít velké podmnožiny $\{1, 2, \dots, n\}$, v nichž se žádná vzdálenost dvou prvků neopakuje. V 4.2 dokážeme Chevalley–Warningovu větu 95 o počtech řešení polynomiální soustavy nad konečným polem $\text{GF}(p^r)$ — přesahuje-li počet neznámých součet stupňů, je počet řešení dělitelný p — a uvedeme její dvě kombinatorická použití. V 4.3 kromě dvou zmíněných důkazů zákona reciprocity popíšeme teorii kvadratických zbytků, hlavně vlastnosti Legendreova symbolu.

Oddíl 4.4 věnujeme elementárnímu důkazu speciálního případu Weilovy věty 111, která patří k hlavním výsledkům teorie čísel ve 20. století. Věta říká, že pro konečné pole F a ireducibilní polynom $P \in F[X, Y]$, který zůstává ireducibilní i v $\overline{F}[X, Y]$ (\overline{F} označuje algebraický uzávěr F), má rovnice $P(x, y) = 0_F$ právě $|F| + O(|F|^{1/2})$ řešení $x, y \in F$. Jde o výsledek mnohem hlubší než Chevalley–Warningova věta, s obtížným důkazem. Spokojíme se s důkazem případu $F = \mathbf{Z}_p$. V pododdílu 4.4.1 dokážeme, že pro každé k existuje „turnaj“ mezi několika hráči, v němž je každých k hráčů poráženo nějakým jiným hráčem. Velmi jednoduchý důkaz užívající pravděpodobnostní metodu je nekonstruktivní. Jediný známý konstruktivní důkaz je založen na Weilově větě.¹

¹V lednu 2000 Tyszkiewicz publikoval nový, velmi jednoduchý konstruktivní důkaz. Viz poznámky.

V kapitole 4 u čtenáře předpokládáme zběhlost v zacházení se základními pojmy komutativní algebry, například v 4.4 pracujeme s pojmem algebraického uzávěru (o němž je ale třeba vědět v podstatě jen to, že existuje). Většinu pojmů se snažíme připomenout. Důkaz případu $F = \mathbf{Z}_p$ Weilovy věty v 4.4.2–4.4.4 je asi nejsložitějším důkazem skript. Chce-li čtenářka získat povšechný přehled o Weilově větě a nezajímají-li ji technické jemnosti důkazu, může si přečíst jen úvod 4.4, 4.4.1 a poznámky k 4.4.

4.1 Konečná pole

Připomínáme, že *těleso* je algebraická struktura $(T, +, \cdot)$ s binárními operacemi „sčítání“ $+$ a „násobení“ \cdot , přičemž $(T, +)$ je komutativní grupa, $T^* = (T \setminus \{0_T\}, \cdot)$ je grupa a obě operace svazuje distributivní zákon. Je-li multiplikatívni grupa nenulových prvků T^* komutativní, mluvíme o komutativním tělese neboli o *poli*. Příkladem nekomutativního tělesa jsou kvaterniony (úloha 3). Dá se dokázat, že všechna konečná tělesa jsou pole (úlohy 4 a 5). Příkladem konečného tělesa je pole zbytků $\mathbf{Z}_p = (\{0, 1, \dots, p-1\}, +, \cdot)$, v němž se sčítá a násobí běžným způsobem modulo prvočíslo p . Nás budou zajímat pouze konečná tělesa a proto se v definicích omezíme na pole.

Nechť F je pole, G jeho podpole a $\alpha \in F$. Řekneme, že α má *stupeň* r nad G , pokud $r = \min\{\deg(a) : a \in G[x] \text{ \& } a(\alpha) = 0_F\}$. Monický polynom $a \in G[x]$ realizující stupeň α je *minimální polynom* α nad G . Nechť F je pole a $n \in \mathbf{N}_0$. Jako n_F označíme prvek $1_F + 1_F + \dots + 1_F$, který vznikne sečtením n jednotkových prvků (0_F je nulový prvek F). Pro $n \in \mathbf{Z}$ a $n < 0$ rozšíříme tuto definici pomocí $n_F = -(-n)_F$. Pokud $n_F \neq 0_F$ pro všechna čísla $n > 0$, říkáme, že F má *charakteristiku* 0. Pokud $n_F = 0_F$ pro některé $n \in \mathbf{N}$, je nejmenší takové n prvočíslo p , jak hned dokážeme. O takových polích řekneme, že mají *charakteristiku* p .

Lemma 84. *Nechť pole F nemá charakteristiku 0. Pak nejmenší číslo $n \in \mathbf{N}$, pro něž $n_F = 0_F$, je nějaké prvočíslo p . V takovém F pro každé $m, n \in \mathbf{Z}$ platí ekvivalence*

$$m_F = n_F \iff m \equiv n \pmod{p} .$$

DŮKAZ. Má-li n uvedenou vlastnost a $n = kl$, kde $k, l \in \mathbf{N}$,

$$0_F = n_F = (kl)_F = k_F l_F .$$

Protože pole nemá dělitele nuly (F^* je grupa), $k_F = 0_F$ nebo $l_F = 0_F$. Podle definice n nutně $k = n$ nebo $l = n$. Číslo n nemá netriviální dělitele a je prvočíslo, $n = p$.

Nechť prvočíslo p je charakteristikou F . Pokud $m - n = pk$, $(m - n)_F = p_F k_F = 0_F$ a $m_F = n_F$. Pokud $m_F = n_F$, vyjádříme $m - n$ jako $m - n = pk + l$, $0 \leq l < p$ (tvrzení 1) a dostáváme, že $0_F = m_F - n_F = (m - n)_F = (pk + l)_F = p_F k_F + l_F = l_F$. Z definice p plyne, že $l = 0$. Tedy $p \mid (m - n)$. \diamond

Tvrzení 85 (F má p^r prvků). *Nechť F je konečné pole. Pak F má charakteristiku p a $|F| = p^r$ pro nějaké číslo $r \in \mathbf{N}$.*

DŮKAZ. Z konečnosti F plyne, že $m_F = n_F$ pro nějaká přirozená čísla $m < n$. Pak ale $n_F - m_F = (n - m)_F = 0_F$ a F má charakteristiku p . Množina $G = \{0_F, 1_F, \dots, (p - 1)_F\}$ tvoří podpole izomorfní poli \mathbf{Z}_p (lemma 84). F je vektorovým prostorem s tělesem skalárů G . Má konečnou dimenzi r a jeho vektory odpovídají vzájemně jednoznačně r -ticím skalárů G . F má $|G|^r = p^r$ prvků. \diamond

Mírně zneužijeme značení a pro konečné pole F charakteristiky p budeme kopii G pole \mathbf{Z}_p v F značit prostě \mathbf{Z}_p .

Tvrzení 86 (struktura F^*). *Nechť F je konečné pole a $|F| = p^r = s$. F^* je cyklická grupa řádu $s - 1$ a má $\varphi(s - 1)$ generátorů. (φ je Eulerova funkce definovaná v oddílu 1.2.)*

DŮKAZ. Ukážeme obecněji, že v grupě F^* je pro každý dělitel d čísla $s - 1$ přesně $\varphi(d)$ prvků řádu d . Množinu takových prvků označíme jako R_d . Zřejmě je R_d podmnožinou řešení $x \in F$ rovnice

$$x^d = 1_F .$$

Prvek $\alpha \in R_d$ buď libovolný. Má řád d a ne menší, protože jsou mocniny $\alpha^1, \alpha^2, \dots, \alpha^d$ vzájemně různé. Zřejmě to jsou řešení hořejší rovnice. Ta však má nejvýše d řešení (mez pro počet různých kořenů polynomu z $F[x]$), a tak to jsou všechna řešení. Takže $R_d \subset \{\alpha^i : i = 1, \dots, d\}$. Řád d dostaneme, právě když $i \perp d$. Proto buď $|R_d| = 0$ (α neexistuje) nebo $|R_d| = \varphi(d)$. Zřejmě (řád každého prvku dělí $s - 1$)

$$\sum_{d \mid (s-1)} |R_d| = s - 1 .$$

Podle tvrzení 9 (kapitola 1) $|R_d| = \varphi(d)$ pro každé $d, d \mid (s-1)$. \diamond

Komutativita násobení v F hraje v důkazu podstatnou roli. (Nehraje však žádnou roli v důkazu tvrzení 85.) V nekomutativním tělese T může totiž rovnice $x^d = 1_T$ mít víc než d řešení. Například $x^4 = 1_T$ má v tělese kvaternionů (viz úloha 3) osm řešení: $\pm 1, \pm i, \pm j$ a $\pm k$. Generátoru F^* se říká *primitivní element* F .

Čtenářka jistě ví, že pro každé pole F v okruhu polynomů $F[x]$ platí obdoba algoritmu dělení se zbytkem (tvrzení 1). Díky tomu je $F[x]$ okruh s jednoznačným rozkladem na ireducibilní prvky: Každý polynom $a \in F[x]$ má, až na pořadí a skalární násobky prvky z F , jednoznačný rozklad $a = b_1 b_2 \dots b_k$, kde $b_i \in F[x]$ jsou ireducibilní v $F[x]$ (obdoba věty 2).

Tvrzení 87 ($|F|$ určuje F). *Každá dvě konečná pole s týmž počtem prvků jsou izomorfní.*

DŮKAZ. Necht' F je konečné pole s $s = p^r$ prvky a $\sigma \in F^*$ je primitivní element. Ukážeme, že $\{\sigma^0, \sigma^1, \dots, \sigma^{r-1}\}$ je báze F jako vektorového prostoru nad \mathbf{Z}_p . Necht' $i \leq r$ je nejmenší počet, pro nějž je množina vektorů $X = \{\sigma^0, \sigma^1, \dots, \sigma^{i-1}\}$ lineárně nezávislá (nad \mathbf{Z}_p), ale $X \cup \{\sigma^i\}$ je lineárně závislá. To znamená, že σ^i je \mathbf{Z}_p -lineární kombinace prvků X . Opakovaným užitím identity $\sigma^k = \sigma^i \sigma^{k-i}$ pro $k > i$ získáme toto vyjádření pro každou mocninu $\sigma^k, k \in \mathbf{N}_0$. Ale $F = \{0_F, \sigma^0, \sigma^1, \dots, \sigma^{s-2}\}$, a tak je X bazí. Nutně $i = r$. Tím jsme také dokázali, že σ má nad \mathbf{Z}_p stupeň r .

Necht' $P(x) \in \mathbf{Z}_p[x]$, $\deg(P) = r$, je minimální polynom σ nad \mathbf{Z}_p . P je ireducibilní v $\mathbf{Z}_p[x]$ a dělí polynom $x^{s-1} - 1_F \in \mathbf{Z}_p[x]$, protože ten se anuluje na σ . Necht' G je jiné konečné pole s $s = p^r$ prvky. P se v $G[x]$ úplně rozkládá, protože dělí polynom $x^{s-1} - 1_G$, který se v $G[x]$ úplně rozkládá (jeho kořeny jsou právě prvky G^*). Můžeme proto vzít prvek $\theta \in G^*$, který je kořenem P . P je minimální polynom θ nad \mathbf{Z}_p (je ireducibilní) a θ má nad \mathbf{Z}_p stupeň r . Proto je $X' = \{\theta^0, \theta^1, \dots, \theta^{r-1}\}$ lineárně nezávislá a je lineární bazí G .

Snadno se ověří, že zobrazení $f : F \rightarrow G$, které prvku $a_0 + a_1\sigma + \dots + a_{r-1}\sigma^{r-1}$ ($a_i \in \mathbf{Z}_p$) přiřadí prvek $a_0 + a_1\theta + \dots + a_{r-1}\theta^{r-1}$, je izomorfismus polí F a G . (Pro platnost identity $f(\alpha\beta) = f(\alpha)f(\beta)$ potřebujeme, že σ a θ mají *týž* minimální polynom P nad \mathbf{Z}_p .) \diamond

Pro úplný popis konečných polí už zbývá jen dokázat, že pro každé prvočíslo p a každé číslo $r \in \mathbf{N}$ existuje pole F s p^r prvky. Ke konstrukci F nám poslouží okruh polynomů $\mathbf{Z}_p[x]$.

Lemma 88. *Nechť $b \in \mathbf{Z}_p[x]$ má stupeň r a je ireducibilní v $\mathbf{Z}_p[x]$. Pak faktorokruh $\mathbf{Z}_p[x]/I$, kde $I = (b) = \{sb : s \in \mathbf{Z}_p[x]\}$ je ideál generovaný b , má p^r prvků a je pole.*

DŮKAZ. Prvky $\mathbf{Z}_p[x]/I$ jsou právě všechny množiny polynomů tvaru $a + I$, kde $a \in \mathbf{Z}_p[x]$ má stupeň $< r$. Proto má $\mathbf{Z}_p[x]/I$ přesně p^r prvků. Jediný z axiomů pole, jehož splnění v $\mathbf{Z}_p[x]/I$ není zřejmé, je existence multiplikatívního inverzu. Dokážeme ji snadno. Polynom b je ireducibilní, a tak b může dělit součin ac , kde a i c mají stupeň $< r$, jen když b dělí a nebo c . Pro každý nenulový $a \in \mathbf{Z}_p[x]$ se stupněm $< r$ tedy třídy $ac + I$, kde c probíhá p^r polynomů stupně $< r$, probíhají všech p^r prvků $\mathbf{Z}_p[x]/I$. Pro vhodný c máme $1 + I = ac + I = (a + I)(c + I)$ a $c + I$ je inverz k $a + I$. \diamond

Vzhledem k tomuto lemmatu stačí dokázat, že v $\mathbf{Z}_p[x]$ je pro každé $n \in \mathbf{N}$ ireducibilní polynom stupně n . Kombinatorickou úvahou nalezneme přesný počet takových polynomů.

Věta 89 (Gauss, 1801). *Počet monických ireducibilních polynomů v $\mathbf{Z}_p[x]$ se stupněm n je roven*

$$\frac{1}{n} \sum_{d \mid n} p^d \mu(n/d) ,$$

kde $\mu(n)$ je Möbiova funkce (definovaná v 1.2).

DŮKAZ. Hledaný počet označíme jako a_n . Tvrdíme, že platí identita

$$\frac{1}{1 - px} = \prod_{d=1}^{\infty} (1 - x^d)^{-a_d} .$$

Abychom ji nahlédli, porovnáme koeficienty u x^n . Vlevo se rovná p^n , což je zřejmě počet všech monických polynomů stupně n v $\mathbf{Z}_p[x]$. Vpravo (použijeme rozvoj $1/(1 - x^d) = 1 + x^d + x^{2d} + \dots$) je roven počtu řešení rovnice

$$n = x_1 + x_2 + \dots , \text{ kde } x_i \in \{1_1, 1_2, \dots, 1_{a_1}, 2_1, 2_2, \dots, 2_{a_2}, 3_1, \dots\} = \mathbf{N}' ,$$

$x_1 \geq x_2 \geq \dots$ a \mathbf{N}' je modifikovaná množina \mathbf{N} , v níž máme a_1 druhů čísla 1, a_2 druhů čísla 2 a tak dále (pro $i_j, k_l \in \mathbf{N}'$ klademe $i_j > k_l$, pokud $i > k$ nebo $i = k$ & $j > l$). Což je vlastně počet všech možných faktorizací

$$a = b_1 b_2 \dots ,$$

kde $a \in \mathbf{Z}_p[x]$ je monický stupně n a $b_i \in \mathbf{Z}_p[x]$ jsou monické a ireducibilní a ne nutně různé. (Máme právě a_k polynomů b_i , $\deg(b_i) = k$.) Koeficient u x^n vpravo tedy opět představuje počet všech monických polynomů stupně n , nyní jsou reprezentovány svými rozklady na součiny ireducibilních polynomů. (Užíváme podstatně, že $\mathbf{Z}_p[x]$ je okruh s jednoznačným rozkladem na ireducibilní prvky.)

Formálním logaritmováním hořejší identity dostáváme

$$\begin{aligned} \sum_{n \geq 1} \frac{(px)^n}{n} &= \sum_{d \geq 1} a_d \log \frac{1}{1 - x^d} \\ &= \sum_{d \geq 1} a_d \sum_{m \geq 1} \frac{dx^{dm}}{dm} \\ &= \sum_{n \geq 1} \frac{x^n}{n} \sum_{d \mid n} da_d . \end{aligned}$$

Porovnání koeficientů u x^n vede ke vztahu

$$p^n = \sum_{d \mid n} da_d .$$

Podle Möbiovy inverzní formule (tvrzení 7 v kapitole 1),

$$na_n = \sum_{d \mid n} p^d \mu(n/d) .$$

Odtud plyne formule pro a_n . ◇

Kombinací věty a lemmatu 88 dostáváme

Tvrzení 90 (existence F). *Pro každé prvočíslo p a každé $n \in \mathbf{N}$ existuje konečné pole s p^n prvky.*

DŮKAZ. Z

$$\begin{aligned} \frac{1}{n} \sum_{d \mid n} p^d \mu(n/d) &\geq \frac{p^n - p^{n-1} - p^{n-2} - \dots - p - 1}{n} \\ &= \frac{(p-2)p^n + 1}{n(p-1)} \\ &> 0 \end{aligned}$$

plyne, že pro každý stupeň n máme v $\mathbf{Z}_p[x]$ ireducibilní polynom. \diamond

Jiný, algebraický důkaz existence konečného pole je popsán v úloze 6. Jednoznačně určené konečné pole s p^n prvky budeme značit $\text{GF}(p^n)$.

Tvrzení 91 (podpole F). *Každé podpole pole $F = \text{GF}(p^n)$ je izomorfní $\text{GF}(p^m)$, přičemž m dělí n . Naopak, pro každý dělitel m čísla n má $\text{GF}(p^n)$ právě jedno podpole s p^m prvky.*

DŮKAZ. Je-li G podpole F , má G charakteristiku p a $|G| = p^m$ pro nějaké $m \in \mathbf{N}$. F je vektorový prostor nad G , a tak $|F| = |G|^k$ pro nějaké $k \in \mathbf{N}$. Takže $n = mk$.

Naopak, nechť $n = mk$. Položíme $s = p^n$ a $t = p^m$ a uvažíme množinu

$$G = \{\alpha \in F : \alpha^t = \alpha\} .$$

Jde o kořeny polynomu $x^t - x$. Protože $m \setminus n$, $(t-1) \setminus (s-1)$ a $x^t - x = x(x^{t-1} - 1)$ dělí $x^s - x = x(x^{s-1} - 1)$. Polynom $x^s - x$ se rozkládá na s různých lineárních faktorů $x - \alpha, \alpha \in F$. Proto má $x^t - x$ v F t různých kořenů a $|G| = t = p^m$.

Ukážeme, že G je pole. Nechť $\alpha, \beta \in G, \beta \neq 0_G$. Pak $(\alpha/\beta)^t = \alpha^t/\beta^t = \alpha/\beta$ a $\alpha/\beta \in G$. Uzavřenost na rozdíl plyne z identity

$$(\alpha - \beta)^p = \sum_{i=0}^p \binom{p}{i}_F \alpha^i (-\beta)^{p-i} = \alpha^p - \beta^p .$$

Ta platí díky tomu, že $\binom{p}{i}_F = 0_F$ pro $0 < i < p$. Po m umocněních na p dostaneme

$$(\alpha - \beta)^t = \alpha^t - \beta^t = \alpha - \beta ,$$

a tak i $\alpha - \beta \in G$.

Nechť G' je libovolné podpole F s $t = p^m$ prvky. Patrně $\alpha^t = \alpha$ pro každé $\alpha \in G'$. G' se skládá z kořenů $x^t - x$ a $G' = G$. \diamond

Tvrzení 92 (shrnutí). *Každé konečné pole F má charakteristiku p a p^n prvků, kde p je prvočíslo. Pro každé prvočíslo p a $n \in \mathbf{N}$ existuje až na izomorfismus jediné pole s p^n prvky, které značíme jako $\text{GF}(p^n)$. Grupa F^* (multiplikativní grupa nenulových prvků) je cyklická. Podpole $\text{GF}(p^n)$ jsou právě ta $\text{GF}(p^m)$, že $m \setminus n$, a pro každé $m, m \setminus n$, existuje právě jedno takové podpole.*

Konečná pole použijeme pro konstrukci velkých Sidonových množin. Podmnožina $X \subset \mathbf{N}$ je *Sidonova*, pokud pro každé čtyři prvky x_1, \dots, x_4 z X rovnost $x_1 + x_2 = x_3 + x_4$ platí, jen když $\{x_1, x_2\} = \{x_3, x_4\}$. Jinými slovy, dvoučlenné součty prvků množiny X se neopakují. Ještě jinak řečeno, X je Sidonova, právě když jsou všechny rozdíly $y - x, y \neq x$, prvků $y, x \in X$ různé. Největší mohutnost Sidonovy podmnožiny množiny $\{1, 2, \dots, n\}$ označíme $\text{Si}(n)$.

Věta 93 (Erdős a Turán, 1941). *Pro $n \in \mathbf{N}$ platí*

$$\text{Si}(n) < n^{1/2} + n^{1/4} + O(1) .$$

DŮKAZ. (Lindström, 1969.) $1 \leq x_1 < x_2 < \dots < x_m \leq n$ buď m -prvková Sidonova množina X . Pro $k \in \mathbf{N}$ uvážíme sumu

$$S(k, X) = \sum_{i,j} \langle 1 \leq i < j \leq m \ \& \ j - i \leq k \rangle \cdot (x_j - x_i) .$$

$S(k, X)$ je součet těch vzdáleností prvků X , které pokrývají méně než k jiných prvků. Hodnotu parametru k zvolíme vhodně v závislosti na n později. Dokážeme nerovnosti

$$\left(km - \binom{k+1}{2} + 1 \right) \leq S(k, X) < \binom{k+1}{2} n .$$

Dolní odhad plyne z toho, že suma $S(k, X)$ má $s = (m-1) + (m-2) + \dots + (m-k) = km - \binom{k+1}{2}$ sčítanců z \mathbf{N} , které jsou vzájemně různé. Proto $S(k, X) \geq 1 + 2 + \dots + s = \binom{s+1}{2}$. Horní odhad plyne z toho, že $x_j - x_i = (x_{i+1} - x_i) + (x_{i+2} - x_{i+1}) + \dots + (x_j - x_{j-1})$ a každý elementární rozdíl $x_{i+1} - x_i$ se v $S(k, X)$ objeví nejvýše $1 + 2 + \dots + k = \binom{k+1}{2}$ krát. Součet elementárních rozdílů je přitom $n - 1$.

Po snadných úpravách odhadu

$$\frac{1}{2} \left(km - \binom{k+1}{2} \right)^2 < \left(km - \binom{k+1}{2} + 1 \right) < \binom{k+1}{2} n$$

dostaneme nerovnost

$$m < \sqrt{(1 + 1/k)n} + \frac{k+1}{2} .$$

Protože $\sqrt{(1 + 1/k)n} = (1 + \frac{1}{2k} + O(k^{-2}))n^{1/2}$, optimální volba k je $k = \lfloor n^{1/4} \rfloor$ a dává nám pro $m = |X|$ dokazovanou nerovnost. \diamond

Jak ukazuje následující věta, pro nekonečně mnoho hodnot n je tento odhad $\text{Si}(n)$ téměř nejlepší možný.

Věta 94 (Chowla, 1944; Erdős, 1944). *Nechť $n = m^2 + m + 1$ a $m = p^r$ je mocnina prvočísla. Pak existuje Sidonova množina $X \subset \{1, 2, \dots, n\}$ s $m + 1$ prvky. Odtud plyne, že*

$$\text{Si}(n) > \sqrt{n}$$

pro nekonečně mnoho hodnot n .

DŮKAZ. Sestrojíme množinu $A = \{a_1, a_2, \dots, a_{m+1}\} \subset \mathbf{N}_0$ takovou, že $m^2 + m = (m + 1)m$ rozdílů $a_i - a_j, i \neq j$, představuje právě všechny nenulové zbytky modulo $n = m^2 + m + 1$. Vezmeme tytéž zbytky v množině $\{1, 2, \dots, n\}$ a dostaneme Sidonovu množinu velikosti $m + 1$.

Položíme $m = p^r$, $F = \text{GF}(m)$, $G = \text{GF}(m^3)$ a chápeme F jako podpole G (tvrzení 91). Nechť θ je primitivní element G^* (tvrzení 86). A definujeme jako

$$A = \{0\} \cup \{a \in \mathbf{N} : 1 \leq a \leq m^3 - 1 \text{ \& } \theta^a = \theta + c, c \in F\}.$$

Patrně $|A| = |F| + 1 = m + 1$. Pro důkaz rozdílové vlastnosti A ukážeme, že
(i) $\{\theta^a, \theta^b\}$ je lineárně závislá nad F , právě když $a \equiv b \pmod{m^2 + m + 1}$ a
(ii) θ má nad F stupeň 3.

Vlastnost (i). Jak víme z důkazu tvrzení 91, $x \in G^*$ padne do F , právě když $x^{m-1} - 1_G = 0_G$. Protože $G^* = \{\theta^a : a = 1, 2, \dots, m^3 - 1\}$, sestává F^* právě z těch θ^a , že a je dělitelné $(m^3 - 1)/(m - 1) = m^2 + m + 1$. Vlastnost (i) je dokázána, protože F -lineární závislost $\{\theta^a, \theta^b\}$ je ekvivalentní s $\theta^{a-b} \in F$. Vlastnost (ii) se dokazuje stejně, jako že θ má nad \mathbf{Z}_p stupeň $3r$ (úvodní partie důkazu tvrzení 87).

Zpět k A . Vzhledem k tomu, že $\theta \notin F$, je pro různé $c, c' \in F$ množina $\{\theta + c, \theta + c'\}$ lineárně nezávislá nad F . Podle (i) jsou proto různé prvky A nekongruentní modulo $m^2 + m + 1$. Nechť nyní $a_1, a_2, a_3, a_4 \in A$ a

$$a_1 - a_2 \equiv a_3 - a_4 \pmod{m^2 + m + 1}.$$

Uvidíme, že $a_1 = a_2$ nebo $a_1 = a_3$. Pro $a \in A$ označíme $L_a(\theta) = \theta^a = \theta + c$ a $L_0(\theta) = 1$. Z kongruence a (i) plyne, že prvky $L_{a_1}(\theta)L_{a_4}(\theta)$ a $L_{a_2}(\theta)L_{a_3}(\theta)$

jsou nad F lineárně závislé. Protože to jsou monické kvadratické polynomy z $F[\theta]$ a platí (ii), je to možné jen tak, že $L_{a_1}(\theta)L_{a_4}(\theta) = L_{a_2}(\theta)L_{a_3}(\theta)$. Rozklad polynomu na lineární faktory je jednoznačný, takže $L_{a_1} = L_{a_2}$ nebo $L_{a_1} = L_{a_3}$. Tudíž $a_1 = a_2$ nebo $a_1 = a_3$. \diamond

Další výsledky o Sidonových množinách jsou zmíněny v úlohách 8–10 a v poznámkách.

4.2 Chevalley–Warningova věta a kombinatorika

Věta 95 (Chevalley, 1936; Warning, 1936). *Nechť $F = \text{GF}(p^r)$ je konečné pole a $N \in \mathbb{N}$ počet řešení $(a_1, \dots, a_m) \in F^m$ soustavy*

$$P_1 = 0_F \ \& \ P_2 = 0_F \ \& \ \dots \ \& \ P_n = 0_F ,$$

kde $P_i \in F[x_1, x_2, \dots, x_m]$. Pokud

$$\sum_{i=1}^n \deg(P_i) < m ,$$

je N dělitelné p .

Nejprve dokážeme

Lemma 96. *$F = \text{GF}(p^r)$ buď konečné pole a $m \in \mathbb{N}$. Pak*

$$\sum_{x \in F} x^m = \begin{cases} -1_F & \dots \ (|F| - 1) \setminus m \\ 0_F & \dots \ \text{jinak} . \end{cases}$$

DŮKAZ. Pokud $(|F| - 1) \setminus m$, pro každé $x \in F^*$ z $x^{|F|-1} = 1_F$ plyne $x^m = 1_F$. Takže

$$\sum_{x \in F} x^m = 0_F + (|F| - 1)_F = (p^r)_F - 1_F = -1_F ,$$

protože F má charakteristiku p . Pro důkaz druhé části použijeme primitivní element $\alpha \in F^*$ (tvrzení 86). Stačí nám, že pro m nedělitelné $|F| - 1$ platí $\alpha^m \neq 1_F$. Probíhá-li x pole F , probíhá je i αx . Proto

$$S = \sum_{x \in F} x^m = \sum_{x \in F} (\alpha x)^m = \alpha^m \sum_{x \in F} x^m = \alpha^m S .$$

Tedy $(\alpha^m - 1_F)S = 0_F$ a $S = 0_F$. ◇

DŮKAZ VĚTY 95. Platí identita

$$\sum_{a_1, \dots, a_m} \prod_{j=1}^n (1_F - P_j(a_1, a_2, \dots, a_m)^{|F|-1}) = N_F,$$

v níž sčítáme přes všech $|F|^m$ m -tic $(a_1, \dots, a_m) \in F^m$. K jejímu nahlédnutí si stačí uvědomit, že $a^{|F|-1} = 1_F$ pro všechny $a \in F^*$ a $0^{|F|-1} = 0_F$.

Podíváme se na výraz vlevo od = jiným způsobem a ukážeme, že je roven 0_F . Protože F má charakteristiku p , lemma 84 dává $N \equiv 0 \pmod{p}$. Po umocnění a roznásobení máme vlevo F -lineární kombinaci členů typu

$$\sum_{a_1, \dots, a_m} \prod_{i=1}^m a_i^{k_i} = \prod_{i=1}^m \sum_{a_i \in F} a_i^{k_i}.$$

Ale

$$\sum_{i=1}^m k_i \leq (|F| - 1) \sum_{i=1}^n \deg(P_i) < (|F| - 1)m.$$

Některé k_i tudíž splňuje $0 \leq k_i < |F| - 1$ a buď $|F| - 1$ nedělí k_i nebo $k_i = 0$. V prvním případě je podle předchozího lemmatu odpovídající suma rovna 0_F . V druhém případě dostáváme sumu $1_F + 1_F + \dots + 1_F = |F|_F$ (proč?), což je rovněž 0_F . Součin je nulový a nulová je i celá lineární kombinace. ◇

Chevalley–Warningovu větu použijeme v kombinatorické teorii čísel. Pro daná přirozená čísla m a n se ptáme, jaký je nejmenší počet v čísel $g_1, g_2, \dots, g_v \in \mathbf{Z}$, který zaručuje, že se mezi nimi vždy najde m čísel se součtem dělitelným n . Pro m nedělitelné n to nezaručí žádné v , špatný je třeba soubor ze samých jedniček. Necht' $m = n$. Jaký je nejmenší počet v , který zaručuje, že se mezi v celými čísly najde n čísel se součtem rovným nule modulo n ?

Věta 97 (Erdős, Ginzburg a Ziv, 1961). *Mezi každými $2n - 1$ celými čísly je vždy n čísel, jejichž součet je dělitelný n . Hodnotu $2n - 1$ již nelze snížit.*

DŮKAZ. Dodatek je jasný, soubor $2n - 2$ čísel sestávající z $n - 1$ nul a $n - 1$ jedniček nemá popsanou vlastnost. Nejprve ukážeme, že z platnosti věty pro $n_1 \in \mathbf{N}$ a $n_2 \in \mathbf{N}$ plyne její platnost pro $n_1 n_2$. Buďte dáno $2n_1 n_2 - 1$ celých

čísel. Opakovaným užitím předpokladu pro n_1 z nich vybereme $2n_2 - 1$ disjunktních souborů $S_1, S_2, \dots, S_{2n_2-1}$, každý o n_1 číslech, že $\sum_{x \in S_i} x = m_i n_1$. Na seznam $(m_1, m_2, \dots, m_{2n_2-1})$ aplikujeme předpoklad pro n_2 a vybereme z něj n_2 čísel se součtem dělitelným n_2 . Odpovídajících n_2 souborů S_i vytváří soubor o $n_1 n_2$ číslech, jejichž součet je dělitelný $n_1 n_2$.

Proto větu stačí dokázat jen pro prvočíselné $n = p$. Nechtě $g_1, g_2, \dots, g_{2p-1}$ jsou libovolná celá čísla. Podíváme se na soustavu nad $F = \text{GF}(p) = \mathbf{Z}_p$

$$\begin{aligned} g_1 x_1^{p-1} + g_2 x_2^{p-1} + \dots + g_{2p-1} x_{2p-1}^{p-1} &= 0_F \\ x_1^{p-1} + x_2^{p-1} + \dots + x_{2p-1}^{p-1} &= 0_F . \end{aligned}$$

Předpoklady Chevalley–Warningovy věty jsou splněny: $p-1 + p-1 < 2p-1$. Jedno řešení je triviální řešení ze samých nul. Podle věty 95 tedy existuje alespoň $p-1 \geq 1$ netriviálních řešení. Vezmeme jedno z nich, $(z_1, z_2, \dots, z_{2p-1}) \in \mathbf{Z}_p^{2p-1}$, a položíme $S = (g_i : z_i \neq 0_F)$. Díky Malé Fermatově větě z první rovnice vyplývá, že $\sum_{x \in S} x \equiv 0 \pmod{p}$, a z druhé, že p dělí $|S|$. Protože $0 < |S| < 2p$, je $|S| = p$. S je hledaná p -tice. \diamond

Pro zobecnění Erdős–Ginzburg–Zivovy věty viz poznámky a úlohy 12 a 13.

Druhé použití Chevalley–Warningovy věty je z kombinatoriky, z teorie grafů. *Grafem* rozumíme strukturu $G = (V, E)$, kde V je konečná množina *vrcholů* a E je multipodmnožina (prvky se mohou opakovat) množiny $\{\{x, y\} : x, y \in V, x \neq y\}$. Prvkům E se říká *hrany*. Dva různé vrcholy x a y jsou tedy spojeny k hranami, kde k je násobnost $\{x, y\}$ v E . *Stupeň* vrcholu x je součet násobností hran, jichž je x prvkem. G je *k -regulární*, mají-li všechny vrcholy stupeň k . $H = (V', E')$ je *podgrafem* G , pokud $V' \subset V$ a $E' \subset E$ (násobnost každé $e \in E'$ v E' je menší nebo rovna násobnosti e v E). To, čemu zde říkáme graf, se v teorii grafů obvykle označuje jako multigraf.

Za příklad nám poslouží graf

$$H = (V, E) , \quad V = \{1, 2, 3, 4, 5\} \quad \text{a} \quad E = \{\{1, 3\}_1, \{1, 3\}_2, \{1, 2\}, \{1, 4\}\} .$$

Má 5 vrcholů a 4 hrany, hrana $\{1, 3\}$ je dvojnásobná, vrchol 1 má stupeň 4, 3 má stupeň 2, 2 a 4 mají stupeň 1 a 5 má stupeň 0.

Věta 98 (Alon, Friedland a Kalai, 1984). *Každý graf, který vznikne ze 4-regulárního grafu přidáním jediné hrany, obsahuje neprázdný 3-regulární podgraf.*

DŮKAZ. $G = (V, E)$ buď náš graf. Budeme pracovat v $F = \text{GF}(3) = \mathbf{Z}_3$. Definujeme matici s prvky $a(v, e)$, $v \in V$, $e \in E$,

$$a(v, e) = \begin{cases} 0_F & \dots & v \notin e \\ 1_F & \dots & v \in e . \end{cases}$$

Za každý řádek $v \in V$ matice vezmeme rovnici

$$\sum_{e \in E} a(v, e)x_e^2 = 0_F .$$

Celkem máme $|V| = n$ rovnic, součet jejich stupňů je $2n$. Není těžké vidět, že G má $2n + 1$ hran, což je počet neznámých. Podle Chevalley–Warningovy věty kromě triviálního nulového řešení existuje i řešení (dokonce alespoň dvě) $(z_e : e \in E)$, v němž ne všechny z_e jsou nulové. Neprázdňá podmnožina $E' \subset E$, $e \in E' \iff z_e \neq 0_F$, definuje podgraf $G' = (W, E') = (\cup E', E')$. Pro každý vrchol $v \in W$ je součet v řádku v dělitelný třemi a G' má všechny stupně dělitelné třemi. Tyto stupně však leží v množině $\{1, 2, 3, 4, 5\}$, a tak je G' 3-regulární. \diamond

Lze sestavit 4-regulární grafy, které neobsahují ani jeden neprázdňý 3-regulární podgraf (úloha 11).

4.3 Zlatá věta

Řekneme, že $a \in \mathbf{Z}$ je *kvadratický zbytek modulo* $m \in \mathbf{N}$, pokud kongruence

$$x^2 \equiv a \pmod{m}$$

má řešení $x \in \mathbf{Z}$. V opačném případě a nazveme *kvadratickým nezbytkem modulo* m . V tomto oddílu vždy $a \in \mathbf{Z}$ a $m \in \mathbf{N}$.

Nechť $d = (a, m) > 1$ a p je prvočíslo s $\text{ord}_p(d) = k > 0$. Položíme $a' = a/p^k$ a $m' = m/p^k$. Pokud $k = 2l$, je hořejší kongruence ekvivalentní kongruenci stejného typu $y^2 \equiv a' \pmod{m'}$, kde $x = p^l y$. Pokud $k = 2l - 1$, je ekvivalentní kongruenci $py^2 \equiv a' \pmod{m'}$, kde opět $x = p^l y$, a pro $p \nmid m'$ tedy nemá řešení (p nedělí současně a' a m'). Pro $p \perp m'$ je ekvivalentní kongruenci stejného typu $y^2 \equiv ba' \pmod{m'}$, kde $b \in \mathbf{Z}$ splňuje $pb \equiv 1 \pmod{m'}$ (a $x = p^l y$). Krácením prvočinitelů (a, m) tak umíme hořejší kongruenci převést na ekvivalentní kongruenci $y^2 \equiv a' \pmod{m'}$, kde $a' \perp m'$, nebo dokázat, že $x^2 \equiv a \pmod{m}$ nemá řešení. Proto se v dalším omezíme na případ $a \perp m$.

Lemma 99. Je-li $m = p_1^{l_1} p_2^{l_2} \dots p_r^{l_r} = m_1 m_2 \dots m_r$, kde $m_i = p_i^{l_i}$, prvočíselný rozklad m , je kongruence

$$x^2 \equiv a \pmod{m}$$

ekvivalentní soustavě

$$x_1^2 \equiv a \pmod{m_1} \& \dots \& x_r^2 \equiv a \pmod{m_r},$$

kde

$$x \equiv x_1 \pmod{m_1} \& \dots \& x \equiv x_r \pmod{m_r}.$$

DŮKAZ. Je-li $x = u \in \mathbf{Z}$ řešení kongruence, je $x_1 = x_2 = \dots = x_r = u$ řešení soustavy. Je-li u_1, \dots, u_r řešení soustavy, existuje podle tvrzení 5 číslo $u \in \mathbf{Z}$ takové, že $u \equiv u_i \pmod{m_i}$ pro $i = 1, \dots, r$. Tudíž $u^2 \equiv a \pmod{m_i}$ pro všechna i a, díky vzájemné nesoudělnosti m_i , $u^2 \equiv a \pmod{m}$. \diamond

Proto se stačí omezit na případ modulu rovného mocnině prvočísla, $m = p^e$.

Tvrzení 100 (redukce modulu z p^e na p). Necht p je prvočíslo nedělicí číslo a .

1. Pokud $p > 2$, má kongruence $x^2 \equiv a \pmod{p^e}$ řešení buď pro všechny exponenty $e \in \mathbf{N}$ nebo pro žádný z nich.
2. Pokud $p = 2$, má kongruence $x^2 \equiv a \pmod{2^e}$ řešení buď pro všechny exponenty $e \in \mathbf{N}$ & $e \geq 3$ nebo pro žádný z nich.

DŮKAZ. 1. Řešení pro nějaký exponent $e \in \mathbf{N}$ je řešením i pro $e = 1$. Stačí tedy ukázat, jak z řešení x_0 kongruence $x^2 \equiv a \pmod{p^e}$ odvodit řešení x_1 pro exponent $e + 1$. Položíme $x_1 = x_0 + bp^e$. Pak

$$x_1^2 \equiv x_0^2 + 2x_0bp^e \pmod{p^{e+1}}.$$

Dostáváme

$$x_1^2 \equiv a \pmod{p^{e+1}} \iff 2x_0b \equiv \frac{a - x_0^2}{p^e} \pmod{p}.$$

Protože $2x_0 \not\equiv 0 \pmod{p}$, existuje řešení b a tím pádem i řešení x_1 .

2. Důkaz je podobný. Necht x_0 je řešením kongruence $x^2 \equiv a \pmod{2^e}$, $e \geq 3$.
3. Položíme $x_1 = x_0 + b2^{e-1}$. Zřejmě

$$x_1^2 = x_0^2 + x_0b2^e + b^22^{2e-2} \equiv x_0^2 + x_0b2^e \pmod{2^{e+1}}.$$

Dostáváme

$$x_1^2 \equiv a \pmod{2^{e+1}} \iff b \equiv \frac{a - x_0^2}{2^e} \pmod{2},$$

neboť $x_0 \equiv 1 \pmod{2}$. Toto b dává řešení x_1 modulo 2^{e+1} . \diamond

Podmínku $e \geq 3$ pro $p = 2$ nelze vynechat: $x^2 \equiv 5 \pmod{2^e}$ má řešení jen pro $e = 1$ a 2 .

Tvrzení 101 (rekapitulace). *V kongruenci*

$$x^2 \equiv a \pmod{m}$$

můžeme předpokládat, že $a \perp m$. Necht $m = 2^l p_1^{l_1} p_2^{l_2} \dots p_r^{l_r}$, kde p_i jsou různá lichá prvočísla, je prvočíselný rozklad čísla m . Kongruence má řešení, právě když platí podmínky 1 a 2.

1. Pro $l = 1$ se nepožaduje nic. Pokud $l = 2$, $a \equiv 1 \pmod{4}$. Pokud $l \geq 3$, $a \equiv 1 \pmod{8}$.

2. Kongruence $x^2 \equiv a \pmod{p_i}$ má řešení pro každé $i = 1, \dots, r$.

DŮKAZ. Argument před lemmatem 99, lemma 99 a tvrzení 100. \diamond

Úlohu rozhodnout, zda a je kvadratický zbytek modulo m , jsme redukovali na tutéž úlohu pro lichý prvočíselný modul. Na ni se teď soustředíme.

Tvrzení 102 (je jich stejně). *Pro každé prvočíсло $p > 2$ máme v množině $\{1, 2, \dots, p-1\}$ právě $\frac{p-1}{2}$ kvadratických zbytků a $\frac{p-1}{2}$ kvadratických nezbytků modulo p .*

DŮKAZ. Probíhá-li x čísla $1, 2, \dots, p-1$, probíhá číslo x^2 (reduované modulo p) právě všechny kvadratické zbytky v uvedené množině. Každý z nich se vyskytne přesně dvakrát, protože $x^2 \equiv y^2 \pmod{p}$ je ekvivalentní s $(x-y)(x+y) \equiv 0$ a to s (p je prvočíсло) $x \equiv \pm y$. \diamond

Legendreův symbol $\left(\frac{a}{p}\right)$ je definován pro prvočíсло $p > 2$ a číslo $a \in \mathbf{Z}$ jako

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \dots & p \mid a \\ 1 & \dots & p \perp a, a \text{ je kvadratický zbytek modulo } p \\ -1 & \dots & p \perp a, a \text{ je kvadratický nezbytek modulo } p. \end{cases}$$

Tvrzení 103 (vlastnosti Legendreova symbolu). *Nechť p je liché prvočíslo a $a, b \in \mathbf{Z}$. Pak platí*

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

DŮKAZ. 1. Této vlastnosti se někdy říká *Eulerovo kritérium (kvadratických zbytků)*. Nechť $a \perp p$ (pro $p \nmid a$ zřejmě platí). Z Malé Fermatovy věty plyne, že

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}.$$

Proto je $a^{(p-1)/2}$ modulo p vždy 1 nebo -1 . Je-li $a \equiv b^2$ kvadratický zbytek, musí to být 1, protože pak $a^{(p-1)/2} \equiv b^{p-1}$. Tím jsou, podle předchozího tvrzení, vyčerpána všechna řešení rovnice $x^{(p-1)/2} = 1_F$ v $F = \mathbf{Z}_p$ a pro nezbytky dostáváme -1 . (Stejný trik jako v důkazu tvrzení 86.)

2. Vlastnost 2 plyne z vlastnosti 1:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Tudíž $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$. Protože hodnota Legendreova symbolu je 0 nebo ± 1 , platí $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

3. To plyne přímo z definice. ◇

Pracuje se i s obecnějším *Jacobiho symbolem*, jehož „jmenovatel“ nemusí být prvočíslo (úloha 15).

Jako $S(p)$ si označíme množinu

$$S(p) = \left\{-\frac{1}{2}(p-1), -\frac{1}{2}(p-3), \dots, -1, 1, \dots, \frac{1}{2}(p-3), \frac{1}{2}(p-1)\right\}.$$

Jde o systém $p-1$ v absolutní hodnotě nejmenších nenulových zbytků modulo p . Pro $a \in \mathbf{Z}$ nedělitelné p definujeme posloupnost délky $\frac{1}{2}(p-1)$

$$M(a) = (a_k \in S(p) : 1 \leq k \leq \frac{1}{2}(p-1), ka \equiv a_k \pmod{p})$$

a jako $m(a)$ označíme počet jejích záporných členů. Například pro $p = 17$ máme

$$M(7) = (7, -3, 4, -6, 1, 8, -2, 5) \quad \text{a} \quad m(7) = 3.$$

Dva členy $M(a)$ s různým indexem jsou různé a liší se více než znaménkem: $Z \cdot a_k = \pm a_l$ plyne $ka \equiv \pm la \pmod{p}$, odtud $k \pm l \equiv 0$, takže $k = l$. Posloupnost $M(a)^+$, která vznikne změnou znaménka u záporných členů, je proto permutací posloupnosti $1, 2, \dots, \frac{1}{2}(p-1)$.

Nahradíme-li $S(p)$ obvyklým systémem nenulových zbytků $Z(p) = \{1, 2, \dots, p-1\}$, dostaneme posloupnost

$$N(a) = (b_k \in Z(p) : 1 \leq k \leq \frac{1}{2}(p-1), ka \equiv b_k \pmod{p})$$

a číslo $n(a)$ rovné počtu jejích *velkých* členů, které přesahují $\frac{1}{2}(p-1)$. Ostatním b_k budeme říkat *malé* členy. $N(a)^-$ vznikne náhradou velkých b_k číslem $p - b_k$. Ze stejného důvodu jako výše je $N(a)^-$ permutace posloupnosti $1, 2, \dots, \frac{1}{2}(p-1)$. Posun $x \rightarrow x - p$ poskytuje bijekci mezi velkými členy $N(a)$ a zápornými členy $M(a)$. Tudíž $n(a) = m(a)$.

Tvrzení 104 (Gaussovo lemma). *Pro prvočíslo $p > 2$ a $a \in \mathbf{Z}$, $a \perp p$, platí*

$$\left(\frac{a}{p}\right) = (-1)^{m(a)} = (-1)^{n(a)} .$$

DŮKAZ. Uvažme výše definovanou množinu

$$M(a)^+ = \{m_1, m_2, \dots, m_{(p-1)/2}\} = \{1, 2, \dots, \frac{1}{2}(p-1)\} .$$

Pronásobením kongruencí

$$1 \cdot a \equiv \pm m_1 \pmod{p}, 2 \cdot a \equiv \pm m_2 \pmod{p}, \dots, \frac{1}{2}(p-1) \cdot a \equiv \pm m_{(p-1)/2} \pmod{p}$$

dostaneme

$$\left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \equiv (-1)^{m(a)} \left(\frac{p-1}{2}\right)! \pmod{p} .$$

Po zkrácení $(\frac{1}{2}(p-1))!$ a užití Eulerova kritéria máme

$$\left(\frac{a}{p}\right) = (-1)^{m(a)} .$$

◇

Tvrzení 105 (1. a 2. dodatek zákona reciprocit). *Nechť $p > 2$ je prvočíslo.*

1. První dodatek zákona reciprocit říká, že

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \dots & p \equiv 1 \pmod{4} \\ -1 & \dots & p \equiv 3 \pmod{4} . \end{cases}$$

2. Druhý dodatek zákona reciprocit říká, že

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \dots & p \equiv 1, 7 \pmod{8} \\ -1 & \dots & p \equiv 3, 5 \pmod{8} . \end{cases}$$

DŮKAZ. 1. Vlastnost 1 je bezprostřední aplikací Eulerova kritéria z tvrzení 103.

2. Číslo $m(2) = n(2)$, pro dané liché prvočíslo p , je počet čísel $1 \cdot 2, 2 \cdot 2, \dots, \frac{1}{2}(p-1) \cdot 2 = p-1$ větších než $\frac{1}{2}(p-1)$. Tedy

$$n(2) = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor .$$

Vše závisí na zbytku p při dělení osmi. Třeba pro $p = 8n + 5$ vychází $n(2) = 4n + 2 - (2n + 1) = 2n + 1$ a podle Gaussova lemmatu je 2 pro takové p kvadratický nezbytek. Zbylé tři případy $p = 8n + 1, 8n + 3$ a $p = 8n + 7$ se určí obdobně. \diamond

Věta 106 (Gauss, 1796). *Nechť $p, q > 2$ jsou různá prvočísla. Zákon reciprocit kvadratických zbytků praví, že*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) .$$

Jinak řečeno,

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{p}{q}\right) \text{ pokud } p \equiv 1 \pmod{4} \text{ nebo } q \equiv 1 \pmod{4} \text{ a} \\ \left(\frac{q}{p}\right) &= -\left(\frac{p}{q}\right) \text{ pokud } p \equiv 3 \pmod{4} \text{ a } q \equiv 3 \pmod{4} . \end{aligned}$$

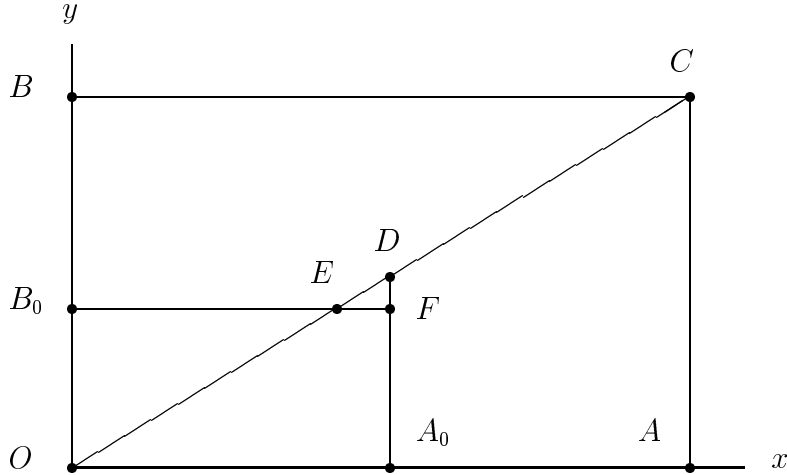
Nechť a a b jsou dvě přirozená čísla, která jsou různá, nesoudělná a lichá. Nejprve dokážeme lemma o součtu

$$S(a, b) = \sum_{i=1}^{(a-1)/2} \left\lfloor \frac{ib}{a} \right\rfloor .$$

Lemma 107. *Platí*

$$S(a, b) + S(b, a) = \frac{a-1}{2} \cdot \frac{b-1}{2} .$$

DŮKAZ. Necht $a > b$. Na obrázku níže $O = (0, 0)$, $A = (a, 0)$, $A_0 = (\frac{1}{2}(a-1), 0)$, $B = (0, b)$, $B_0 = (0, \frac{1}{2}(b-1))$, $C = (a, b)$ a $F = (\frac{1}{2}(a-1), \frac{1}{2}(b-1))$. Body E a D jsou průsečíky přímky OC s přímkami B_0F a A_0F . Skutečně $D_y = \frac{1}{2}(a-1)(b/a) > F_y = \frac{1}{2}(b-1)$.



Součet vlevo je počet mřížových bodů v trojúhelníku OA_0D plus počet mřížových bodů v trojúhelníku OB_0E , bez os x a y . Na úsečce OC neleží kromě O a C žádné mřížové body, protože $a \perp b$. Průnik trojúhelníků, úsečka OE , proto neobsahuje mřížový bod kromě O . Rovněž úsečka FD neobsahuje mřížový bod kromě F , protože $D_y = \frac{1}{2}(a-1)(b/a) < F_y + 1 = \frac{1}{2}(b+1)$. Uvnitř trojúhelníku EFD proto neleží mřížový bod. $S(a, b) + S(b, a)$ se proto rovná počtu mřížových bodů v obdélníku OA_0FB_0 , bez os x a y . Což je $\frac{1}{2}(a-1) \cdot \frac{1}{2}(b-1)$. \diamond

DŮKAZ VĚTY 106. Necht $p > q$ jsou dvě lichá prvočísla. Uvažme posloupnost $N(q)^-$ délky $\frac{1}{2}(p-1)$ a číslo $n(q)$, které jsme zavedli před Gaussovým lemmatem. Protože $N(q)^-$ je permutace čísel $1, 2, \dots, \frac{1}{2}(p-1)$, sečtením jejich prvků dostaneme první rovnost

$$\frac{p^2-1}{8} = r + n(q)p - t ,$$

kde r je součet malých členů $N(q)$ a t je součet velkých členů. Explicitní vyjádření členu b_k posloupnosti $N(q)$ je

$$kq = p \left\lfloor \frac{kq}{p} \right\rfloor + b_k .$$

Sečtením pro $k = 1, 2, \dots, \frac{1}{2}(p-1)$ dostáváme druhou rovnost

$$\frac{q(p^2-1)}{8} = pS(p, q) + r + t .$$

Odečtením první rovnosti od druhé dostaneme

$$\frac{(q-1)(p^2-1)}{8} = pS(p, q) + 2t - n(q)p .$$

Levá strana je sudé číslo, a tak

$$S(p, q) \equiv n(q) \pmod{2} .$$

Podle Gaussova lemmatu

$$\left(\frac{q}{p} \right) = (-1)^{n(q)} = (-1)^{S(p, q)} .$$

Po záměně p a q obdobně

$$\left(\frac{p}{q} \right) = (-1)^{n(p)} = (-1)^{S(q, p)} .$$

Lemma 107 dává

$$\left(\frac{q}{p} \right) \left(\frac{p}{q} \right) = (-1)^{S(p, q) + S(q, p)} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} .$$

To je zákon reciprocity. ◇

V předešlých kapitolách jsme teorii kvadratických zbytků použili dvakrát. V kapitole 2 jsme v důkazu věty 20 využili skutečnosti, že pro prvočísla tvaru $p = 4n + 1$ je -1 kvadratický zbytek. To plyne z 1 tvrzení 105. V kapitole 3

jsme v důkazu tvrzení 52 potřebovali vědět, že pokud -3 je kvadratický zbytek modulo p , platí $p \equiv 1 \pmod{3}$. Vskutku, podle 2 tvrzení 103, 1 tvrzení 105, věty 106 a 3 tvrzení 103 máme

$$\begin{aligned} 1 &= \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)/2 \cdot (3-1)/2} \left(\frac{p}{3}\right) \\ &= \left(\frac{p}{3}\right) \\ &= \left(\frac{\text{zby}(p, 3)}{3}\right). \end{aligned}$$

Platí dokonce ekvivalence $\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{3}$.

Jako příklad zjistíme, zda 1986 je kvadratický zbytek modulo 49985 (obě čísla jsou nesoudělná). Protože prvočíselný rozklad modulu je $49985 = 5^2 \cdot 1999$, musíme určit hodnoty dvou Legendreových symbolů. Pomocí vlastností Legendreova symbolu a zákona reciprocity s doplňky spočítáme, že

$$\begin{aligned} \left(\frac{1986}{1999}\right) &= \left(\frac{2}{1999}\right) \left(\frac{3}{1999}\right) \left(\frac{331}{1999}\right) \\ &= 1 \cdot (-1) \left(\frac{1999}{3}\right) \cdot (-1) \left(\frac{1999}{331}\right) \\ &= \left(\frac{1}{3}\right) \left(\frac{13}{331}\right) \\ &= \left(\frac{331}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right) \left(\frac{3}{13}\right) \\ &= (-1) \cdot \left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) \\ &= -1. \end{aligned}$$

Druhý výpočet je snadný a vlastně už zbytečný:

$$\left(\frac{1986}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Podle (triviální části) tvrzení 101 je číslo 1986 modulo 49985 kvadratický nezbytek.

Oddíl zakončíme alternativním Eisensteinovým důkazem zákona reciprocity pomocí komplexních čísel. Vždy $n \in \mathbf{N}$ a $\zeta = \exp(2\pi i/n) \in \mathbf{C}$ je primitivní n -tá odmocnina z 1.

Lemma 108. *Nechť n je liché. Pak*

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) .$$

DŮKAZ. Máme faktorizaci $z^n - 1 = (z - \zeta^0)(z - \zeta^1) \cdots (z - \zeta^{n-1})$. Substituce $z = x/y$ dává

$$x^n - y^n = \prod_{k=0}^{n-1} (x - \zeta^k y) .$$

Protože n je liché, probíhá spolu s k úplný systém zbytků modulo n i $-2k$. Tudíž

$$\begin{aligned} x^n - y^n &= \prod_{k=0}^{n-1} (x - \zeta^{-2k} y) \\ &= \zeta^{-(0+1+2+\cdots+(n-1))} \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) \\ &= \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) . \end{aligned}$$

(Pro liché n máme $\zeta^{n(n-1)/2} = 1$.)

◇

Klíčovým nástrojem je komplexní funkce

$$f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i \sin(2\pi z) .$$

Zřejmě $f(z+1) = f(z)$ (f je periodická s periodou 1), $f(-z) = -f(z)$ (f je lichá funkce) a $f(z) \neq 0 \Leftrightarrow 2z \notin \mathbf{Z}$.

Lemma 109. *Pro každé liché n a $z \in \mathbf{C}$, $2z \notin \mathbf{Z}$,*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f(z + k/n) f(z - k/n) .$$

DŮKAZ. V předcházejícím lemmatu dosadíme $x = e^{2\pi iz}$ a $y = e^{-2\pi iz}$:

$$f(nz) = \prod_{k=0}^{n-1} f(z + k/n) .$$

Proto

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f(z + k/n) \prod_{k=(n+1)/2}^{n-1} f(z + k/n) .$$

Protože $f(z + k/n) = f(z - (n - k)/n)$ (vlastnosti f), je poslední součin roven

$$\prod_{k=1}^{(n-1)/2} f(z - k/n) .$$

◇

Lemma 110. *Nechť $p > 2$ je prvočíslo, $a \in \mathbf{Z}$ a p nedělí a . Pak*

$$\prod_{l=1}^{(p-1)/2} f(la/p) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f(l/p) .$$

DŮKAZ. Pro $l = 1, 2, \dots, \frac{1}{2}(p-1)$ vynásobíme $f(\pm m_l/p)$, kde $\pm m_l$ jsou členy posloupnosti $M(a)^+$. Jak víme, $M(a)^+$ je permutace čísel $1, 2, \dots, \frac{1}{2}(p-1)$. Z $la \equiv m_l \pmod{p}$ a vlastností f plyne, že

$$f(\pm m_l/p) = \pm f(m_l/p) = \pm f(la/p) .$$

Tudíž

$$\prod_{l=1}^{(p-1)/2} f(l/p) = \prod_{l=1}^{(p-1)/2} f(\pm m_l/p) = (-1)^{m(a)} \prod_{l=1}^{(p-1)/2} f(la/p) ,$$

kde $m(a)$ je počet znamének $-$ v $\pm m_l$. Nyní stačit užít tvrzení 104. ◇

DŮKAZ VĚTY 106. (**Eisenstein, 1844.**) p, q buďte dvě různá lichá prvočísla. Podle předchozího lemmatu

$$\prod_{l=1}^{(p-1)/2} f(lq/p) = \left(\frac{q}{p}\right) \prod_{l=1}^{(p-1)/2} f(l/p) .$$

Podle lemmatu 109 platí

$$\frac{f(lq/p)}{f(l/p)} = \prod_{m=1}^{(q-1)/2} f(l/p + m/q) f(l/p - m/q) .$$

Sloučením obou vztahů získáme první rovnici a jako vedlejší výsledek pozoruhodnou identitu mezi Legendreovým symbolem a funkcí sinus:

$$\begin{aligned} \left(\frac{q}{p}\right) &= \prod_{l=1}^{(p-1)/2} \prod_{m=1}^{(q-1)/2} f(l/p + m/q) f(l/p - m/q) \\ &= (-4)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \prod_{l=1}^{(p-1)/2} \prod_{m=1}^{(q-1)/2} \sin(2\pi(l/p + m/q)) \cdot \sin(2\pi(l/p - m/q)) . \end{aligned}$$

Jednodušší identita stejného typu je popsána v úloze 14.

Záměnou $p \leftrightarrow q$ a $l \leftrightarrow m$ získáme druhou rovnici

$$\left(\frac{p}{q}\right) = \prod_{l=1}^{(p-1)/2} \prod_{m=1}^{(q-1)/2} f(l/p + m/q) f(m/q - l/p) .$$

Z porovnání obou rovnic a lichosti f plyne, že

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) .$$

4.4 Weilova věta pro $F = \mathbf{Z}_p$

Pro pole F označuje \overline{F} jeho algebraický uzávěr. X, Y, \dots označují neznámé a x, y, \dots jejich konkrétní hodnoty. Polynomy budeme označovat velkými latinskými písmeny, kromě symetrických polynomů e_i . *Absolutně ireducibilní* je ten polynom $P \in F[X, Y]$, který je ireducibilní i v $\overline{F}[X, Y]$. Platí následující fundamentální věta o počtu řešení polynomiální rovnice v konečném poli.

Věta 111 (Weil, 1948). *Nechť $F = \text{GF}(p^r)$ je konečné pole a $P \in F[X, Y]$ absolutně ireducibilní polynom. Počet řešení N rovnice $P = 0_F$ splňuje odhad*

$$N = \sum_{x, y \in F} \langle P(x, y) = 0_F \rangle = |F| + O(|F|^{1/2}) ,$$

kde konstanta v O závisí pouze na $\deg(P)$.

Weil dokázal silnější výsledek, který vysvětlíme v poznámkách. Větu v této obecnosti nedokážeme. Omezíme se na případ $F = \mathbf{Z}_p$ a dokážeme

Tvrzení 112 (Weil pro $F = \mathbf{Z}_p$). Pro každé prvočíslo p a absolutně ireducibilní polynom $P \in \mathbf{Z}_p[X, Y]$ stupně d , přičemž platí nerovnost $p > 250d^5$, počet řešení N polynomiální kongruence $P(X, Y) \equiv 0 \pmod{p}$ splňuje odhad

$$|N - p| < \sqrt{2d^5} \cdot \sqrt{p} .$$

Omezuje nás pouze rozsah skript. Po překonání potíží s derivováním v poli nenulové charakteristiky, což je ryze algebraická záležitost, umí elementární Stěpanovova–Schmidtova metoda, kterou si předvedeme v akci pro $F = \mathbf{Z}_p$, dokázat větu 111 v plné síle.

Dva příklady osvětlí nutnost požadavku absolutní ireducibility, bez něhož tvrzení 112 neplatí. První příklad: kongruence $Y^2 \equiv X^2 \pmod{p}$. Má $2p - 1$ řešení $y = \pm x$. Polynom $P(X, Y) = X^2 - Y^2$ se totiž rozkládá už v $\mathbf{Z}_p[X, Y]$. Druhý příklad: kongruence

$$Y^2 \equiv -X^4 - 2X^2 - 1 \pmod{p} ,$$

kde $p \equiv 3 \pmod{4}$. Nyní je polynom

$$P(X, Y) = Y^2 + X^4 + 2X^2 + 1 = (Y - \sqrt{-1}(X^2 + 1)) \cdot (Y + \sqrt{-1}(X^2 + 1))$$

ireducibilní v $\mathbf{Z}_p[X, Y]$, protože $\sqrt{-1} \in \overline{\mathbf{Z}_p} \setminus \mathbf{Z}_p$ pro takové p podle 1 tvrzení 105 ($\sqrt{-1}$ zde znamená $\sqrt{(-1)_{\mathbf{Z}_p}}$). Není ale pochopitelně absolutně ireducibilní. Hledáme tedy všechna $x, y \in \mathbf{Z}_p$ taková, že $y - \sqrt{-1}(x^2 + 1)$ nebo $y + \sqrt{-1}(x^2 + 1)$ je nula. Avšak 1 a $\sqrt{-1}$ jsou lineárně nezávislé nad \mathbf{Z}_p , a tak y a $x^2 + 1$ jsou nulové. Avšak $x^2 + 1 = 0_{\mathbf{Z}_p}$ nemá pro dané p řešení v \mathbf{Z}_p . Vidíme, že pro takový polynom P neexistuje pro změnu vůbec žádné řešení.

Kritérium pro generování absolutně ireducibilních polynomů je popsáno v úloze 16. Viz rovněž lemma 117.

V 4.4.1 připomeneme charaktery Abelových grup a zavedeme Paleyho turnaje, o nichž pomocí Weilovy věty dokážeme, že mají kombinatorickou vlastnost zmíněnou v úvodu ke kapitole 4. V 4.4.2–4.4.4 elementární Stěpanovovou–Schmidtovou metodou dokážeme tvrzení 112. V 4.4.2 ho odvodíme z tvrzení 124, jež představuje základní myšlenku metody. Tvrdí, že existují polynomy, jejichž stupeň je vhodně omezen a které mají v každém bodě jisté množiny kořen dostatečně velké násobnosti. Tvrzení 124 dokážeme pomocí neurčitých koeficientů v 4.4.3, zůstanou nám však algebraické dluhy, které vyrovnáme v 4.4.4.

4.4.1 Paleyho turnaje

S pomocí Weilovy věty dokážeme kombinatorickou vlastnost Paleyho turnajů. Nejdříve však připomeneme několik pojmů.

Charakter χ konečné Abelovy grupy (G, \cdot) je zobrazení $\chi : G \rightarrow \mathbf{C}$ takové, že (i) $\chi(xy) = \chi(x)\chi(y)$ pro všechny $x, y \in G$ a (ii) $|\chi(x)| = 1$ pro všechny $x \in G$. Nejjednodušší je *hlavní charakter* χ_0 : $\chi_0(x) = 1$ pro všechny $x \in G$. Pro $e \in \mathbf{N}$ definujeme χ^e jako charakter $x \rightarrow \chi(x)^e$. Pokud $\chi^e = \chi_0$, řekneme, že χ má *exponent* e . Každý charakter χ má exponent $|G|$, protože $\chi(1_G) = 1$ pro každé χ , a tak $\chi^{|G|}(x) = (\chi(x))^{|G|} = \chi(x^{|G|}) = \chi(1_G) = 1$ pro všechna $x \in G$. *Řád* d charakteru χ je jeho nejmenší exponent. Jediný charakter řádu 1 je χ_0 . Řád χ dělí $|G|$ a exponenty χ jsou právě všechny přirozené násobky řádu. Jeden charakter grupy (\mathbf{Z}_p^*, \cdot) už dobře známe. Je to Legendreův symbol

$$x \rightarrow \left(\frac{x}{p}\right) \in \{-1, 1\},$$

který má řád 2. Nejdůležitější výsledek o charakterech je

Lemma 113. *Je-li χ charakter grupy (G, \cdot) ,*

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{pokud je } \chi \text{ hlavní a} \\ 0 & \text{jinak.} \end{cases}$$

DŮKAZ. Příklad hlavního charakteru je jasný. Pro nehlavní charakter vezmeme $a \in G$ tak, že $\chi(a) \neq 1$. Protože

$$S = \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(ax) = \sum_{x \in G} \chi(a)\chi(x) = \chi(a)S,$$

$$(1 - \chi(a))S = 0 \text{ a } S = 0.$$

◇

Turnaj T na konečné množině X , $|X| = n$, je množina $\binom{n}{2}$ *uspořádaných* dvojic prvků z X , která — odhlížíme-li od uspořádání v dvojici — obsahuje všech $\binom{n}{2}$ dvouprvkových podmnožin X . Pokud $(x, y) \in T$, řekneme, že (hráč) x *poráží* (hráče) y . Například v turnaji

$$T = \{(1, 2), (2, 3), (3, 1)\}$$

1 poráží 2, 2 poráží 3 a 3 poráží 1.

Existuje pro každé $k \in \mathbf{N}$ takový turnaj, v němž se pro každých k hráčů najde jiný hráč, který je všechny poráží? Ukážeme, že tuto vlastnost má každý dostatečně velký *Paleyho turnaj* P_p na množině $\{0, 1, \dots, p-1\}$. Ten se pro prvočíslo p , $p \equiv 3 \pmod{4}$, definuje pomocí Legendreova symbolu:

$$(x, y) \in P_p \iff \left(\frac{x-y}{p} \right) = 1 .$$

Protože -1 je kvadratický nezbytek modulo p , je definice korektní.

Věta 114 (Graham a Spencer, 1971). *Pro $p > 10k^6 4^k$ se v Paleyho turnaji P_p pro každých k hráčů najde jiný hráč, který je všechny poráží.*

Větu dokážeme pomocí výsledku o charakterech.

Tvrzení 115 (odhad charakteru). χ buď charakter grupy (\mathbf{Z}_p^*, \cdot) řádu $d > 1$ a $P \in \mathbf{Z}_p[X]$ buď polynom, který má stupeň m , $m \geq d$, a není tvaru cQ^d pro $c \in \mathbf{Z}_p$ a $Q \in \mathbf{Z}_p[X]$. Pak pro každé prvočíslo p , $p > 250m^5$, platí

$$\left| \sum_{x \in \mathbf{Z}_p} \chi(P(x)) \right| < 3\sqrt{m^5} \cdot \sqrt{p} .$$

DŮKAZ VĚTY 114. Necht' χ je Legendreův symbol modulo p , takže řád χ je 2, a $A = \{a_1, a_2, \dots, a_k\}$ je k různých prvků ze \mathbf{Z}_p . Hledáme prvek $y \in \mathbf{Z}_p \setminus A$ takový, že $\chi(y - a_i) = 1$ pro $1 \leq i \leq k$. Necht'

$$g(A) = \sum_{y \in (\mathbf{Z}_p \setminus A)} \prod_{j=1}^k (1 + \chi(y - a_j)) .$$

Stačí zřejmě dokázat, že $g(A) > 0$.

Výraz $h(A)$ definujeme podobně jako $g(A)$, pouze vnější suma jde přes celé \mathbf{Z}_p . Po roznásobení vnitřního součinu dostáváme

$$\begin{aligned} h(A) &= \sum_{y \in \mathbf{Z}_p} 1 + \sum_{y \in \mathbf{Z}_p} \sum_{j=1}^k \chi(y - a_j) + \dots \\ &\quad + \sum_{y \in \mathbf{Z}_p} \sum_{j_1 < \dots < j_k} \chi(y - a_{j_1}) \cdots \chi(y - a_{j_k}) \\ &= h_0(A) + h_1(A) + \dots + h_k(A) . \end{aligned}$$

Patrně $h_0(A) = p$ a $h_1(A) = 0$ (lemma 113). Podle tvrzení 115 máme (pokud $p > 250k^5$) pro $h_s(A)$, $s \geq 2$, odhad

$$|h_s(A)| = \left| \sum_{j_1 < \dots < j_s} \sum_{y \in \mathbf{Z}_p} \chi((y - a_{j_1}) \cdots (y - a_{j_s})) \right| < \binom{k}{s} \cdot 3\sqrt{s^5} \cdot \sqrt{p} .$$

(V $h_s(A)$ jsme vyměnili pořadí sumace a použili multiplikativitu χ . Polynom $P(X) = (X - a_{j_1}) \cdots (X - a_{j_s})$ má stupeň s , $k \geq s \geq 2 = d$, a jistě se nerovná $cQ(X)^2$.)

Takže

$$|h(A) - p| < 3p^{1/2} \sum_{s=2}^k \binom{k}{s} s^{5/2} < 3k^3 2^k p^{1/2}$$

a

$$h(A) > p - 3k^3 2^k p^{1/2} .$$

Podle definice $g(A)$ a $h(A)$

$$g(A) = h(A) - \sum_{i=1}^k \prod_{j=1}^k (1 + \chi(a_i - a_j)) ,$$

a tak $g(A) \geq h(A) - k2^{k-1}$. Celkem

$$g(A) > p - 3k^3 2^k \sqrt{p} - k2^{k-1} .$$

Z $p > 10k^6 4^k$ a $k \geq 2$ ($10k^6 4^k \geq 250k^5$ pro $k > 1$) plyne, že $g(A) > 0$. Pro $k = 1$ věta platí triviálně. \diamond

Zbývá dokázat tvrzení 115. Budeme k tomu potřebovat čtyři lemmata. Ve zbytku pododdílu F označuje $\mathbf{Z}_p = \text{GF}(p)$.

Lemma 116. *Nechť $\theta \in F^*$ je primitivní element a χ je charakter grupy (F^*, \cdot) řádu $d > 1$. Pak*

$$\sum_{k=0}^{d-1} \chi(\theta^k) = 0 .$$

DŮKAZ. χ je též (nikoli hlavní) charakter faktorgrupy $F^*/(F^*)^d$. Prvky $\theta^0, \theta^1, \dots, \theta^{d-1}$ jsou reprezentanty d faktorových tříd. Dokazovaná rovnost je proto zvláštní případ lemmatu 113. \diamond

Lemma 117. *Nechť $Y^d - P(X) \in K[X, Y]$, kde K je libovolné pole. Následující tři podmínky jsou vzájemně ekvivalentní.*

1. $Y^d - P(X)$ je absolutně ireducibilní.
2. $Y^d - cP(X)$ je absolutně ireducibilní pro všechny nenulové $c \in K$.
3. Je-li $P(X) = a(X - x_1)^{d_1} \dots (X - x_s)^{d_s}$ faktorizace P v $\overline{K}[X]$ (kořeny x_i jsou vzájemně různé), pak $(d, d_1, \dots, d_s) = 1$.

DŮKAZ. Nechť 2 neplatí a $Y^d - cP(X)$ se v $\overline{K}[X, Y]$ pro nějaké nenulové $c \in K$ rozkládá. Pak se tam ale rozkládá i $c((Y/c^{1/d})^d - P(X))$ a tedy i polynom $Y^d - P(X)$ (substituce $Y = c^{1/d}Y$) a 1 neplatí.

Nechť neplatí 3 a $t > 1$ dělí všechna čísla d, d_1, \dots, d_s . Označme d/t jako e a $(X - x_1)^{d_1/t} \dots (X - x_s)^{d_s/t}$ jako $Q(X)$. Pak máme faktorizaci

$$Y^d - (1/a)P(X) = (Y^e - Q(X))(Y^{e(t-1)} + Y^{e(t-2)}Q(X) + \dots + Q(X)^{t-1})$$

a 2 neplatí.

Nechť 1 neplatí a $Y^d - P(X)$ se v $\overline{K}[X, Y]$ rozkládá. Uvažme faktorizaci

$$Y^d - P(X) = (Y - \eta_1) \dots (Y - \eta_d) ,$$

kde η_i jsou prvky algebraického uzávěru pole $\overline{K}(X)$. Kořeny η_i můžeme vyjádřit ve tvaru $\eta_i = \zeta_i \eta$, kde η je fixovaný jeden z nich a ζ_1, \dots, ζ_d jsou d -té odmocniny z 1_K v \overline{K} . Protože se $Y^d - P(X)$ rozkládá, existuje podmnožina $X \subset \{1, 2, \dots, d\}$, která má h prvků, $0 < h < d$, a

$$\prod_{i \in X} (Y - \zeta_i \eta) \in \overline{K}[X, Y] .$$

Absolutní člen tohoto součinu $\pm \eta^h (\prod_{i \in X} \zeta_i)$ leží v $\overline{K}[X]$, a tak $\eta^h \in \overline{K}[X]$. Nechť $l \in \mathbf{N}$ je nejmenší exponent takový, že $\eta^l \in \overline{K}(X)$. Pak každé $m \in \mathbf{N}$, pro něž $\eta^m \in \overline{K}(X)$, je násobek l . Protože $\eta^d = P(X) \in \overline{K}[X]$, $l \mid d$. Nechť $\eta^l = H \in \overline{K}(X)$. Máme

$$H(X)^{d/l} = P(X) ,$$

a proto $H \in \overline{K}[X]$ a $t = d/l$ dělí každé d_1, \dots, d_s a také d . Samozřejmě $t > 1$, protože $l \leq h < d$. Tedy 3 neplatí. \diamond

Lemma 118. *Nechť $d \in \mathbf{N}$, $d > 1$ a χ je charakter grupy (F^*, \cdot) řádu d . Nechť $P \in F[X]$ má stupeň m , $Y^d - P(X)$ je absolutně ireducibilní a $m \geq d$. Pak pro $p > 250m^5$ platí*

$$\left| \sum_{x \in F} \chi(P(x)) \right| < 3\sqrt{m^5} \cdot \sqrt{p} .$$

DŮKAZ. Nechť $\theta \in F^*$ je primitivní element. Položíme

$$Z_k = \#\{x \in F : P(x) \in \theta^k (F^*)^d\} \text{ a } N_k = \#\{(x, y) \in F^2 : y^d = P(x)\theta^{-k}\} .$$

Takže

$$\sum_{x \in F} \chi(P(x)) = \sum_{k=0}^{d-1} Z_k \chi(\theta^k) .$$

Protože podle předešlého lemmatu je $Y^d - P(X)\theta^{-k}$ absolutně ireducibilní, můžeme použít tvrzení 112 a máme odhad $|N_k - p| < \sqrt{2m^5} \cdot \sqrt{p}$ (nyní používáme, že $m \geq d$). Nechť N'_k je počet těch z N_k řešení (x, y) , v nichž $y \neq 0_F$. Pak $N_k - N'_k \leq m$, a tak $|N'_k - p| < 3\sqrt{m^5} \cdot \sqrt{p}$. Z_k vyjádříme jako $Z_k = p/d + R_k$ a uvědomíme si, že $Z_k = N'_k/d$. Tudíž

$$|R_k| < 3\sqrt{m^5/d^2} \cdot \sqrt{p} .$$

Vyjádření součtu hodnot $\chi(P(x))$ pomocí Z_k a lemma 116 dávají

$$\begin{aligned} \left| \sum_{x \in F} \chi(P(x)) \right| &= \left| \sum_{k=0}^{d-1} \left(\frac{p}{d} + R_k \right) \chi(\theta^k) \right| = \left| \sum_{k=0}^{d-1} R_k \chi(\theta^k) \right| \\ &\leq \sum_{k=0}^{d-1} |R_k| < 3\sqrt{m^5} \cdot \sqrt{p} . \end{aligned}$$

◇

Lemma 119. *Nechť*

$$P(X) = c(X - x_1)^{e_1} \dots (X - x_s)^{e_s} ,$$

kde $P \in F[X]$, $c \in F$, $e_i \in \mathbf{N}$ a $x_i \in \overline{F}$. Nechť dále $d \in \mathbf{N}$ dělí všechna e_i a $p \perp d$. Pak

$$P(X) = cK(X)^d ,$$

kde $K \in F[X]$.

DŮKAZ. Dokážeme, že $K(X) = (X - x_1)^{e_1/d} \dots (X - x_s)^{e_s/d}$ padne do $F[X]$. Necht' $K(X) = X^u + c_1X^{u-1} + \dots + c_u$. Víme, že $K(X)^d \in F[X]$. Koeficient X^{du-i} v $K(X)^d$ je $d_F c_i$ plus polynom z $F[c_1, \dots, c_{i-1}]$ (pro $i = 1$ je tento polynom nulový). Protože $d_F \neq 0_F$, indukcí podle i plyne, že $c_i \in F$. \diamond

DŮKAZ TVRZENÍ 115. Pišme $P(X) = c(X - x_1)^{e_1}(X - x_2)^{e_2} \dots (X - x_s)^{e_s}$, kde $c \in F$ a x_i jsou vzájemně různé prvky \overline{F} . Podle předpokladu je číslo $e = (e_1, \dots, e_s, d)$ vlastním dělitelem d . Takže $P(X) = cK(X)^e$, kde $K(X) = (X - x_1)^{e_1/e} \dots (X - x_s)^{e_s/e}$. Podle předchozího lemmatu s e v roli d (předpoklad je splněn, $e < d \leq m < p$) platí, že $K \in F[X]$. Protože $(e_1/e, \dots, e_s/e, d/e) = 1$, podle lemmatu 117 je

$$Y^{d/e} - K(X)$$

absolutně ireducibilní. K má stupeň m/e a χ^e má řád $d/e, m/e \geq d/e > 1$. Podle lemmatu 118

$$\begin{aligned} \left| \sum_{x \in F} \chi(P(x)) \right| &= \left| \chi(c) \sum_{x \in F} \chi^e(K(x)) \right| \\ &< 3\sqrt{(m/e)^5} \cdot \sqrt{p} \\ &\leq 3\sqrt{m^5} \cdot \sqrt{p}. \end{aligned}$$

4.4.2 První část důkazu

Nyní přejdeme k důkazu tvrzení 112. V celém důkazu $F = \mathbf{Z}_p$, kde \mathbf{Z}_p je konečné pole zbytků modulo p , a $P(X, Y) \in F[X, Y]$ je absolutně ireducibilní polynom stupně $d \geq 2$ (pro $d = 1$ věta triviálně platí). Řekneme, že P je *redukováný*, pokud (i) Y^d má koeficient 1_F , to jest

$$P(X, Y) = Y^d + G_1(X)Y^{d-1} + G_2(X)Y^{d-2} + \dots + G_d(X),$$

kde $G_i(X) \in F[X]$ a má stupeň nejvýše i , a (ii) P není polynomem v X a Y^p , to jest P má monom aX^iY^j , kde $a \neq 0_F$ a p nedělí j . Vlastnosti (ii) se říká *separovanost* P vzhledem k Y .

Tvrzení 120 (redukce P). *Bez újmy na obecnosti můžeme předpokládat, že polynom P je redukováný.*

DŮKAZ. Nechť $P(X, Y)$ je výchozí polynom. Pokud $P(X, Y) = Q(X, Y^p)$, můžeme P nahradit polynomem Q , protože v F platí $y^p = y$ a počet řešení rovnice se tedy nezmění. To opakujeme tak dlouho, až dostaneme polynom $P(X, Y)$ separovaný v Y . Nechť $P = \sum_{i,j} a_{ij} X^i Y^j$ a $\deg(P) = d$. Abychom dosáhli vlastnost (i), zavedeme substituci

$$Q(X, Y) = P(X + CY, Y) = \sum_{i,j} A_{ij}(C) X^i Y^j .$$

Polynomy $A_{ij}(C) \in F[C]$ mají stupeň nejvýše d . Separovanost již máme, tudíž existuje koeficient $a_{i_0 j_0} \neq 0_F$ s j_0 nedělitelným p . Platí

$$A_{i_0 j_0}(0_F) = a_{i_0 j_0} \quad \text{a} \quad A_{0d}(C) = P_d(C, 1_F) ,$$

kde $P_d(X, Y)$ sestává z monomů P se stupněm d . Polynomy $A_{i_0 j_0}(C)$ a $A_{0d}(C)$ nejsou identicky nulové. Podle předpokladů tvrzení 112 $|F| = p > 2d$, můžeme tedy zvolit $c \in F$ tak, že $A_{i_0 j_0}(c) \neq 0_F$ a $A_{0d}(c) \neq 0_F$. Polynom $P(X, Y)$ pak nahradíme $Q(X, Y) = P(X + cY, Y)/A_{0d}(c)$. Polynom $Q(X, Y)$ stupně d má vlastnosti (i) a (ii), zůstává absolutně ireducibilní a rovnice $Q(X, Y) = 0_F$ má v F stejný počet řešení jako $P(X, Y) = 0_F$. \diamond

V dalším je proto $P(X, Y) \in F[X, Y]$ redukovaný absolutně ireducibilní polynom stupně $d \geq 2$.

P je ireducibilní i v $F(X)[Y]$. To plyne ze zobecnění tvrzení 12: P je ireducibilní v $F[X][Y]$ a $F(X)$ je podílové pole okruhu $F[X]$ s jednoznačným rozkladem na ireducibilní prvky. P jako prvek $F(X)[Y]$ je tedy minimální polynom každého svého kořene $\delta \in \overline{F(X)}$. Tyto kořeny jsou navíc jednoduché, protože derivace P podle Y není identicky nulová. (P je redukovaný; v polích nenulové charakteristiky je třeba být opatrný.)

Operátor derivování v $F[X]$ označujeme pomocí D : $D(a_t X^t + a_{t-1} X^{t-1} + \dots + a_1 X + a_0) = t_F a_t X^{t-1} + (t-1)_F a_{t-1} X^{t-2} + \dots + a_1$.

Tvrzení 121 (o derivaci). *Nechť $A(X) \in F[X]$ ($F = \mathbf{Z}_p$, ale tvrzení platí pro každé pole charakteristiky p) a $m \in \mathbf{N}$ splňuje $m \leq p$. Když pro nějaké $x \in F$ platí*

$$(D^{m-1}A)(x) = (D^{m-2}A)(x) = \dots = (DA)(x) = A(x) = 0_F ,$$

dělí $(X - x)^m$ polynom $A(X)$. Jinými slovy, $A(X)$ má v x kořen násobnosti alespoň m .

DŮKAZ. Vyjádříme-li polynom A jako $A(X) = c_t(X-x)^t + \dots + c_1(X-x) + c_0$, dostáváme

$$D^l A = l!_F \cdot \left(\binom{t}{l}_F c_t(X-x)^{t-l} + \dots + \binom{l+1}{l}_F c_{l+1}(X-x) + c_l \right).$$

Pro $X = x$ a $0 \leq l < m$ dostáváme $0_F = l!_F \cdot c_l$. Avšak $l < p$, a tak $l!_F \neq 0_F$ a $c_l = 0_F$. Takže $c_0 = c_1 = \dots = c_{m-1} = 0_F$ a $(X-x)^m$ dělí $A(X)$. \diamond

Podmínka $m \leq p$ je podstatná. Například $A(X) = X^p$ má všechny derivace identicky nulové, ale v 0_F má kořen násobnosti pouze p . Pro $m > p$ proto tvrzení obecně neplatí. To je jediná, avšak nezanedbatelná potíž, kterou nutno překonat při přechodu od $F = \mathbf{Z}_p$ k obecnému poli $F = \text{GF}(p^r)$.

Tvrzení 122 (diskriminant). $G = F(A_0, \dots, A_d)$ buď pole racionálních funkcí v neznámých A_0, \dots, A_d a polynom $Q(Y) = A_0 Y^d + A_1 Y^{d-1} + \dots + A_d \in G[Y]$ měj kořeny $y_i \in \overline{G}$:

$$Q(Y) = A_0(Y - y_1)(Y - y_2) \cdots (Y - y_d).$$

Pak

$$\Delta = A_0^{2d-2} \prod_{1 \leq i < j \leq d} (y_i - y_j)^2$$

je polynom z $F[A_0, \dots, A_d]$, který je nenulový, právě když Q má pouze jednoduché kořeny. Je-li nenulový, má stupeň $2d - 2$ a jeho každý monom $aA_0^{i_0} \dots A_d^{i_d}$ splňuje $i_1 + 2i_2 + \dots + di_d = d(d - 1)$. Polynomu Δ se říká diskriminant Q .

DŮKAZ. Polynom $\prod (y_i - y_j)^2$ je symetrický v y_i . Podle tvrzení 13 v kapitole 1 je proto polynomem v elementárních symetrických funkcích $e_i(y_1, \dots, y_d)$ a tedy polynomem z $F[A_1/A_0, \dots, A_d/A_0]$ stupně $2(d - 1)$ (y_i má v $\prod (y_i - y_j)^2$ stupeň $2(d - 1)$). Takže $\Delta \in F[A_0, \dots, A_d]$ a má stupeň $2(d - 1)$. Poslední část tvrzení plyne z poslední části tvrzení 13. \diamond

Nechť $\Delta(X) \in F[X]$ je diskriminant polynomu $P(X, Y) \in F(X)[Y]$ vzhledem k Y . Protože $\deg(G_i) \leq i$ (G_i je koeficient Y^{d-i} v P), poslední část tvrzení 122 implikuje $\deg(\Delta) \leq d(d - 1)$. Pokud $\Delta(x) \neq 0_F$, kde $x \in F$, má $P(x, Y)$ d různých kořenů $y_1, \dots, y_d \in \overline{F}$. Definujeme množinu

$$I = \{x \in F : \Delta(x) \neq 0_F\}$$

a pro $x \in I$ množiny

$$J_1(x) = \{y_i : y_i \in F\} \quad \text{a} \quad J_2(x) = \{y_i : y_i \in \overline{F} \setminus F\} .$$

Je jasné, že pro každé $x \in I$ platí $|J_1(x)| + |J_2(x)| = d$. Počet řešení N rovnice $P(X, Y) = 0_F$ v F splňuje

$$N = \sum_{x \in I} |J_1(x)| + N' ,$$

kde N' je počet těch řešení (x, y) , pro něž $\Delta(x) = 0_F$. Zřejmě $N' \leq d \cdot \deg(\Delta) \leq d^2(d-1)$, a tak stačí odhadnout pouze sumu.

Definujeme polynomy

$$\begin{aligned} E_1(X, Y, Y') &= Y - Y' \quad \text{a} \\ E_2(X, Y, Y') &= \sum_{j=1}^d G_{d-j}(X)(Y^{j-1} + Y^{j-2}Y' + \dots + (Y')^{j-1}) , \end{aligned}$$

kde $G_j(X)$ jsou koeficienty Y v $P(X, Y)$. Položíme $e_i = \deg(E_i)$, takže $e_1 = 1$ a $e_2 = d - 1$. (Nehrozí záměna se symetrickými polynomy.)

Lemma 123. *Pro $i = 1, 2$ a $x \in I$ platí*

$$J_i(x) = \{y \in \overline{F} : E_i(x, y, y^p) = 0_F\} .$$

DŮKAZ. Máme faktorizaci

$$P(X, Y) - P(X, Y') = E_1(X, Y, Y') \cdot E_2(X, Y, Y') .$$

Pro $x \in I$ a $y \in J_1(x) \cup J_2(x)$ platí rovnosti $0_F = P(x, y) = P(x, y)^p = P(x, y^p)$, protože $u = u^p$ v F (ale ne v $\overline{F} \setminus F$) a $(u + v)^p = u^p + v^p$ pro všechna $u, v \in \overline{F}$. Tudíž

$$0_F = P(x, y) - P(x, y^p) = E_1(x, y, y^p) \cdot E_2(x, y, y^p) .$$

Pokud $y \in J_1(x)$, máme $y \in F$ a $y = y^p$. Takže $E_1(x, y, y^p) = 0_F$. Ovšem $E_2(x, y, y^p) = E_2(x, y, y) \neq 0_F$, protože y je jednoduchý kořen $P(x, Y)$ a $E_2(x, y, y) = P_Y(x, y)$ (derivace P podle Y). Pokud $y \in J_2(x)$, máme $y \in \overline{F} \setminus F$ a $y \neq y^p$. Takže $E_1(x, y, y^p) \neq 0_F$. V důsledku hořejší rovnosti však $E_2(x, y, y^p) = 0_F$. \diamond

Dospíváme k výsledku, na němž je elementární důkaz tvrzení 112 založen. Dokážeme ho v příštím pododdílu.

Tvrzení 124 (klíčové). Necht $i = 1, 2$ a číslo $m \in \mathbf{N}$ je takové, že

$$d \nmid m, \quad m \geq d^2 \quad \text{a} \quad 2(d-1)(m+8)^2 \leq p.$$

Pak existuje nenulový polynom $R_i(X) \in F[X]$ takový, že

1. $(D^l R_i)(x) = 0_F$ pro každé $x \in I$ a $0 \leq l < m|J_i(x)|$.
2. $\deg(R_i) \leq e_i p m + p d(d-1)$. ($e_1 = 1$ a $e_2 = d-1$ jsou stupně E_i .)

DŮKAZ TVRZENÍ 112. (**Stěpanov, 1969–74; Schmidt, 1973.**) Veličiny $\Delta(X)$, I a $J_i(x)$ buďte jako výše a m a $R_i(X)$ jako v posledním tvrzení. Pro každé $x \in I$ a $i = 1, 2$ platí

$$m|J_i(x)| \leq m d < p.$$

Pro polynomy $R_i(X)$ tedy můžeme použít tvrzení 121.

Položíme, pro $i = 1$ a 2 ,

$$N_i = \sum_{x \in I} |J_i(x)|.$$

Protože $p - d(d-1) \leq |I| \leq p$ (neboť $\deg(\Delta) \leq d(d-1)$), máme nerovnosti

$$d(p - d(d-1)) \leq N_1 + N_2 \leq d p.$$

Počet kořenů polynomu $R_i(X)$ v F , včetně násobností, nepřesahuje jeho stupeň. Podle 1 tvrzení 124 a tvrzení 121 má $R_i(X)$ v každém $x \in I$ alespoň $m|J_i(x)|$ -násobný kořen. Tedy $m N_i \leq \deg(R_i)$. Podle 2 tvrzení 124

$$N_i \leq \frac{\deg(R_i)}{m} \leq e_i p + \frac{p d(d-1)}{m}.$$

N_1 je počet těch z N řešení $(x, y) \in F^2$ rovnice $P(X, Y) = 0_F$, pro něž $\Delta(x) \neq 0_F$. Díky $\deg(\Delta) \leq d(d-1)$ a poslednímu odhadu máme

$$N \leq N_1 + d^2(d-1) < p + \frac{p d(d-1)}{m} + d^3.$$

Z druhé strany, podle dolního odhadu $N_1 + N_2$ a horního odhadu N_2 ,

$$\begin{aligned} N &\geq N_1 > p d - d^3 - N_2 \\ &\geq p d - d^3 - (d-1)p - \frac{p d(d-1)}{m} \\ &= p - \frac{p d(d-1)}{m} - d^3. \end{aligned}$$

Pro každé $m \in \mathbf{N}$ splňující podmínky tvrzení 124 máme odhad

$$|N - p| < \frac{pd(d-1)}{m} + d^3 .$$

Číslo m zvolíme jako násobek d v rozmezí

$$\sqrt{p/(2d)} - 5d < m \leq \sqrt{p/(2d)} - 4d .$$

Pak $(m+8)^2 \leq p/(2d)$ a požadovaná nerovnost $2(d-1)(m+8)^2 \leq p$ je splněna. Rovněž platí, vzhledem k $p > 250d^5$,

$$m > \left(\frac{p}{2d}\right)^{1/2} \left(1 - \frac{5 \cdot 2^{1/2} \cdot d^{3/2}}{p^{1/2}}\right) > \frac{1}{2} \left(\frac{p}{2d}\right)^{1/2} > d^2 .$$

Jaký odhad nám toto m dá? Z $p > 250d^5$ plyne ještě i

$$\frac{5 \cdot 2^{1/2} \cdot d^{3/2}}{p^{1/2}} < \frac{1}{3} .$$

Pro všechna reálná x v intervalu $0 < x < 1/3$ platí $1/(1-x) < 1 + 3x/2$. Takže

$$\frac{1}{m} < \left(\frac{2d}{p}\right)^{1/2} \left(1 + \frac{3}{2} \cdot \frac{5 \cdot 2^{1/2} \cdot d^{3/2}}{p^{1/2}}\right) .$$

Po dosazení do horního odhadu $|N - p|$ máme

$$\begin{aligned} |N - p| &< 2^{1/2}d(d-1)d^{1/2}p^{1/2} \left(1 + \frac{8 \cdot 2^{1/2} \cdot d^{3/2}}{p^{1/2}}\right) + d^3 \\ &< 2^{1/2}d^{5/2}p^{1/2} - 2^{1/2}d^{3/2}p^{1/2} + 16d^4 + d^3 \\ &< 2^{1/2}d^{5/2}p^{1/2} . \end{aligned}$$

Tím je speciální případ Weilovy věty dokázán.

4.4.3 Druhá část důkazu

Zbývá však dokázat tvrzení 124. K tomu budeme potřebovat několik lemat. Připomínáme, že $F = \mathbf{Z}_p$. Polynom $P(X, Y) = Y^d + G_1(X)Y^{d-1} + \dots + G_d(X) \in F[X, Y]$ stupně d v Y je absolutně ireducibilní a separovaný v Y , $\deg(G_i) \leq i$ a $\delta \in \overline{F(X)}$ je jeho kořen, $P(X, \delta) \equiv 0$. Místo $P(X, \delta) = 0_{\overline{F(X)}}$ a podobně budeme v případě funkcionálních polí psát $\dots \equiv 0$.

Lemma 125. $P(X, Y)$ a $\delta \in \overline{F(X)}$ jsou jako výše. Pokud $A \in F[X, Y, Z, W]$ je nenulový polynom, jehož stupně splňují $\deg_X(A) \leq p/d - d$, $\deg_Y(A) \leq d - 1$ a $\deg_W(A) \leq d - 1$, potom

$$A(X, \delta, X^p, \delta^p) \neq 0 .$$

Důkaz tohoto lemmatu odsouváme do příštího pododdílu.

Protože P je separovaný v Y , dá se operátor derivace D rozšířit z $F(X)$ na $F(X, \delta)$. Má platit (proměnné, podle nichž se derivuje, klademe do indexu)

$$0 \equiv D(P(X, \delta)) = P_X(X, \delta) + P_Y(X, \delta) \cdot (D\delta) .$$

Odtud

$$D\delta = -\frac{P_X(X, \delta)}{P_Y(X, \delta)}$$

a D rozšíříme na $F(X, \delta)$ zřejmým způsobem.

Lemma 126. Polynom $P(X, Y)$ je jako výše (zejména je P separovaný v Y) a $\delta \in \overline{F(X)}$ je jeho kořen. Nechť $m, l \in \mathbf{N}_0$, $0 \leq l < m$ a $A \in F[X, Y]$. Pak

$$D^l(P_Y^{2m}(X, \delta) \cdot A(X, \delta)) = P_Y^{2m-l}(X, \delta) \cdot A^{(l)}(X, \delta) ,$$

kde $A^{(l)} \in F[X, Y]$ a má stupeň nejvýše $\deg(A) + (2d - 3)l$.

DŮKAZ. Indukce podle l . Pro $l = 0$ lemma platí. Z předpokladu platnosti pro l odvodíme platnost pro $l + 1$. Pro přehlednost zápisu pomíjíme argument (X, δ) .

$$\begin{aligned} D^{l+1}(P_Y^{2m}(X, \delta) \cdot A(X, \delta)) &= D(P_Y^{2m-2l}(X, \delta) \cdot A^{(l)}(X, \delta)) \\ &= (2m - 2l)P_Y^{2m-2l-1} \cdot (P_{YX} + P_{YY}D\delta) \cdot A^{(l)} + P_Y^{2m-2l} \cdot (A_X^{(l)} + A_Y^{(l)}D\delta). \end{aligned}$$

Dosadíme vyjádření pro $D\delta$ a dostaneme

$$\begin{aligned} &P_Y^{2m-2(l+1)} \cdot [(2m - 2l) \cdot (P_{YX}P_Y - P_{YY}P_X) \cdot A^{(l)} + A_X^{(l)}P_Y^2 - A_Y^{(l)}P_XP_Y] \\ &= P_Y^{2m-2(l+1)} \cdot A^{(l+1)}. \end{aligned}$$

Zřejmě $\deg(A^{(l+1)}) \leq \deg(A^{(l)}) + (2d - 3)$. Odtud plyne uvedený odhad stupně polynomu $A^{(l)}$. \diamond

Lemma 127. *Nechť*

$$P(X, Y) = Y^d + G_1(X)Y^{d-1} + \cdots + G_d(X) = (y - \delta_1)(y - \delta_2) \cdots (y - \delta_d) ,$$

kde $\deg(G_i) \leq i$ a $\delta_i \in \overline{F(X)}$. Je-li $A \in F[X, Y_1, \dots, Y_d]$ polynom symetrický v Y_1, \dots, Y_d , pak

$$A(X, \delta_1, \dots, \delta_d) = B(X) ,$$

kde $B \in F[X]$ a $\deg(B) \leq \deg(A)$.

DŮKAZ. Stupeň polynomu A označíme jako s . Pak

$$A(X, Y_1, \dots, Y_d) = \sum_{v=0}^s X^v \cdot C_v(Y_1, \dots, Y_d) ,$$

kde $\deg(C_v) \leq s - v$ a C_v je symetrický v Y_1, \dots, Y_d . Podle tvrzení 13 v kapitole 1

$$C_v(Y_1, \dots, Y_d) = H_v(e_1, \dots, e_d) ,$$

kde $H_v \in F[S_1, \dots, S_d]$ a $e_i \in F[Y_1, \dots, Y_d]$ jsou elementární symetrické polynomy. Podle téhož tvrzení každý monom $S_1^{i_1} S_2^{i_2} \cdots S_d^{i_d}$ polynomu H_v splňuje nerovnost $i_1 + 2i_2 + \cdots + di_d \leq s - v$. Takže v

$$C_v(\delta_1, \dots, \delta_d) = H_v(-G_1(X), \dots, (-1)^d G_d(X))$$

má každý monom $G_1(X)^{i_1} G_2(X)^{i_2} \cdots G_d(X)^{i_d}$ stupeň v X nejvýše $i_1 + 2i_2 + \cdots + di_d \leq s - v$. Každý sčítanec $X^v \cdot C_v(\delta_1, \dots, \delta_d)$ ve vyjádření $A(X, \delta_1, \dots, \delta_d)$ je polynom stupně nejvýše $v + s - v = s$. \diamond

Lemma 128. *Nechť $i = 1, 2$ a číslo $m \in \mathbf{N}$ je takové, že*

$$d \nmid m, \quad m \geq d^2 \quad \text{a} \quad 2(d-1)(m+8)^2 \leq p .$$

$P(X, Y) \in F[X, Y]$ a $\delta \in \overline{F(X)}$ jsou jako výše. Pak existuje polynom $A = A_i \in F[X, Y]$ takový, že

1. $A(X, \delta) \neq 0$.
2. $A^{(l)}(x, y) = 0_{\overline{F}}$ pro všechny $x \in I, y \in J_i(x)$ a $0 \leq l < m$ (polynom $A^{(l)}$ je definován v lemmatu 126, I a $J_i(x)$ v předešlém pododdílu.)

3. $\deg(A) \leq e_i pm/d + p(d - 3/2)$. (Čísla e_i jsou definována v předešlém pododdílu.)

DŮKAZ. Polynom A hledáme ve tvaru

$$A(X, Y) = \sum_{j=0}^K \sum_{k=0}^{d-1} \langle j + k \leq K \rangle \cdot B_{j,k}(X, Y) \cdot X^{pj} Y^{pk} ,$$

kde $K = e_i m/d + d - 2$ a

$$B_{j,k}(X, Y) = \sum_{i=0}^{d-1} A_{i,j,k}(X) \cdot Y^i ,$$

přičemž $\deg(A_{i,j,k}) \leq p/d - d - i - j - k$. Tudíž

$$\begin{aligned} \deg(A) &\leq Kp + p/d \\ &= e_i pm/d + p(d - 2 + 1/d) \\ &\leq e_i pm/d + p(d - 3/2) \end{aligned}$$

a A má požadovaný stupeň. Nejsou-li všechny polynomy $A_{i,j,k}$ nulové, vyplývá pomocí lemmatu 125, že $A(X, \delta) \not\equiv 0$. Tím jsou dosaženy vlastnosti 1 a 3. Zbývá dokázat, že lze zvolit ne všechny nulové $A_{i,j,k}$ tak, že platí 2.

Derivace X^p a δ^p jsou identicky nulové. Proto

$$A^{(l)}(X, Y) = \sum_{j=0}^K \sum_{k=0}^{d-1} \langle j + k \leq K \rangle \cdot B_{j,k}^{(l)}(X, Y) \cdot X^{pj} Y^{pk} ,$$

kde, podle lemmatu 126,

$$\deg(B_{j,k}^{(l)}) \leq \deg(B_{j,k}) + (2d - 3)l \leq p/d - d - j - k + (2d - 3)l .$$

Potřebujeme, aby pro $0 \leq l < m$, $x \in I$ a $y \in J_i(x)$ nastalo $A^{(l)}(x, y) = 0_{\overline{F}}$.

První případ je $i = 1$. Nyní $x, y \in F$ a tedy $x^p = x$ a $y^p = y$. Potřebujeme, aby se polynom

$$C^{(l)}(X, Y) = \sum_{j=0}^K \sum_{k=0}^{d-1} \langle j + k \leq K \rangle \cdot B_{j,k}^{(l)}(X, Y) \cdot X^j Y^k$$

anuloval na $x \in I, y \in J_1(x)$. Povšimněme si, že

$$\deg(C^{(l)}) \leq p/d + (2d - 3)l - 2 .$$

Druhý případ je $i = 2$. Nyní $x \in F$ a $y \in \overline{F} \setminus F$. Takže $x^p = x$, $y^p \neq y$ a, podle lemmatu 123,

$$0_{\overline{F}} = E_2(x, y, y^p) = \sum_{i=1}^d G_{d-i}(x) \cdot (y^{i-1} + y^{i-2}y^p + y^{i-3}y^{2p} + \dots + y^{p(i-1)}) .$$

Dosadíme v $A^{(l)}(X, Y)$ x za X a y za Y . Protože $G_0 = 1_F$, lze pomocí poslední rovnice vyjádřit $y^{p(d-1)}$ pomocí $1, y^p, y^{2p}, \dots, y^{p(d-2)}$ a koeficientů, které jsou polynomy z $F[x, y]$ stupně nejvýše $d - 1$. Pro $i = 2$ tedy $A^{(l)}$ přechází na polynom $C^{(l)}(X, Y, Z)$, kde Z odpovídá mocninám y^p a za Z^{d-1} jsme dosadili zmíněné vyjádření. Tedy $\deg_Z(C^{(l)}) \leq d - 2$. Monomy $A^{(l)}$ přispívají do X, Y -stupně $C^{(l)}$ nejvýše $p/d - d - j - k + (2d - 3)l + j \leq p/d + (2d - 3)l - 2$ pro $k < d - 1$ a $p/d - d - j - k + (2d - 3)l + j + (d - 1) \leq p/d + (2d - 3)l - 2$ pro $k = d - 1$. Takže $\deg_{X,Y}(C^{(l)}) \leq p/d + (2d - 3)l - 2$. Chceme $C^{(l)}(x, y, y^p) = 0_{\overline{F}}$ pro všechny $x \in I$ a $y \in J_2(x)$.

V obou případech potřebujeme, aby se $C^{(l)}(X, Y, Z)$ anuloval na x, y, y^p , $x \in I$, $y \in J_i(x)$, přičemž

$$\deg_{X,Y}(C^{(l)}) \leq p/d + (2d - 3)l - 2 \quad \text{a} \quad \deg_Z(C^{(l)}) \leq e_i - 1 \quad (e_1 = 1, e_2 = d - 1) .$$

Indukcí se lehce dokáže, že pro dvojice (x, y) splňující $P(x, y) = 0_{\overline{F}}$ a $t \in \mathbf{N}_0$ máme vyjádření

$$y^{d-1+t} = G_1^{(t)}(x)y^{d-1} + \dots + G_d^{(t)}(x) ,$$

kde $\deg(G_i^{(t)}) \leq t + i - 1$ a $G_i^{(0)}(X) = G_i(X)$. Díky této redukci $C^{(l)}(x, y, y^p) = 0_{\overline{F}}$, právě když $D^{(l)}(x, y, y^p) = 0_{\overline{F}}$, kde polynom $D^{(l)}$ splňuje

$$\begin{aligned} \deg_X(D^{(l)}) &\leq p/d + (2d - 3)l - 2 \\ \deg_Y(D^{(l)}) &\leq d - 1 \\ \deg_Z(D^{(l)}) &\leq e_i - 1 . \end{aligned}$$

Požadavek 2 v lemmatu je tedy splněn, je-li polynom $D^{(l)}(X, Y, Z)$ identicky nulový pro všechny $0 \leq l < m$.

Počet koeficientů polynomu $D^{(l)}$ je nejvýše

$$e_i d(p/d + (2d - 3)l - 1) < e_i p + (2d^2 - 3d)e_i l .$$

Počet b koeficientů všech polynomů $D^{(l)}(X, Y, Z)$, $0 \leq l < m$, tak splňuje, vzhledem k $1 + 2 + \dots + (m - 1) < m^2/2$,

$$b < e_i p m + \frac{1}{2} e_i m^2 (2d^2 - 3d) .$$

Tyto neznámé koeficienty jsou lineárními kombinacemi dosud neurčených koeficientů polynomů $A_{i,j,k}(X)$. Dostáváme homogenní lineární soustavu pro $A_{i,j,k}$ -koeficienty.

Počet koeficientů jednoho polynomu $A_{i,j,k}$ je alespoň

$$p/d - d - i - j - k \geq p/d - d - 2(d - 1) - j \geq p/d - 3d - j .$$

Sečtením přes j v oboru $0 \leq j \leq K - k$ získáme dolní odhad

$$(p/d - 3d)(K + 1) - (K - k)(K - k + 1)/2 - pk/d .$$

Sečtení přes k probíhající $0, 1, \dots, d - 1$ dá dolní odhad

$$(p - 3d^2)(K + 1) - K^2d/2 - (p/d)d(d - 1)/2 .$$

Konečně sečtením přes i probíhající $0, 1, \dots, d - 1$ získáme celkový dolní odhad a pro počet všech neznámých koeficientů ve všech $A_{i,j,k}(X)$. Totiž

$$\begin{aligned} a &> (p - 3d^2)(Kd + d) - pd(d - 1)/2 - K^2d^2/2 \\ &> (p - 3d^2)(e_i m + d^2 - d) - pd(d - 1)/2 - (e_i m + d^2)^2/2 \\ &> e_i p m + p(d^2 - d)/2 - e_i^2 m^2/2 - 6e_i m d^2 - 2e_i m d^2 , \end{aligned}$$

protože, podle předpokladu, $m \geq d^2$.

Pokud $b < a$, má soustava b homogenních lineárních rovnic o alespoň a neznámých netriviální řešení a polynomy $D^{(l)}(X, Y, Z)$ jsou identicky nulové. To nastane, je-li horní odhad čísla b menší než dolní odhad čísla a , tedy pro

$$e_i m^2(2d^2 - 3d + e_i)/2 + 8e_i m d^2 < pd(d - 1)/2 .$$

Protože $e_i = 1$ nebo $d - 1$, tato nerovnost jistě platí, pokud platí nerovnost

$$m^2(d - 1)(2d^2 - 2d - 1)/2 + 8md^2(d - 1) < pd(d - 1)/2 .$$

Ta platí, pokud $m^2(d - 1) + 8md < p/2$. A to je splněno díky $d \geq 2$ a předpokladu $2(d - 1)(m + 8)^2 \leq p$. Tím je důkaz lemmatu dokončen. \diamond

DŮKAZ TVRZENÍ 124. Položíme

$$C(X, Y) = P_Y^{2m}(X, Y) \cdot A(X, Y) ,$$

kde $A = A_i \in F[X, Y]$ je polynom z lemmatu 128. Pak $C(X, \delta) \not\equiv 0$, protože $P_Y(X, \delta) \not\equiv 0$ (P je ireducibilní v $F(X)[Y]$, tudíž je δ jednoduchý kořen P) a $A(X, \delta) \not\equiv 0$ podle 1 lemmatu 128. Pro $0 \leq l < m$ platí

$$D^l C(X, \delta) = P_Y^{2m-2l}(X, \delta) \cdot A^{(l)}(X, \delta) .$$

(Polynom $A^{(l)}$ je definován v lemmatu 126.) Takže, podle 2 lemmatu 128, pro $x \in I$ a $y \in J_i(x)$ máme $(D^l C(X, \delta))(x, y) = 0_{\overline{F}}$. Dále

$$\deg(C) \leq e_i p m / d + p(d - 3/2) + 2md .$$

Ale z $p > 250d^5$ a $p \geq 2(d - 1)(m + 8)^2$ plyne, že $2md < 2d\sqrt{p} = 2dp/\sqrt{p} < p/2$, a tak

$$\deg(C) \leq e_i p m / d + p(d - 1) .$$

Hledaný polynom bude

$$R_i(X) = \prod_{j=1}^d C(X, \delta_j) ,$$

kde $P(X, Y) = (X - \delta_1)(X - \delta_2) \dots (X - \delta_d)$. Místo $R_i(X)$, kde $i = 1$ nebo 2 , budeme psát jen $R(X)$. Necht' nyní $0 \leq l < m|J_i(X)|$. Pravá strana rovnice

$$D^l R(X) = \sum_{u_1 + \dots + u_d = l} \binom{l}{u_1, \dots, u_d}_F D^{u_1} C(X, \delta_1) \cdot \dots \cdot D^{u_d} C(X, \delta_d)$$

je polynom symetrický v $\delta_1, \dots, \delta_d$. Podle tvrzení 13 máme vyjádření $D^l R(X) = K(X, G_1(X), \dots, G_d(X))$, kde $K \in F[X, Y_1, \dots, Y_d]$. Pro $x \in F$ máme $(D^l R)(x) = K(x, G_1(x), \dots, G_d(x))$. Pro $x \in I$ má $P(x, Y)$ d různých kořenů y_1, \dots, y_d . Specializace $X, \delta_1, \dots, \delta_d \rightarrow x, y_1, \dots, y_d$ dává

$$D^l R(x) = \sum_{u_1 + \dots + u_d = l} \binom{l}{u_1, \dots, u_d}_F D^{u_1} C(x, y_1) \cdot \dots \cdot D^{u_d} C(x, y_d) .$$

($D^u C(x, y)$ je $(D^u C(X, \delta))(x, y)$, nikoli $(D^u C(X, Y))(x, y)$.)

Víme, že $\{y_1, y_2, \dots, y_d\} = J_1(x) \cup J_2(x)$. Bez újmy na obecnosti můžeme předpokládat, že $|J_i(x)| = t$ a $y_1, y_2, \dots, y_t \in J_i(x)$. Protože v hořejším vyjádření $D^l R(x)$ vždy $u_1 + u_2 + \dots + u_t \leq l$, existuje číslo s , $1 \leq s \leq t$, takové, že

$$u_s \leq \frac{l}{t} = \frac{l}{|J_i(x)|} < \frac{m|J_i(x)|}{|J_i(x)|} = m .$$

Tudíž $(D^{u_s}C(X, \delta))(x, y_s) = 0_{\overline{F}}$ a každý sčítanec ve vyjádření $D^l R(x)$ má nulový faktor. Pro každé $x \in I$ proto platí

$$(D^l R)(x) = 0_F, \quad 0 \leq l < m|J_i(x)|.$$

Podle definice je $R(X) \in F[X, \delta_1, \dots, \delta_d]$ symetrický v $\delta_1, \dots, \delta_d$, a má celkový stupeň nejvýše

$$d(e_i pm/d + p(d-1)) = e_i pm + pd(d-1).$$

Tudíž, podle lemmatu 127, $R(X) \in F[X]$ a

$$\deg(R) \leq e_i pm + pd(d-1).$$

Důkaz tvrzení 124 je dokončen.

4.4.4 Třetí část důkazu

Zbývá dokázat lemma 125. Budeme potřebovat ještě jedno lemma. Je-li K podpole pole L , dimenzi vektorového prostoru L se skaláry K označíme (standardně) jako $[L : K]$.

Lemma 129. *Nechť absolutně ireducibilní polynom $P \in F[X, Y]$ má stupeň $d > 0$ v neznámé Y . Nechť U a Z jsou další dvě neznámé a $\delta \in \overline{F(X)}$ a $\eta \in \overline{F(Z)}$ jsou kořeny polynomu P chápaného nejprve jako prvek $F(X)[Y]$ a pak $F(Z)[U]$, to jest*

$$P(X, \delta) \equiv 0 \quad \text{a} \quad P(Z, \eta) \equiv 0.$$

Potom

$$[F(X, Z, \delta, \eta) : F(X, Z)] = d^2.$$

DŮKAZ. Stačí dokázat, že

$$[F(X, Z, \delta, \eta) : F(X, Z, \delta)] = d \quad \text{a} \quad [F(X, Z, \delta) : F(X, Z)] = d.$$

Dokážeme jen první rovnost, druhá se dokazuje podobně (a jednodušeji). K tomu stačí dokázat, že polynom $P(Z, U) \in F[Z][U]$ je ireducibilní v $F(X, Z, \delta)[U] = F(X, \delta)(Z)[U]$. To je ekvivalentní ireducibilitě v

$F(X, \delta)[Z][U] = F(X, \delta)[Z, U]$ (podle zobecnění tvrzení 12). Pro spor předpokládejme, že $P = P_1P_2$, kde $P_i \in F(X, \delta)[Z, U]$ a mají stupeň ostře menší než d . Rozepsáno,

$$P_i(Z, U) = \sum_{j,k} c_{i,j,k} Z^j U^k ,$$

kde $c_{i,j,k} \in F(X, \delta) = F(X)(\delta)$. Ale δ je algebraický nad $F(X)$, takže $F(X)(\delta) = F(X)[\delta]$ a každý prvek $c_{i,j,k}$ lze reprezentovat jako polynom v δ s koeficienty v $F(X)$.

Zvolíme $x \in \overline{F}$ tak, že není kořenem jmenovatele žádného z těchto koeficientů, v žádném $c_{i,j,k}$, a ani není kořenem koeficientu Y^d v $P(X, Y)$. Pak zvolíme $y \in \overline{F}$ tak, že $P(x, y) = 0_{\overline{F}}$. Nechť $\overline{c}_{i,j,k} \in \overline{F}$ vznikne z $c_{i,j,k}$ substitucí $X := x$ a $\delta := y$ a $\overline{P}_i(Z, U)$ vznikne z $P_i(Z, U)$ náhradou $\overline{c}_{i,j,k}$ za $c_{i,j,k}$. Z rovnosti $P = P_1P_2$ v $F(X, \delta)[Z, U]$ plyne rovnost

$$P(Z, U) = \overline{P}_1(Z, U)\overline{P}_2(Z, U)$$

v $\overline{F}[Z, U]$. (Platnost rovnosti znamená splnění d identit typu $A(X, \delta) \equiv 0$, kde $A(X, Y) \in F[X, Y]$. $P(X, Y)$ je minimální polynom δ nad $F(X)$, tudíž $A = PB$ pro nějaký $B \in F[X, Y]$. Díky volbě x a y máme $A(x, y) = P(x, y)B(x, y) = 0_{\overline{F}}$ a identity a rovnost se substitucí zachovávají.) Ta je ale ve sporu s absolutní ireducibilitou P . \diamond

DŮKAZ LEMMATU 125. Polynom

$$A^*(X, Y, Z; W_1, \dots, W_d) = \prod_{i=1}^d A(X, Y, Z, W_i)$$

je symetrický v neznámých W_1, \dots, W_d . Podle tvrzení 13 v kapitole 1

$$A^*(X, Y, Z, W_1, \dots, W_d) = B(X, Y, Z; -e_1, e_2, -e_3, \dots, (-1)^d e_d) ,$$

kde $B \in F[X, Y, Z; V_1, \dots, V_d]$ a $e_i \in F[W_1, \dots, W_d]$ jsou elementární symetrické polynomy. Z $\deg_W(A) \leq d - 1$ plyne, že B má v neznámých V_1, \dots, V_d celkový stupeň nejvýše $d - 1$.

Protože

$$\delta^d = -G_1(X)\delta^{d-1} - \dots - G_d(X)$$

(G_i je koeficient Y^{d-i} v P), pro každé $t \in \mathbf{N}$ máme vyjádření

$$\delta^{d-1+t} = G_1^{(t)}(X)\delta^{d-1} + \dots + G_d^{(t)}(X) ,$$

kde $G_i^{(t)} \in F[X]$. Jak víme,

$$\deg(G_i^{(t)}) \leq t - 1 + i .$$

Protože $\deg_Y(B) = \deg_Y(A^*) = d \cdot \deg_Y(A) \leq d(d-1) = (d-1) + (d-1)^2$, redukci mocnin δ^{d-1+t} pro $t \leq (d-1)^2$ dostaneme

$$B(X, \delta, Z; V_1, \dots, V_d) = C(X, \delta, Z; V_1, \dots, V_d) ,$$

kde $C \in F[X, Y, Z; V_1, \dots, V_d]$ a $\deg_Y(C) \leq d-1$. Co se týče stupně v X , díky $\deg(G_i^{(t)}) \leq t-1+i$ a $\deg_X(A) \leq p/d - d$ máme

$$\begin{aligned} \deg_X(C) &\leq \deg_X(B) + (d-1)^2 - 1 + d = \deg_X(A^*) + d(d-1) \\ &\leq d \cdot \deg_X(A) + d(d-1) \leq p - d^2 + d(d-1) \\ &< p . \end{aligned}$$

Předpokládejme pro spor, že $A(X, \delta, X^p, \delta^p) \equiv 0$. Nechť $\delta = \delta_1$, kde $P(X, Y) = (Y - \delta_1)(Y - \delta_2) \dots (Y - \delta_d)$ je faktorizace P nad $\overline{F(X)}$. Pak

$$A^*(X, \delta, X^p; \delta_1^p, \dots, \delta_d^p) \equiv 0 .$$

Protože, podle Viětových vztahů, $(-1)^i e_i(\delta_1, \dots, \delta_d) = G_i(X)$, umocněním na p dostáváme $(-1)^i e_i(\delta_1^p, \dots, \delta_d^p) = G_i(X^p)$. Tedy

$$\begin{aligned} C(X, \delta, X^p; G_1(X^p), \dots, G_d(X^p)) &= B(X, \delta, X^p; G_1(X^p), \dots, G_d(X^p)) \\ &= A^*(X, \delta, X^p; \delta_1^p, \dots, \delta_d^p) \\ &\equiv 0 . \end{aligned}$$

Ale $\deg_Y(C) \leq d-1$ a δ je stupně d nad $F(X)$. Proto

$$C(X, Y, X^p; G_1(X^p), \dots, G_d(X^p)) \equiv 0$$

jako polynom z $F[X, Y]$.

Protože v F platí $X^p = X_1^p + X_2^p$, dosazením $X = X_1 + X_2$ přejde poslední identita na

$$C(X_1 + X_2, Y, X_1^p; G_1(X_1^p), \dots, G_d(X_1^p)) + X_2^p \cdot L(X_1, X_2, Y) \equiv 0 ,$$

kde $L \in F[X_1, X_2, Y]$. Protože $\deg_X(C) < p$, má první sčítanec v X_2 stupeň menší než p a máme identitu

$$C(X_1 + X_2, Y, X_1^p; G_1(X_1^p), \dots, G_d(X_1^p)) \equiv 0 .$$

Protože $X_1 + X_2, Y$ a X_1^p jsou algebraicky nezávislé, můžeme je nahradit neznámými X, Y a Z a dostáváme

$$C(X, Y, Z; G_1(Z), \dots, G_d(Z)) \equiv 0 .$$

Za Y dosadíme δ a dostáváme

$$B(X, \delta, Z; G_1(Z), \dots, G_d(Z)) = C(X, \delta, Z; G_1(Z), \dots, G_d(Z)) \equiv 0 .$$

Uvažme znovu faktorizaci P , nyní v neznámých Z a U :

$$P(Z, U) = (Z - \theta_1)(Z - \theta_2) \dots (Z - \theta_d) ,$$

kde $\theta_i \in \overline{F(U)}$. Pro $i = 1, \dots, d$ opět máme $(-1)^i e_i(\theta_1, \dots, \theta_d) = G_i(Z)$. Tudíž

$$A^*(X, \delta, Z; \theta_1, \dots, \theta_d) = B(X, \delta, Z; G_1(Z), \dots, G_d(Z)) \equiv 0 .$$

Pro některé i proto kořen $\theta = \theta_i$ splňuje

$$A(X, \delta, Z, \theta) \equiv 0 .$$

Avšak $\deg_Y(A), \deg_W(A) \leq d - 1$ a podle lematu 129 je množina d^2 prvků $\{\delta^j \theta^k : 0 \leq j, k \leq d - 1\}$ lineárně nezávislá nad $F(X, Z)$. Polynom $A(X, Y, Z, W)$ je proto identicky nulový, což je spor s předpokladem.

Tím je dokázáno lemma 125, což dokončuje důkaz tvrzení 124 a tím i tvrzení 112.

4.5 Poznámky

O historii zákona reciprocit píše Frei [16].

4.1 Konečná pole. Literatura: Ireland a Rosen [22] a Halberstam a Roth [19]. Obsáhlá monografie věnovaná teorii konečných polí a aplikacím konečných polí je Lidl a Niederreiter [25]. Její „učebnicová“ verze je Lidl a Niederreiter [26].

Erdős a Turán v [15] dokázali trochu slabší výsledek, než Lindström [27] a než jak jsme zformulovali větu 93. Dokázali, že $S_i(n) < n^{1/2} + O(n^{1/4})$ a jejich metoda dává v O konstantu $\sqrt{2}$. Zda se dá člen $O(n^{1/4})$ nahradit menší funkcí je otevřený problém (úloha 8). Erdős publikoval domněnku, že $O(n^{1/4})$

lze zlepšit až na $O_\varepsilon(n^\varepsilon)$ pro každé pevné $\varepsilon > 0$. Další výsledky o Sidonových množinách lze nalézt například v [19], [13] a [14]. Zmíníme jeden zajímavý výsledek týkající se hustých nekonečných Sidonových množin.

Velmi jednoduše lze sestavit Sidonovu množinu $X \subset \mathbf{N}$, která má v každém počátečním intervalu $\{1, 2, \dots, n\}$ alespoň $cn^{1/3}$ prvků (úloha 9). Dlouho bylo známo jen mírné vylepšení, které v r. 1981 dosáhli Ajtai, Komlós a Szemerédi [1]: Existuje nekonečná Sidonova množina, která má v $\{1, 2, \dots, n\}$ alespoň $c(n \log n)^{1/3}$ prvků. V roce 1998 Ruzsa [29] sestavil Sidonovu množinu, která má v $\{1, 2, \dots, n\}$ alespoň $c_\varepsilon n^{0.41421\dots-\varepsilon}$ prvků ($0.41421\dots = \sqrt{2}-1$). Otevřeným problémem je dosáhnout hustoty $c_\varepsilon n^{1/2-\varepsilon}$. Podle výsledku Erdőse (úloha 10) však nelze dosáhnout hustoty $cn^{1/2}$ (narozdíl od konečné verze).

V důkazu věty 94 jsme použili *rozdílovou množinu* A . Teorie rozdílových množin (difference sets) je posána například v Hallovi [20]. Tato kniha se zabývá i řadou dalších použití konečných polí v kombinatorice (konečné geometrie, kombinatorické designy, latinské čtverce, teorie kódů).

4.2 Chevalley–Warningova věta a kombinatorika. Literatura: Alon [2], Borevič a Šafarevič [8] a Schmidt [31]. Alon uvádí další aplikace Chevalley–Warningovy věty a podává zajímavý přehled algebraických metod v kombinatorice. Zobecnění věty 98 ([6]) je v článku [5]. Podle Berge–Sauerovy domněnky má každý 4-regulární graf *bez násobných hran* neprázdný 3-regulární podgraf. Domněnku dokázal v roce 1982 Taškinov [36].

Otázka, kterou v $(\mathbf{Z}, +)$ zodpověděla věta 97, se zkoumá i obecněji v $(\mathbf{Z}^d, +)$. Jako $f(n, d)$ označíme nejmenší počet m takový, že každá m -prvková posloupnost v \mathbf{Z}^d obsahuje n -prvkovou podposloupnost y_1, \dots, y_n splňující $\frac{1}{n}(y_1 + y_2 + \dots + y_n) \in \mathbf{Z}^d$. Alon a Dubiner [4] dokázali, že

$$f(n, d) \leq (cd \log_2 d)^d n ,$$

kde $c > 0$ je absolutní konstanta a \log_2 binární logaritmus. V pevné dimenzi d tedy pro vhodnou konstantu $c' > 0$ každých $c'n$ mřížových bodů v \mathbf{R}^d obsahuje n -tici, jejíž těžiště je opět mřížový bod. Další výsledky o $f(n, d)$ a pět důkazů věty 97 lze nalézt v [3].

4.3 Zlatá věta. Literatura: Ireland a Rosen [22] a Hardy a Wright [21]. V literatuře existuje mnoho důkazů zákona reciprocity. K roku 1921 jich bylo podle Bachmana známo 56 a v současnosti už více než 100. Základních myšlenek tolik samozřejmě není, mnohé důkazy jsou jen variacemi na totéž téma. Viz třeba [9] a [17].

Zákon reciprocity kvadratických zbytků je jen jedním z řady zákonů reciprocity. V kubickém a bikvadratickém přebírají roli čísla -1 primitivní třetí a čtvrtá odmocnina z 1, čísla $\omega = (-1 + \sqrt{-3})/2$ a $\sqrt{-1}$, a pracuje se v okruzích $\mathbf{Z}[\omega]$ a $\mathbf{Z}[\sqrt{-1}]$. O kubickém a bikvadratickém zákoně reciprocity se lze poučit v [22], kde je i mnoho odkazů na literaturu. Zhuštěný kurz algebraické teorie čísel vedoucí k obecnému Artinovu zákonu reciprocity poskytuje Stark [32]. Viz též [24] a [43].

Speciální případy kubického a bikvadratického zákona reciprocity publikoval Euler v letech 1748–50. V r. 1832 Gauss publikoval memoár, v němž bez důkazu uvedl bikvadratický zákon reciprocity. Důkaz měl být uveřejněn v následujícím memoáru, který však nikdy nevyšel. V r. 1844 Eisenstein publikoval několik důkazů. Kubický zákon reciprocity si nárokoval Jacobi, který podal jeho důkaz údajně ve svých přednáškách v Königsbergu v r. 1837. První publikovaný důkaz z r. 1844 však náleží Eisensteinovi. Spory o prioritu mezi Jacobim a Eisensteinem byly velmi ostré.

4.4 Weilova věta pro $F = \mathbf{Z}_p$. Literatura: Alon [2], Lidl a Niederreiter [25] a zejména Schmidt [31]. Vysvětlíme, co vlastně Weil dokázal. Nechť $F = \text{GF}(q) = \text{GF}(p^n)$ je konečné pole a $P \in F[X, Y]$, $d = \deg(P)$, je absolutně ireducibilní polynom. Pro $s \in \mathbf{N}$ nechť N_s označuje počet $\text{GF}(q^s)$ -racionálních bodů na projektivní křivce P . Podrobněji řečeno, označíme-li $G = \text{GF}(q^s) = \text{GF}(p^{sn})$ a $Q(X, Y, Z) = Z^d P(X/Z, Y/Z)$ (zhomogenizování P), pak

$$N_s = |\{(x, y, z) \in G^3 : Q(x, y, z) = 0_G\} / \sim| ,$$

kde \sim je ekvivalence definující body projektivní roviny (dvě trojice jsou ekvivalentní, je-li jedna nenulovým skalárním násobkem druhé). *Zeta funkce* $Z(t)$ křivky P je pak definována pomocí

$$Z(t) = \exp \left(\sum_{s \geq 1} N_s t^s / s \right) .$$

V roce 1948 Weil podstatně zobecnil předchozí výsledky Artina a Hasseho a v [40] dokázal, že $Z(t)$ je racionální funkce tvaru

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)} ,$$

přičemž $L \in \mathbf{Z}[t]$ má stupeň $2g$, kde g je rod křivky P , a konstantní člen 1. Napíšeme-li $L(t)$ jako

$$L(t) = (1 - \omega_1 t)(1 - \omega_2 t) \dots (1 - \omega_{2g} t) ,$$

je $\omega_i \in \mathbf{C}^{\text{alg}}$. Weil zejména dokázal příslušnou *Riemannovu hypotézu* pro křivky nad konečnými poli (terminologicky přesnější je mluvit o *riemannovské hypotéze*), podle níž

$$|\omega_i| = q^{1/2}$$

pro všechna $i = 1, \dots, 2g$. Dále dokázal, že $Z(t)$ splňuje jistou funkcionální rovnici. Své fundamentální výsledky oznámil bez důkazu už v [38] a [39].

Logaritmickým derivováním formule pro $Z(t)$ a porovnáním koeficientů se lehce odvodí, že pro $s \in \mathbf{N}$ platí

$$N_s = q^s + 1 - \sum_{i=1}^{2g} \omega_i^s .$$

Takže, díky $|\omega_i| = q^{1/2}$,

$$|N_1 - q - 1| \leq 2gq^{1/2} .$$

Jak známo z algebraické geometrie, $2g \leq (d-1)(d-2)$ a $N_1 \leq N + d^2$. (N je počet řešení rovnice $P = 0_F$ v F , což je počet těch z N_1 F -racionálních bodů na projektivní křivce P , které jsou konečné.) Máme tedy odhad

$$|N - q| \leq (d-1)(d-2)q^{1/2} + d^2 .$$

To je explicitní forma věty 111.

Weil použil aparátu algebraické geometrie. Po publikaci [40] byly podány další důkazy Weilových výsledků, z nichž Bombieriho [7] je kromě odkazu na Riemann–Rochovu větu jinak elementární. Stěpanovovi se v letech 1969–74 podařilo v sérii článků dokázat weilovské odhady počtu N pro různé třídy polynomů P zcela elementárně, bez použití algebraické geometrie. (Z teorie zeta funkce plyne, že zdánlivě slabší odhady zbytkového členu typu $O_d(\sqrt{q})$ implikují silnější weilovské odhady s konstantou $(d-1)(d-2)$.) Nejobecnějšího výsledku dosáhl v [33] a [34]. Stěpanovovo úsilí završil Schmidt [30] přechodem k obecnému absolutně ireducibilnímu P . Stěpanovovy a Schmidtovy výsledky jsou významným úspěchem elementárních metod v teorii čísel.

Pro úplný důkaz věty 111, pro nějž je ještě třeba zavést hyperderivace, odkazujeme do Schmidtovy monografie [31]. Lze říci, že Stěpanov použil *Thucho metodu* (srovnej důkaz v oddílu 2.7), protože základem jeho postupu je sestavení vhodného polynomu s mnoha kořeny. Vše se nakonec zredukuje, stejně jako v oddílu 2.7, na argument z lineární algebry. Podrobná diskuse výsledků o rovnicích nad konečnými poli s detailní bibliografií je v poznámkách k 6. kapitole [25].

Weil předložil v [41] ve formě hypotéz zobecnění svých výsledků pro obecnou algebraickou varietu. Přesnou formulaci *Weilových hypotéz* lze nalézt například v Maninovi a Panchiskinovi [28]. Weilovy hypotézy dokázal za pomoci velmi abstraktního aparátu v roce 1974 Deligne [10]. V r. 1978 mu za to byla udělena Fieldsova medaile. (Zde elementární přístup není zatím v dohledu.) Pro další reference k Deligneho výsledku viz [25] a [28]. Významným mezikrokem k důkazu hypotéz byla Dworkova věta [11], podle níž je zeta funkce nadplochy (variety definované jedinou rovnicí) racionální. Ekvivalentně řečeno, posloupnost $(N_s)_{s \geq 1}$ počtů $\text{GF}(q^s)$ -racionálních bodů na nadploše splňuje rekurenci s konstantními koeficienty. Dworkův důmyslný důkaz (bez použití algebraické geometrie, za pomoci p -adických technik) je uveden v 5. kapitole Koblitze [23].

Na Raymonda Paleyho (1907–1933), velmi talentovaného matematika a vášnivého lyžaře, který tragicky zahynul v lavině, vzpomíná Wiener [42]. Problém, zda pro každé k existuje turnaj, v němž je každých k hráčů poráženo jiným hráčem předložil v r. 1962 Schütte. O rok později Erdős [12] dokázal, že pro každé k takový turnaj s $O(k^2 2^k)$ vrcholy existuje. Erdősův odhad je výrazně lepší než ve větě 114 a důkaz doslova několikařádkový, opírá se však o nekonstruktivní obrat (o pravděpodobnostní metodu, úloha 18). Proto je Grahamova a Spencerova věta, která podává explicitní konstrukci takových turnajů, stále velmi cenná. Jejich výsledek [18], turnaj s $O(k^2 4^k)$ vrcholy, je o něco lepší než věta 114. Užili totiž silnějších odhadů pro charaktery, které však mají podstatně složitější důkaz, viz [2] a [31]. Na druhou stranu je třeba říci, že pro důkaz tvrzení 115 je tvrzení 112 zbytečně obecné. Stačí jeho verze pro polynomy $Y^d - P(X)$, která se dá dokázat snáze. Viz [31]. Informaci o dalších použitích Weilovy věty v kombinatorice lze nalézt v [2] a [35].

V lednu 2000 Tyszkiewicz [37] publikoval velmi jednoduché konstruktivní řešení Schütteho problému. Jeho konstrukce pro dané k dává turnaj se zhruba $7^{(k/2)^{2.71}}$ hráči.

4.6 Úlohy

1. (1) Ukažte, že konečný, ne nutně komutativní okruh, který nemá dělitele nuly (součin nenulových prvků je nenulový), je těleso.
2. (1) Dokažte, že každé algebraicky uzavřené pole je nekonečné.

3. (2) Dokažte, že algebra nad tělesem \mathbf{R} se čtyřmi „imaginárními“ jednotkami $1, i, j$ a k , v níž se násobí pomocí pravidel $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$ a $i^2 = j^2 = k^2 = -1$ (1 je samozřejmě neutrální prvek), je nekomutativní těleso, *těleso kvaternionů*.
4. (2) Pro $n \in \mathbf{N}$ buď $M \subset \mathbf{C}$ množina všech primitivních n -tých odmocnin z jedné (M má $\varphi(n)$ prvků). Dokažte, že *kruhový polynom*

$$\Phi_n(x) = \prod_{\omega \in M} (x - \omega)$$

je monický celočíselný polynom.

5. (3) V sérii kroků dokážeme, že každé konečné těleso je komutativní. Nechť K je konečné těleso a P jeho centrum (množina těch $x \in K$, které komutují s každým $y \in K$). Patrně je P pole a K je vektorový prostor nad P s dimenzí $n \in \mathbf{N}$. Předpoklad $n \geq 2$ přivedeme ke sporu.

- (a) Nechť $|P| = q \in \mathbf{N}$ (q je mocnina prvočísla), g_1, \dots, g_r jsou reprezentanti nejednoprvkových konjugovaných tříd K_1, \dots, K_r grupy K^* , $C_i = \{x \in K : g_i x = x g_i\}$ a $C_i^* = C_i \setminus \{0_K\}$. Odvoďte identitu

$$q^n - 1 = q - 1 + \sum_{i=1}^r \frac{q^n - 1}{|C_i^*|}.$$

- (b) Dokažte, že C_i je podtěleso K obsahující P . Odvoďte, že $|C_i^*| = q^{t_i} - 1$ pro nějaké $t_i \in \mathbf{N}$, kde $t_i \setminus n$ a $t_i < n$.

- (c) Polynom $\Psi_i(x)$ definujeme vztahem

$$\frac{x^n - 1}{x^{t_i} - 1} = \Phi_n(x) \Psi_i(x)$$

($\Phi_n(x)$ je kruhový polynom definovaný v předchozí úloze). Dokažte identitu

$$q - 1 = \Phi_n(q) \left(\prod_{d \setminus n, d < n} \Phi_d(q) - \sum_{i=1}^r \Psi_i(q) \right)$$

a odvoďte z ní, že $|\Phi_n(q)| \leq q - 1$.

- (d) Z definice $\Phi_n(x)$ odvoďte, že pro $n \geq 2$ máme $|\Phi_n(u)| > u - 1$ pro každé reálné $u \geq 2$. To je kýžený spor.

6. (1) Necht' G je algebraický uzávěr pole \mathbf{Z}_p . Dokažte, že pro $s = p^r$ tvoří kořeny polynomu $x^s - x \in G[x]$ s -prvkové podpole pole G .
7. (2) Dokažte identitu

$$e^x = \prod_{n=1}^{\infty} (1 - x^n)^{-\mu(n)/n} .$$

8. (5) Je možné zlepšit horní odhad z věty 93 na

$$\text{Si}(n) < n^{1/2} + O_{\varepsilon}(n^{\varepsilon})$$

pro každé $\varepsilon > 0$? Nebo alespoň na $\text{Si}(n) < n^{1/2} + o(n^{1/4})$?

9. (2) Ukažte, že existuje nekonečná Sidonova množina $X \subset \mathbf{N}$ taková, že pro $n \in \mathbf{N}$ platí

$$|X \cap \{1, 2, \dots, n\}| \gg n^{1/3} .$$

10. (3) Dokažte, že každá (nekonečná) Sidonova množina $X \subset \mathbf{N}$ splňuje odhad

$$\liminf_{n \rightarrow \infty} \frac{|X \cap \{1, 2, \dots, n\}|}{(n/\log n)^{1/2}} < c ,$$

kde $c > 0$ je absolutní konstanta.

11. (2) Zjistěte, pro která $n \in \mathbf{N}$ existuje 4-regulární graf na n vrcholech bez neprázdného 3-regulárního podgrafu. (Připomínáme, že naše grafy mohou mít násobné hrany.)
12. (1) Vnitřek každého konvexního 5-úhelníka s vrcholy v \mathbf{Z}^2 obsahuje mřížový bod.
13. (2) Platí odhady

$$(n-1)2^d + 1 \leq f(n, d) \leq (n-1)n^d + 1 .$$

(Veličina $f(n, d)$ je definovaná v poznámkách k 4.2.)

14. (3) Pro prvočíslo $p > 2$ dokažte identitu

$$\left(\frac{2}{p}\right) = \prod_{j=1}^{(p-1)/2} \cos(2\pi j/p)$$

a odvoďte z ní důkaz druhého dodatku zákona reciprocity.

15. (3) *Jacobiho symbol* je pro liché $b \in \mathbf{N}$ s rozkladem $b = p_1 p_2 \dots p_r$ (prvočísla p_i nejsou nutně různá) a $a \in \mathbf{Z}$ definován pomocí

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_r}\right) .$$

Dokažte, že pro Jacobiho symbol platí zákon reciprocity a jeho dva doplňky.

16. (3) Necht' F je pole a

$$P(X, Y) = G_0 Y^d + G_1(X) Y^{d-1} + \dots + G_d(X)$$

je polynom z $F[X, Y]$, přičemž $G_0 \in F$ není nula. Pokud platí, že

$$\max_{i=1, \dots, d} \deg(G_i)/i = m/d$$

s $d \perp m$, je P absolutně ireducibilní.

17. (1) Jakou slabší podmínkou lze nahradit (ii) v definici charakteru grupy?
18. (2) Na $\{1, 2, \dots, n\}$ definujeme náhodný turnaj tak, že pro $1 \leq i < j \leq n$ s pravděpodobností $1/2$ položíme $(i, j) \in T$ a s pravděpodobností $1/2$ naopak $(j, i) \in T$. Dokažte, že pro $n \gg k^2 2^k$ má turnaj s kladnou pravděpodobností vlastnost, že každých k hráčů nějaký jiný hráč poráží.
19. (3) *Hamiltonova cesta* v turnaji T na množině $\{1, 2, \dots, n\}$ je permutace $a_1 a_2 \dots a_n$ nosné množiny taková, že $(a_i a_{i+1}) \in T$ pro každé $i = 1, 2, \dots, n - 1$. Dokažte, že každý turnaj má lichý počet Hamiltonových cest.

Literatura

- [1] M. AJTAI, J. KOMLÓS AND E. SZEMERÉDI, A dense infinite Sidon sequence, *Eur. J. Comb.*, **2** (1981), 1–11.
- [2] N. ALON, Tools from higher algebra, 1749–1783. In: R. L. Graham, M. Grötschel and L. Lovász (ed.), *Handbook of Combinatorics (Volume 2)*, North-Holland, Amsterdam 1995.
- [3] N. ALON AND M. DUBINER, Zero-sum sets of prescribed size, 33–50. In: D. Miklós, V. T. Sós and T. Szönyi (ed.), *Combinatorics, Paul Erdős is Eighty (Volume 1)*, János Bolyai Mathematical Society, Budapest 1993.
- [4] N. ALON AND M. DUBINER, A lattice point problem and additive number theory, *Combinatorica*, **15** (1995), 301–309.
- [5] N. ALON, S. FRIEDLAND AND G. KALAI, Regular subgraphs of almost regular graphs, *J. Comb. Theory, Ser. B*, **37** (1984), 79–91.
- [6] N. ALON, S. FRIEDLAND AND G. KALAI, Every 4-regular graph plus an edge contains a 3-regular subgraph, *J. Comb. Theory, Ser. B*, **37** (1984), 92–93.
- [7] E. BOMBIERI, Counting points on curves over finite fields (d’après S. A. Stepanov), 234–241. In: ??? (ed.), *Séminaire Bourbaki, Exp. No. 430 (1972/73)*, Springer, Berlin 1974. [Lecture Notes in Mathematics 383.]
- [8] Z. I. BOREVIČ A I. R. ŠAFAREVIČ, *Těorija Čisel*, Mir, Moskva 1985. [Anglický překlad: Z. I. BOREVICH AND I. R. SHAFAREVICH, *Number Theory*, Academic Press, New York 1966.]

- [9] E. BROWN, The first proof of the quadratic reciprocity law, revisited, *Amer. Math. Monthly*, **88** (1981), 257–264.
- [10] P. DELIGNE, La conjecture de Weil, *Inst. Hautes Etudes Sci. Publ. Math.*, **43** (1974), 273–307.
- [11] B. DWORK, On the rationality of the zeta function of an algebraic variety, *Amer. J. Math.*, **82** (1960), 631–648.
- [12] P. ERDŐS, On a problem in graph theory, *Math. Gaz.*, **47** (1963), 220–223.
- [13] P. ERDŐS, A. SÁRKÖZY AND V. T. SÓS, On sum sets of Sidon sets, I, *J. Number Theory*, **47** (1994), 329–347.
- [14] P. ERDŐS, A. SÁRKÖZY AND V. T. SÓS, On sum sets of Sidon sets, II, *Israel J. Math.*, **90** (1995), 221–233.
- [15] P. ERDŐS AND P. TURÁN, On a problem in additive number theory, *J. London Math. Soc.*, **16** (1941), 212–215.
- [16] G. FREI, The reciprocity law from Euler to Eisenstein, 67–90. In: Ch. Sasaki, J. W. Dauben and M. Sugiura (ed.), *The Intersection of History and Mathematics*, Birkhäuser, Basel 1994.
- [17] M. GERSTENHABER, The 152nd proof of the law of quadratic reciprocity, *Amer. Math. Monthly*, **70** (1963), 397–398.
- [18] R. L. GRAHAM AND J. SPENCER, A constructive solution to a tournament problem, *Canad. Math. Bull.*, **1971** (14), 45–48.
- [19] H. HALBERSTAM AND K. F. ROTH, *Sequences*, Oxford University Press, Oxford 1966. [Reprint v r. 1983 v Springer-Verlag.]
- [20] M. HALL, JR., *Combinatorial Theory*, John Wiley & Sons, New York 1986.
- [21] G. H. HARDY AND E. M. WRIGHT, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford 1945. [Tato klasická učebnice se dočkala od r. 1938 celkem 5 vydání, posledního v roce 1979.]

- [22] K. IRELAND AND M. ROSEN, *A Classical Introduction to Modern Number Theory*, Springer, New York 1990.
- [23] N. KOBLITZ, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer, Berlin 1984.
- [24] E. LEHMER, Rational reciprocity laws, *Amer. Math. Monthly*, **85** (1978), 467–472.
- [25] R. LIDL AND H. NIEDERREITER, *Finite Fields*, Cambridge University Press, Cambridge 1996. [Encyclopedia of Mathematics and its Applications, volume 20.]
- [26] R. LIDL AND H. NIEDERREITER, *Introduction to Finite Fields and their Applications*, Cambridge University Press, Cambridge 1994.
- [27] B. LINDSTRÖM, An inequality for B_2 -sequences, *J. Comb. Theory*, **6** (1969), 211–212.
- [28] YU. I. MANIN AND A. A. PANCHISKIN, *Number Theory I*, Springer, Berlin 1995. [Encyclopaedia of Mathematical Sciences, Volume 49.]
- [29] I. RUZSA, An infinite Sidon sequence, *J. Number Theory*, **68** (1998), 63–71.
- [30] W. M. SCHMIDT, Zur Methode von Stepanov, *Acta Arith.*, **24** (1973), 347–367.
- [31] W. M. SCHMIDT, *Equations over Finite Fields. An Elementary Approach*, Springer, Berlin 1976. [Lecture Notes in Mathematics 536.]
- [32] H. M. STARK, Galois theory, algebraic number theory, and zeta functions, 313–393. In: M. Waldschmidt, P. Moussa, J.-M. Luck and C. Itzykson (ed.), *From Number Theory to Physics*, Springer, Berlin 1989.
- [33] S. A. STĚPANOV, Congruences in two unknowns, *Izv. Akad. Nauk SSSR Ser. Mat.*, **36** (1972), 683–711. [V ruštině.]
- [34] S. A. STĚPANOV, Rational points of algebraic curves over finite fields, 223–243. In: ??? (ed.), *Proceedings of the Summer School on Analytic Number Theory in Minsk*, Nauka i Technika, Minsk 1974. [V ruštině.]

- [35] T. SZŐNYI, Some applications of algebraic curves in finite geometry and combinatorics, 197–236. In: R. A. Bailey (ed.), *Surveys in Combinatorics, 1997*, Cambridge University Press, Cambridge, UK 1997.
- [36] V. A. TAŠKINOV, Regular subgraphs of regular graphs, *Soviet. Math. Dokl.*, **26** (1982), 37–38.
- [37] J. TYSZKIEWICZ, A simple construction for tournaments with every k players beaten by a single player, *Amer. Math. Monthly*, **107** (2000), 53–54.
- [38] A. WEIL, Sur les fonctions algébriques à corps de constantes fini, *C. R. Acad. Sci. Paris*, **210** (1940), 592–594.
- [39] A. WEIL, On the Riemann hypothesis in function fields, *Proc. Nat. Acad. Sci. U. S. A.*, **27** (1941), 345–347.
- [40] A. WEIL, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris 1948. [Actualités Sci. et Ind., no. 1041.]
- [41] A. WEIL, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.*, **55** (1949), 497–508.
- [42] N. WIENER, *I Am a Mathematician*, Victor Gollancz, London 1956. [České vydání: N. WIENER, *Můj Život*, Mladá fronta, Praha 1970.]
- [43] B. F. WYMAN, What is a reciprocity law?, *Amer. Math. Monthly*, **79** (1972), 571–586.