Věta o rozložení prvočísel

Věta. *Pro libovolné přirozené číslo* $n \geq 2$ *platí* $\prod_{p \leq 2n} p > 2^n$, *kde v součinu* p *probíhá všechna prvočísla nepřevyšující* $2n$.

Důkaz. Jako v důkaze lemmatu 4 rozložme binomický koeficient $\binom{2n}{n}$ na prvočinitele $\binom{2n}{n} = p_1^{k_1} \dots p_r^{k_r}$. Víme, že libovolné prvočíslo, které se zde vyskytuje, je menší než $2n$. Je-li $p_i \leq \sqrt{2n}$, užijeme odhad $p_i^{k_i} \leq 2n$ z lemmatu 2. Je-li naopak $p_i > \sqrt{2n}$, platí $p_i^2 > 2n$, a odhad $p_i^{k_i} \leq 2n$ z lemmatu 2 dává $k_i = 1$. Užitím lemmatu 5

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \leq 2n} p.$$

Označme $s_n = \prod_{p \leq 2n} p$. Pak předchozí nerovnost spolu s větou 1 dávají

$$\frac{2^{2n}}{2n} \leq (2n)^{\pi(\sqrt{2n})} \cdot s_n < (2n)^{3\sqrt{2n} \big/ \log_2 \sqrt{2n}} \cdot s_n.$$

Dostali jsme

$$\frac{2^{2n}}{2n} \leq (2n)^{\pi(\sqrt{2n})} \cdot s_n < (2n)^{3\sqrt{2n}/\log_2 \sqrt{2n}} \cdot s_n.$$

Protože $(2n)^{1/\log_2 \sqrt{2n}} = (2n)^{2/\log_2 2n} = 2^2$, z poslední nerovnosti plyne

$$s_n > 2^{2n}/(2n \cdot 2^{6\sqrt{2n}}).$$

Abychom dokázali větu, musíme ukázat, že $2^n \geq 2n \cdot 2^{6\sqrt{2n}}$, neboli po zlogaritmování

$$n - 1 - \log_2 n - 6\sqrt{2n} \geq 0.$$

Uvažme funkci $f(x) = x - 1 - \log_2 x - 6\sqrt{2x}$. Platí $f(100) = 99 - \log_2 100 - 6\sqrt{200} > 7$ a derivace $f'(x) = 1 - \frac{1}{x \ln 2} - \frac{6}{\sqrt{2x}}$ je větší než $1 - \frac{1}{100 \ln 2} - \frac{6}{10\sqrt{2}} > 0$ pro $x \geq 100$. Tím jsme dokázali lemma pro $n \geq 100$. Nerovnost $s_n > 2^n$ pro hodnoty $2 \leq n < 100$ je možné ověřit numericky.

AKS test na prvočíselnost

M. Agrawal, N. Kayal a N. Saxena, Indian Institute of Technology Kanpur, Indie (2002)

První test na prvočíselnost, který je

- **obecný** - na vstupu může být libovolné přirozené číslo, ne jen čísla speciálního tvaru,
- **polynomiální** - čas výpočtu (nikoliv jen pravděpodobný, ale skutečný) je omezen polynomem v počtu cifer vstupu,
- **deterministický** - není pravděpodobnostní, v jeho průběhu se nic náhodně nevolí,
- **nepodmíněný** - správnost výstupu i polynomiálnost času výpočtu jsou dokázány, nejsou na ničem závislé (například na platnosti obecné Riemannovy hypotézy a podobně).

Základní myšlenka

Věta 1. *Nechť $a, n \in \mathbb{Z}$, $n > 1$, $(a, n) = 1$. Pak n je prvočíslo, právě když v okruhu $\mathbb{Z}_n[x]$, tj. okruhu polynomů nad okruhem zbytkových tříd modulo n, platí $(x + a)^n = x^n + a$.*

Důkaz. Z binomické věty $(x + a)^n = x^n + a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i x^{n-i}$.
Je-li n prvočíslo, pak z Fermatovy věty plyne $a^n \equiv a \pmod{n}$.
Dále pro libovolné $i = 1, 2, \ldots, n-1$ má binomický koeficient $\binom{n}{i} = \frac{n(n-1)\ldots(n-i+1)}{i!}$ prvočíslo n v čitateli a $n \nmid i!$, tedy $\binom{n}{i} \equiv 0 \pmod{n}$. Proto $(x + a)^n = x^n + a$.
Je-li naopak n složené číslo, zvolme prvočíslo p dělící n. Nechť $s = \nu_p(n)$, tj. přirozené číslo s je určené podmínkami $p^s \mid n$, $p^{s+1} \nmid n$. Pak koeficient u x^{n-p} v $(x + a)^n$ je

$$\binom{n}{p} a^p = \frac{n(n-1)\ldots(n-p+1)}{p!} \cdot a^p,$$

což není dělitelné p^s (vždyť $p \nmid a$ a $p \nmid (n-1)\ldots(n-p+1)$), a tedy ani n. To znamená $(x + a)^n \neq x^n + a$.

Využití věty 1

Věta 1 nabízí jednoduchou metodu na testování, zda je celé číslo n prvočíslo: zvolíme celé číslo a nesoudělné s n (například $a = 1$) a spočítáme pomocí rychlého umocňování v okruhu polynomů $\mathbb{Z}_n[x]$ mocninu $(x + a)^n$.

Tato metoda však není tak rychlá, jak se zdá na první pohled: v průběhu umocňování vzniká u polynomů, které jsou mezivýsledky, mnoho nenulových koeficientů. Vždyť stupeň polynomu, který má být naposledy umocňován na druhou, je nejméně $\frac{n-1}{2}$, a tedy může mít až $\frac{n+1}{2}$ nenulových koeficientů. To znamená, že počet prováděných operací nemůže být omezen shora ničím lepším než $O(n)$, a tedy tato metoda je horší než metoda pokusného dělení.

Efektivní využití věty 1

Místo rovnosti $(x+a)^n = x^n + a$ budeme kontrolovat jen kongruenci $(x+a)^n \equiv x^n + a \pmod{x^r - 1}$ pro vhodné r. Zbytek po dělení mocniny $(x+a)^n$ polynomem $x^r - 1$ pak spočítáme algoritmem rychlého umocňování, ale po každém násobení polynomů bude každá mocnina x^s nahrazena mocninou $x^{s'}$, kde s' je zbytek po dělení čísla s číslem r. Přitom pracujeme v $\mathbb{Z}_n[x]$ takto: počítáme s polynomy ze $\mathbb{Z}[x]$ a po každém provedeném výpočtu redukujeme celočíselné koeficienty modulo n. Složitost výpočtu bude polynomiální, jestliže $r = O((\log_2 n)^c)$ pro nějaké c. Je-li n prvočíslo, dávají $(x+a)^n$ a $x^n + a$ stejné zbytky po dělení polynomem $x^r - 1$, ať je r jakékoli.

Obtížné bylo dokázat, že pro libovolné n, které není mocninou prvočísla, existuje prvočíslo r (ohraničené polynomiálně), pro které $(x+a)^n$ a $x^n + a$ dávají různé zbytky po dělení $x^r - 1$ pro alespoň jednu hodnotu čísla a v jistém intervalu (jehož délka je opět ohraničena polynomiálně). To, že metoda „nepozná“ mocniny prvočísel, nevadí: tato n pozná jednoduchý polynomiální algoritmus, který provedeme hned na začátku metody.

Test na mocninu

Tímto testem bude AKS test začínat:

Algoritmus (Test na mocninu). *Pro dané celé číslo $n \geq 3$ algoritmus rozhodne, zda $n = a^b$, kde $a, b \in \mathbb{N}$, $b > 1$.*

1. *[Inicializace] Polož $b \leftarrow 2$, $a \leftarrow 1$, $c \leftarrow n$.*
2. *[Výpočet mocniny] Polož $m \leftarrow [\frac{a+c}{2}]$ a rychlým umocňováním spočti $d \leftarrow \min\{m^b, n+1\}$.*
3. *[Aktualizace mezí a, c] Je-li $d = n$, vytiskni zprávu, že $n = m^b$ je mocninou a skonči. Jinak, je-li $d < n$, polož $a \leftarrow m$, v opačném případě polož $c \leftarrow m$. Je-li $c - a \geq 2$, pokračuj bodem 2, jinak bodem 4.*
4. *[Zvýšení exponentu b] Nejmenší prvočíslo větší než b ulož do b. Je-li $2^b > n$, vytiskni zprávu, že n není mocninou a skonči. Jinak polož $a \leftarrow 1$, $c \leftarrow n$ a pokračuj bodem 2.*

Algoritmus je jistě správný: v průběhu výpočtu neustále platí $a^b < n < c^b$ a rozdíl $c - a$ se zmenšuje, dokud není $c - a = 1$.

Test na mocninu - odhad časové náročnosti

Výpočet mocniny v kroku 2 se provádí binárním umocňováním, jakmile se však v průběhu výpočtu objeví čísla větší než n, výpočet se přeruší a vrací se hodnota $n + 1$.

Protože pro dané b se rozdíl $c - a$ půlí při každém průchodu kroky 2 a 3, provedou se tyto kroky zhruba $\log_2 n$ krát. Rovněž počet kontrolovaných b je možné omezit shora číslem $\log_2 n$ (tato malá prvočísla budou uložena v tabulce, takže čas pro provedení kroku 4 je konstantní, jakmile se jednou provždy spočítá horní hranice $[\log_2 n]$ pro b).

V průběhu celého algoritmu je tedy třeba provést $O((\log_2 n)^2 \log_2 \log_2 n)$ násobení čísel menších než n, počet potřebných bitových operací lze odhadnout shora $O((\log_2 n)^4 \log_2 \log_2 n)$.

Algoritmus AKS

Algoritmus (Agrawal, Kayal, Saxena). *Pro dané přirozené číslo* $n > 1$ *algoritmus rozhodne, zda je* n *prvočíslo nebo složené.*

1. *[Mocniny] Pokud je* $n = a^b$, *kde* $a, b \in \mathbb{N}$, $b > 1$, *vytiskni, že* n *je složené a skonči. Jinak polož* $r \leftarrow 2$.
2. *[První cyklus] Jestliže* $r \geq n$, *pak vytiskni, že* n *je prvočíslo a skonči. Jestliže* $r|n$, *pak vytiskni, že* n *je složené a skonči. Jinak pro každé* i *od* 1 *do* $[4(\log_2 n)^2]$ *prověřuj: jestliže pro všechna taková* i *platí* $n^i \not\equiv 1 \pmod{r}$, *pokračuj krokem 3, jestliže naopak pro nějaké takové* i *platí* $n^i \equiv 1 \pmod{r}$, *pak nejmenší prvočíslo větší než* r *ulož do* r *a znovu prováděj krok 2.*
3. *[Druhý cyklus] Pro* a *od* 1 *do* $[2\sqrt{r}\log_2 n]$ *prováděj: jestliže pro některé takové* a *platí*

$$(x + a)^n \not\equiv (x^n + a) \pmod{x^r - 1} \text{ v } \mathbb{Z}_n[x],$$

   pak vytiskni, že n *je složené a skonči.*
4. *[Závěr] Vytiskni, že* n *je prvočíslo a skonči.*

Algoritmus AKS - důkaz správnosti algoritmu

Nejprve si promysleme, že nikdy na začátku kroku 2 nemůže být $r > n$. Protože r prochází postupně všechna prvočísla, znamenalo by to, že n je složené, ale pak by se algoritmus musel zastavit již dříve, když r se rovnalo nejmenšímu prvočíslu, které dělí n. Je tedy jasné, že pokud algoritmus skončí v kroku 1, 2 nebo 3, jistě odpoví správně. Zbývá dokázat, že i při zastavení v kroku 4 je odpověď správná.

Ve druhém kroku jsme hledali nejmenší prvočíslo r, pro které je řád čísla n modulo r větší než $4(\log_2 n)^2$.
Pokud jsme se dostali až do kroku 4, musí pro každé přirozené $a \leq 2\sqrt{r}\log_2 n$ platit $(x+a)^n \equiv (x^n + a) \pmod{x^r - 1}$ v $\mathbb{Z}_n[x]$.
Protože proběhl krok 2, víme, že n není dělitelné žádným prvočíslem menším nebo rovným r. Pak je n podle následující věty mocnina prvočísla.

Vzhledem k tomu, že proběhl krok 1, víme, že n není druhou nebo vyšší mocninou přirozeného čísla, a tedy n je prvočíslo a odpověď ve kroku 4 je správná.

Algoritmus AKS - důkaz správnosti algoritmu - věta

Věta 2. Nechť n a r jsou celá čísla splňující všechny následující podmínky:

(α) *r je prvočíslo a $r < n$;*

(β) *pro každé a splňující $2 \leq a \leq r$ platí $a \nmid n$;*

(γ) *řád čísla n modulo r je větší než $4(\log_2 n)^2$;*

(δ) *$(x+a)^n \equiv (x^n + a) \pmod{x^r - 1}$ v $\mathbb{Z}_n[x]$ pro všechna $1 \leq a \leq 2\sqrt{r}\log_2 n$.*

Pak n je mocninou prvočísla.

Důkaz provedeme později.

Pro důkaz polynomiální časové náročnosti algoritmu AKS potřebujeme pro každé celé $n \geq 2$ dokázat existenci „malého“ prvočísla r takového, že buď $r \mid n$ anebo (pokud $r \nmid n$) číslo n má modulo r řád větší než $4(\log_2 n)^2$.

Zde „malé“ znamená, že prvočíslo $r < f(\log_2 n)$ pro nějaký vhodný polynom f nezávisející na n. Následující věta ukáže, že tuto podmínku splní $f(x) = 20x^5$.

Algoritmus AKS - odhad časové náročnosti - věta

Věta 3. *Pro libovolné přirozené číslo $n \geq 2$ existuje prvočíslo $r \leq 20(\log_2 n)^5$ takové, že buď $r \mid n$ anebo platí $r \nmid n$ a současně řád čísla n modulo r je větší než $4(\log_2 n)^2$.*

Důkaz. Můžeme předpokládat, že $n \geq 4$, neboť pro menší n věta zřejmě platí. Označme $L = \log_2 n$ a $P = \prod_{i=1}^{[4L^2]}(n^i - 1)$. Zřejmě

$$P < \prod_{i=1}^{[4L^2]} n^i = n^{[4L^2][4L^2+1]/2} \leq 2^{L(4L^2)(4L^2+1)/2} \leq 2^{8L^5+2L^3}.$$

Z věty z úvodu přednášky plyne dolní odhad pro součin všech prvočísel p nepřevyšujících $20L^5$

$$\prod_{p \leq [20L^5]} p \geq \prod_{p \leq 2[10L^5]} p > 2^{[10L^5]} > 2^{10L^5-1}.$$

Ovšem $L \geq 2$ a tedy $2L^5 - 1 > 2L^3$, odkud $P < \prod_{p \leq [20L^5]} p$. Existuje tedy prvočíslo $r \leq [20L^5]$ takové, že $r \nmid P$, a tedy pro všechna přirozená čísla $i \leq 4L^2$ platí $r \nmid n^i - 1$. Pokud $r \nmid n$, je řád čísla n modulo r větší než $4L^2$ a jsme hotovi.

Odhad časové náročnosti vytvoření tabulky prvočísel

Potřebujeme tabulku prvočísel nepřevyšujících $20(\log_2 n)^5$. Máme-li připravit tabulku prvočísel menších než m pomocí Eratosthenova síta, sestavíme tabulku všech přirozených čísel od 2 do m a opakujeme toto: první neškrtlé číslo p vyznačíme jako prvočíslo a všechny jeho násobky počínaje $p \cdot p$ až po $p \cdot [\frac{m}{p}]$ škrtneme. To děláme až do doby, kdy je první neškrtlé číslo větší než $\sqrt{m}$; pak všechna zbylá neškrtlá čísla jsou prvočísla. Zřejmě $\int_{i-1}^{i} \frac{dx}{x} > 1/i$ (stačí funkci $1/x$ nahradit jejím minimem na tomto intervalu). Počet škrtání (a tedy i aritmetických operací) lze proto odhadnout shora číslem

$$\sum_{p \le \sqrt{m}} \frac{m}{p} < m \sum_{i=2}^{[\sqrt{m}]} \int_{i-1}^{i} \frac{dx}{x} = m \int_{1}^{[\sqrt{m}]} \frac{dx}{x} = m \ln [\sqrt{m}] \le \frac{m}{2} \ln m.$$

Počet bitových operací potřebných k tvorbě této tabulky je tedy $O(m(\log_2 m)^2)$. V našem případě je $m = 20(\log_2 n)^5$, a tedy časová náročnost tvorby tabulky v bitových operacích je $O((\log_2 n)^5 (\log_2 \log_2 n)^2)$.

Algoritmus AKS - odhad časové náročnosti

V kroku 2 pro každé r, kterých je $O((\log_2 n)^5)$, provádíme $O((\log_2 n)^2)$ násobení čísel nepřevyšujících r, časová náročnost kroku 2 v bitových operacích je proto $O((\log_2 n)^7(\log_2 \log_2 n)^2)$. V kroku 3 pro výpočet n-té mocniny v okruhu $\mathbb{Z}_n[x]/(x^r - 1)$ je zapotřebí $O(\log_2 n)$ okruhových násobení, která jsou prováděna jako násobení polynomů, jejichž stupeň je menší než r; každé takové okruhové násobení znamená $O(r^2)$ násobení a sčítání v $\mathbb{Z}_n$. Existují dokonce složitější algoritmy, které potřebují jen $O(r(\log_2 r)(\log_2 \log_2 r))$ operací (s větší O-konstantou). Časová náročnost obyčejného umocnění polynomu v bitových operacích je proto $O(r^2(\log_2 n)^2)$, těchto umocnění musíme provést celkem $O(\sqrt{r}\log_2 n)$. Časová náročnost kroku 3 v bitových operacích je $O(r^{5/2}(\log_2 n)^3)$, po dosazení $O((\log_2 n)^{31/2})$. Časová náročnost celého algoritmu v bitových operacích je proto $O((\log_2 n)^{31/2})$.

Pokud bychom užili v kroku 3 složitější algoritmus pro násobení polynomů, dosáhli bychom ještě lepšího výsledku $O((\log_2 n)^{21/2}(\log_2 \log_2 n)(\log_2 \log_2 \log_2 n))$.

Důkaz věty 2

Předpokládejme tedy, že celá čísla n a r splňují podmínky věty, a zvolme libovolné prvočíslo p dělící n. Je-li $p = n$, není co dokazovat, proto předpokládejme, že $p < n$, odkud plyne $p \leq \frac{n}{2}$. Označme $\ell = [2\sqrt{r}\log_2 n]$. Z podmínky (γ) ihned plyne $r > 4(\log_2 n)^2$, tj. $\sqrt{r} > 2\log_2 n$ a tedy z (β) dostáváme

$$p > r > \ell \qquad \text{a} \qquad r \nmid n. \tag{1}$$

Budeme se zabývat součiny mocnin polynomů $x + a \in \mathbb{F}_p[x]$ pro $1 \leq a \leq \ell$, zaveďme proto označení

$$P = \left\{ \prod_{a=1}^{\ell} (x+a)^{b_a};\ b_a \in \mathbb{Z},\ b_a \geq 0 \right\} \subseteq \mathbb{F}_p[x].$$

Pro stručnost vyjadřování zaveďme výrok $I(u, f)$ znamenající

$$u \in \mathbb{N},\ f \in \mathbb{F}_p[x],\ (f(x))^u \equiv f(x^u) \pmod{x^r - 1} \text{ v } \mathbb{F}_p[x].$$

Například pro $f = x + a$, kde $1 \leq a \leq \ell$, platí $I(n, f)$ díky $p \mid n$ a podmínce (δ) a současně platí též $I(p, f)$ díky větě 1.

$$I(u,f) \Leftrightarrow u \in \mathbb{N}, f \in \mathbb{F}_p[x], (f(x))^u \equiv f(x^u) \pmod{x^r - 1}$$

Lemma 1. *Z $I(u,f)$ a $I(v,f)$ plyne $I(uv,f)$.*

Důkaz. Umocněním kongruence z $I(u,f)$ dostáváme

$$(f(x))^{uv} \equiv (f(x^u))^v \pmod{x^r - 1}.$$

Dosazením x^u za x do kongruence z $I(v,f)$ dostáváme

$$(f(x^u))^v \equiv (f(x^{uv})) \pmod{x^{ur} - 1}.$$

Protože $x^r - 1 \mid x^{ur} - 1$, platí tato kongruence i modulo $x^r - 1$, a proto odtud plyne $I(uv,f)$.

Lemma 2. *Z $I(u,f)$ a $I(u,g)$ plyne $I(u,fg)$.*

Důkaz. Stačí vynásobit obě kongruence, které dostáváme z $I(u,f)$ a $I(u,g)$ a využít toho, že $(f \cdot g)(x^u) = f(x^u) \cdot g(x^u)$.

Důsledek. *Označme $U = \{n^i p^j;\ i,j \in \mathbb{Z},\ i \geq 0,\ j \geq 0\}$. Pak $I(u,f)$ platí pro všechna $f \in P$ a všechna $u \in U$.*

Konstrukce tělesa F

Polynom $x^{r-1} + x^{r-2} + \cdots + x + 1 \in \mathbb{F}_p[x]$ rozložme v $\mathbb{F}_p[x]$ na normované ireducibilní faktory; jeden z nich označme h.
Je tedy $h \in \mathbb{F}_p[x]$ normovaný ireducibilní polynom dělící $x^{r-1} + x^{r-2} + \cdots + x + 1$ a tedy i $x^r - 1$. Označme d stupeň polynomu h. Těleso $F = \mathbb{F}_p[x]/(h)$ má tedy p^d prvků a jeho prvek $\zeta = x + (h)$ je kořenem polynomu h, a tedy i polynomu $x^r - 1$.
Protože $p \nmid r$, není 1 kořenem polynomu $x^{r-1} + x^{r-2} + \cdots + x + 1$, a tedy $\zeta \neq 1$. Proto řád ζ v $F^\times$ je r.
Označme G množinu hodnot polynomů z P v ζ, tj.

$$G = \{f(\zeta);\ f \in P\} = \left\{ \prod_{a=1}^{\ell} (\zeta + a)^{b_a};\ b_a \in \mathbb{Z},\ b_a \geq 0 \right\} \subseteq F.$$

Lemma 3. *Pro* $1 \leq a \leq \ell$ *jsou* $x + a$ *různé polynomy z* $\mathbb{F}_p[x]$.

Důkaz. Je-li $1 \leq a < a' \leq \ell$, pak $0 < a' - a \leq \ell < p$ podle (1) a tedy skutečně a a a' jsou různé prvky tělesa $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Lemma 4. *Pro každé $f \in P$ a každé $u \in U$ platí $f(\zeta)^u = f(\zeta^u)$.*

Důkaz. Z důsledku lemmat 1 a 2 víme, že existuje polynom $q \in \mathbb{F}_p[x]$ splňující

$$(f(x))^u = f(x^u) + (x^r - 1) \cdot q(x).$$

Dosazením ζ za x dostáváme dokazované.

Označme $T = \{\zeta^u;\ u \in U\} \subseteq F^\times$ a $t = |T|$.

Lemma 5. *Platí $r > t > 4(\log_2 n)^2$.*

Důkaz. Protože ζ má řád r, platí $T \subseteq \{1, \zeta, \ldots, \zeta^{r-1}\}$. Ovšem pro každé $u \in U$ platí $r \nmid u$ dle definice U a (1), a tedy $1 \notin T$. Proto $t < r$. Jistě $\zeta^{n^i} \in T$ pro každé $i \geq 0$. Protože ζ má řád r, platí $\zeta^{n^i} = \zeta^{n^j}$ právě tehdy, když $n^i \equiv n^j \pmod{r}$, což je ekvivalentní s $i \equiv j \pmod{e}$, kde e je řád čísla n modulo r. Proto $\zeta^{n^0}, \zeta^{n^1}, \ldots, \zeta^{n^{e-1}}$ jsou různé prvky T a předpoklad (γ) dává $t \geq e > 4(\log_2 n)^2$.

$T = \{\zeta^u;\ u \in U\} \subseteq F^\times,\ \ t = |T|$

Lemma 4. Pro každé $f \in P$ a každé $u \in U$ platí $f(\zeta)^u = f(\zeta^u)$.

Lemma 6. Jsou-li f_1 a f_2 různé polynomy z P a oba mají stupeň menší než t, pak $f_1(\zeta) \neq f_2(\zeta)$.

Důkaz. Předpokládejme naopak, že $f_1(\zeta) = f_2(\zeta)$. Pak pro každé $u \in U$ z lemmatu 4 plyne $f_1(\zeta^u) = f_1(\zeta)^u = f_2(\zeta)^u = f_2(\zeta^u)$, a tedy libovolný prvek z T je kořenem polynomu $f_1 - f_2$. Tento polynom má tedy alespoň t kořenů a stupeň menší než t, proto $f_1 = f_2$.

$P = \{\prod_{a=1}^{\ell}(x+a)^{b_a};\ b_a \geq 0\}$, $G = \{f(\zeta);\ f \in P\} \subseteq F$

Lemma 5. *Platí* $r > t > 4(\log_2 n)^2$.

Lemma 6. *Jsou-li* f_1 *a* f_2 *různé polynomy z* P *a oba mají stupeň menší než* t, *pak* $f_1(\zeta) \neq f_2(\zeta)$.

Lemma 7. *Platí* $|G| > \frac{1}{2}n^{2\sqrt{t}}$.

Důkaz. Nechť $\mu = \min\{\ell, t-1\}$. Z věty o jednoznačném rozkladu polynomů v $\mathbb{F}_p[x]$ na ireducibilní faktory a z lemmatu 3 plyne, že $\prod_{a=1}^{\mu}(x+a)^{b_a}$, kde $b_a \in \{0,1\}$, jsou různé polynomy z P stupně menšího než t. Podle lemmatu 6 jsou jejich funkční hodnoty v ζ různé a z toho plyne odhad $|G| \geq 2^{\mu}$. Jsou dvě možnosti: je-li $\mu = t-1$, platí díky odhadu $t > 4(\log_2 n)^2$ z lemmatu 5

$$\mu = t - 1 > 2\sqrt{t}\log_2 n - 1.$$

Je-li naopak $\mu = \ell$, platí díky odhadu $r > t$ z lemmatu 5

$$\mu = [2\sqrt{r}\log_2 n] > 2\sqrt{r}\log_2 n - 1 > 2\sqrt{t}\log_2 n - 1.$$

V obou případech dostáváme $|G| \geq 2^{\mu} > 2^{2\sqrt{t}\log_2 n - 1} = \frac{1}{2}n^{2\sqrt{t}}$ a lemma je dokázáno.

$G = \{f(\zeta);\ f \in P\} \subseteq F$

Lemma 4. *Pro každé $f \in P$ a každé $u \in U$ platí $f(\zeta)^u = f(\zeta^u)$.*

Lemma 7. *Platí $|G| > \frac{1}{2}n^{2\sqrt{t}}$.*

Označme $U_0 = \{n^i p^j;\ i, j \in \mathbb{Z},\ 0 \leq i \leq [\sqrt{t}],\ 0 \leq j \leq [\sqrt{t}]\} \subseteq U$.

Lemma 8. *Pro různá $u, v \in U_0$ platí $\zeta^u \neq \zeta^v$.*

Důkaz. Z $p \leq \frac{n}{2}$ plyne $np \leq \frac{1}{2}n^2$, a tedy pro každé $u \in U_0$ je $u \leq (\frac{1}{2}n^2)^{\sqrt{t}} \leq \frac{1}{2}n^{2\sqrt{t}} < |G|$ podle lemmatu 7.
Sporem: předpokládejme, že pro různá $u, v \in U_0$ platí $\zeta^u = \zeta^v$. Libovolné $g \in G$ je tvaru $g = f(\zeta)$ pro nějaké $f \in P$. Podle lemmatu 4 platí $g^u = f(\zeta)^u = f(\zeta^u) = f(\zeta^v) = f(\zeta)^v = g^v$ a tedy každé $g \in G$ je kořenem polynomu $x^u - x^v$. Na začátku tohoto důkazu jsme ukázali, že u a v jsou menší než $|G|$. Ovšem $u \neq v$, a tedy nenulový polynom $x^u - x^v$ má více kořenů než je jeho stupeň. To je spor.

Dokončení důkazu věty 2

$T = \{\zeta^u;\ u \in U\} \subseteq F^\times, \quad t = |T|$

$U_0 = \{n^i p^j;\ i, j \in \mathbb{Z},\ 0 \le i \le [\sqrt{t}],\ 0 \le j \le [\sqrt{t}]\} \subseteq U$

Lemma 8. Pro různá $u, v \in U_0$ platí $\zeta^u \neq \zeta^v$.

Počet dvojic (i, j), kde $i, j \in \mathbb{Z}$, $0 \le i \le [\sqrt{t}]$, $0 \le j \le [\sqrt{t}]$, je roven $([\sqrt{t}] + 1)^2 > \sqrt{t}^2 = t$, na druhou stranu z lemmatu 8 plyne $|U_0| \le |T| = t$. Znamená to, že existují různé dvojice (i, j) a (k, m) takové, že $i, j, k, m \in \{0, 1, \ldots, [\sqrt{t}]\}$ a že $n^i p^j = n^k p^m$. Lze navíc předpokládat, že $i \ge k$. Kdyby $i = k$, muselo by platit i $j = m$ a dvojice by nebyly různé. Je tedy $i > k$ a platí $n^{i-k} = p^{m-j}$. Odtud plyne, že v rozkladu čísla n na prvočinitele se nevyskytují jiná prvočísla než p, a tedy n je mocninou prvočísla p. Věta 2 je dokázána.