Testování prvočíselnosti a faktorizace

Ľubomíra Balková

Úvod do kryptologie

21. března 2011

Problémy

1. **Primality problem**: Rozhodni, zda je dané $n \in \mathbb{N}$ prvočíslo.
2. **Factoring problem**: Najdi prvočíselný rozklad daného $n \in \mathbb{N}$.

- po staletí jen teoretický význam
- v současnosti obrovský praktický význam - díky *kryptologii*

Algoritmus RSA - Rivest, Shamir, Adleman 1978

Definice: $\varphi(n) =$ počet čísel $\in \{1, 2, \ldots, n-1\}$ nesoudělných s n

POZN.:
$$\begin{aligned} \varphi(p) &= p-1 && \text{pro } p \in \mathbb{P} \\ \varphi(p \cdot q) &= (p-1)(q-1) && \text{pro } p, q \in \mathbb{P} \end{aligned}$$

Věta (Eulerova-Fermatova): Nechť $m, n \in \mathbb{N}$.
$NSD(m, n) = 1 \quad \Rightarrow \quad m^{\varphi(n)} \bmod n = 1$.

1. *generování klíče* **Primality problem**
   - Bob generuje velká $p, q \in \mathbb{P}$, $n := pq$ ... *modul RSA*
   - zvolí $1 < e < \varphi(n) = (p-1)(q-1)$ a $\mathrm{NSD}(e, \varphi(n)) = 1$
   - Eukleidovým algoritmem najde jediné $1 < d < \varphi(n)$... *soukromý klíč*

     $$ed \bmod \varphi(n) = 1, \quad \text{tj. } ed = \varphi(n)k + 1 \text{ pro } k \in \mathbb{N}$$

   - zveřejní (n, e) ... *veřejný klíč*
2. *šifrování*
   - Alice vyhledá v databázi Bobův klíč (n, e)
   - odešle $c = m^e \bmod n$, kde $m < n$ a $\mathrm{NSD}(m, n) = 1$
3. *dešifrování*
   - Bob spočte $m = c^d \bmod n$

Algoritmus RSA - Rivest, Shamir, Adleman 1978

Definice: $\varphi(n) =$ počet čísel $\in \{1, 2, \ldots, n-1\}$ nesoudělných s n
Věta (Eulerova-Fermatova): Nechť $m, n \in \mathbb{N}$.
$NSD(m, n) = 1 \quad \Rightarrow \quad m^{\varphi(n)} \bmod n = 1.$

- *dešifrování*
  - Bob spočte $c^d \bmod n$

$$\begin{aligned} c^d \bmod n &= (m^e)^d \bmod n \\ &= m^{ed} \bmod n \\ &= m^{\varphi(n)k+1} \bmod n \\ &= m \cdot (m^{\varphi(n)})^k \bmod n \\ &= m \end{aligned}$$

- *kryptoanalýza* **Factoring problem**
  - rozklad $n = pq$

Program

1. Eratosthenovo síto
2. Fermatův test
3. Pravděpodobnostní testy
   - Solovayův-Strassenův test
   - Rabinův-Millerův test
4. Deterministické testy
   - Lucasův-Lehmerův test
   - AKS test
5. Fermatova faktorizace

Program

1. Eratosthenovo síto
2. Fermatův test
3. Pravděpodobnostní testy
   - Solovayův-Strassenův test
   - Rabinův-Millerův test
4. Deterministické testy
   - Lucasův-Lehmerův test
   - AKS test
5. Fermatova faktorizace

Eratosthenovo síto

Eratosthenes z Kyrény (276 - 194 př.n.l.)

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Program

1 Eratosthenovo síto

2 Fermatův test

3 Pravděpodobnostní testy
- Solovayův-Strassenův test
- Rabinův-Millerův test

4 Deterministické testy
- Lucasův-Lehmerův test
- AKS test

5 Fermatova faktorizace

Pierre de Fermat (1601 - 1665)

- fr. právník a matematik-amatér
- teorie čísel - Velká a Malá Fermatova věta
- teorie pravděpodobnosti - spolu s Pascalem jejím zakladatelem
- předchůdce diferenciálního počtu

Malá Fermatova věta

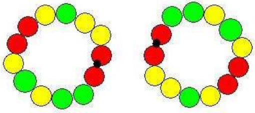
Malá Fermatova věta: Nechť p je prvočíslo, $a \in \{1, 2, \ldots, p-1\}$.
Pak $a^p \bmod p = a$ nebo ekvivalentně $a^{p-1} \bmod p = 1$.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 45 10 1

Malá Fermatova věta

Malá Fermatova věta: Nechť p je prvočíslo, $a \in \{1, 2, \ldots, p-1\}$.
Pak $a^p \bmod p = a$ nebo ekvivalentně $a^{p-1} \bmod p = 1$.
Důkaz[Golombův]:

- náhrdelníky složené z p perel o a barvách $\Rightarrow$ počet a^p
- p prvočíslo $\Rightarrow$ otáčením náhrdelníku dostaneme opět stejný náhrdelník pouze, je-li složený z perel stejné barvy



- počet náhrdelníků z perel stejné barvy je a
- všechny náhrdelníky, co nejsou složené z jedné barvy (těch je $a^p - a$), dostaneme otáčením určitého počtu k z nich p-krát o jednu pozici
- závěr: $a^p - a = kp$, a tedy $a^p \bmod p = a$

Algoritmus Fermatova testu

- testujeme, zda n je prvočíslo
- bereme libovolné $a < n$ a počítáme $a^{n-1} \bmod n$
- pokud nevyjde $1 \Rightarrow n$ je složené
- pokud vyjde $1 \Rightarrow$ nic s jistotou nevíme

Carmichaelova čísla

Definice: Složená čísla n taková, že pro každé $a < n$ a $NSD(a, n) = 1$ platí $a^{n-1} \bmod n = 1$, nazýváme *Carmichaelova*.

- nejmenší $561 = 3 \times 11 \times 17$
- Chernik 1939: $(6k + 1)(12k + 1)(18k + 1)$ je Carmichaelovo číslo, pokud je každý faktor prvočíslem
- Alford, Ganville, Pomerance 1994: existuje ∞-mnoho Carmichaleových čísel
- Důsledek: Fermatův test nedostatečný k testování prvočíselnosti!

Program

1. Eratosthenovo síto
2. Fermatův test
3. Pravděpodobnostní testy
   - Solovayův-Strassenův test
   - Rabinův-Millerův test
4. Deterministické testy
   - Lucasův-Lehmerův test
   - AKS test
5. Fermatova faktorizace

Kvadratické reziduum

- **Definice**: Nechť p je liché prvočíslo. Pak $a \in \mathbb{N} \setminus p\mathbb{N}$ nazveme *kvadratické reziduum*, pokud $a = x^2 \bmod p$ pro nějaké $x \in \{1, 2, \ldots, p-1\}$. V opačném případě nazveme a *kvadratické nereziduum*.
- např. $p = 7$, pak

$$\begin{array}{rcl} 1 & = & 1^2 \bmod 7 \quad (= \; 6^2 \bmod 7) \\ 2 & = & 3^2 \bmod 7 \quad (= \; 4^2 \bmod 7) \\ 4 & = & 2^2 \bmod 7 \quad (= \; 5^2 \bmod 7) \end{array}$$

Legendrův symbol

- **Definice**: Nechť p je liché prvočíslo a $a \in \mathbb{N}$. Pak definujeme

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{je-li } a \text{ násobkem } p, \\ 1 & \text{je-li } a \text{ kvadratické reziduum} \mod p, \\ -1 & \text{je-li } a \text{ kvadratické nereziduum} \mod p. \end{cases}$$

- Jak spočíst Legendrův symbol $\left(\frac{a}{p}\right)$?

Vlastnosti Legendrova symbolu

- **Eulerova věta**: Nechť p je liché prvočíslo a $a \in \mathbb{N}$. Pak $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$.
- $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
  (speciálně když b není násobek p, pak $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$)
- $\left(\frac{1}{p}\right) = 1,\ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$,
  tj. $\left(\frac{2}{p}\right) = -1$ pro $p = \pm 3 \mod 8$ a $\left(\frac{2}{p}\right) = 1$ pro $p = \pm 1 \mod 8$
- **Zákon kvadratické reciprocity**: Nechť p, q jsou lichá prvočísla, pak $\left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)(p-1)}{4}} \left(\frac{p}{q}\right)$,
  tj. $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ pro $p = q = 3 \mod 4$ a $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ jinak.

Jacobiho symbol

- **Definice**: Nechť $n > 1$ je liché přirozené číslo a jeho prvočíselný rozklad má tvar $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Pak definujeme

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_r}\right)^{\alpha_r} .$$

- vlastnosti Legendrova symbolu platí i pro Jacobiho symbol $\Rightarrow$ rychlý výpočet Jacobiho symbolu

Princip Solovayova-Strassenova testu

- n je liché prvočíslo $\Rightarrow$ pro každé $a < n$ platí $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \bmod n$
- n je složené číslo $\Rightarrow$ existuje $a < n$, pro které $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \bmod n$ (takových a je aspoň $1/2$, tj. $\frac{n-1}{2}$)

Algoritmus Solovayova-Strassenova testu

- testujeme, zda n je prvočíslo
- bereme libovolná $a_1, a_2, \ldots, a_r \in \{2, \ldots, n-1\}$
- kontrolujeme $NSD(a_i, n) = 1$
- spočteme $\left(\frac{a_i}{n}\right)$ a $a_i^{\frac{n-1}{2}} \bmod n$
- pro nějaké a_i neplatí $\left(\frac{a_i}{n}\right) = a_i^{\frac{n-1}{2}} \bmod n \Rightarrow n$ složené
- pro všechna a_i platí $\left(\frac{a_i}{n}\right) = a_i^{\frac{n-1}{2}} \bmod n \Rightarrow n$ prvočíslo s pravděpodobností $1 - \frac{1}{2^r}$

Princip Rabinova-Millerova testu

pravděpodobnostní - rychlý, v praxi nejvíce užívaný

- n liché prvočíslo a $n-1=2^k t$
- Malá Fermatova věta $\Rightarrow$ pro každé $a<n$ platí

$$0=(a^{n-1}-1) \ \mathrm{mod}\ n=(a^{2^k t}-1) \ \mathrm{mod}\ n$$

- n nutně dělí aspoň jednu ze závorek:

$$(a^{2^{k-1}t}-1)(a^{2^{k-1}t}+1)=(a^{2^{k-2}t}-1)(a^{2^{k-2}t}+1)(a^{2^{k-1}t}+1)=$$

$$=\underline{\underline{(a^t-1)(a^t+1)\dots(a^{2^{k-2}t}+1)(a^{2^{k-1}t}+1)}}$$

- n složené číslo, pak existuje $a<n$, pro které n nedělí žádnou ze závorek (takových a jsou aspoň $3/4$, tj. $\frac{3(n-1)}{4}$)

Algoritmus Rabinova-Millerova testu

- testujeme, zda n je prvočíslo
- rozložíme $n - 1 = 2^k t$
- bereme libovolná $a_1, a_2, \ldots, a_r \in \{2, \ldots, n-1\}$
- kontrolujeme $NSD(a_i, n) = 1$
- klademe $b_i = a_i^t$
- pokud pro některé b_i platí:
    - $b_i \bmod n \neq \pm 1$,
    - $b_i^{2^j} \bmod n \neq -1$ pro každé $j \in \{1, \ldots, k-1\}$,

  $\Rightarrow$ n je složené
- jinak je n prvočíslo s pravděpodobností $1 - \frac{1}{4^r}$

Příklad: Rabinův-Millerův test

- testujeme, zda 49 je prvočíslo
- rozložíme $49 - 1 = 2^4 \cdot 3$
- $a_1 := 2$
- kontrolujeme $NSD(2, 49) = 1$
- klademe $b_1 = 2^3 = 8$
  - $b_1 \bmod 49 \neq \pm 1$, protože $8 \bmod 49 = 8$
  - $b_1^2 \bmod 49 \neq -1$, protože $8 \cdot 8 \bmod 49 = 64 \bmod 49 = 15$
  - $b_1^{2^2} \bmod 49 \neq -1$, protože $(b_1^2)^2 \bmod 49 = 15^2 \bmod 49 = 45 \cdot 5 \bmod 49 = (-4) \cdot 5 \bmod 49 = 29$
  - $b_1^{2^3} \bmod 49 \neq -1$, protože $((b_1^2)^2)^2 \bmod 49 = (-20)^2 \bmod 49 = 8$

$\Rightarrow$ 49 je složené

Logická otázka

"Kolik náhodných přirozených čísel je třeba otestovat, než najdeme prvočíslo?"

Definice: $\pi(n) =$ počet prvočísel $\leq n$

Prime Number Theorem: $\pi(n) \sim \frac{n}{\ln n}$

Důsledek: vybereme-li p náhodně mezi 1 a n, pak pravděpodobnost, že p je prvočíslo $\sim \frac{1}{\ln n}$

Příklad

Náhodné číslo o ≤ 512 *bitech je prvočíslo s pravděpodobností* $\sim \frac{1}{\ln 2^{512}} \doteq \frac{1}{355}$. *Stačí uvažovat jen lichá čísla* $\Rightarrow$ *pravděpodobnost* $\sim \frac{2}{355}$.

Program

1. Eratosthenovo síto
2. Fermatův test
3. Pravděpodobnostní testy
   - Solovayův-Strassenův test
   - Rabinův-Millerův test
4. Deterministické testy
   - Lucasův-Lehmerův test
   - AKS test
5. Fermatova faktorizace

Marin Mersenne (1588-1648)

- fr. matematik (teorie čísel), fyzik (mechanika, optika)
- mnich (řád minimů): “le bon père Mersenne”, “Maxime de Minimes”
- v jeho pařížském bytě schůzky učenců (Descartes, Pascalové) $\Rightarrow$ založení Akademie věd roku 1666
- “arXiv” 17. století - korespondence se 78 učenci (Descartes, Huyghens, Fermat, Galilei, Torricelli, Komenský)

Mersennova prvočísla

Definice: Nechť p je prvočíslo. Pak $M_p = 2^p - 1$ nazýváme *Mersennovo číslo*, případně *Mersennovo prvočíslo*.

- $2^{mn} - 1 = (2^m)^n - 1 = (2^m - 1)(1 + 2^m + 2^{2m} + \cdots + 2^{(n-1)m})$
- Mersenne není první (před ním Regius, Cataldi)
- Mersenne tvrdí v roce 1644, že
  - M_p prvočíslo pro $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$
  - M_p složené číslo pro ostatní $p < 257$
- v seznamu chybí 61, 89, 107 a přebývá 67, 257
- Coleova přednáška beze slov v roce 1903, dk., že M_{67} není prvočíslo
- University of Illinois - nalezeno 23. Mersennovo prvočíslo, na počest vydána poštovní známka

Lucasův-Lehmerův test

Definujme $y_1 := 4, \quad y_{k+1} := y_k^2 - 2$ pro $k = 1, 2, \ldots$.
Věta: Nechť p je liché prvočíslo. Pak $M_p = 2^p - 1$ je Mersennovo prvočíslo $\Leftrightarrow M_p / y_{p-1}$.

- menší složitost než u všech ostatních testů, včetně pravděpodobnostních $\Rightarrow$ největší známá pročísla jsou Mersennova
- ovšem testujeme jen část prvočísel - jen Mersennova $\Rightarrow$ nemožnost využití v kryptografii
- Lucas (1842 - 1891) - fr. profesor ma na gymnáziu, pomocí testu ukázal, že $2^{127} - 1$ je prvočíslo (největší prvočíslo nalezené bez PC)
- Lehmer (1905 - 1991) - am. matematik, Lehmerův generátor náhodných čísel, 1. numerické výpočty - ENIAC, CALDIC

Algoritmus Lucasova-Lehmerova testu

- nechť p liché prvočíslo, testujeme, zda $M_p = 2^p - 1$ je prvočíslo
- klademe $y_1 := 4$ a spočteme $y_k := (y_{k-1}^2 - 2) \bmod M_p$ pro $k = 2, \ldots, p-1$
- pokud $y_{p-1} = 0 \Rightarrow M_p$ je prvočíslo
- jinak je M_p složené číslo

GIMPS

GIMPS = Great Internet Mersenne Prime Search
http://www.mersenne.org/

- založen 1996 Georgem Woltmanem, programy od firmy Scotta Kurowského
- 1998 - 19-letý student Clarkson objevil $M(37) = M_{3021377}$, které má > 900000 cifer
- odměny od Electronic Frontier Foundation 150 000 USD za Mersennovo prvočíslo s $> 10^8$ ciframi, 250 000 USD s $> 10^9$ ciframi
- ze 47 známých Mersennových prvočísel v projektu GIMPS nalezeno 13

Dokonalá čísla

Definice: Nechť $n \in \mathbb{N}$. Pak n nazveme *dokonalé*, pokud $n = \sum_{d/n, d<n} d$.

Příklad

$6 = 1 + 2 + 3,\ 28 = 1 + 2 + 4 + 7 + 14,\ 496,\ 8128$ *(už staří Řekové)*

Věta(Eukleidés 300 př.n.l. $\Leftarrow$, Euler 18.stol. $\Rightarrow$): Nechť n je sudé přirozené číslo. Pak n je dokonalé $\Leftrightarrow n = 2^{p-1}(2^p - 1)$, kde p je prvočíslo a $M_p = 2^p - 1$ je prvočíslo.

- Důsledek: nové Mersennovo prvočíslo $\Rightarrow$ nové sudé dokonalé číslo

Dokonalá čísla - otevřené problémy

1. Existuje ∞ mnoho Mersennových prvočísel (a tedy ∞ mnoho sudých dokonalých čísel)?
2. Existuje liché dokonalé číslo? Pokud ano, pak
    1. $> 10^{300}$
    2. má aspoň 9 různých prvočinitelů
    3. z nich aspoň jeden $> 10^{20}$ atd.
3. Existuje ∞ mnoho složených Mersennových čísel?

Agrawal - Kalyan - Saxena

- 2002 - *PRIMES is in P*
- Manindra Agrawal, Neeraj Kayal, Nitin Saxena from the Indian Institute of Technology Kanpur
- složitost polynomiální $\mathcal{O}^{\sim}(\log^6 n)$

Agrawal Kayal Saxena

Hlavní myšlenka

Věta

Nechť $n \geq 2$ *a* $a \in \{1, 2, \ldots, n-1\}$ *nesoudělné s* n*. Pak* $n \in \mathbb{P} \Leftrightarrow (x-a)^n \equiv x^n - a \bmod n$*.*

- výpočet $n-1$ koeficientů $\Rightarrow$ náročné
- **zjednodušení**: volba vhodného r tak, že (ne)splnění identity

$$(x-a)^n \equiv x^n - a \mod (x^r - 1), n$$

pro málo hodnot a rozhodne o tom, zda $n \in \mathbb{P}$

Volba r

- chceme, aby multiplikativní řád $n \bmod r$ byl $> \log^2 n$
- najdeme minimální takové r
- $B := \lceil \log^5 n \rceil$ a $A := n^{\lfloor \log B \rfloor} \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$
- $r :=$ nejmenší přirozené číslo, které nedělí A
- snadno se ověří, že
  1. $NSD(r, n) = 1$
  2. $r \leq B$
  3. $o_r(n) > \log^2 n$

Algoritmus AKS

1. if $n = a^b$ pro $a \in \mathbb{N}$ a $b > 1 \Rightarrow n$ složené
2. najdi nejmenší r tak, že $o_r(n) > \log^2 n$
3. if $1 < NSD(a, n) < n$ pro nějaké $a \leq r \Rightarrow n$ složené
4. if $n \leq r \Rightarrow n$ prvočíslo
5. for $a = 1$ to $\lfloor \sqrt{\varphi(r)} \log n \rfloor$
   if $(x - a)^n \not\equiv x^n - a \bmod n(x^r - 1), n \Rightarrow n$ složené
6. n prvočíslo

Náznak důkazu - sporem

- předpokládejme, že n je složené a přesto output prvočíslo $\Rightarrow$ konec krokem 6
- uvažujme p/n a $p > r$ a $\ell := \lfloor \sqrt{\varphi(r)} \log n \rfloor$
- množina G prvků $k \bmod r$, pro které $(x-a)^k \equiv x^k - a \mod (x^r - 1), n$ pro všechna $a < \ell$ tvoří grupu o velikosti aspoň $\log^2 n$
- množina produktů $(x-a)^k \mod h(x), p$ pro $a < \ell$, kde $h(x)$ je vhodně zvolený ireducibilní faktor $x^r - 1$, je také grupa $\mathcal{G}$
- lze určit horní a dolní odhady na velikost grupy $\mathcal{G}$

$$\binom{\#G + \ell}{\#G - 1} \leq \#\mathcal{G} \leq n^{\sqrt{\#G}},$$

které se ale vylučují, pokud n není p^b pro nějaké $b > 1 \Rightarrow$ SPOR

Složitost algoritmu

- nejdelší částí je ověření, zda $(x-a)^n \equiv x^n - a \bmod (x^r - 1), n$ pro všechna $a \leq l$
- jednoduchá analýza $\Rightarrow \mathcal{O}^{\sim}(\log^{21/2} n)$
- jemnější analýza $\Rightarrow \mathcal{O}^{\sim}(\log^{15/2} n)$
- se změnou v algoritmu $\Rightarrow \mathcal{O}^{\sim}(\log^{6} n)$
- stále mnohem pomalejší než Rabin-Miller

Program

1. Eratosthenovo síto
2. Fermatův test
3. Pravděpodobnostní testy
   - Solovayův-Strassenův test
   - Rabinův-Millerův test
4. Deterministické testy
   - Lucasův-Lehmerův test
   - AKS test
5. Fermatova faktorizace

Hlavní myšlenka

- nechť $n = pq$, $a = \frac{p+q}{2}$, $b = \frac{p-q}{2}$, pak $p = a + b$, $q = a - b$, $n = a^2 - b^2$, tj. každé složené číslo je rozdílem kvadrátů
- pro $p \doteq q$ efektivní test (také pro $p \doteq 2q$, $p \doteq 3q$)

Příklad

$n = 200819$, *pak* $[\sqrt{n}] + 1 = 449$

$$449^2 - n = 782 \quad \textit{není čtverec}$$

$$450^2 - n = 1681 = 41^2,$$

$$\textit{a tedy} \;\; a = 450,\; b = 41,\; p = 491,\; q = 409$$

Zobecnění pomocí kongruencí

- hledáme a, b

$$a^2 = b^2 \mod n, \quad a \neq \pm b \mod n$$

- pak $n^2 \mid (a^2 - b^2) = (a+b)(a-b)$, ale $n \nmid (a-b)$ a $n \nmid (a+b) \Rightarrow NSD(n, a+b) > 1$ a $NSD(n, a-b) > 1$

Příklad

$n = 4633$

$$118^2 = 5^2 \mod n, \quad 118 \neq \pm 5 \mod n$$

$$NSD(4633, 118+5) = 41$$

$$NSD(4633, 118-5) = 113$$