Proč je dobré míti . . . . . . prvočísla?

Michal Bulant

Brkomoni 2016, Zdobnice v Orlických horách

29.8. – 4.9.2016

Plán přednášky

Zašifrovaná motivace

Cíl:

Zachytili jsme tajnou zprávu

$$C = 2396750279412805487568122053434668954177902079236 42$$

pro našeho nepřítele A, kterou bychom rádi dešifrovali.

Zašifrovaná motivace

Cíl:

Zachytili jsme tajnou zprávu

$$C = 239675027941280548756812205343466895417790207923642$$

pro našeho nepřítele A, kterou bychom rádi dešifrovali. Jako každý jiný účastník víme, že A komunikuje prostřednictvím RSA a že veřejný klíč V_A je tvořen čísly

$$n = 374144419156711146897884040346152783797331507019777$$

a

$$e = 240911337096020749615795248242245864391942105373709.$$

Zašifrovaná motivace

Cíl:

Zachytili jsme tajnou zprávu

$$C = 2396750279412805487568122053434668954177902079236 42$$

pro našeho nepřítele A, kterou bychom rádi dešifrovali. Jako každý jiný účastník víme, že A komunikuje prostřednictvím RSA a že veřejný klíč V_A je tvořen čísly

$$n = 374144419156711146897884040346152783797331507019777$$

a

$$e = 240911337096020749615795248242245864391942105373709.$$

Jsme schopni s těmito údaji zprávu dešifrovat?

Zašifrovaná motivace – RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A

Zašifrovaná motivace – RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ **nelze** snadno spočítat]

Zašifrovaná motivace – RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ **nelze** snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$

Zašifrovaná motivace – RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ **nelze** snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$

Zašifrovaná motivace – RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ **nelze** snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M:

$$C = C_e(M) \equiv M^e \pmod{n}$$

Zašifrovaná motivace – RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ **nelze** snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M:

$$C = C_e(M) \equiv M^e \pmod{n}$$

- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$

Plán přednášky

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Definice (alternativní)

Přirozené číslo n je prvočíslo, právě když pro libovolná $a, b \in \mathbb{Z}$ platí

$$n \mid ab \implies n \mid a \text{ nebo } n \mid b.$$

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Definice (alternativní)

Přirozené číslo n je prvočíslo, právě když pro libovolná $a, b \in \mathbb{Z}$ platí

$$n \mid ab \implies n \mid a \text{ nebo } n \mid b.$$

Je vidět, že obě definice popisují totéž?

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Definice (alternativní)

Přirozené číslo n je prvočíslo, právě když pro libovolná $a, b \in \mathbb{Z}$ platí

$$n \mid ab \implies n \mid a \text{ nebo } n \mid b.$$

Je vidět, že obě definice popisují totéž?

Věta (Základní věta aritmetiky)

Každé přirozené číslo se dá jednoznačně (až na pořadí) zapsat jako součin prvočísel.

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Definice (alternativní)

Přirozené číslo n je prvočíslo, právě když pro libovolná $a, b \in \mathbb{Z}$ platí

$$n \mid ab \implies n \mid a \text{ nebo } n \mid b.$$

Je vidět, že obě definice popisují totéž?

Věta (Základní věta aritmetiky)

Každé přirozené číslo se dá jednoznačně (až na pořadí) zapsat jako součin prvočísel.

Tuto zásadní větu uvádíme nyní, ale dokážeme později, až k tomu budeme mít prostředky!

Předchozí tvrzení nejsou úplně *zadarmo*, navíc se ukazuje, že zdaleka neplatí při přirozeném rozšíření těchto definic do jiných číselných oborů, kde umíme rozumným způsobem sčítat, násobit a *krátit* (tzv. *obory integrity* – např. $\mathbb{Q}, \mathbb{R}, \mathbb{Z}[\sqrt{2}], \mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}]$ apod.).

Předchozí tvrzení nejsou úplně *zadarmo*, navíc se ukazuje, že zdaleka neplatí při přirozeném rozšíření těchto definic do jiných číselných oborů, kde umíme rozumným způsobem sčítat, násobit a *krátit* (tzv. *obory integrity* – např. $\mathbb{Q}, \mathbb{R}, \mathbb{Z}[\sqrt{2}], \mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}]$ apod.).

Příklad

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Přitom zde selhává i zaměnitelnost obou definic prvočíselnosti, *být nerozložitelný* (ireducibilní) je obecně slabší vlastnost než být *primitivní* (alternativní definice) – v tomto příkladu je 2 nerozložitelná, ale přitom $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, i když nedělí žádného z činitelů.

Předchozí tvrzení nejsou úplně *zadarmo*, navíc se ukazuje, že zdaleka neplatí při přirozeném rozšíření těchto definic do jiných číselných oborů, kde umíme rozumným způsobem sčítat, násobit a *krátit* (tzv. *obory integrity* – např. $\mathbb{Q}, \mathbb{R}, \mathbb{Z}[\sqrt{2}], \mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}]$ apod.).

Příklad

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Přitom zde selhává i zaměnitelnost obou definic prvočíselnosti, *být nerozložitelný* (ireducibilní) je obecně slabší vlastnost než být *primitivní* (alternativní definice) – v tomto příkladu je 2 nerozložitelná, ale přitom $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, i když nedělí žádného z činitelů.

V $\mathbb{Z}[i]$ žádné takové potíže nenastávají, zde je rozklad na prvočísla jednoznačný: $6 = -i \cdot (1 + i)^2 \cdot 3$.

S pomocí programu SAGE, který budeme využívat, lze spočítat např. všechna prvočísla nebo všechna složená čísla v zadaném intervalu:

```
sage: prime_range(10,50)
[11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47]
sage: [n for n in range(10,30) if not is_prime(n)]
[10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28]
```

Největší společný dělitel

To, že v případě celých čísel prvočísla splňují i alternativní definici, lze snadno dokázat pomocí pojmu *největší společný dělitel*.

Největší společný dělitel

To, že v případě celých čísel prvočísla splňují i alternativní definici, lze snadno dokázat pomocí pojmu *největší společný dělitel*.

Definice

Mějme celá čísla a, b. Libovolné celé číslo m takové, že $m \mid a$, $m \mid b$ se nazývá *společný dělitel* čísel a, b. Společný dělitel $m \geq 0$ čísel a, b, který je dělitelný libovolným společným dělitelem čísel a, b, se nazývá *největší společný dělitel* čísel a, b a značí se (a, b).

Největší společný dělitel

To, že v případě celých čísel prvočísla splňují i alternativní definici, lze snadno dokázat pomocí pojmu *největší společný dělitel*.

Definice

Mějme celá čísla a, b. Libovolné celé číslo m takové, že $m \mid a$, $m \mid b$ se nazývá *společný dělitel* čísel a, b. Společný dělitel $m \geq 0$ čísel a, b, který je dělitelný libovolným společným dělitelem čísel a, b, se nazývá *největší společný dělitel* čísel a, b a značí se (a, b).
Analogicky se definuje nejmenší společný násobek $[a, b]$.

Největšího společného dělitele lze u malých čísel vyčíst z obrázku - viz `http://wiki.sagemath.org/interact/number_theory`.

Jak spočítat GCD?

Největšího společného dělitele lze jistě spočítat z rozkladu na prvočísla – pokud tedy umíme daná čísla rozložit.

```
sage: gcd(97 * 10^15, 19^20 * 97^2)
97
```

Ale co v případě, že chceme spočítat něco takového?

```
gcd(353684060262049920641282849809,\
97000000000000000)
```

Euklidův algoritmus

Ukazuje, že spočítat největšího společného dělitele je výpočetně daleko snazší než rozkládat čísla na prvočísla. Euklidův algoritmus je založen na větě o dělení se zbytkem (a v ní je rovněž skryt rozdíl např. mezi $\mathbb{Z}[i]$ a $\mathbb{Z}[\sqrt{-5}]$).

Euklidův algoritmus

Ukazuje, že spočítat největšího společného dělitele je výpočetně daleko snazší než rozkládat čísla na prvočísla. Euklidův algoritmus je založen na větě o dělení se zbytkem (a v ní je rovněž skryt rozdíl např. mezi $\mathbb{Z}[i]$ a $\mathbb{Z}[\sqrt{-5}]$).

Věta

Pro libovolně zvolená čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, m-1\}$ tak, že $a = qm + r$.

Euklidův algoritmus

Ukazuje, že spočítat největšího společného dělitele je výpočetně daleko snazší než rozkládat čísla na prvočísla. Euklidův algoritmus je založen na větě o dělení se zbytkem (a v ní je rovněž skryt rozdíl např. mezi $\mathbb{Z}[i]$ a $\mathbb{Z}[\sqrt{-5}]$).

Věta

Pro libovolně zvolená čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \dots, m-1\}$ tak, že $a = qm + r$.

Věta (Euklidův algoritmus)

Nechť a_1, a_2 jsou přirozená čísla. Pro každé $n \geq 3$, pro které $a_{n-1} \neq 0$, označme a_n zbytek po dělení čísla a_{n-2} číslem a_{n-1}. Pak po konečném počtu kroků dostaneme $a_k = 0$ a platí $a_{k-1} = (a_1, a_2)$.

Z Euklidova algoritmu vyplývá jedno z nejužitečnějších tvrzení v elementární teorii čísel – tzv. Bezoutova věta.

Věta (Bezoutova)

Pro libovolná celá čísla a, b *existuje jejich největší společný dělitel* (a, b)*, přitom existují celá čísla* k, l *tak, že* $(a, b) = ka + lb$*.*

Z Euklidova algoritmu vyplývá jedno z nejužitečnějších tvrzení v elementární teorii čísel – tzv. Bezoutova věta.

Věta (Bezoutova)

Pro libovolná celá čísla a, b *existuje jejich největší společný dělitel* (a, b), *přitom existují celá čísla* k, l *tak, že* $(a, b) = ka + lb$.

Příklad

1. Rozhodněte, jestli je možné pomocí mincí o nominální hodnotě 5 a 7 Kč zaplatit (s vracením) jakoukoliv částku.

Z Euklidova algoritmu vyplývá jedno z nejužitečnějších tvrzení v elementární teorii čísel – tzv. Bezoutova věta.

Věta (Bezoutova)

Pro libovolná celá čísla a, b existuje jejich největší společný dělitel (a, b), přitom existují celá čísla k, l tak, že $(a, b) = ka + lb$.

Příklad

1. Rozhodněte, jestli je možné pomocí mincí o nominální hodnotě 5 a 7 Kč zaplatit (s vracením) jakoukoliv částku.
2. Bruce Willis a Samuel Jackson mají ve filmu Smrtonosná past 3 za úkol zlikvidovat bombu pomocí 4 galonů vody, přičemž k dispozici mají pouze nádoby na 3, resp. 5 galonů.

Z Euklidova algoritmu vyplývá jedno z nejužitečnějších tvrzení v elementární teorii čísel – tzv. Bezoutova věta.

Věta (Bezoutova)

Pro libovolná celá čísla a, b *existuje jejich největší společný dělitel* (a, b)*, přitom existují celá čísla* k, l *tak, že* $(a, b) = ka + lb$.

Příklad

1. Rozhodněte, jestli je možné pomocí mincí o nominální hodnotě 5 a 7 Kč zaplatit (s vracením) jakoukoliv částku.
2. Bruce Willis a Samuel Jackson mají ve filmu Smrtonosná past 3 za úkol zlikvidovat bombu pomocí 4 galonů vody, přičemž k dispozici mají pouze nádoby na 3, resp. 5 galonů.
3. Mezi největším společným dělitelem a nejmenším společným násobkem celých čísel a, b platí vztah $|a \cdot b| = (a, b) \cdot [a, b]$.


3
5

Důležité důsledky

Věta

Jsou-li a, b nesoudělná celá čísla a platí-li $a \mid b \cdot c$, pak nutně $a \mid c$.

Důležité důsledky

Věta

Jsou-li a, b *nesoudělná celá čísla a platí-li* $a \mid b \cdot c$*, pak nutně* $a \mid c$.

Věta

Pokud je p *prvočíslo, pak splňuje i alternativní definici prvočíselnosti.*

Důležité důsledky

Věta

Jsou-li a, b nesoudělná celá čísla a platí-li $a \mid b \cdot c$, pak nutně $a \mid c$.

Věta

Pokud je p prvočíslo, pak splňuje i alternativní definici prvočíselnosti.

Důkaz základní věty aritmetiky

Teprve nyní jsme schopni základní větu aritmetiky (alespoň v náznaku) dokázat.

Příklad

Dobrou vlastností Euklidova algoritmu (i jeho rozšíření, které zároveň najde koeficienty do Bezoutovy rovnosti) je to, že je velmi efektivní. Zatímco rozkládat čtyřciferná čísla na prvočísla na papíře většině z nás zabere asi dost času, spočítat největšího společného dělitele dvou takových čísel je daleko snazší. A podobně je na tom i počítač (i když s čísly podstatně většími – o několika stovkách cifer).

Příklad

Dobrou vlastností Euklidova algoritmu (i jeho rozšíření, které zároveň najde koeficienty do Bezoutovy rovnosti) je to, že je velmi efektivní. Zatímco rozkládat čtyřciferná čísla na prvočísla na papíře většině z nás zabere asi dost času, spočítat největšího společného dělitele dvou takových čísel je daleko snazší. A podobně je na tom i počítač (i když s čísly podstatně většími – o několika stovkách cifer).

```
sage: gcd(10^2016+1,19^1000-1)
1
sage: xgcd(42,27)
(3, 2, -3)
```

Příklad

Dobrou vlastností Euklidova algoritmu (i jeho rozšíření, které zároveň najde koeficienty do Bezoutovy rovnosti) je to, že je velmi efektivní. Zatímco rozkládat čtyřciferná čísla na prvočísla na papíře většině z nás zabere asi dost času, spočítat největšího společného dělitele dvou takových čísel je daleko snazší. A podobně je na tom i počítač (i když s čísly podstatně většími – o několika stovkách cifer).

```
sage: gcd(10^2016+1,19^1000-1)
1
sage: xgcd(42,27)
(3, 2, -3)
```

Pro další úvahy si všimněme, že Sage umí velmi rychle odpovědět na otázku, jestli je nějaké číslo prvočíslo, přitom jej ale často neumí rozložit (a dokonce nezná ani žádného dělitele).

```
sage: is_prime(10^2016+1)
```

Eulerova funkce φ

Definice

Nechť $n \in \mathbb{N}$. Definujme Eulerovu funkci φ předpisem

$$\varphi(n) = \left|\{a \in \mathbb{N}; 0 < a \leq n,\ (a, n) = 1\}\right|$$

Eulerova funkce φ

Definice

Nechť $n \in \mathbb{N}$. Definujme Eulerovu funkci φ předpisem

$$\varphi(n) = \left|\{a \in \mathbb{N}; 0 < a \leq n,\ (a, n) = 1\}\right|$$

Věta

Nechť $n \in \mathbb{N}$, jehož rozklad je tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Pak

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Důkaz.

1. Pomocí principu inkluze a exkluze na základě zjištění počtu čísel soudělných s n v určitém intervalu.

$\square$

Důkaz.

1. Pomocí principu inkluze a exkluze na základě zjištění počtu čísel soudělných s n v určitém intervalu.
2. Tvrzení lze odvodit i jiným způsobem na základě poznatku $(n, ab) = 1 \iff (n, a) = 1 \wedge (n, b) = 1$, spolu se snadno odvoditelným výsledkem

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1) \cdot p^{\alpha-1}.$$

$\square$

Plán přednášky

Kongruence

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

Definice

Jestliže dvě celá čísla a, b mají při dělení přirozeným číslem m týž zbytek r, kde $0 \leq r < m$, nazývají se a, b *kongruentní modulo* m, tj. $a \equiv b \pmod{m}$.

Kongruence

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

Definice

Jestliže dvě celá čísla a, b mají při dělení přirozeným číslem m týž zbytek r, kde $0 \le r < m$, nazývají se a, b *kongruentní modulo* m, tj. $a \equiv b \pmod{m}$.

Lemma

Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ *jsou následující podmínky ekvivalentní:*

1. $a \equiv b \pmod{m}$,
2. $a = b + mt \quad$ *pro vhodné* $t \in \mathbb{Z}$,
3. $m \mid a - b$.

Vlastnosti kongruencí

Vlastnosti

1. Kongruence podle téhož modulu můžeme sčítat a násobit.

Vlastnosti kongruencí

Vlastnosti

1. Kongruence podle téhož modulu můžeme sčítat a násobit.
2. K libovolné straně kongruence můžeme přičíst jakýkoliv násobek modulu.

Vlastnosti kongruencí

Vlastnosti

1. Kongruence podle téhož modulu můžeme sčítat a násobit.
2. K libovolné straně kongruence můžeme přičíst jakýkoliv násobek modulu.
3. Obě strany kongruence je možné umocnit na totéž přirozené číslo. Obě strany kongruence je možné vynásobit stejným celým číslem.

Vlastnosti kongruencí

Vlastnosti

1. Kongruence podle téhož modulu můžeme sčítat a násobit.
2. K libovolné straně kongruence můžeme přičíst jakýkoliv násobek modulu.
3. Obě strany kongruence je možné umocnit na totéž přirozené číslo. Obě strany kongruence je možné vynásobit stejným celým číslem.
4. Obě strany kongruence můžeme vydělit jejich společným dělitelem, jestliže je tento dělitel nesoudělný s modulem.

Vlastnosti kongruencí

Vlastnosti

1. Kongruence podle téhož modulu můžeme sčítat a násobit.
2. K libovolné straně kongruence můžeme přičíst jakýkoliv násobek modulu.
3. Obě strany kongruence je možné umocnit na totéž přirozené číslo. Obě strany kongruence je možné vynásobit stejným celým číslem.
4. Obě strany kongruence můžeme vydělit jejich společným dělitelem, jestliže je tento dělitel nesoudělný s modulem.
5. Jestliže kongruence $a \equiv b$ platí podle různých modulů $m_1, \ldots, m_k$, platí i podle modulu, kterým je nejmenší společný násobek $[m_1, \ldots, m_k]$ těchto čísel.

Některé důležité věty

Věta (Fermatova)

Je-li a nedělitelné prvočíslem p, pak $p \mid a^{p-1} - 1$, *tj.*

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

Některé důležité věty

Věta (Fermatova)

Je-li a nedělitelné prvočíslem p, pak $p \mid a^{p-1} - 1$, *tj.*

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

Důkaz.

Lze dokázat poměrně snadno například matematickou indukcí (pro přirozená a, na celá se již rozšíří snadno) ekvivalentní tvrzení $p \mid a^p - a$.

Některé důležité věty

Věta (Fermatova)

Je-li a nedělitelné prvočíslem p, pak $p \mid a^{p-1} - 1$, *tj.*

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

Důkaz.

Lze dokázat poměrně snadno například matematickou indukcí (pro přirozená a, na celá se již rozšíří snadno) ekvivalentní tvrzení $p \mid a^p - a$. Další možností je kombinatorický důkaz, kdy počet možných náhrdelníků o p špercích vybíraných z a druhů vyjde

Některé důležité věty

Věta (Fermatova)

Je-li a nedělitelné prvočíslem p, pak $p \mid a^{p-1} - 1$, tj.

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

Důkaz.

Lze dokázat poměrně snadno například matematickou indukcí (pro přirozená a, na celá se již rozšíří snadno) ekvivalentní tvrzení $p \mid a^p - a$. Další možností je kombinatorický důkaz, kdy počet možných náhrdelníků o p špercích vybíraných z a druhů vyjde

$$\frac{a^p - a}{p} + a.$$

□

Příklad (IMO 2005)

Uvažte posloupnost $a_1, a_2, \dots$ definovanou předpisem
$a_n = 2^n + 3^n + 6^n - 1 \quad n = 1, 2, \dots .$
Určete všechna přirozená čísla, která jsou nesoudělná se všemi členy této posloupnosti.

Příklad (IMO 2005)

Uvažte posloupnost $a_1, a_2, \dots$ definovanou předpisem
$a_n = 2^n + 3^n + 6^n - 1 \quad n = 1, 2, \dots$.
Určete všechna přirozená čísla, která jsou nesoudělná se všemi členy této posloupnosti.

Řešení

Z Fermatovy věty vyplyne, že pro $p > 3$ platí $p \mid a_{p-2}$. Dále $2 \mid a_1, 3 \mid a_2$, proto nevyhovuje jiné číslo než 1.

Některé důležité věty II.

Věta (Eulerova)

Je-li $a \in \mathbb{Z}$, $m \in \mathbb{N}$ *a* $(a, m) = 1$, *pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Některé důležité věty II.

Věta (Eulerova)

Je-li $a \in \mathbb{Z}$, $m \in \mathbb{N}$ *a* $(a, m) = 1$, *pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Věta (Wilsonova)

Přirozené číslo n *je prvočíslo, právě když*

$$(n-1)! \equiv -1 \pmod{n}.$$

Příklad

Pro každé $n \in \mathbb{N}$ určete

$$(n! + 1, (n + 1)!).$$

Příklad

Pro každé $n \in \mathbb{N}$ určete

$$(n! + 1, (n+1)!).$$

Řešení

Návod: rozlište případy, kdy $n+1$ je prvočíslo a kdy není.

Řešení lineárních kongruencí

Jak za chvíli uvidime, důležité pro nás bude umět „dělit číslo b číslem a modulo m“, přesněji řešit kongruence tvaru

$$ax \equiv b \pmod{m}$$

se zadanými celými $a, b, m \in \mathbb{N}$ a neznámými celými x.

Řešení lineárních kongruencí

Jak za chvíli uvidime, důležité pro nás bude umět „dělit číslo b číslem a modulo m“, přesněji řešit kongruence tvaru

$$ax \equiv b \pmod{m}$$

se zadanými celými $a, b, m \in \mathbb{N}$ a neznámými celými x.

Věta

Výše uvedená kongruence s neznámou x má řešení, právě když $(a, m) \mid b$.

Poznámka

Nejdůležitejším případem je situace, kdy $b = 1$; v takovém případě lze řešení (jediné modulo m) nalézt pomocí Euklidova algoritmu a Bezoutovy věty.

K motivačnímu příkladu – RSA

Připomeňme, že při inicializaci protokolu RSA si každý účastník volí veřejný klíč e a k němu dopočítává soukromý d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$.

K motivačnímu příkladu – RSA

Připomeňme, že při inicializaci protokolu RSA si každý účastník volí veřejný klíč e a k němu dopočítává soukromý d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Z předchozího víme, že při znalosti e a $\varphi(n)$ je zjištění d velmi jednoduché. Z postupu na dešifrování je vidět, že znalost d nám umožní přečíst libovolnou zprávu určenou jen uživateli s tímto soukromým klíčem.

K motivačnímu příkladu – RSA

Připomeňme, že při inicializaci protokolu RSA si každý účastník volí veřejný klíč e a k němu dopočítává soukromý d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Z předchozího víme, že při znalosti e a $\varphi(n)$ je zjištění d velmi jednoduché. Z postupu na dešifrování je vidět, že znalost d nám umožní přečíst libovolnou zprávu určenou jen uživateli s tímto soukromým klíčem. Bezpečnost RSA tedy závisí na tom, že nejsme schopni spočítat $\varphi(n)$ ani při znalosti n, tedy rozložit n na prvočísla.

Modulární výpočty

Zásadní pro praktické používání RSA (ale i dalších protokolů) je to, že jsme schopni velmi efektivně počítat „modulo m". Nejméně intuitivní (a přitom velmi podstatný) je fakt, že umíme velmi efektivně **umocňovat** modulo m, a to i na velmi vysoký exponent (uvědomme si, jak se zašifrovává a dešifrovává v RSA).

Modulární výpočty

Zásadní pro praktické používání RSA (ale i dalších protokolů) je to, že jsme schopni velmi efektivně počítat „modulo m“. Nejméně intuitivní (a přitom velmi podstatný) je fakt, že umíme velmi efektivně **umocňovat** modulo m, a to i na velmi vysoký exponent (uvědomme si, jak se zašifrovává a dešifrovává v RSA).
Efektivita algoritmu umocňování je založena na tom, že se výsledná mocnina počítá postupně a kdykoliv je to možné, redukuje se výsledek modulo m.

Modulární výpočty

Zásadní pro praktické používání RSA (ale i dalších protokolů) je to, že jsme schopni velmi efektivně počítat „modulo m“. Nejméně intuitivní (a přitom velmi podstatný) je fakt, že umíme velmi efektivně **umocňovat** modulo m, a to i na velmi vysoký exponent (uvědomme si, jak se zašifrovává a dešifrovává v RSA).

Efektivita algoritmu umocňování je založena na tom, že se výsledná mocnina počítá postupně a kdykoliv je to možné, redukuje se výsledek modulo m.

Stejně důležité (a asi ještě méně zřejmé) je to, že na rozdíl od modulárního umocňování je modulární **logaritmování** velmi časově náročné. Spousta praktických protokolů je založena na tom, že ani se znalostí $g, b, m \in \mathbb{Z}$ neumíme snadno určit pro které celé a platí

$$g^a \equiv b \pmod{m}.$$

Příklad

Vypočtěme dvě poslední cifry dekadického zápisu čísla 7^{91} tak, že určíme $7^{91} \pmod{100}$.

Příklad

Vypočtěme dvě poslední cifry dekadického zápisu čísla 7^{91} tak, že určíme $7^{91} \pmod{100}$.
Protože $(7, 100) = 1$, dostáváme z Eulerovy věty, že $7^{\varphi(100)} = 7^{40} \equiv 1 \pmod{100}$, odkud $7^{91} = 7^{40} \cdot 7^{40} \cdot 7^{11} \pmod{100}$. Zbývá tedy určit $7^{11} \pmod{100}$.

Příklad

Vypočtěme dvě poslední cifry dekadického zápisu čísla 7^{91} tak, že určíme $7^{91} \pmod{100}$.
Protože $(7, 100) = 1$, dostáváme z Eulerovy věty, že $7^{\varphi(100)} = 7^{40} \equiv 1 \pmod{100}$, odkud $7^{91} = 7^{40} \cdot 7^{40} \cdot 7^{11} \pmod{100}$. Zbývá tedy určit $7^{11} \pmod{100}$.
Zapišme exponent 11 ve dvojkové soustavě: $11 = (1011)_2$.
Následně pro $a = 7$ určíme $a^2, a^4, a^8, \dots \pmod{100}$ a spočítáme

$$a^{11} = a^8 \cdot a^2 \cdot a \equiv 1 \cdot 49 \cdot 7 \equiv 43 \pmod{100}.$$

Příklad

Vypočtěme dvě poslední cifry dekadického zápisu čísla 7^{91} tak, že určíme $7^{91} \pmod{100}$.

Protože $(7, 100) = 1$, dostáváme z Eulerovy věty, že $7^{\varphi(100)} = 7^{40} \equiv 1 \pmod{100}$, odkud $7^{91} = 7^{40} \cdot 7^{40} \cdot 7^{11} \pmod{100}$. Zbývá tedy určit $7^{11} \pmod{100}$.

Zapišme exponent 11 ve dvojkové soustavě: $11 = (1011)_2$.

Následně pro $a = 7$ určíme $a^2, a^4, a^8, \dots \pmod{100}$ a spočítáme

$$a^{11} = a^8 \cdot a^2 \cdot a \equiv 1 \cdot 49 \cdot 7 \equiv 43 \pmod{100}.$$

Všimněme si zejména, že vypočítat 7^{91} by nám dalo podstatně větší práci (přitom většinu získaných číslic vůbec nepotřebujeme).

Čínská zbytková věta (CRT)

Ve čtvrtém století se čínský matematik Sun Ze (Sun Tsu) ptal na číslo, které při dělení třemi dává zbytek 2, při dělení pěti zbytek 3 a při dělení sedmi je zbytek opět 2.

Řešení

Odpověď je (prý) ukryta v následující písni:

Čínská zbytková věta (CRT)

Ve čtvrtém století se čínský matematik Sun Ze (Sun Tsu) ptal na číslo, které při dělení třemi dává zbytek 2, při dělení pěti zbytek 3 a při dělení sedmi je zbytek opět 2.

Řešení

Odpověď je (prý) ukryta v následující písni:

孫子歌 Sunzi Ge

三人同行七十里
五樹梅花廿一枝
七子團圓正月半
一百零五轉回起

V moderní terminologii nás tedy zajímá, které přirozené číslo x vyhovuje soustavě kongruencí

$$
\begin{aligned}
x &\equiv 2 \pmod 3\\
x &\equiv 3 \pmod 5\\
x &\equiv 2 \pmod 7.
\end{aligned}
$$

Věta (Čínská zbytková věta)

Nechť $m_1, , \ldots, m_k \in \mathbb{N}$ *jsou po dvou nesoudělná,* $a_1, \ldots, a_k \in \mathbb{Z}$. *Pak platí: soustava*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

má jediné řešení modulo $m = m_1 \cdot m_2 \cdots m_k$.

Věta (Čínská zbytková věta)

Nechť $m_1, , \ldots, m_k \in \mathbb{N}$ *jsou po dvou nesoudělná,* $a_1, \ldots, a_k \in \mathbb{Z}$. *Pak platí: soustava*

$$x \equiv a_1 \pmod{m_1}$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k}$$

má jediné řešení modulo $m = m_1 \cdot m_2 \cdots m_k$.

Důkaz.

Označme $n_j = m/m_j$. Z předchozího vím, že kongruence $n_j \cdot y \equiv 1 \pmod{m_j}$ je řešitelná (a její řešení navíc umíme snadno určit pomocí Euklidova algoritmu). Označíme-li její řešení b_j, pak je snadno vidět, že $x = \sum_1^k b_j a_j n_j$ je hledaným řešením soustavy. □

Příklad

Řešme soustavu

$$
\begin{aligned}
x &\equiv 2 \pmod{3}\\
x &\equiv 3 \pmod{5}\\
x &\equiv 2 \pmod{7}.
\end{aligned}
$$

Je možné využít postupu z důkazu nebo si uvědomit, že z vlastností kongruencí plyne ihned $x \equiv 2 \pmod{21}, x \equiv 3 \pmod{5}$ a dosazením $x = 2 + 21k, k \in \mathbb{Z}$ dostaneme kongruenci $2 + 21k \equiv 3 \pmod{5}$, neboli $k \equiv 1 \pmod{5}$, odkud $x \equiv 23 \pmod{105}$.

Čínská zbytková věta nám umožní spoustu problémů a výpočtů zabývajících se velkými čísly paralelizovat (výpočet modulo složené $m_1 \cdot m_2$ lze provést na jednom počítači modulo m_1 a na druhém modulo m_2 a oba výsledky pak zkombinovat).

Čínská zbytková věta nám umožní spoustu problémů a výpočtů zabývajících se velkými čísly paralelizovat (výpočet modulo složené $m_1 \cdot m_2$ lze provést na jednom počítači modulo m_1 a na druhém modulo m_2 a oba výsledky pak zkombinovat).

Příklad

Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Čínská zbytková věta nám umožní spoustu problémů a výpočtů zabývajících se velkými čísly paralelizovat (výpočet modulo složené $m_1 \cdot m_2$ lze provést na jednom počítači modulo m_1 a na druhém modulo m_2 a oba výsledky pak zkombinovat).

Příklad

Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Řešení

Rozložme $3564 = 2^2 \cdot 3^4 \cdot 11$. Protože ani 2, ani 3, ani 11 nedělí číslo $23\,941$, platí $(23\,941, 3564) = 1$ a má tedy kongruence řešení.

Čínská zbytková věta nám umožní spoustu problémů a výpočtů zabývajících se velkými čísly paralelizovat (výpočet modulo složené $m_1 \cdot m_2$ lze provést na jednom počítači modulo m_1 a na druhém modulo m_2 a oba výsledky pak zkombinovat).

Příklad

Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Řešení

Rozložme $3564 = 2^2 \cdot 3^4 \cdot 11$. Protože ani 2, ani 3, ani 11 nedělí číslo 23 941, platí $(23\,941, 3564) = 1$ a má tedy kongruence řešení. Ze základních vlastností kongruencí vyplývá, že $x \in \mathbb{Z}$ je řešením dané kongruence, právě když je řešením soustavy

$$\begin{aligned} 23941x &\equiv 915 \pmod{2^2} \\ 23941x &\equiv 915 \pmod{3^4} \\ 23941x &\equiv 915 \pmod{11} \end{aligned}$$

Řešení (pokr.)

Vyřešíme nyní každou z kongruencí soustavy zvlášť a dostaneme ekvivalentní soustavu

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv -3 \pmod{81} \\ x &\equiv -4 \pmod{11}, \end{aligned}$$

jejímž řešením je $x \equiv -1137 \pmod{3564}$.

Příklad (IMO 1989)

Pro která $n \in \mathbb{N}$ existuje $N \in \mathbb{N}$ tak, že žádné z čísel

$$1 + N, 2 + N, \ldots, n + N$$

není mocninou prvočísla.

Příklad (IMO 1989)

Pro která $n \in \mathbb{N}$ existuje $N \in \mathbb{N}$ tak, že žádné z čísel

$$1+N, 2+N, \ldots, n+N$$

není mocninou prvočísla.

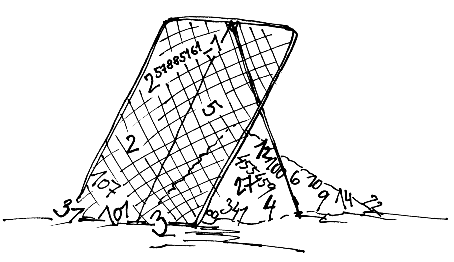
Řešení

1. Pro dané n položíme $N = ((n+1)!)^2 + 1$ a ukážeme, že splňuje zadání.
2. Buďte $p_1, p_2, \ldots, p_{2n}$ různá prvočísla. Díky CRT existuje $N \in \mathbb{N}$ tak, že $N \equiv -1 \pmod{p_1 p_2}$, $N \equiv -2 \pmod{p_3 p_4}, \ldots, N \equiv -n \pmod{p_{2n-1} p_{2n}}$. Takové N ale splňuje zadání.

Plán přednášky

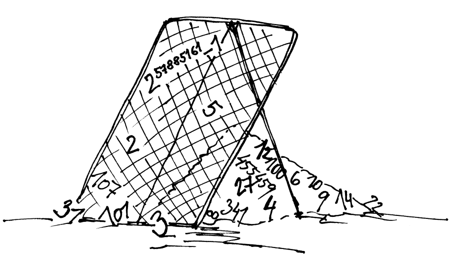
Eratosthenovo síto

Známá metoda, která poskytuje postup, jak nalézt dokonce všechna prvočísla až do jisté hranice.



Eratosthenovo síto

Známá metoda, která poskytuje postup, jak nalézt dokonce všechna prvočísla až do jisté hranice.



Její jediný, zato však zásadní, problém je časová náročnost – pro zjištění prvočísel až do velikosti N potřebujeme znát prvočísla až do velikosti $\sqrt{N}$, což je obvykle příliš mnoho.

Řád čísla modulo, primitivní kořen

Definice

Řádem čísla a modulo m, kde $(a, m) = 1$, nazveme nejmenší přirozené číslo r takové, že $a^r \equiv 1 \pmod{m}$.

Řád čísla modulo, primitivní kořen

Definice

Řádem čísla a modulo m, kde $(a, m) = 1$, nazveme nejmenší přirozené číslo r takové, že $a^r \equiv 1 \pmod{m}$.

Fakt

- $r \mid \varphi(m)$;
- modulo prvočíslo p existuje právě $\varphi(p-1)$ čísel řádu $\varphi(p) = p - 1$ modulo p (menších než p), jde o takzvané primitivní kořeny.

Kvadratické (ne)zbytky

Definice

Buď p prvočíslo. Číslo a splňující $(a,p)=1$ nazveme kvadratickým zbytkem modulo p, jestliže existuje x takové, že $x^2 \equiv a \pmod p$, v opačném případě jde o kvadratický nezbytek. Píšeme $(a/p)=1$, resp. $(a/p)=-1$ (Legendreův symbol). Dále pro $p \mid a$ píšeme $(a/p)=0$.

Kvadratické (ne)zbytky

Definice

Buď p prvočíslo. Číslo a splňující $(a,p)=1$ nazveme kvadratickým zbytkem modulo p, jestliže existuje x takové, že $x^2 \equiv a \pmod p$, v opačném případě jde o kvadratický nezbytek. Píšeme $(a/p)=1$, resp. $(a/p)=-1$ (Legendreův symbol). Dále pro $p \mid a$ píšeme $(a/p)=0$.

Fakt

- $(a/p) \equiv a^{\frac{p-1}{2}} \pmod p$.
- pro $a \equiv b \pmod p$ platí $(a/p)=(b/p)$.
- $(a \cdot b/p) = (a/p)\cdot(b/p)$.
- $(-1/p) = (-1)^{\frac{p-1}{2}}, (2/p) = (-1)^{\frac{p^2-1}{8}}, (p/q) = (q/p)\cdot(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Klasické testy s využitím kongruencí

Wilsonova věta dává sice nutnou i postačující podmínku prvočíselnosti, bohužel nikdo na světě dosud neumít *rychle* vypočítat faktoriál modulo velké číslo. Proto využijeme ostatní věty, které sice dávají pouze nutnou podmínku prvočíselnosti (*je-li p prvočíslo, pak ...*).

Klasické testy s využitím kongruencí

Wilsonova věta dává sice nutnou i postačující podmínku prvočíselnosti, bohužel nikdo na světě dosud neumít *rychle* vypočítat faktoriál modulo velké číslo. Proto využijeme ostatní věty, které sice dávají pouze nutnou podmínku prvočíselnosti (*je-li p prvočíslo, pak ...*).
Takovým testem je např. klasický Fermatův test plynoucí ze stejnojmenné věty.

Fermatův test

Existuje-li pro dané N nějaké $a \not\equiv 0 \pmod{N}$ takové, že $a^{N-1} \not\equiv 1 \pmod{N}$, pak N není prvočíslo.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N; pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N; pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.

Skutečně existují taková nehezká (nebo extrémně hezká?) složená čísla N, která splňují, že pro libovolné a nesoudělné s N platí $a^{N-1} \equiv 1 \pmod{N}$. Taková čísla se nazývají Carmichaelova, nejmenší z nich je $561 = 3 \cdot 11 \cdot 17$ (Dokažte) a teprve v roce 1992 se podařilo dokázat, že jich je dokonce nekonečně mnoho.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N; pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.

Skutečně existují taková nehezká (nebo extrémně hezká?) složená čísla N, která splňují, že pro libovolné a nesoudělné s N platí $a^{N-1} \equiv 1 \pmod{N}$.

Taková čísla se nazývají Carmichaelova, nejmenší z nich je $561 = 3 \cdot 11 \cdot 17$ (Dokažte) a teprve v roce 1992 se podařilo dokázat, že jich je dokonce nekonečně mnoho.

Fermatův test lze zlepšit s využitím kvadratických zbytků na Eulerův test $a^{\frac{N-1}{2}} \equiv (a/N) \pmod{N}$, ale výše zmíněný problém se zcela neodstraní ani tímto vylepšením.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N; pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.

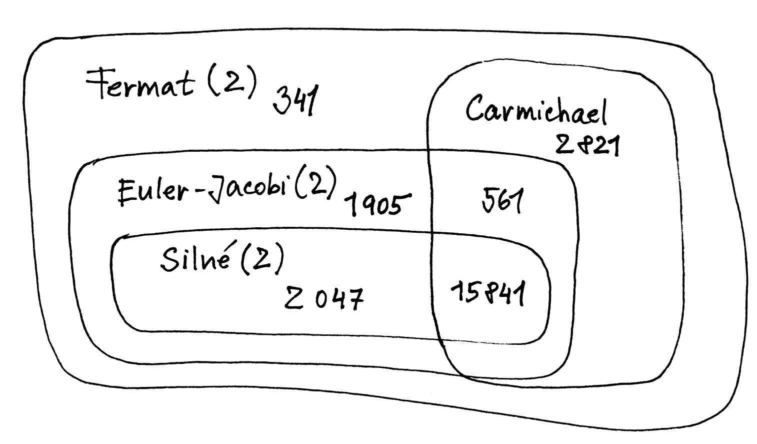
Skutečně existují taková nehezká (nebo extrémně hezká?) složená čísla N, která splňují, že pro libovolné a nesoudělné s N platí $a^{N-1} \equiv 1 \pmod{N}$.

Taková čísla se nazývají Carmichaelova, nejmenší z nich je $561 = 3 \cdot 11 \cdot 17$ (Dokažte) a teprve v roce 1992 se podařilo dokázat, že jich je dokonce nekonečně mnoho.

Fermatův test lze zlepšit s využitím kvadratických zbytků na Eulerův test $a^{\frac{N-1}{2}} \equiv (a/N) \pmod{N}$, ale výše zmíněný problém se zcela neodstraní ani tímto vylepšením.

V praxi se často používají další vylepšení, zejména tzv. Rabin-Millerův test.

Různé typy pseudoprvočísel



Carmichaelova čísla

Věta (Korseltovo kritérium)

Složené číslo je Carmichaelovým číslem, právě když je nedělitelné čtvercem (square-free) a pro všechna prvočísla p dělící n platí $p - 1 \mid n - 1$.

Carmichaelova čísla

Věta (Korseltovo kritérium)

Složené číslo je Carmichaelovým číslem, právě když je nedělitelné čtvercem (square-free) a pro všechna prvočísla p dělící n platí $p - 1 \mid n - 1$.

Příklad

Dokažte, že čísla 2465 a 2821 jsou Carmichaelova.

Rabin-Millerův test na složenost

Věta

Nechť p je liché prvočíslo. Pišme $p - 1 = 2^t \cdot q$*, kde t je přirozené číslo a q je liché. Pak pro každé celé číslo a nedělitelné p buď platí* $a^q \equiv 1 \pmod{p}$ *nebo existuje* $e \in \{0, 1, \dots, t-1\}$ *splňující* $a^{2^e q} \equiv -1 \pmod{p}$.

Rabin-Millerův test na složenost

Věta

Nechť p je liché prvočíslo. Pišme $p-1 = 2^t \cdot q$, kde t je přirozené číslo a q je liché. Pak pro každé celé číslo a nedělitelné p buď platí $a^q \equiv 1 \pmod p$ nebo existuje $e \in \{0, 1, \dots, t-1\}$ splňující $a^{2^e q} \equiv -1 \pmod p$.

Lze ukázat, že pro lichá složená čísla N v roli prvočísla p v přechozí větě splňuje uvedenou podmínku nejvýše $\frac{1}{4}$ z čísel a (najdeme-li tedy a, které podmínku nesplňuje, našli jsme tzv. svědka složenosti).

Rabin-Millerův test na složenost

Věta

Nechť p je liché prvočíslo. Pišme $p - 1 = 2^t \cdot q$, kde t je přirozené číslo a q je liché. Pak pro každé celé číslo a nedělitelné p buď platí $a^q \equiv 1 \pmod{p}$ nebo existuje $e \in \{0, 1, \ldots, t-1\}$ splňující $a^{2^e q} \equiv -1 \pmod{p}$.

Lze ukázat, že pro lichá složená čísla N v roli prvočísla p v přechozí větě splňuje uvedenou podmínku nejvýše $\frac{1}{4}$ z čísel a (najdeme-li tedy a, které podmínku nesplňuje, našli jsme tzv. svědka složenosti).

Příklad

Pomocí SAGE dokážeme, že Carmichaelova čísla 2465 i 2821 jsou složená (díky bázi $a = 2$).

Rabin-Millerův test na složenost

Věta

Nechť p je liché prvočíslo. Pišme $p-1 = 2^t \cdot q$*, kde t je přirozené číslo a q je liché. Pak pro každé celé číslo a nedělitelné p buď platí* $a^q \equiv 1 \pmod{p}$ *nebo existuje* $e \in \{0, 1, \ldots, t-1\}$ *splňující* $a^{2^e q} \equiv -1 \pmod{p}$*.*

Lze ukázat, že pro lichá složená čísla N v roli prvočísla p v přechozí větě splňuje uvedenou podmínku nejvýše $\frac{1}{4}$ z čísel a (najdeme-li tedy a, které podmínku nesplňuje, našli jsme tzv. svědka složenosti).

Příklad

Pomocí SAGE dokážeme, že Carmichaelova čísla 2465 i 2821 jsou složená (díky bázi $a = 2$).

Složené číslo n, které není tímto testem odhaleno pomocí báze a se nazývá silné pseudoprvočíslo v bázi a. Např. 2047 je silné pseudoprvočíslo vzhledem k bázi 2, 121 vzhledem k bázi 3, ...

Test prvočíselnosti

Ukázali jsme si, jak je možné odhalit složená čísla. Co ale s těmi, která tento test za složená neoznačí? Jsou to prvočísla nebo čísla složená. K ověření toho slouží (časově daleko náročnější) testy na prvočíselnost.

Lucas-Lehmer

Pokud pro libovolný prvočíselný dělitel q čísla $N-1$ existuje a tak, že $a^{N-1} \equiv 1 \pmod{N}$, $a^{\frac{N-1}{q}} \not\equiv 1 \pmod{N}$, pak je N prvočíslo.

Test prvočíselnosti

Ukázali jsme si, jak je možné odhalit složená čísla. Co ale s těmi, která tento test za složená neoznačí? Jsou to prvočísla nebo čísla složená. K ověření toho slouží (časově daleko náročnější) testy na prvočíselnost.

Lucas-Lehmer

Pokud pro libovolný prvočíselný dělitel q čísla $N-1$ existuje a tak, že $a^{N-1} \equiv 1 \pmod{N}$, $a^{\frac{N-1}{q}} \not\equiv 1 \pmod{N}$, pak je N prvočíslo.

Důkaz.

Stačí dokázat, že $N-1$ dělí $\varphi(N)$. Pokud ne, tak existuje prvočíslo q a $r \in \mathbb{N}$ tak, že q^r dělí $N-1$, ale ne $\varphi(N)$. Řád e prvku a dělí $N-1$ (první podmínka) a nedělí $(N-1)/q$ (druhá podmínka), proto q^r dělí e. Navíc e dělí $\varphi(N)$, tedy i q^r dělí $\varphi(N)$, spor. $\square$

AKS – nedávná indická bomba

Předchozí test má tu nevýhodu, že je třeba umět kompletně rozložit $N-1$ na prvočísla. To je snadné třeba u Fermatových čísel, ale obvykle je to obtížné. Proto je užitečné mít k dispozici variantu tohoto testu, která kompletní faktorizaci nepožaduje – viz např. test Pocklingtona a Lehmera.

AKS – nedávná indická bomba

Předchozí test má tu nevýhodu, že je třeba umět kompletně rozložit $N-1$ na prvočísla. To je snadné třeba u Fermatových čísel, ale obvykle je to obtížné. Proto je užitečné mít k dispozici variantu tohoto testu, která kompletní faktorizaci nepožaduje – viz např. test Pocklingtona a Lehmera.

AKS

Veškeré předchozí testy (alespoň teoreticky) *strčili do kapsy* v roce 2002 indičtí matematici [a] Agrawal, Kayal a Saxena, kteří Fermatův test aplikovali v (jen o málo) složitější algebraické situaci a odvodili z něj test, který je polynomiální časové složitosti (do té doby se vůbec nevědělo, jakou složitost tohoto problému očekávat).

[a] nebo tedy spíše informatici

Výměna klíčů

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, ...).

Výměna klíčů

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, …).

- Dohoda stran na **modulu** m a primitivním kořenu g (veřejné)

Výměna klíčů

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974) Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, ...).

- Dohoda stran na **modulu** m a primitivním kořenu g (veřejné)
- Alice vybere náhodné a a pošle $g^a \pmod{m}$

Výměna klíčů

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, ...).

- Dohoda stran na **modulu** m a primitivním kořenu g (veřejné)
- Alice vybere náhodné a a pošle $g^a \pmod{m}$
- Bob vybere náhodné b a pošle $g^b \pmod{m}$

Výměna klíčů

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, ...).

- Dohoda stran na **modulu** m a primitivním kořenu g (veřejné)
- Alice vybere náhodné a a pošle $g^a \pmod{m}$
- Bob vybere náhodné b a pošle $g^b \pmod{m}$
- Společným klíčem pro komunikaci je $g^{ab} \pmod{m}$.

Dokončení motivačního příkladu RSA

Protože jsme schopni (díky počítači) rozložit n, jsme schopni zprávu dešifrovat:

```
C=239675027941280548756812205343466895417790207923642
n=374144419156711146897884040346152783797331507019777
e=240911337096020749615795248242245864391942105373709

bezout = xgcd(e, euler_phi(n))
d = Integer(mod(bezout[1], euler_phi(n))) ; d
```

Odtud umocněním

```
M=Mod(C,n)^d
```

dostaneme

$$M = 6988806982737769788478698689836976.$$

Ještě kvůli zobrazení upravme

```
L=list(reversed(M.lift().digits(100)))
```

$$L = [69, 88, 80, 69, 82, 73, 77, 69, 78, 84, 78, 69, 86, 89, 83, 69, 76]\,.$$

Celkem tak dostáváme

```
import string
S=string.joinfields(map(chr, L), "")
```

EXPERIMENTNEVYSEL.

Několik úloh na závěr k přemýšlení

1. Zjistěte, jak rozložit $n = p \cdot q$, znáte-li $\varphi(n)$.

Několik úloh na závěr k přemýšlení

1. Zjistěte, jak rozložit $n = p \cdot q$, znáte-li $\varphi(n)$.

Několik úloh na závěr k přemýšlení

1. Zjistěte, jak rozložit $n = p \cdot q$, znáte-li $\varphi(n)$.

Příklad

Rozložte $n = 31615577110997599711$, víte-li, že
$\varphi(n) = 31615577098574867424$.

Několik úloh na závěr k přemýšlení

1. Zjistěte, jak rozložit $n = p \cdot q$, znáte-li $\varphi(n)$.

Příklad

Rozložte $n = 31615577110997599711$, víte-li, že $\varphi(n) = 31615577098574867424$.

2. Navrhněte způsob, jak rozložit $n = p \cdot q$, víte-li, že p a q jsou podobně velká prvočísla.

Několik úloh na závěr k přemýšlení

1. Zjistěte, jak rozložit $n = p \cdot q$, znáte-li $\varphi(n)$.

Příklad

Rozložte $n = 316155771109975997111$, víte-li, že
$\varphi(n) = 316155770985748674 24$.

2. Navrhněte způsob, jak rozložit $n = p \cdot q$, víte-li, že p a q jsou podobně velká prvočísla.
3. Navrhněte způsob, jak rozložit n, pokud zjistíte k veřejnému klíči odpovídající soukromý klíč d.

Několik úloh na závěr k přemýšlení

1. Zjistěte, jak rozložit $n = p \cdot q$, znáte-li $\varphi(n)$.

Příklad

Rozložte $n = 31615577110997599711$, víte-li, že
$\varphi(n) = 31615577098574867424$.

2. Navrhněte způsob, jak rozložit $n = p \cdot q$, víte-li, že p a q jsou podobně velká prvočísla.
3. Navrhněte způsob, jak rozložit n, pokud zjistíte k veřejnému klíči odpovídající soukromý klíč d.
4. Kvůli rychlosti šifrování bývá někdy doporučováno použít malý veřejný klíč e. Ukažte, že pokud si zvolí $e = 3$ tři lidé, kterým posíláme tutéž zprávu M, může útočník, který komunikaci odposlouchává, zprávu snadno rozšifrovat.