KATEDRA ELEKTRONIKY A MULTIMEDIÁLNYCH TELEKOMUNIKÁCIÍ
ELEKTRONIKA A TELEKOMUNIKAČNÁ TECHNIKA
FEI TU KOŠICE

Aplikovaná kryptografia

2000/2001
4B.ročník

Vypracovali : Milan Podstrelenec
Andrea Tadlová

FERMATOV TEST

Fermatova veta hovorí, že ak *n* je prvočíslo a *a* je nejaké celé číslo, $1 \le a \le n$-1, potom $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$. Z toho dôvodu, pre dané celé číslo *n*, ktorého prvočíselnosť je otázkou, hľadáme nejaké celé číslo *a* v tomto intervale, pre ktoré táto ekvivalencia nie je pravdivá, a to stačí k dokázaniu, že *n* je zložené číslo.

4.6 Definícia
Nech *n* je akési nepárne zložené celé číslo. Celé číslo *a*, $1 \le a \le n$-1, také že $a^{n-1} \neq 1 (\mathrm{mod}\, n)$ sa volá Fermat witness (k zloženému) pre *n.*
Obrátene, nájdenie celého čísla *a* medzi 1 a *n*-1 také, že $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, *n* sa javí ako prvočíslo v tom zmysle, že to zodpovedá Fermatovej vete pre základ *a.* Toto odôvodňuje nasledujúca definícia a Algoritmus 4.9.

4.7 Definícia
Nech *n* je nepárne zložené celé číslo a nech *a* je celé číslo, $1 \le a \le n$-1. Potom *n* sa nazýva pseudoprvočíslom k základu *a*, ak $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$. Potom celé číslo *a* sa volá Fermat liar pre *n*.

4.8 Príklad
(Pseudoprvočíslo) Zložené celé číslo *n* =341 (=11x31) je pseudoprvočíslo k základu 2, pretože $2^{340} \equiv 1 (\mathrm{mod}\, 341)$.

4.9 Algoritmus - Fermatov test prvočíselnosti
FERMAT (*n*,*t*)
vstup: nepárne celé číslo $n \ge 3$ a bezpečnostný parameter $t \ge 1$.
Výstup: odpoveď "prvočíslo" alebo "zložené číslo" na otázku : "Je *n* prvočíslo?"

1. Pre *i* od 1 do *t* urobte následovné:
   1.1 Zvoľte si náhodné celé číslo *a*, $2 \le a \le n - 2$.
   1.2 Vypočítajte $r = a^{n-1} \bmod n$ použitím Algoritmu 2.143.
   1.3 Ak $r \neq 1$, potom návrat (" zložené číslo").
2. Návrat ("prvočíslo").

Ak algoritmus 4.9 tvrdí "zložené číslo", potom *n* je určite zložené. Na druhej strane, ak algoritmus tvrdí "prvočíslo", potom nie je poskytnutý žiaden dôkaz, že *n* je skutočne prvočíslo. Jednako, pretože pseudoprvočísla pre daný základ *a* sú zriedkavo známe, Fermatova veta poskytuje správnu odpoveď na väčšinu vstupov, toto ale je úplne jednoznačné za predpokladu správnej odpovede (e. g. ak to spustíme s odlišnými základňami) na každý vstup. V skutočnosti tu sú zložené čísla, ktoré sú pseudoprvočíslami ku každému základu a, pre ktoré gcd (*a,n*) =1.

4.10 Definícia
Carmichaelove číslo *n* je také zložené celé číslo, že $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ pre všetky celé čísla *a*, ktoré spĺňajú gcd (*a, n*) = 1.

Ak *n* je Carmichaelovo číslo, potom len Fermat witnesses pre *n*, sú tie celé čísla *a*, $1 \le a \le n-1$, pre ktoré gcd (*a, n*) > 1. Teda, ak prvočíselné faktory od *n* sú všetky veľké, potom s vysokou pravdepodobnosťou Fermatov test tvrdí, že *n* je "prvočíslo", aj keď počet iterácií *t* je veľký. Tento nedostatok vo Fermatovom teste je vybratý v Solovay-Strassen a Miller-Rabin pravdepodobnostných prvočíselných testoch pri spoliehaní sa na kritériá, ktoré sú silnejšie než Fermatová veta.
Táto podčasť je ukončená niektorými faktami o Carmichaelových číslach. Ak prvočíslo rozložíme na činitele od *n* je známe, potom Fakt 4.11 sa môže používať k ľahkému určeniu či *n* je Carmichaelovo číslo.

4.11 Fakt (nutné a postačujúce podmienky pre Carmichaelove čísla)
Zložené celé číslo *n* je Carmichaelovo číslo vtedy a len vtedy, ak sú splnené nasledujúce dve podmienky:

(i) *n* je druhá mocnina-voľná, t.j., *n* nie je deliteľné mocninou hocijakého prvočísla
(ii) *p*-1 delí *n*-1 pre každý prvočíselný deliteľ *p* z *n*.

Význam od Faktu 4.11 je nasledovný.

4.12 Fakt Každé Carmichaelovo číslo je výsledkom od najmenej troch jednoznačných prvočísel.

4.13 Fakt (hranice pre niekoľko Carmichaelových čísel)

(i) tu je nekonečne veľa čísel Carmichaelových čísel. V skutočnosti, je tu viac než $n^{2/7}$ Carmichaelových čísiel v intervale [2,n], keď *n* je dostatočne veľké.
(ii) Najväčšia horná hranica známa pre C(n), číslo Carmichaelových čísel $\le n$, je:

$$C(n) \le n^{1-\{1+o(1)\}\ln\ln\ln n / \ln\ln n} \quad \text{pre } n \to \infty$$

Najmenšie Carmichaelovo číslo je n = 561 = 3 x 11 x 17. Carmichaelove čísla sú pomerne obmedzené; je tu len 105 212 Carmichaelových čísel $\le 10^{15}$.

Príklad 1: Fermatov test

Fermat (345, 10)
a.)
1.1 Voľba náhodného celého čísla *a*, v našom prípade *a*=127
1.2 Výpočet $r = a^{n-1} \bmod n$
$r = 127^{344} \bmod 345$
$r = 256 \quad \Rightarrow \quad$ "zložené číslo"

b.) *a*=333
$r = 333^{344} \bmod 345$
$r = 141 \quad \Rightarrow \quad$ "zložené číslo"

c.) a=250

$r = 250^{344} \bmod 345$

$r = 280 \quad \Rightarrow$ "zložené číslo"

d.) a=98

$r = 98^{344} \bmod 345$

$r = 331 \quad \Rightarrow$ "zložené číslo"

e.) a=23

$r = 23^{344} \bmod 345$

$r = 48 \quad \Rightarrow$ "zložené číslo"

f.) a=103

$r = 103^{344} \bmod 345$

$r = 256 \quad \Rightarrow$ "zložené číslo"

g.) a=159

$r = 159^{344} \bmod 345$

$r = 261 \quad \Rightarrow$ "zložené číslo"

h.) a=222

$r = 222^{344} \bmod 345$

$r = 6 \quad \Rightarrow$ "zložené číslo"

i.) a=269

$r = 269^{344} \bmod 345$

$r = 301 \quad \Rightarrow$ "zložené číslo"

j.) a=336

$r = 336^{344} \bmod 345$

$r = 246 \quad \Rightarrow$ "zložené číslo"

Príklad 2: Frematov test

Fermat (5059, 5)

a.)

1.1 Voľba náhodného celého čísla a, v našom prípade a=1100

1.2 Výpočet $r = a^{n-1} \bmod n$

$r = 1100^{5058} \bmod 5059$

$r = 1 \quad \Rightarrow$ "prvočíslo"

b.) a=3428

$r = 3428^{5058} \bmod 5059$

$r = 1 \quad \Rightarrow$ "prvočíslo"

c.) a=963

$r = 963^{5058} \bmod 5059$

$r = 1 \quad \Rightarrow \quad$ “prvočíslo“

d.) a=5003

$r = 5003^{5058} \bmod 5059$

$r = 1 \quad \Rightarrow \quad$ “prvočíslo“

e.) a=28

$r = 28^{5058} \bmod 5059$

$r = 1 \quad \Rightarrow \quad$ “prvočíslo“