AKS-algoritmus

Martin Sleziak

21. júna 2004

Testovanie prvočíselnosti

Známe algoritmy

- Eratostenovo sito
- Lucas-Lehmerov test
- Rabin-Millerov test
- ECPP
- APR a APRCL
- AKS-algoritmus

AKS-algoritmus

Výhody AKS-algoritmu

- prvý známy polynomiálny a deterministický algoritmus
- najjednoduchší matematický aparát

Nevýhody AKS-algoritmu

- pomalý v porovnaní s používanými algoritmami
- hoci je asymptoticky rýchlejší, pre "rozumné" vstupy zaostáva

AKS-algoritmus má (v súčasnej podobe) skôr teoretický než praktický význam.

Malá Fermatova veta

Veta

Nech p je prvočíslo. Potom

$$a^p \equiv a \pmod{p} \tag{1}$$

pre každé celé číslo a.

Veta

Nech $n \geq 2$ a $a \geq 0$ sú celé čísla.

(i) Ak n je prvočíslo, tak v okruhu $\mathbb{Z}_n[x]$ platí rovnosť

$$(x + a)^n = x^n + a.$$

(ii) Ak $(a, n) = 1$ a n nie je prvočíslo tak

$$(x + a)^n \neq x^n + a.$$

v okruhu polynómov $\mathbb{Z}_n[x]$.

Identita použitá v AKS-algoritme

Veta

Nech $n \geq 2$ je prirodzené číslo, p a r sú prvočísla, p delí n a $\ell = \lfloor 2\sqrt{r} \lg n \rfloor + 1$. Multiplikatívny rád čísla n modulo r označme d. Nech platia nasledujúce predpoklady:

(i) $(r, n) = 1$,

(ii) $p > r$,

(iii) $d > 4 \lg^2 n$,

(iv) pre každé a také, že $1 \leq a \leq \ell$ platí v $\mathbb{Z}_n[x]$

$$(x - a)^n = (x^n - a) \mod (x^r - 1).$$

Potom n je mocnina prvočísla p.

1. Ak $n = a^b$ pre nejaké prirodzené čísla $a, b > 1$, tak vrátime `FALSE`.
2. Hľadáme najmenšie prvočíslo r také, že platí buď $(n, r) > 1$ alebo $(n, r) = 1$ a multiplikatívny rád d čísla n modulo r je viac než $4 \lg^2 n$.
3. Ak $r = n$, tak vrátime `TRUE`.
4. Ak $(n, r) > 1$ tak vrátime `FALSE`.
5. Postupne pre a od 1 po $\ell = \lfloor 2\sqrt{r} \lg n \rfloor + 1$ testujeme rovnosť

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

   v $\mathbb{Z}_n[x]$. Akonáhle nájdeme najmenšie a, pre ktoré táto rovnosť neplatí, vrátime `FALSE`.
6. Ak rovnosť platí pre všetky $a = 1, \ldots, \ell$, tak vrátime `TRUE`.

p, r - prvočísla, $p \mid n$
$\ell = \lfloor 2\sqrt{r} \lg n \rfloor + 1$
d =Multiplikatívny rád n modulo r

(i) $(r, n) = 1$,

(ii) $p > r$,

(iii) $d > 4 \lg^2 n$,

(iv) Pre $a = 1, \ldots, \ell$ platí v $\mathbb{Z}_n[x]$

$$(x-a)^n = (x^n - a) \mod (x^r - 1).$$

$$\Downarrow$$

$$n = p^k$$

1. $n = a^b \rightarrow$ `FALSE`.
2. Hľadáme najmenšie prvočíslo r, že $(n, r) > 1$ alebo $(n, r) = 1$ a $d > 4 \lg^2 n$.
3. $r = n \rightarrow$ `TRUE`.
4. $(n, r) > 1 \rightarrow$ `FALSE`.
5. Ak pre $a = 1, \ldots, \ell$ platí

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

   v $\mathbb{Z}_n[x]$ vrátime `TRUE` inak `FALSE`.

Časová zložitosť

$f(x) = \tilde{O}(g(x))$, ak $f(x) = O(g(x)p(\lg g(x)))$ pre nejaký polynóm $p(x)$.
$r :=$ číslo nájdené v kroku 2
$r = O(\lg^5 n)$
Krok 1: Overenie či $n = a^b$ - $\tilde{O}(\lg^3 n)$
Krok 2: Overujeme či $r \mid n$ a opakovaným násobením zisťujeme multiplikatívny rád - $\tilde{O}(r \lg^2 n) = \tilde{O}(\lg^7 n)$
Krok 5: Overenie najviac ℓ kongruencií - $\tilde{O}(r^{1.5} \lg^3 n) = \tilde{O}(\lg^{10.5} n)$
AKS-algoritmus je **polynomiálny**.