WYKŁAD

Algorytm AKS : Agrawal, Kayal, Saxena , 2004

prof. — studenci

Dane: $n \in \mathbb{N}$
Pyt. czy $n \in P$?

Pierwszy det. alg. w PTIME, bez założeń (były chyba, ale np. przy zał. że hip. Riemanna (uogólniona) zachodzi)

9 stron, 1,5 wstępu, 1,5 bibliografii.

Po poprawkach w ogóle alg. elementarny, wcześniej prawie.

Nic zmienił nic w praktyce, bo np. test Millera-Rabina działa w $O(n^3)$ i z ~~prawd.~~ dużym prawd. daje dobry wynik.

Ten $\tilde{O}(n^{15/2})$, przy zał. hipotezy Sophie Germain o gęstości liczb pierwszych $\tilde{O}(n^6)$.
Tu $\tilde{O}(n^{21/2})$.

Jest modyf., co działa w $O(n^6)$ (Lenstra, Pomerance)

Główna idea (uogólnienie MTF):

Lemat 1
Niech $a \in \mathbb{Z}, n \in \mathbb{N}, n \geq 2, a \perp n$. Wtedy $n \in P$ wtw gdy

$$(x+a)^n = x^n + a \mod n$$

D-d

$\Rightarrow$ Niech $n \in P$. Przy x^n mamy $1 = 1$.
Przy x^0 mamy a^n, a. z MTF mamy, że $p \mid a^p - a$, czyli OK.
Przy x^i dla $0 < i < n$ mamy $\binom{n}{i} = \frac{n!}{i!(n-i)!}$
Łatwo zobaczyć, że $n \mid \binom{n}{i}$, nie dzieli mianownika, a dzieli licznik.

$\Leftarrow$ Niech $n \notin P$. Niech $q \mid n$ i $q^k \mid n$, ale $q^{k+1} \nmid n$.
Rozważmy wsp. $\binom{n}{q} = \frac{n!}{q!(n-q)!} = \frac{n^{\underline{q}}}{q!}$ $\quad q^k \mid n^{\underline{q}}$, ale $q^{k+1} \nmid n^{\underline{q}}$.
$q \mid q!$, czyli $q^k \nmid \binom{n}{q}$
Czyli $n \nmid \binom{n}{q}$.

Jednak sprawdzanie $(x+a)^n = x^n + a \mod n$

tak po prostu zajęłoby $O(n)$ czasu.

Pomysł: sprawdzać to modulo $(x^r - 1)$ dla odpowiednio dobranych ~~a~~ a oraz r. Pokażemy, że dla dość dużego zbioru to wystarczy i da się zrobić w PTIME.

Rząd a modulo r to najmniejsze k t.że $a^k = 1 \mod r$.

Oznaczamy: $O_r(a)$. $\varphi(r) = |\{n < r, n \perp r\}|$.

Łatwo zobaczyć, że $O_r(a) \mid \varphi(r)$ (bo $a^{\varphi(r)} \equiv 1 \mod r$).

dla $a \perp r$ tw. Eulera

ALGORYTM

1. Jeśli $n = a^b$ dla $a \in \mathbb{N}, b > 1$ to ZŁOŻONA
2. Znajdź najmniejsze r t.że $O_r(n) > \log^2 n$.
3. Jeśli $1 < (a,n) < n$ dla pewnego $a \leq r$ to ZŁOŻONA
4. Jeśli $n \leq r$ to PIERWSZA
5. Dla $a = 1$ do $\lfloor \sqrt{\phi(r)} \cdot \log n \rfloor$ rób

   jeśli $(x+a)^n \neq x^n + a \pmod{x^r - 1, n}$ to ZŁOŻONA
6. PIERWSZA

Fakt 1

Jeśli n pierwsza, to alg. zwraca pierwszą

D-d

Jasne, że nie może się zatrzymać w 1, 3 oraz z Lematu 1 w 5.

Czyli zatrzyma się w 4 lub w 6 i zwróci PIERWSZA

Chcemy pokazać, że jeśli $n \notin P$, to alg. zwróci ZŁOŻ.

Jak mógłby się pomylić? Na pewno nie w linii 4.

Czyli tylko w 6.

Trzeba pokazać, że nie ma ~~...~~ możliwości dojścia

do linii 6 dla $n \notin P$.

Fakt 2 $\boxed{\text{może na ćwiczeniach}}$

Istnieje $r \le \max(3, \lceil \log^5 n \rceil)$ t., że $O_r(n) > \log^2 n$.

D-d

Dla $n=2$ mamy $r=3$ i OK.

Załóżmy $n > 2$. Wtedy $\lceil \log^5 n \rceil > 10$. Niech $B = \lceil \log^5 n \rceil$

Niech r to najmniejsza liczba, która nie jest dzielnikiem

$$n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

Niech $r = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Jeśli $p_i | n$, to $p_i^{\alpha_i} | n^{\alpha_i} | n^{\lfloor \log B \rfloor}$, bo musi być $\alpha_i \le \log B$. Zatem jest pewne p_j t., że $p_j^{\alpha_j} \nmid$ iloczyn. i $p_j \nmid n$. Zatem $\frac{r}{(r,n)}$ też nie dzieli iloczynu.

Czyli $r \perp n$.

Poza tym $r \nmid n^i - 1$, czyli $n^i \not\equiv 1 \mod r$ dla $i \le \lfloor \log^2 n \rfloor$.

Czyli $O_r(n) > \log^2 n$. Czyli r jest OK. Trzeba pokazać jeszcze, że $r \le \lceil \log^5 n \rceil = B$.

Fakt: Dla $m \geq 7$ $LCM(1, 2, \dots, m) \geq 2^m$. (pół strony dowodu)

Mamy

$$n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1) < n^{\lfloor \log B \rfloor + \frac{1}{2}\log^2 n(\log^2 n - 1)} \leq n^{\log^4 n} = 2^{\log^5 n} \leq 2^B$$

Skoro $B \geq 10 > 7$, to $LCM(1, \ldots, B) \geq 2^B$. Więc $\exists\, r \in \{1, \ldots, B\}$ taki, że

$r \nmid$ iloczyn. Czyli $r \leq B$. OK. $\square$

Zobaczmy, że to implikuje, że alg. jest w PTIME.

$\boxed{\text{ĆW}}$ Krok 1 – ćwiczenie.

Krok 2 – spr. nie więcej niż $\lceil \log^5 n \rceil$, każde $\lceil \log^2 n \rceil$ kroków.

Krok 3 – NWD jest szybkie

Krok 4 – jasne

$\boxed{\text{ĆW}}$ Krok 5 – trzeba policzyć dla danego r jest to szybkie.

Prawą str. wyznaczmy łatwo. Lewą potęgujemy $\log n$ razy (tzn. rozkładamy na binarne i każdy czynnik tak). To proste szybkie potęgowanie.

Krok 6 – jasne

DOWÓD

Przechodzimy do trudniejszej części. Zakładamy, że doszliśmy do 6, chcemy, by $n \in P$.

Ponieważ $o_r(n) > 1$, to istnieje $p \in P$, $p \mid n$ taki, że $o_r(p) > 1$.

Mamy ~~...~~ $p > r$, bo przeszliśmy krok 3 (a może 4).

Ustalmy na cały dowód $p, r \in \mathbb{N}$. Oznaczmy $\ell = \lfloor \sqrt{\varphi(r)} \cdot \log n \rfloor$.

Mamy $(x+a)^n = x^n + a \pmod{x^r - 1, n}$

dla $0 \leq a \leq \ell$.

W szczególności też

$$(x+a)^n = x^n + a \pmod{x^r - 1, p} \qquad (1)$$

dla $0 \leq a \leq \ell$.

Dzięki Lematowi 1 mamy

$$(x+a)^p = x^p + a \pmod{x^r - 1, p} \qquad (2)$$

dla $0 \leq a \leq \ell$.

Fakt 3 Z tego wynika, że

$$(x+a)^{\frac{n}{p}} = x^{\frac{n}{p}} + a \pmod{x^r - 1, p} \qquad (?)$$

dla $0 \leq a \leq \ell$.

D-d $\boxed{\text{ĆW}}$

Niech $f \in F_p[x]$ dla $p \in P$. Wtedy z MTF wynika, że $f(x^p) = [f(x)]^p$.

Mamy więc

$$\left(x^{\frac{n}{p}} + a\right)^p \underset{\substack{\text{fakt pow.}\\ \text{(chyba tego}\\ \text{nie trzeba)}}}{=} \left(x^{p \cdot \frac{n}{p}} + a\right) = x^n + a \underset{(1)}{=} (x+a)^n = (x+a)^{p \cdot \frac{n}{p}} \pmod{x^r - 1, p}$$

Mamy

$f = x^{\frac{n}{p}} + a$, $g = (x+a)^{\frac{n}{p}}$. Mamy $f^p = g^p$, chcemy $f = g$.

$(f-g)^p = f^p - g^p$ ~~mod p~~ w $F_p[x]$, stąd $(f-g)^p = 0$ w $F_p[x]/x^r - 1$

To wychodzi dalej używając wiel. cyklotomicznych, ale może da się inaczej

$\square$

Def. 1 Mówimy, że dla wiel. $f(x)$ liczba $m \in \mathbb{N}$ jest introspektywna jeśli

$$f(x)^m = f(x^m) \pmod{x^r - 1, p}$$

Czyli np. $n, p, \frac{n}{p}$ są introspektywne dla $(x+a)$ dla $0 \le a \le \ell$.

Fakt 4

Jeśli m, k są intr. dla $f(x)$, to $m \cdot k$ też.

D-d

Ponieważ k jest intr., to

$$f(x)^{m \cdot k} = f(x^k)^m \pmod{x^r - 1, p}$$

$$f(x^k)^m = f(x^{km}) \pmod{x^{kr} - 1, p}$$

$$= f(x^{km}) \pmod{x^r - 1, p}, \text{ bo } x^r - 1 \mid x^{kr} - 1$$

$\square$

Podobnie

Fakt 5

Jeśli m jest intr. dla $f(x)$ i $g(x)$, to dla $f(x) \cdot g(x)$ też.

D-d

$$[f(x) \cdot g(x)]^m = f(x)^m \cdot g(x)^m = f(x^m) \cdot g(x^m) \pmod{x^r - 1, p}$$

W związku z tym każda liczba ze zbioru $I = \{ (\frac{n}{p})^i p^j \mid i,j \geq 0 \}$ jest introspektywna dla każdego wielomianu ze zbioru $P = \{ \prod_{a=0}^{\ell} (x+a)^{e_a} \mid e_a \geq 0 \}$.

Na bazie tego zdefiniujemy dwie grupy, które będą ~~ważne~~ kluczowe w dowodzie.

Niech pierwsza grupa ~~to~~ G to zbiór reszt liczb z I modulo r.

To podgrupa Z_r^*, bo $n \perp r$, $p \perp r$. Niech $|G| = t$.

G jest generowane przez n i p mod r, ponieważ $o_r(n) > \log^2 n$, to też $t > \log^2 n$.

Teraz przechodzimy do drugiej grupy. Niech $Q_r(x)$ to r-ty wiel. cyklotomiczny nad F_p. $Q_r(x) \mid x^r - 1$ (bo to tylko niektóre pierwiastki) ~~...~~.

Oprócz tego

$\boxed{\text{Św}}$ może ($^3/_2$ strony dowodu)

<u>Fakt 6</u> [LN86 - Intr. to finite fields and their appl.]

$Q_r(x)$ rozkłada się na ~~...~~ nierozkładalne czynniki rzędu $o_r(p)$

(zbaczmy, że $\deg Q_r(x) = \varphi(r)$, czyli $\underset{\text{istotnie}}{\underline{\quad}}$ $o_r(p) \neq \varphi(r) = \deg Q_r(x)$)

Niech $h(x)$ będzie jednym z takich czynników.

~~Jest~~ Ponieważ $o_r(p) > 1$, to $\deg h(x) > 1$.

Druga grupa to $\mathcal{G}$. To są wszystkie reszty wielomianów z P modulo $h(x), p$. ~~...~~ Grupa $\mathcal{G}$ jest generowana przez $x, x+1, \ldots, x+\ell$ mod $h(x), p$ (czyli w ciele $F_p[x]/h(x)$).

Reszta dowodu to 3 lematy pokazujące, że:

- $|\mathcal{G}| \geq \binom{t+l}{t-1}$ (lemat 2)
- $|\mathcal{G}| \leq n^{\sqrt{t}}$ o ile n nie jest potęgą p (lemat 3)
- $\binom{t+l}{t-1} > n^{\sqrt{t}}$ (lemat 4)

Czyli n to potęga p, czyli $n=p$, czyli $n \in P$.

Dlaczego to tak idzie – nie wiem. Pewnie to już trochę techniczne próby dopasowania tego.

Jednak pewnie jest jakaś idea dlaczego liczymy $|\mathcal{G}|$.

Lemat 2

$|\mathcal{G}| \geq \binom{t+l}{t-1}$

D-d Niech $F = F_p[x]/h(x)$

Wiemy, że $h(x) \mid Q_r(x) \mid X^r - 1$, więc $X^r = 1 \mod h(x)$, więc $X^r = 1$ w F.

$\boxed{?}$ Z jakiegoś powodu $X^k \neq 1$ w F dla $k<r$.

Pokażemy teraz, że każde dwa wielomiany stopnia $<t$ z P mapują się na różne rzeczy w F. Potem pokażemy, że jest ich co najmniej $\binom{t+l}{t-1}$.

Załóżmy, że $f(x) = g(x)$ w F. Niech $m \in I$.

Mamy $f(x^m) = g(x^m)$ w F. Zatem x^m to pierwiastek $Q(y) = f(y) - g(y)$ dla każdego $m \in I$. Ponieważ $m \perp r$ ($\mathcal{G}$ jest to podgrupa $\mathbb{Z}_r^*$), to X^m jest pierwiastkiem z jedynki st. dokładnie r.

A więc jest co najmniej $|\mathcal{G}|=t$ różnych pierwiastków z 1 st. dokł. r.

Jednak st. $Q < t$ z tego jak wybraliśmy f i g.

Sprz. z zał. że $f = g$ w F.

(ostatnie, że $x^i \neq x^j$, czyli $h \nmid x^{j-i}$

Teraz policzmy ile jest takich wiel. (przynajmniej).

Mamy $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor < \sqrt{r} \log n < r$ oraz $p > r$
(krok 3 i ćw. 4)

Zatem ~~to~~ dla $1 \le i \ne j \le l$ mamy $i \ne j$ w F_p.

Zatem $X, X+1, \dots, X+l$ są różne w F. Ponieważ $\deg h(x) > 1$, to $X+a \ne 0$ dla $0 \le a \le l$. A więc jest min. $l+1$ różnych wiel. st. 1. Żeby mieć ~~st. ...~~ st. ~~...~~ $< t$, to $t-1$ rzeczy wst. w $l+2$ miejsc.

Bierzemy $l+1$ barier i wstawiamy w $t-1$ rzeczy.

No to trzeba wybrać $t-1$ rzeczy z $t-1+l+1$ miejsc, wychodzi

~~...~~ $\binom{t+l}{t-1}$. $\square$

Lemat 3

Jeśli n nie jest potęgą p, to $|\mathcal{G}| \le n^{\sqrt{t}}$.

D-d

Rozważmy $\hat{I} = \{ (\frac{n}{p})^i \cdot p^j \mid 0 \le i,j \le \lfloor \sqrt{t} \rfloor \} \subseteq I$

Jeśli n nie jest potęgą p, to $\hat{I}$ ma ~~...~~ $(\lfloor \sqrt{t} \rfloor + 1)^2 > t$ różnych elementów. Ponieważ $|G| = t$ to wśród wszystkich reszt liczb z I modulo r, to pewne dwie liczby z $\hat{I}$ mają tą samą resztę.

Niech będzie to m_1 i m_2, $m_1 > m_2$. Wtedy

~~$X^{m_1} = X^{m_2} \mod X^r - 1$~~

$$X^{m_1} = X^{m_2} \mod X^r - 1$$

~~...~~ Niech $f(x) \in P$. Wtedy

$$f(x)^{m_1} = f(X^{m_1}) = f(X^{m_2}) = f(x)^{m_2} \qquad (\mathrm{mod}\ X^r - 1, p)$$

Zatem $f(x)^{m_1} = f(x)^{m_2}$ w F.

A więc $f(x) \in G$ jest pierwiastkiem wielomianu

$Q'(Y) = Y^{m_1} - Y^{m_2}$ w F. Skoro $f(x)$ to dowolny element G, to $\deg Q' \geq |G|$.

Jednak $\deg Q' = m_1 \leq \left(\frac{n}{p} \cdot p\right)^{\lfloor \sqrt{t} \rfloor} = n^{\lfloor \sqrt{t} \rfloor}$.

Zatem $|G| \leq n^{\lfloor \sqrt{t} \rfloor}$ □

Lemat 4

$t \leq \varphi(r)$

$t > \log^2 n$

$l = \lfloor \sqrt{\varphi(r)} \log n \rfloor$

$$\binom{t+l}{t-1} > n^{\sqrt{t}}$$

D-d

$\boxed{EW?}$

bo $t > \log^2 n$, czyli $t > \sqrt{t} \log n$, czyli $t \geq \lfloor \sqrt{t} \log n \rfloor + 1$

$\boxed{EW}$ Pokażcie, że dla $x \geq y$ zachodzi $\binom{x+a}{x} \geq \binom{y+a}{y}$

$$\binom{t+l}{t-1} \geq \binom{\lfloor \sqrt{t} \log n \rfloor + 1 + l}{\lfloor \sqrt{t} \log n \rfloor + 1 - 1}$$

$\binom{2n+1}{n} > 2^n$

$\left(\frac{2^{2n+1}}{2n+2}\right)$

$$\geq \binom{2 \lfloor \sqrt{t} \log n \rfloor + 1}{\lfloor \sqrt{t} \log n \rfloor} > 2^{\lfloor \sqrt{t} \log n \rfloor + 1}$$

pokażcie

$\binom{x}{a} \geq \binom{y}{a}$

dla $x \geq y$

$\lfloor \sqrt{t} \log n \rfloor > \lfloor \log^2 n \rfloor \geq 1$

to prawda potw. dla $\binom{2n+1}{n} > 2^n$

$$\geq 2^{\sqrt{t} \log n} = n^{\sqrt{t}}$$

□