WIELOMIANOWY TEST PIERWSZOŚCI

Algorytm AKS.

A : Manindra AGRAWAL `manindracse.iitk.ac.in`
K : Neeraj KAYAL `kayalncse.iitk.ac.in`
S : Nitin SAXENA `ninitsacse.iitk.ac.in`

Department of Computer Science & Engineering
Indian Institute of Technology Kanpur
Kanpur – 208016, INDIA

`http://www.cse.iitk.ac.in/primality.pdf`

Inne przydatne adresy:

`http://cr.yp.to/papers/aks.ps`
Daniel J. Bernstein
An Exposition of the AKS Primality-Proving Theorem

`http://www.lix.polytechnique.fr/Labo/Francois.Morain/aks-f.pdf`
F. Morain
Primalité théorique et primalité pratique ou AKS vs. ECPP

`http://mathworld.wolfram.com/news/2002-08-07_primtest/`

Wiele przydatnych adresów znajduje się na stronie
`http://www.fatphil.org/maths/AKS/`

W szczególności warto zobaczyć strony
`http://www.scs.carleton.ca/~michiel/primes.ps.gz`
`http://www.tcs.tifr.res.in/~jaikumar/mypage.html`
`http://www.ma.utexas.edu/users/voloch/prepront.html`

GŁÓWNY POMYSŁ

Twierdzenie 1. Załóżmy, że $\mathrm{NWD}(a,p)=1$. Liczba p jest pierwsza wtedy i tylko wtedy, gdy

$$(X-a)^p \equiv (X^p - a) \pmod{p}.$$

Uwaga. Wyrażenia $(X-a)^p$ i (X^p-a) stojące po obu stronach znaku $\equiv$ w powyższej kongruencji są wielomianami stopnia p. Kongruencję tę należy rozumieć tak, że te wielomiany są identyczne w pierścieniu wielomianów $\mathbb{Z}_p[X]$.

Dowód. Dowodzimy dwóch implikacji.

- Jeśli liczba p jest pierwsza oraz $0<k<p$, to $p \mid \binom{p}{k}$, skąd wynika, że w pierścieniu $\mathbb{Z}_p[X]$ mamy równość $(X-a)^p = X^p - a^p$. Z małego twierdzenia Fermata wynika, że $a^p \equiv a \pmod{p}$, co dowodzi, że $(X-a)^p = X^p - a$.

- Jeśli liczba p jest złożona, to bierzemy dzielnik pierwszy q liczby p. Załóżmy, że $q^k \parallel p$. Wtedy
$$\binom{p}{q} = \frac{p(p-1)\cdot\ldots\cdot(p-q+1)}{q!}.$$
Liczby $p-1,\ldots,p-q+1$ nie dzielą się przez q, a więc $q^k \parallel p(p-1)\cdot\ldots\cdot(p-q+1)$. Z drugiej strony, $q^1 \parallel q!$. Zatem
$$q^{k-1} \parallel \frac{p(p-1)\cdot\ldots\cdot(p-q+1)}{q!} = \binom{p}{q}.$$
Stąd wynika, że $q^k \not\mid \binom{p}{q}$, a zatem $p \not\mid \binom{p}{q}$. Współczynnik stojący przy X^q w wielomianie $(X-a)^p$ jest równy $\binom{p}{q}a^{p-q}$. Ponieważ $p \not\mid \binom{p}{q}$ oraz $\mathrm{NWD}(a,p)=1$, więc ten współczynnik jest niezerowy w pierścieniu $\mathbb{Z}_p$. Zatem wielomian $(X-a)^p$ jest różny od wielomianu $X^p - a$ w pierścieniu $\mathbb{Z}_p[X]$. ♠

Sprawdzenie, czy wielomiany $(X-a)^p$ i X^p-a są identyczne nie może być wykonane w czasie wielomianowym: trzeba obliczyć $p-1$ współczynników. Dlatego dobieramy liczbę r mniejszą od p i sprawdzamy, czy

$$(X-a)^p \equiv (X^p-a) \pmod{X^r-1, p}$$

dla dostatecznie wielu a. Inaczej mówiąc, sprawdzamy, czy wielomiany $(X-a)^p$ i X^p-a przystają do siebie modulo wielomian X^r-1 w pierścieniu $\mathbb{Z}_p[X]$.

Wielomian stopnia mniejszego od r ma r współczynników. Obliczenie wszystkich współczynników wielomianu $(X-a)^p$ wymaga co najwyżej $2p$ mnożeń wielomianów stopnia mniejszego od p (za pomocą algorytmu iterowanego podnoszenia do kwadratu). Jeżeli liczba r jest dostatecznie mała, to wykonywana liczba działań jest wielomianowa względem rozmiaru danych. Wystarczy zatem pokazać, że można się ograniczyć do sprawdzenia równości wielomianów dla dostatecznie małej liczby współczynników a.

GŁÓWNE TWIERDZENIE

Twierdzenie 2. Niech N będzie liczbą naturalną, r liczbą pierwszą i q największym dzielnikiem pierwszym liczby $r-1$. Niech wreszcie s będzie liczbą naturalną o tej własności, że wszystkie dzielniki pierwsze liczby N są większe od s. Załóżmy, że liczby N, q i s spełniają nierówność

$$\binom{q+s-1}{s} > N^{2\lfloor\sqrt{r}\rfloor}.$$

Załóżmy następnie, że liczba N nie dzieli się przez r oraz

$$N^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}.$$

Załóżmy wreszcie, że dla każdego a takiego, że $1 \leq a \leq s$ mamy przystawanie wielomianów

$$(X-a)^N \equiv X^N - a \pmod{X^r - 1, N}.$$

Wówczas liczba N jest potęgą liczby pierwszej.

Przed dowodem twierdzenia pokażemy, w jaki sposób otrzymujemy z niego deterministyczny algorytm sprawdzania, czy liczba N jest pierwsza. Pokażemy również, w jaki sposób w tym algorytmie sprawdzamy warunki zakończenia pętli, tzn. jak dobieramy parametry r, q i s.

0. **Dane:** liczba naturalna nieparzysta N;
1. sprawdź, czy N jest potęgą liczby pierwszej; **jeśli tak, to zwróć** ZŁOŻONA;
2. $r := 2$;
3. **powtarzaj do skutku**

3.1. **powtarzaj** $r := r + 1$ **dotąd aż** liczba r będzie pierwsza;

3.2. **jeśli** $r \mid N$, **to zwróć** ZŁOŻONA;

3.3. znajdź największy dzielnik pierwszy q liczby $r-1$;

3.4. **jeśli** liczba q jest za mała lub $N^{\frac{r-1}{q}} \equiv 1 \pmod{r}$, **to wróć do** (3.1);

4. znajdź liczbę s taką, że $\binom{q+s-1}{s} > N^{2\lfloor\sqrt{r}\rfloor}$;
5. $a := 1$;
6. **powtarzaj do skutku**

6.1. **jeśli** $(X-a)^N \not\equiv (X^n - a) \pmod{X^r - 1, N}$, **to zwróć** ZŁOŻONA;

6.2. $a := a + 1$;

6.3. **jeśli** $a > s$, **to zwróć** PIERWSZA.

Zajmiemy się teraz enigmatycznie sformułowanym warunkiem zakończenia pętli (3). Naszym celem jest znalezienie r, q i s takich, by spełniona była nierówność

$$\binom{q+s-1}{q} > N^{2\lfloor\sqrt{r}\rfloor}$$

i przy tym, by liczby r i s były dostatecznie małe.

Zauważmy najpierw, że

$$\binom{q+s-1}{s} > \left(\frac{q}{s}\right)^s.$$

Przyjmijmy następnie, że $q \geq 2s$. Wówczas

$$\binom{q+s-1}{s} > 2^s.$$

Chcemy zatem dobrać r i s tak, by spełniona była nierówność

$$2^s > N^{2\lfloor\sqrt{r}\rfloor}.$$

Zatem

$$q \geq 2s \geq 4\lfloor\sqrt{r}\rfloor \log_2 N.$$

Warunkiem zakończenia pętli jest zatem znalezienie liczby q spełniającej nierówność

$$q \geq 4\lfloor\sqrt{r}\rfloor \log_2 N.$$

Powstaje pytanie, czy można znaleźć dostatecznie małą liczbę r o tej własności, że jej największy dzielnik pierwszy q spełnia nierówność $q \geq 4\lfloor\sqrt{r}\rfloor \log_2 N$.

Lemat. (Fouvry, 1985; Baker, Harman, 1996) Istnieją dwie stałe c_1 i c_2 takie, że w przedziale $[c_1(\log_2 N)^6, c_2(\log_2 N)^6]$ istnieje liczba pierwsza r o tej własności, że największy dzielnik pierwszy q liczby $r-1$ spełnia nierówność $q \geq 4\sqrt{r}\log_2 N$ oraz rząd liczby N modulo r jest podzielny przez q.

W szczególności mamy wtedy kongruencję $N^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$.

Podsumowując: $r \leq c_2(\log_2 N)^6$ oraz $s \leq \frac{r-1}{4}$; zatem tak dobrane liczby r i s gwarantują wielomianowy czas wykonywania algorytmu AKS. Dokładne szacowanie złożoności obliczeniowej pozostawimy jako ćwiczenie (otrzymany wynik zależy od przyjętej złożoności działań arytmetycznych i działań na wielomianach).

Poprawność tego algorytmu wynika natychmiast z głównego twierdzenia. Pozostaje więc tylko dowieść tego twierdzenia.

DOWÓD GŁÓWNEGO TWIERDZENIA

1. Istnieje liczba pierwsza p taka, że $p \mid N$ oraz $p^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$.
2. Bierzemy wielomian nierozkładalny $h(X)$ (nad ciałem $\mathbb{Z}_p$) będący dzielnikiem r-tego wielomianu cyklotomicznego $\Phi_r(X) = X^{r-1} + X^{r-2} + \ldots + X + 1$.
3. **Lemat.** $d = \deg(h) \geq q$.
4. Rozważamy ciało $K = \mathbb{Z}_p[X]/(h(X))$; jest to ciało skończone charakterystyki p, mające p^d elementów. Jego grupa multyplikatywna K^* jest cykliczna.
5. Niech G będzie podgrupą K^* generowaną przez wielomiany $X - a$, gdzie $1 \leq a \leq s$.
6. **Lemat.** Grupa G jest cykliczna i ma co najmniej $\binom{q+s-1}{s}$ elementów.
7. Niech wielomian $g(X) = (X-1)^{e_1}(X-2)^{2_2} \cdot \ldots \cdot (X-s)^{e_s}$ będzie generatorem grupy G. Rząd $\mathrm{ord}(g(X))$ wielomianu $g(X)$ modulo $h(X)$ jest równy rzędowi grupy G.
8. Definiujemy zbiór T: $\quad T = \{k : \ g(X)^k \equiv g(X^k) \pmod{X^r - 1, p}\}$.
9. **Lemat.** $1, p, N \in T$.
10. **Lemat.** Zbiór T jest zamknięty na mnożenie.
11. $\forall i, j \left[N^i p^j \in T\right]$.
12. Zbiór $\{N^i p^j : \ 0 \leq i, j \leq \lfloor\sqrt{r}\rfloor\}$ ma $(\lfloor\sqrt{r}\rfloor + 1)^2 > r$ elementów.
13. $\exists (i,j) \neq (k,l) \left[N^i p^j \equiv N^k p^l \pmod{r}\right]$.
14. Kładziemy $t = N^i p^j$ oraz $u = N^k p^l$. Wtedy $t, u \in T$, więc
$$g(X^t) \equiv g(X)^t \pmod{X^r - 1, p} \quad \text{oraz} \quad g(X^u) \equiv g(X)^u \pmod{X^r - 1, p}.$$
15. Ponieważ $t \equiv u \pmod{r}$, więc $X^t \equiv X^u \pmod{X^r - 1, p}$, a zatem
$$g(X^t) \equiv g(X^u) \pmod{X^r - 1, p}.$$
16. $g(X)^t \equiv g(X)^u \pmod{X^r - 1, p}$; zatem $g(X)^t \equiv g(X)^u \pmod{h(X), p}$. Stąd wynika, że $t \equiv u \pmod{\mathrm{ord}(g(X))}$.
17. $t, u \leq N^{\lfloor\sqrt{r}\rfloor} p^{\lfloor\sqrt{r}\rfloor} \leq (N^{\lfloor\sqrt{r}\rfloor})^2 = N^{2\lfloor\sqrt{r}\rfloor} < \binom{q+s-1}{s} \leq |G| = \mathrm{ord}(g(X))$. Zatem $t = u$.
18. $N^i p^j = N^k p^l$; zatem $N^{i-k} = p^{l-j}$. A więc N jest potęgą liczby pierwszej p. ♠

Dowodów wymagają lematy 3, 6, 9, 10.

DOWODY LEMATÓW

Lemat 3. Wielomian $h(X)$ jest nierozkłalnym (nad ciałem $\mathbb{Z}_p$) dzielnikiem r-tego wielomianu cyklotomicznego $\Phi_r(X) = X^{r-1} + X^{r-2} + \ldots + X + 1$. Wtedy $d = \deg(h) \geq q$.

Dowód. Ponieważ wielomian $h(X)$ jest nierozkładalny na ciałem $\mathbb{Z}_p$, więc pierścień ilorazowy $K = \mathbb{Z}_p[X]/(h(X))$ jest ciałem charakterystyki p mającym p^d elementów. Grupa multyplikatywna K^* tego ciała jest cykliczna i ma rząd $p^d - 1$. Zatem dla dowolnego elementu b ciała K mamy $b^{p^d-1} = 1$. W szczególności $X^{p^d-1} = X$ w ciele K. To znaczy, że $h(X) \mid X^{p^d-1}$. Ponieważ $h(X) \mid X^r - 1$, więc

$$h(X) \mid \mathrm{NWD}(X^{p^d-1} - 1, X^r - 1) = X^{\mathrm{NWD}(p^d-1,r)} - 1.$$

Jeśli $\mathrm{NWD}(p^d - 1, r) = 1$, to $h(X) \mid X - 1$, a więc $h(X) = X - 1$. Ale wtedy $h(1) \mid \Phi_r(1)$, $h(1) = 0$ oraz $\Phi_r(1) = r$, skąd dostajemy $0 \mid 1$; sprzeczność.

Zatem $\mathrm{NWD}(p^d - 1, r) = r$, czyli $r \mid p^d - 1$. Zatem stopień p modulo r jest nie większy od d. Z drugiej strony, ten stopień jest co najmniej równy q, skąd wynika, że $q \leq d$.

Mianowicie $r - 1 = q \cdot m$. Stopień p modulo r jest dzielnikiem $r - 1$. Zatem albo ten stopień jest podzielny przez q, albo jest dzielnikiem m. Jeśli jest on dzielnikiem m, to $p^m \equiv 1 \pmod r$, czyli $p^{\frac{r-1}{q}} \equiv 1 \pmod r$, wbrew wyborowi p. Zatem stopień p modulo r jest podzielny przez q, a więc nie mniejszy od q. ♠

Zachodzi twierdzenie ogólniejsze: jeśli d jest rzędem p modulo r, to wielomian $\Phi_r(X)$ rozkłada się nad ciałem $\mathbb{Z}_p$ na iloczyn wielomianów nierozkładalnych stopnia d.

Dowód tego twierdzenia ogólniejszego można znaleźć w oryginalnej pracy. Ogólną teorię wielomianów cyklotomicznych można znaleźć w książce:

Rudolf Liedl, Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge 1986 (II wyd. 1994)

Lemat 6. Grupa G jest cykliczna i ma co najmniej $\binom{q+s-1}{s}$ elementów.

Dowód. Grupa G jest podgrupą grupy cyklicznej, więc jest cykliczna.

Zauważamy następnie, że wielomiany $X - a$, gdzie $1 \leq a \leq s$, dla różnych a są różne. Wynika to stąd, że $p > s$: mianowicie $p \mid N$ oraz wszystkie dzielniki N są większe od s.

Zatem wielomiany $(X - 1)^{k_1}(X - 2)^{k_2} \cdot \ldots \cdot (X - s)^{k_s}$ są różnymi elementami grupy G, jeśli tylko

$$k_1 + k_2 + \ldots + k_s \leq q - 1 < \deg(h(X)).$$

Takich ciągów wykładników $(k_1, k_2, \ldots, k_s)$ jest $\binom{q+s-1}{s}$. ♠

Lemat 9. $1, p, N \in T$.

Dowód. Oczywiście $1 \in T$. Ponieważ p jest liczbą pierwszą, więc

$$(X-a)^p \equiv X^p - a^p \equiv X^p - a \pmod{p}.$$

Zatem wielomiany $(X-a)^p$ i $X^p - a$ są identyczne w pierścieniu $\mathbb{Z}_p[X]$. Stąd wynika, że

$$\begin{aligned} g(X)^p &= ((X-1)^{e_1} \cdot \ldots \cdot (X-s)^{e_s})^p = ((X-1)^p)^{e_1} \cdot \ldots \cdot ((X-s)^p)^{e_s} \equiv \\ &\equiv (X^p-1)^{e_1} \cdot \ldots \cdot (X^p-s)^{e_s} = g(X^p) \pmod{X^r-1, p}. \end{aligned}$$

Zatem $p \in T$.

Z założenia mamy

$$(X-a)^N \equiv X^N - a \pmod{X^r-1, p}$$

dla $1 \le a \le s$. Zatem

$$\begin{aligned} g(X)^N &= ((X-1)^{e_1} \cdot \ldots \cdot (X-s)^{e_s})^N = ((X-1)^N)^{e_1} \cdot \ldots \cdot ((X-s)^N)^{e_s} \equiv \\ &\equiv (X^N-1)^{e_1} \cdot \ldots \cdot (X^N-s)^{e_s} = g(X^N) \pmod{X^r-1, p}. \end{aligned}$$

Stąd mamy $N \in T$. ♠

Lemat 10. Zbiór T jest zamknięty na mnożenie.

Dowód. Niech $k, l \in T$. Wtedy

$$g(X)^k \equiv g(X^k) \pmod{X^r-1, p}.$$

Podstawiając X^l w miejsce X, otrzymujemy

$$g(X^l)^k \equiv g(X^{kl}) \pmod{X^{lr}-1, p}.$$

Ale $X^r - 1 \mid X^{lr} - 1$. Zatem

$$g(X^l)^k \equiv g(X^{kl}) \pmod{X^r-1, p}.$$

Następnie

$$g(X)^{kl} = (g(X)^l)^k \equiv g(X^l)^k \equiv g(X^{kl}) \pmod{X^r-1, p},$$

co dowodzi, że $kl \in T$. ♠

W ten sposób dowód głownego twierdzenia został zakończony.