Szkic deterministycznego wielomianowego algorytmu testowania pierwszości [AKS02]

Paweł Zalewski
Uniwersytet Wrocławski, Instytut Informatyki

1 Konwencje

symbol	**znaczenie**
$o_r(n)$	rząd n modulo r
p, q, r	liczby pierwsze
F_{p^d}	ciało skończone o rozmiarze p^d
$a \equiv b \pmod{h(x), n}$	$a = b$ w pierścieniu $(\mathbb{Z}/n)[x]/h(x)$

2 Główna tożsamość

Twierdzenie 1. *Jeżeli $(a, n) = 1$, to przystawanie wielomianów*

$$(x - a)^n \equiv x^n - a \pmod{n} \tag{1}$$

zachodzi wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

Dowód.

$$(x - a)^n = \sum_{i=0}^{n} \binom{n}{i} (-1)^i x^i a^{n-i}$$

1° Niech n będzie liczbą pierwszą. Wówczas $n | \binom{n}{i}$ dla $1 \le i \le n - 1$. Ponadto, $a^n \equiv a \pmod{n}$.

2° Niech $p^k || n$, $p > 1$. Wówczas $p^k \not| \binom{n}{p}$ oraz $p \not| a^{n-p}$, co oznacza, że nie wszystkie współczynniki poza skrajnymi (przy x^n oraz x^0) są zerowe.

□

Uwagi:

- Niezawodny sposób sprawdzania pierwszości
- Obliczenie współczynników wielomianu po lewej stronie (1) może wymagać wykładniczego czasu
- Nie jest znany szybki sposób obliczenia wartości lub samego stwierdzenia istnienia niezerowych współczynników

- ► Autorzy przełomowego algorytmu [AKS02] badają zachodzenie tożsamości (1) w pierścieniu $(\mathbb{Z}/n)[x]/(x^r - 1)$ dla wielomianów $(x - a)$ przy różnych wartościach a. Sednem dowodu jest wykazanie, że stosunkowo niewiele tych wartości wystarcza do rozstrzygnięcia pierwszości.
- ► Algorytm nie ma widocznego związku z faktoryzacją.

3 Uwagi do algorytmu

1. W linii `1` oblicza się co najwyżej logarytmicznie wiele pierwiastków.

2. W linii `6` można zastosować dowolny deterministyczny algorytm działający w czasie $O(r) = O(\log^c n)$.

3. Ograniczenie w linii `7` ($q \geq 4\sqrt{r} \log n$) nie jest spełnione dla $r < 64 \log^2 n$.

4. W linii `7` mamy

$$n^{\frac{r-1}{q}} \not\equiv 1 \pmod r \iff q | o_r(n)$$

5. Główny wysiłek obliczeniowy tkwi w testowaniu warunku z drugiej pętli (linie `11-12`).

4 Poprawność algorytmu

Algorytm dla odpowiednio dużych n zawsze się zatrzymuje, co wynika z następującego lematu:

Lemat 2. *Istnieją dodatnie stałe c_1, c_2, dla których istnieje liczba pierwsza r w przedziale $[c_1(\log n)^6, c_2(\log n)^6]$ taka, że $r - 1$ ma dzielnik pierwszy $q \geq 4\sqrt{r} \log n$ i $q | o_r(n)$.*

Dowód. Dowód wynika z dwóch twierdzeń teorioliczbowych opublikowanych w 1985 i 1997 roku. W pracy [AKS02] jest przedstawiony jako dowód lematu 4.2. □

Lemat 3. *Dla każdej odpowiednio dużej liczby pierwszej n algorytm zwróci wartość* `PRIME`.

Dowód. Algorytm może zwrócić `COMPOSITE` tylko przy sprawdzaniu warunków w liniach `1, 4, 12`. W linii `1` jest to niemożliwe, ponieważ liczba pierwsza nie jest potęgą stopnia większego niż 1. W linii `4` jest to niemożliwe, ponieważ liczba pierwsza nie ma nietrywialnych dzielników. W linii `12` jest to niemożliwe z Twierdzenia 1. □

Sednem pracy jest dowód, że każda odpowiednio duża liczba złożona n zostanie poprawnie zidentyfikowana:

Lemat 4. *Dla każdej odpowiednio dużej liczby złożonej n algorytm zwróci* `COMPOSITE`.

Szkic dowodu. Załóżmy, że dla pewnej liczby złożonej n algorytm odpowie `PRIME`. Niech liczby q, r będą określone jak w algorytmie.

1. Niech n ma następujący rozkład na liczby pierwsze p_i:

$$n = \prod_i p_i^{\alpha_i}.$$

2. Istnieje takie i_0, że $q | o_r(p_{i_0})$. Niech $p = p_{i_0}$.

3. Jeżeli $(x-a)^n \equiv x^n - a \pmod{x^r-1, n}$, to również $(x-a)^n \equiv x^n - a \pmod{x^r-1, p}$.

4. Dla każdego $a \in [1, 2\sqrt{r}\log n]$ zachodzi

$$(x-a)^{n^i} \equiv x^{n^j} - a \pmod{x^{r-1}, p}.$$

5. Dla każdego $a \in [1, 2\sqrt{r}\log n]$ zachodzi

$$(x-a)^{n^i p^j} \equiv x^{n^i p^j} - a \pmod{x^{r-1}, p}.$$

6. Rozważmy wykładniki postaci $n^i p^j$ dla $0 \le i, j \le \lfloor\sqrt{n}\rfloor$. Wykładników tych jest więcej niż r, co oznacza, że istnieją wśród nich takie $(i_1, j_1) \neq (i_2, j_2)$, że dla $u = n^{i_1} p^{j_1}, t = n^{i_2} p^{j_2}$, zachodzi $u \equiv t \pmod{r}$.

7. Dla każdego $a \in [1, 2\sqrt{r}\log n]$ zachodzi

$$(x-a)^t \equiv (x-a)^u \pmod{x^{r-1}, p}.$$

8. W $F_p[x]$ istnieje wielomian nierozkładalny $h(x)$ o stopniu $d = o_r(p)$.
Co więcej, $h(x) | (x^r - 1)$.

9. $F_p[x]/h(x)$ jest ciałem, którego grupa multyplikatywna jest cykliczna.

10. Jeżeli $(x-a)^n \equiv x^n - a \pmod{x^r-1, p}$, to również$(x-a)^n \equiv x^n - a \pmod{h(x), p}$.

11. Iloczyny wielomianów $(x-a)$ dla $a = 1, \ldots, 2\sqrt{r}\log n$ tworzą podgrupę cykliczną G w ciele $F_p[x]/(h(x))$. Grupa ta ma rząd większy niż $n^{2\sqrt{r}}$.

12. Generator g grupy G spełnia warunek z linii 12 algorytmu i ma rząd większy niż $n^{2\sqrt{r}}$. Co więcej, $g^t = g^u$ w G.

13. Ponieważ $|t-u| < n^{2\sqrt{r}}$, więc $t = u$.

14. Skoro $n^{i_1} p^{j_1} = n^{i_2} p^{j_2}$ i $(i_1, j_1) \neq (i_2, j_2)$, to $n = p^k$. Taki przypadek został wykluczony jednak w pierwszej linii algorytmu.

□

Bibliografia

[AKS02] Manindra Agrawal, Neeraj Kayal, Nitin Saxena. PRIMES is in P, 2002, preprint. Dostępne na stronie `http://www.cse.iitk.ac.in/news/primality.html`