Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Marcin Stefaniak
Nr albumu: 181097

Algorytmy testowania pierwszości liczb

Praca magisterska
na kierunku INFORMATYKA

Praca wykonana pod kierunkiem
dr hab Krzysztofa Diksa
Instytut Informatyki

Maj 2003

Pracę przedkładam do oceny

Data Podpis autora pracy:

Praca jest gotowa do oceny przez recenzenta

Data Podpis kierującego pracą:

Streszczenie

Praca zawiera przegląd algorytmów testowania pierwszości liczb naturalnych, ze szczególnym uwzględnieniem świeżych odkryć w tej dziedzinie – wielomianowego i deterministycznego algorytmu Agrawala-Kayala-Saxeny, oraz jego ulepszeń.

Słowa kluczowe

algorytmy, liczby pierwsze, algebra, pierścienie wielomianów, testy pierwszości, dowodzenie pierwszości

Klasyfikacja tematyczna

G. Mathematics of Computing
G.2 Discrete Mathematics
G.2.m Miscellaneous
[[???]]

Spis treści

Wprowadzenie

Liczby pierwsze to fundamentalne pojęcie matematyki. Już Euklides pokazał, że jest ich nieskończenie wiele, oraz że każda liczba naturalna jednoznacznie przedstawia się w postaci iloczynu liczb pierwszych. Przez wieki trudny problem znajdowania takiego rozkładu dla zadanej liczby nie został zadowalająco rozwiązany. W 1801 roku Gauss pisał:

„Wiadomo, iż zadanie polegające na odróżnieniu liczb pierwszych od liczb złożonych i następnie rozłożeniu tych ostatnich na czynniki pierwsze jest jednym z najważniejszych i najbardziej przydatnych w arytmetyce."

Zaskakujące jest, że jedno z tych zadań – odróżnianie liczby pierwsze od złożonych – można wykonać praktycznie i efektywnie, podczas gdy rozkładanie liczb na czynniki pierwsze wciąż pozostaje dużo trudniejszym problemem. Ta przepaść stoi za popularnym algorytmem kryptografii klucza publicznego, RSA, w którym używa się właśnie liczb pierwszych. Gdyby ktoś opracował szybką metodę rozkładania liczb na czynniki pierwsze, byłby w stanie złamać każdy szyfr RSA.

Aby rozstrzygnąć sprawnie, czy liczba jest pierwsza, czy złożona, wykorzystujemy pewne algebraiczne własności tych liczb, by znaleźć certyfikat, który w oparciu o pewne twierdzenie matematyczne stanowi dowód złożoności lub pierwszości badanej liczby. Prostym i praktycznie używanym testem pierwszości jest test Millera-Rabina. Jest to test randomizowany i myli się z pewnym niedużym lecz dodatmi prawdowodobieństwem.

Długo nie było wiadomo, czy istnieje deterministyczny i wielomianowy algorytm testowania pierwszości liczb. Niektóre proponowane wielomianowe testy (test Millera) opierają się o nieudowodnione hipotezy, na przykład uogólnioną hipotezę Riemanna. Złożoność innych deterministycznych testów pierwszości jest ponadwielomianowa. Podejrzewano, że problem rozpoznawania liczb pierwszych może nie mieć rozwiązania wielomianowego.

Dopiero w sierpniu 2002 roku Agrawal, Kayal i Saxena opublikowali w Internecie artykuł „PRIMES is in P", w którym pokazali w pełni deterministyczny i wielomianowy test pierwszości. Choć jest to znaczny wynik teoretyczny, w praktyce rewolucji nie było – złożoność czasowa tego algorytmu jest wielomianowa, ale ze sporym wykładnikiem. Późniejsze usprawnienia zredukowały czas obliczeń tej metody do stopnia porównywalnego z innymi algorytmami dowodzenia pierwszości liczb, takimi jak metoda krzywych eliptycznych ECPP czy ponadwielomianowy algorytm APR.

Jakkolwiek w praktyce nie ma potrzeby zastąpienia prostego i skutecznego testu Millera-Rabina lepszym, badania nad testami pierwszości i teorią liczb w ogólności przyniosły wiele ciekawych wyników ważnych w kryptografii, takich jak np. efektywniejsze algorytmy rozkładania liczb na czynniki pierwsze.

Praca stanowi przegląd algorytmów testów pierwszości, ze szczególnym uwzględnieniem algorytmu Agrawala-Kayala-Saxeny. Praca składa się z 6 rozdziałów. W rozdziale 1 przedstawione są pojęcia matematyczne używane w testach pierwszości. W rozdziale 2 omówione są probabilistyczne testy pierwszości, takie jak test Millera-Rabina czy też bardziej skomplikowany test Frobeniusza ciał kwadratowych. Tradycyjne metody dowodzenia pierwszości opisane

są w rozdziale 3. Rozdział 4 zawiera szczegółowe omówienie metody Agrawala-Kayala-Saxeny, włącznie z jej ulepszeniami i metodą certyfikatów Bernsteina. Moje uwagi na temat hipotezy nr 4 z artykułu „PRIMES is in P" zawarłem w rodziale 5. Kwestie implementacji arytmetyki dużych liczb w kontekście algorytmów testowania pierwszości poruszonone są w rozdziale 6.

Rozdział 1

Podstawowe pojęcia

W niniejszym rozdziale krótko przedstawimy używane w pracy podstawowe pojęcia z teorii liczb, algebry i algorytmiki. Pozwolimy sobie zacząć od najważniejszego dla nas pojęcia pierwszości liczb.

Definicja 1.1 *Liczbę całkowitą n nazywamy* pierwszą, *gdy ma dokładnie dwa różne dzielniki, 1 oraz n. Gdy n ma więcej dzielników niż dwa, nazywamy ją liczbą* złożoną.

Zauważmy, że 1 nie jest liczbą złożoną, ani też liczbą pierwszą. Dzięki temu każdą liczbę naturalną możemy przedstawić jednoznacznie w postaci iloczynu liczb pierwszych $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Tradycyjnie będziemy zwykle używać notacji słownej „liczba jest pierwsza", „liczba jest złożona", ale czasem przyda się też zbiór liczb pierwszych $\{2, 3, 5, 7, \ldots\}$, oznaczmy go PRIMES. Liczby pierwsze zwykle będziemy literami $p, q, \ldots$, a liczby całkowite których status jest nieznany bądź nieistotny przez np. $n, m, k, l, \ldots$

Największy wspólny dzielnik liczb m i n oznaczamy $\gcd(m, n)$. Dwie liczby są względnie pierwsze, gdy nie mają żadnych wspólnych dzielnikow prócz 1, czyli $\gcd(m, n) = 1$. Ilość liczb naturalnych względnie pierwszych z n mniejszych od n oznaczamy przez $\varphi(n)$ (funkcja Eulera). Łatwo ją obliczyć znając rozkład n na czynniki pierwsze:

$$\varphi(n) = n \prod_{\substack{p \in \text{PRIMES} \\ p|n}} \left(1 - \frac{1}{p}\right)$$

Warto wiedzieć, jak gęsto rozmieszczone są liczby pierwsze. Otóż ilość liczb pierwszych mniejszych od x asymptotycznie wynosi $x/\ln(x)$. To oznacza praktycznie, że szansa na trafienie liczby pierwszej losując liczbę bliską x wynosi $1/\ln(x)$.

W dalszym ciągu testowaną oznaczać będziemy przez n. Oczywiście jest tylko jedna parzysta liczba pierwsza $n = 2$, dlatego zakładać będziemy z góry, że badana liczba n jest nieparzysta.

1.1. Pierścień Z_n – działania modulo n

Testy pierwszości na ogół opierają się na różnych własnościach algebraicznych struktur związanych z badaną liczbą. Najczęściej będzie to dodawanie i mnożenie liczb *modulo* n. Operacje te tworzą pierścień liczb modulo n, który oznaczamy Z_n. Grupę multiplikatywną tego pierścienia (mnożenie modulo n) oznaczamy Z_n^*. Należą do niej elementy odwracalne, czyli względnie pierwsze z n, a tych jest $\varphi(n)$.

Rząd elementu a w grupie $ord(a)$ to najmniejszy dodatni wykładnik k taki, że $a^k = 1$. Zachodzi fakt, że rząd elementu dzieli rząd (inaczej rozmiar, liczbę elementów) grupy. Stąd jako prosty wniosek uzyskujemy twierdzenie:

Twierdzenie 1.1 (Euler) *Dla $a \in Z_n$, $\gcd(a,n) = 1$ zachodzi $a^{\varphi(n)} = 1 \pmod n$.*

Gdy n jest liczbą pierwszą, wtedy $\varphi(n) = n - 1$, pierścień Z_n jest ciałem (wszystkie elementy prócz 0 są odwracalne), a analog twierdzenia Eulera nosi nazwę małego twierdzenia Fermata.

Twierdzenie 1.2 (Małe tw. Fermata) *Dla liczby pierwszej p, $a \in Z_p$, $a \not\equiv 0$ zachodzi $a^{p-1} \equiv 1 \pmod n$.*

Jeśli n jest liczbą złożoną, rozkład $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, to istnieje naturalna odpowiedniość pierścieni $Z_n \sim Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$. Fakt ten znany jest pod mianem chińskiego twierdzenia o resztach.

1.2. Liczby Carmichaela

Definicja 1.2 (liczby Carmicheala) *Liczbę złożoną n nazywamy liczbą Carmicheala, gdy dla wszystkich liczb a względnie pierwszych z n zachodzi $a^{n-1} \equiv 1 \pmod n$.*

Twierdzenie 1.3 (kryterium Korselta) *Liczba złożona n jest liczbą Carmicheala wtedy i tylko wtedy, gdy jest bezkwadratowa (nie dzieli się przez żaden kwadrat liczby pierwszej) i dla każdego dzielnika pierwszego $p|n$ zachodzi $p - 1|n - 1$.*

Wniosek 1.4 *Każda liczba Carmichaela jest iloczynem co najmniej trzech liczb pierwszych.*

Dowód. Dowody powyższych faktów znajduje się w [Koblitz].

Liczb Carmicheala jest nieskończenie wiele, co pokazano w [AGP94].

1.3. Pierścienie wielomianów

Rozważmy zbiór wielomianów jednej zmiennej o współczynnikach z pewnego pierścienia R. Wielomiany te można dodawać i mnożyć, tworzą one pierścień, oznaczamy go przez $R[x]$, gdzie x jest zmienną wielomianu. Rozważmy dzielenie z resztą wielomianów z $R[x]$ przez wielomian $f(x) \in R[x]$. Dzielenie to jest zawsze wykonalne, o ile tylko współczynnik $f(x)$ przy najwyższej potędze x jest odwracalny w R, na przykład wynosi 1 – takie wielomiany nazywamy monicznymi.

Reszty z dzielenia modulo $f(x)$ możemy naturalnie dodawać i mnożyć. Zatem tworzą one pierścień, który oznaczamy $R[x]/f(x)$. Gdy R jest skończony, to wiadomo, że liczba elementów $R[x]/f(x)$ wynosi $|R|^{degf}$. Taki pierścień ilorazowy wielomianów będzie ciałem (czyli wykonalne będzie w nim dzielenie przez wszystkie elementy za wyjątkiem zera), gdy R jest ciałem i wielomian $f(x)$ jest nierozkładalny nad R, tj. nie da się go przedstawić w postaci $f(x) = g(x)h(x)$, gdzie $g, h \in R[x]$ to wielomiany różne od stałych.

Jeśli F jest ciałem skończonym, a d - stopniem wielomianu to istnieją w $F[x]$ nierozkładalne wielomiany moniczne stopnia d, a nawet jest ich tam dla ustalonego d co najmniej stały ułamek wszystkich. Na przykład, dla $d = 2$, jest $|F|^2$ wszystkich wielomianów monicznych stopnia 2 (postaci $x^2 + ax + b$), a wielomianów rozkładalnych wśród nich (postaci $(x - a)(x - b)$) jest najwyżej tyle co różnych par jednomianów, czyli $(|F|^2 + |F|)/2$.

Wszystkie ciała skończone o p^k elementach są izomorficzne ze sobą, mają strukuturę ciała $Z_p[x]/f(x)$, $degf = k$, f – nierozkładalny nad Z_p. Takie ciało oznaczamy przez $GF(p^k)$.

Przyda się nam następujący fakt:

Fakt 1.5 *Jeśli p jest pierwsze, to dla $w(x) \in Z_p[x]$ zachodzi $w(x^p) = (w(x))^p$.*

Oczywiście to samo zachodzi też dla $w(x) \in Z_p[x]/f(x)$.

Dowód. Jest to prosta konsekwencja przystawania $(a+b)^p \equiv a^p + b^p \pmod p$, które wynika z rozwinięcia w dwumian Newtona

$$(a+b)^p = \sum_{i=0}^{p} \binom{k}{p} a^k b^{p-k}$$

i z faktu, że $\binom{k}{p} \equiv 0 \pmod p$ dla $0 < k < p$.

Definicja 1.3 (Wielomiany cyklotomiczne) *Niech $r > 0$. Niech ζ będzie pierwiastkiem dokładnie r-tego stopnia z 1, tj. $\zeta^r = 1$ oraz $\zeta^i \neq 1$ dla $0 < i < r$. Wielomian $x^r - 1$ rozkłada się na jednomiany*

$$x^r - 1 = \prod_{0 \leqslant i < r} (x - \zeta^i)$$

Wielomianem **cyklotomicznym** Φ_r *nazywamy iloczyn niektórych z tych jednomianów*

$$\Phi_r(x) = \prod_{\substack{0 \leqslant i < r \\ \gcd(i,r)=1}} (x - \zeta^i)$$

Zauważmy, że wielomian cyklotomiczny spełnia $\Phi_r(x) | x^r - 1$, $\deg \Phi_r = \varphi(r)$. Co mniej oczywiste, Φ_r jest wielomianem o współczynnikach całkowitych. Wielomiany Φ_r mogą być rozkładalne nad Z_n. Znany jest fakt:

Fakt 1.6 *Jeśli p będzie liczbą pierwszą, to wielomian cyklotomiczny Φ_r rozkłada się nad ciałem Z_p na nierozkładalne wielomiany stopnia $ord_r(p)$.*

1.4. Symbole Legendre'a i Jacobiego

Przydatnym narzędziem do testowania pierwszości są pochodzące z teorii liczb symbole Legendre'a i Jacobiego. Mówimy, że a jest resztą kwadratową modulo n, gdy a jest kwadratem pewnej liczby w Z_n. Mniej niż połowa elementów Z_n^* jest resztą kwadratową (ponieważ $x^2 = a \Rightarrow (-x)^2 = a$), pozostałe nazywamy nieresztami.

Definicja 1.4 (Symbol Legendre'a) *Dla liczby całkowitej a i liczby pierwszej p określamy symbol Legendre'a $\left(\frac{a}{p}\right)$ jako*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \textit{jeśli } p|a \\ 1, & \textit{jeśli } a \textit{ jest resztą kwadratową modulo } p \\ -1, & \textit{wpp.} \end{cases}$$

Uogólnieniem symbolu Legendre'a na liczby złożone jest symbol Jacobiego.

Definicja 1.5 (Symbol Jacobiego) *Dla liczby całkowitej a i nieparzystej dodatniej liczby n o rozkładzie na czynniki pierwsze $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ definiujemy symbol Jacobiego $\left(\frac{a}{n}\right)$ jako iloczyn symboli Legendre'a:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

Zauważmy, że jeśli a jest resztą kwadratową modulo n, to $\left(\frac{a}{n}\right) = 1$ — a w drugą stronę już niekoniecznie, w przypadku gdy n jest złożone.

Te symbole, pomimo ich ciekawych matematycznych własności, nie byłyby użyteczne gdyby nie dało się ich łatwo obliczać. Na szczęście istnieje szybki algorytm obliczania symbolu Jacobiego, w swej strukturze podobny do algorytmu obliczania najwiekszego wspólnego dzielnika. Zachodzą bowiem następujące własności:

$$\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right)$$

$$\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{jeśli } n = \pm 1 \pmod 8 \\ -1, & \text{jeśli } n = \pm 3 \pmod 8 \end{cases}$$

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

Co najważniejsze, dla m, n nieparzystych zachodzi prawo wzajemności:

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), & \text{jeśli } n = m = 3 \pmod 4 \\ \left(\frac{n}{m}\right), & \text{wpp.} \end{cases}$$

Za pomocą tych własności symbol Jacobiego $\left(\frac{a}{n}\right)$ $(0 \leqslant a < n)$ można wyznaczyć, podobnie jak obliczanie największego wspólnego dzielnika, w czasie $O((\lg n)^2)$. Dowody tych i innych własności symbolu Jacobiego znajdują się np. w [Koblitz].

1.5. Złożoność obliczeniowa

— tą sekcję trzeba napisać lepiej, w odniesieniu do rodziału o arytmetyce dużych liczb

Badając złożoność problemów algorytmicznych, interesuje nas ile zasobów - czasu i pamięci wymaga rozwiązanie, w zależności od wielkości danych wejściowych. W problemie PRIMES dana jest jedna liczba liczba n, którą należy zbadać i orzec, czy jest ona pierwsza. Długość tej liczby to $\lg(n)$ bitów, dlatego też złożoność testów pierwszości rozważać będziemy względem $\lg(n)$. Na przykład, powiemy że test pierwszości jest wielomianowy, gdy czas jego działania jest rzędu $O(\lg(n)^k)$.

Szacując koszt obliczeń arytmetycznych schodzimy do poziomu operacji na bitach, i tak na przykład dodawanie dwóch liczb $\lg n$-bitowych ma koszt rzędu $O(\lg n)$, a mnożenie najprostszym sposobem $O((\lg n)^2)$ operacji na bitach.

Do nie dawna nie wiadomo było, czy problem PRIMES jest w klasie P – klasie problemów rozwiązywalnych w czasie wielomianowym. Wiadomo było, że należy do klasy NP. Klasę NP można określić jako problemy rozwiązywalne w czasie wielomianowym pod warunkiem otrzymania odpowiedniego certyfikatu. Konstrukcję takiego certyfikatu pokażemy w rozdziale 3. Co więcej, ten problem należy też do klasy co-NP, bo problem komplementarny, czy liczba jest złożona, da się łatwo pokazać, odpowiednim certyfikatem jest w tym przypadku nietrywialny dzielnik tej liczby.

W klasie NP jest wiele problemów NP-zupełnych, dla których nie znamy rozwiązania wielomianowego, i mało kto wierzy w istnienie takiego. Jednakże, problem PRIMES nie jest NP-zupełny, więc pokazanie wielomianowego testu pierwszości nie pociąga rozstrzygnięcia słynnej hipotezy P=NP.

Niektóre algorytmy testowania pierwszości są probabilistyczne, np. gdy dana liczba jest pierwsza, orzekną zgodnie z prawdą, a gdy złożona, to mogą się pomylić, z ograniczonym prawdopodobieństwem pomyłki.

Jakie to są klasy złożoności? BPP ZPP RP [[???]]

Rozdział 2

Probabilistyczne testy pierwszości

Wiele testów pierwszości bazuje na identycznym schemacie. Wybieramy pewną (łatwo obliczalną) matematyczną prawidłowość, wiążącą liczbę n oraz inne parametry, która jest zawsze spełniona, gdy liczba n jest pierwsza, natomiast gdy n jest złożona, spełniona jest rzadko (dla niewielu wartości parametrów spośród możliwych). Liczbę złożoną spełniającą tą tożsamość dla pewnych parametrów nazywamy liczbą pseudopierwszą odpowiedniego rodzaju dla tychże parametrów. Sprawdzając jeden raz nasz warunek możemy się omylić, jeśli wybierzemy parametry, dla których n pseudopierwsza. Jednakże, gdy powtórzymy wielokrotnie sprawdzanie warunku dla różnych, losowo wybranych wartości parametrów, szansa pomyłki maleje w postępie geometrycznym.

2.1. Test Fermata

Za punktem wyjścia obierzemy małe tw. Fermata (patrz rozdział 1). Wynika z niego, że gdy n jest pierwsze, to dla $n \not| a$

$$a^{n-1} \equiv 1 \pmod{n} \tag{2.1}$$

Wartość $a^{n-1} \bmod n$ możemy obliczyć efektywnie algorytmem binarnego potęgowania. Zabiera to najwyżej $2 \lg n$ mnożeń modulo n.

Zatem, jeśli weźmiemy $a \in Z_n \setminus \{0\}$, i okaże się, że $a^{n-1} \not\equiv 1 \pmod{n}$, to mamy w ręku niezbity dowód, że n jest liczbą złożoną. W drugą stronę nie jest już tak prosto – zdarza się, że $a^{n-1} \equiv 1 \pmod{n}$ dla wielu liczb a, a mimo to n jest liczbą złożoną. Liczbę, która spełnia warunek 2.1 nazywamy pseudopierwszą przy podstawie a. Gdyby każda liczba złożona była pseudopierwsza tylko przy α z możliwych swoich podstaw,

$$|\{a \in Z_n \setminus \{0\} : a^{n-1} = 1\}| \leqslant \alpha(n-1)$$

to wtedy losując a z jednostajnym rozkładem pradwopodobieństwa mamy szansę pomyłki testu ograniczoną z góry przez α

Niestety, istnieją takie liczby złożone n (liczby Carmicheala), które są pseudopierwsze przy każdej podstawie a względnie pierwszej z n. Oczywiście, gdy $\gcd(n, a) \neq 1$, równanie 2.1 nie ma szans zajść, ale równie dobrze możemy liczyć na znalezienie dzielnika n.

Wobec tego nie można uznać tego testu za zadowalający.

2.2. Test Millera-Rabina

Popularnym testem pierwszości, używanym praktycznie do generowania dużych liczb pierwszych, jest test Millera-Rabina ([Mi76], [Ra80]), opisany m.in. w [CLR], [Koblitz]. Jest on

rozszerzeniem opisanego wyżej testu Fermata. Skorzystamy z następującego prostego faktu o wyciąganiu pierwiastka z 1 w Z_n.

Twierdzenie 2.1 *Gdy n jest pierwsze, x całkowite, to*

$$x^2 \equiv 1 \Rightarrow x \equiv \pm 1 \pmod{n} \tag{2.2}$$

Dowód. Jeśli n jest pierwsze, to w ciele $Z_n[x]$ wielomianów modulo n wielomian $w(x) = x^2 - 1 = (x-1)(x+1)$ ma najwyżej $\deg w$ pierwiastków, i rzecz jasna są to $\pm 1 \in Z_n$.

Zastanówmy się, co jeśli n jest złożone? Na przykład załóżmy, że n ma dwa różne czynniki pierwsze $n = pq$. Wtedy (na mocy chińskiego tw. o resztach) $Z_n \sim Z_p \times Z_q$. Jeśli $x^2 \equiv 1 \pmod{n}$, to $x^2 \equiv 1 \pmod{p}$ i $x^2 \equiv 1 \pmod{q}$. Zgodnie z powyższym faktem, $x \equiv 1 \vee x \equiv -1 \pmod{p}$ i $x \equiv 1 \vee x \equiv -1 \pmod{q}$, co daje nam 4 przypadki. Spośród nich tylko dwa prowadzą do wyniku $x \equiv 1, -1 \pmod{n}$. Jeśli więc x jest dobrane w sposób „losowy", tak, że $x^2 \equiv 1 \pmod{n}$ to jest tylko $1/2$ szansy, że zachodzi warunek . Gdy n ma k różnych czynników pierwszych, to szansa ta spada do 2^{1-k}. A skoro liczby Carmicheala mają co najmniej 3 czynniki pierwsze... Oczywiście, to rozumowanie dalekie jest od ścisłości, ale pozwala sobie wyrobić pewną intuicję.

Możemy skorztystać z tej własności w następujący sposób: skoro $a^{n-1} \equiv 1 \pmod{n}$, to powinno zachodzić $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$. Dalej, dopóki $(n-1)/2^k$ jest parzyste, oraz $a^{(n-1)/2^k} \equiv 1 \pmod{n}$, to powinno także dalej zachodzić $a^{(n-1)/2^{k+1}} \equiv \pm 1 \pmod{n}$. Wobec

Algorytm 1 jedna iteracja testu Millera-Rabina

Dane wejściowe: n, a
  rozłóż $n - 1 = 2^s t$, $2 \not| t$, $s > 0$
  $x \leftarrow a^t \bmod n$
  if $x = 1$ **then**
    n jest prawdopodobnie pierwsze
  else
    for $r \leftarrow 0, 1, \ldots, s$ **do**
      if $x = -1$ **then**
        n jest prawdopodobnie pierwsze
      else
        $x \leftarrow x^2 \bmod n$
      end if
    end for
    n jest złożone
  end if

tego w teście Millera-Rabina rozkładamy $n - 1 = 2^s t$, t nieparzyste, losujemy podstawę a, obliczamy (potęgowaniem binarnym) $a^t \bmod n$, potem podnosimy do kwadratu, obliczając $a^{2^r t} \bmod n, r = 0, 1, \ldots, s$. Jeśli $a^t \equiv 1 \pmod{n}$ lub istnieje $r \in \{0, 1, \ldots, s\}$, takie, że $a^{2^r t} \equiv -1 \pmod{n}$, to możliwe, że n jest liczbą pierwszą. Jeśli liczba złożona n przejdzie taki test, mówimy, że n jest liczbą silnie pseudopierwszą przy podstawie a.

Szczegóły testu pokazane są w algorytmie 1

Twierdzenie 2.2 (Rabin) *Każda nieparzysta złożona liczba n jest silnie pseudopierwsza przy nie więcej niż $1/4$ podstawach $0 < a < n$.*

Dowód można znaleźć np. w [Koblitz]. Rozpatruje się tam trzy przypadki. Pierwszy, łatwy, gdy n dzieli się przez kwadrat liczby pierwszej p, to liczba tych podstaw nie przekracza $1/p + 1$

wszystkich. Drugi przypadek jest taki, że n ma dokładnie dwa dzielniki pierwsze, a trzeci, że n jest iloczynem więcej niż trzech liczb pierwszych. W obu szacuje się stosunek podstaw sprzyjających silnej pseudopierwszości do wszyskich podstaw przez 1/4.

Wniosek 2.3 *Jedna iteracja testu Millera-Rabina myli się z prawdopodobieństem conajwyżej* 1/4. *Powtórzenie k-krotne gwarantuje nam poprawność testu z prawdopodobieństwem* $1-4^{-k}$.

Co więcej, ograniczenie 1/4 jest dla wielu liczb n znacznie zawyżone. Większe liczby mają z reguły więcej czynników pierwszych, często też występują liczby podzielne przez kwadrat liczby pierwszej. Gdy uwzględnić te szczegóły i dokładnie zaanalizować test Millera-Rabina, można otrzymać silniejsze rezultaty:

Fakt 2.4 *Jeśli będziemy generować losowe liczby k-bitowe i szukać liczb pierwszych t-krotnym testem Millera-Rabina, to szansa błędnego znalezienia liczby złożonej $p_{k,t}$ da się ograniczyć przez*

$$p_{k,1} \leqslant k^2 4^{2-\sqrt{k}}$$

$$p_{k,t} \leqslant k^{3/2} \frac{2^t}{\sqrt{t}} 4^{2-\sqrt{tk}}$$

$$p_{k,t} \leqslant \frac{1}{7} k^{15/4} 2^{-k/2-2t}$$

dla dostatecznie dużych k.

Dowód. Oszacowania te pochodzą z pracy [DLP93].

Algortym Millera-Rabina jest bardzo łatwo zaimplementować. Jego złożoność czasowa wynosi $O(k(\lg n)^3)$, zakładając koszt mnożenia liczb n cyfrowych rzędu $O((\lg n)^2)$. W połączeniu z powyższym faktem pozwala to stwierdzić, że jest to najlepszy test do generowania losowych liczb pierwszych używanych w kryptografii RSA.

Zauważmy jeszcze, że szukając losowej liczby pierwszej o m cyfrach znajdziemy taką po oczekiwanej liczbie prób $O(\lg m)$, gdyż liczby złożone test wykrywa w oczekiwanym czasie $O(1)$. Optymalizując ten algorytm korzysta się z też z podzielności przez małe liczby pierwsze, które odsiewają natychmiast wielu kandydatów.

Warto wspomnieć, że przy założeniu uogólnionej hipotezy Riemanna (a jest to jedna z wielkich nieudowodnionych jak dotąd hipotez matematycznych) Bach pokazał [Ba85], że dla każdej liczby złożonej n istnieje podstawa $a < 2(\lg n)^2$, dla której n nie spełnia tego testu. Wobec tego wystarczyłoby wykonać $2(\lg n)^2$ iteracji testu, by otrzymać poprawny wynik. Taki algorytm jest wielomianowy, jego koszt jest rzędu $O((\lg n)^5$.

2.3. Test Solovaya-Strassena

Inny znany test pierwszości, opiera się na tożsamości

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n} \tag{2.3}$$

która jest prawdziwa dla każdej nieparzystej liczby pierwszej n i dowolnej liczby całkowitej a. Liczby złożone n, które spełniają 2.3, nazywamy liczbami pseudopierwszymi Eulera, a test oparty na tej równości testem Solovaya-Strassena. Jest on nieco słabszy od testu Rabina-Millera, w tym sensie, że

Fakt 2.5 *Jeśli n jest liczbą silnie pseudopierwszą przy podstawie a, to też jest liczbą pseudopierwszą Eulera przy podstawie a.*

Fakt 2.6 *Dla każdej liczby nieparzystej złożonej n, conajmniej $1/2$ wszystkich podstaw $a \in Z_n^*$ nie spełnia warunku 2.3*

Dowód. Dowody tych faktów zawarto w [Koblitz].

2.4. Test Frobeniusza

Wynaleziono i opisano jeszcze wiele innych testów pierwszości, jak np. oparte na ciągach rekurencyjnych modulo n testy: Lucasa, Fibonacciego, Lehmera i Perrina. Grantham w [Gr01] przeformułował je w kontekście ciał skończonych, tj. obliczeń modulo wielomian, uogólnił i zaproponował nowy test, nazwany przezeń testem Frobeniusza. Nazwa pochodzi od wykorzystania algebraicznych własności tzw. automorfizmu Frobeniusza. Jego szczególnym przypadkiem – dla wielomianów kwadratowych – jest test QFT (skrót od Quadratic Frobenius Test), który opiszemy.

Grantham pokazał w [Gr98] oszacowanie błędu testu QFT $1/7710$, oraz wyrafinowany sposób jego implementacji, w którym złożoność czasowa wynosi asymptotycznie 3 razy tyle, co testu Millera-Rabina. Interesujący wynik, choć nie zapowiada się, by mógł zdetronizować użyteczność testu Millera-Rabina, ponieważ ewentualne korzyści czasowe są niewielkie, a poziom skomplikowania wysoki.

2.4.1. Algorytm testu QFT

Zakładamy, że n jest liczbą nieparzystą, bez dzielników pierwszych mniejszych od $B = 50000$, nie będącą kwadratem liczby całkowitej.

Wybieramy wielomian $f(x) = x^2 - bx - c$, taki, że $\left(\frac{b^2+4c}{n}\right) = -1$, oraz $\left(\frac{-c}{n}\right) = 1$. Możemy to robić losując liczby $b, c \in Z_n$ i sprawdzając te warunki, mniej więcej $1/4$ wszystkich takich wielomianów się nadaje.

Dalej przeprowadzamy kilka obliczeń, podobnych do tych z testu Rabina-Millera, w pierścieniu $R = Z_n[x]/f(x)$. Pierścień ten składa się z wielomianów stopnia co najwyżej jeden o współczynnikach z Z_n. Pierścień Z_n zanurza się w R w naturalny sposób jako wielomiany stałe. Oto tożsamości, jakie są spełnione, gdy p jest liczbą pierwszą:

$$x^{(n+1)/2} \in Z_n$$

$$x^{n+1} \equiv -c$$

$$x^{n^2-1} \equiv 1$$

Szczegóły testu przedstawione są w algorytmie 2

Może się zdarzyć, że w trakcie testu wystąpi problem z wykonaniem dzielenia w Z_n, na przykład przy obliczaniu symboli Jacobiego. Ale wtedy możemy być zadowoleni, bo to oznacza, że znaleźliśmy dzielnik liczby złożonej n.

2.4.2. Analiza testu QFT

Twierdzenie 2.7 *Jeśli n jest liczbą pierwszą, to test QFT na pewno rozpozna n jako przypuszczalnie pierwszą.*

Algorytm 2 test QFT

Dane wejściowe: n, $f(x) = x^2 - bx - c$, $\left(\frac{b^2+4c}{n}\right) = -1$, $(\frac{-c}{n}) = 1$

if $x^{(n+1)/2} \notin Z_n$ w R **then**
n jest na pewno złożone
end if
if $x^{n+1} \not\equiv -c$ w R **then**
n jest na pewno złożone
end if
Niech $n^2 - 1 = 2^r s$, gdzie $2 \not| n$.
if $x^s \not\equiv 1$ w R, oraz $x^{2^j s} \not\equiv -1$ w R dla wszystkich $0 \leqslant j \leqslant r-2$ **then**
n jest na pewno złożone
end if
n jest przypuszczalnie pierwsze

Dowód. Skoro n jest pierwsze, to wielomian f jest nierozkładalny nad ciałem Z_n, bo wiemy, że jego wyróżnik $b^2 + 4c$ nie jest resztą kwadratową modulo n. Wtedy $R = Z_n[x]/f(x)$ jest ciałem.

Rozważmy wielomian $f(y) = y^2 - by - c \in R[y]$. Jednym z jego pierwiastków jest wielomian x, bo $f(x) = 0$ w R. Ponadto z faktu 1.5 mamy $f(x^n) \equiv f(x)^n = 0^n = 0$ w R, a zatem x^n też jest pierwiastkiem f. Oczywiście $x^n \neq x$, ponieważ wtedy dla każdego $w \in R$ byłoby $w^n = w$ a to równanie może mieć najwyżej n pierwiastków. Zatem x i x^n są dwoma różnymi pierwiastkami wielomianu f. Z wzoru Viete'y otrzymujemy drugi krok testu $x^{n+1} = x^n x = -c$.

Skoro $x^{n+1} \equiv -c$, oraz $-c$ jest resztą kwadratową modulo n (z założenia $(\frac{-c}{n}) = 1$), to oba pierwiastki z liczby $-c$ należą do Z_n. Zatem $x^{(n+1)/2} \in Z_n$, czyli pierwszy krok testu jest spełniony.

Ostatni krok testu jest analogiczny do testu Millera-Rabina. Rozmiar grupy multiplikatywnej R wynosi $N = n^2 - 1$, więc musi być spełnione $x^N \equiv 1$ w R. Ponieważ R jest ciałem, pierwiastki kwadratowe z 1 to tylko ± 1, i stosujemy identyczne rozumowanie jak w tamtym teście. Jedyna różnica jest taka, że nie musimy sprawdzać potęg $x^{2^j s}$ dla $j > r - 2$, gdyż $x^{2^{r-1} s} = x^{(n^2-1)/2} = (x^{(n+1)/2})^n - 1 \equiv 1$, jako że $x^{(n+1)/2} \in Z_n$.

Twierdzenie 2.8 *Niech n jest liczbą nieparzystą nie będącą pełnym kwadratem. Istnieje co najmniej $\frac{(n-1)^2}{4}$ różnych par $(b, c) \in Z_n \times Z_n$ takich, że $\left(\frac{b^2+4c}{n}\right) = -1$ i $(\frac{-c}{n}) = 1$ albo $1 < \gcd(b^2 + 4c, n) < n$ lub $1 < \gcd(c, n) < n$. To ostanie oznacza że obliczając symbol Jacobiego znajdziemy nietrywialny dzielnik n.*

Dla liczby n pierwszej można dokładnie pokazać, że jest tych par $\frac{(n-1)^2}{4}$. Gdy liczba n jest złożona, rozkładamy ją na czynniki pierwsze i analizujemy ten przypadek korzystając z chińskiego tw. o resztach oraz iloczynowej definicji symbolu Jacobiego.

To twierdzenie nie zachodzi, gdy n jest pełnym kwadratem, bo wtedy zgodnie z definicją $(\frac{a}{n}) = (\left(\frac{a}{\sqrt{n}}\right))^2 \neq -1$. Dlatego ten przypadek musimy osobno sprawdzić przed przystąpieniem do testu QFT.

Wniosek 2.9 *Szansa porażki przy znajdowaniu odpowiednich współczynników b, c po k krokach nie przekracza $(3/4)^k$. Oczekiwany koszt ich znajdowania to nie więcej jak 4 iteracje, czyli $O((\lg n)^2)$ operacji na bitach.*

Twierdzenie 2.10 *Każda złożona liczby nieparzysta jest rozpoznawana przez test QFT jako przypuszczalnie pierwsza z prawdopodobieństwem nie większym niż* $1/7710$.

Dowód. Dowód, rozpatrujący wiele przypadków, znajduje się w [Gr98]. To oszacowanie zapewne nie jest ostateczne, jako że trudno skonstruować przykład liczby złożonej o tak dużej szansie błędnego rozpoznania.

Nie przeprowadzono też szczegółowej analizy tego testu użytego do generowania losowych liczb zadanej długości.

2.4.3. Implementacja i złożoność testu QFT

Na potrzeby tego podrozdziału będziemy liczyć koszty operacji w mnożeniach w Z_n. Dodawanie, obliczanie $(\frac{-}{n})$ zajmują $o(1)$ mnożeń.

Test QFT można zaimplementować tak, by jego koszt obliczeniowy wynosił tyle co 3 iteracje testu Millera-Rabina, czyli $(3+o(1))\lg n$ mnożeń modulo Z_n. Zauważmy, że 3 iteracje testu MR dają szansę błędu na poziomie $(1/4)^3 = 1/64$, zdecydowanie większą niż test QFT. Niestety, taka implementacja testu QFT jest bardzo skomplikowana. Zarysujemy tu tylko jej kluczowe idee.

Fakt 2.11 *Określmy trzy ciągi* $A_j, B_j, C_j \in Z_n$ *wzorami* $A_j = x^j + (b-x)^j \bmod (x^2 - bx - c)$, $B_j = \frac{x^j - (b-x)^j}{2x-b} \bmod (x^2 - bx - c)$, $C_j = c^j$.

Mając dane wartości (A_j, B_j, C_j) *i* (A_k, B_k, C_k) *można obliczyć* $(A_{j+k}, B_{j+k}, C_{j+k})$ *za pomocą* $8 + o(1)$ *mnożeń. Taką operację nazywamy dodawaniem łańcuchowym. Można też obliczyć* (A_{2j}, B_{2j}, C_{2j}) *z* (A_j, B_j, C_j) *przy użyciu* $3 + o(1)$ *mnożeń. Tą operację nazwiemy podwojeniem.*

Z wartości A_j *i* B_j *można wyliczyć* x^j *poprzez* $2 + o(1)$ *mnożeń.*

Dowód. Zauważmy, że chociaż w definicji A_j, B_j, C_j używamy wyrażeń z wielomianami, ich wyniki są stałymi. Istotnie, jest tak dla $j = 0, 1$ i zachodzą rekurencyjne wzory

$$A_{j+k} = \frac{1}{2}(A_j A_k + (b^2 + 4c) B_j B_k)$$

$$B_{j+k} = \frac{1}{2}(A_j B_k + A_k B_j)$$

$$C_{j+k} = C_j C_k$$

$$A_{2j} = A_j^2 - 2(-1)^j C_j$$

z których też otrzymujemy szybkie metody obliczania tych liczb.

Fakt 2.12 *Można wyliczyć* (A_j, B_j, C_j) *za pomocą* $(1 + o(1))\lg j$ *podwojeń i* $o(\lg j)$ *dodawań łańcuchowych, czyli przy użyciu* $(3 + o(1))\lg j$ *mnożeń. Algorytm który to potrafi opisany jest w drugim tomie „Sztuki programowania" [KnuthII].*

Możemy zatem obliczyć $x^{(n-1)/2}, x^{(n+1)/2}, x^{n+1}$ w czasie $(3 + o(1))\lg n$ mnożeń. Jeśli, jak wyjść w teście powinno, $x^{n+1} \equiv -c$, to $x^n \equiv b - x$. Korzystając z tego i obliczonych wcześniej wartości, można obliczyć wartość $x^{2^e s}$ w stałej liczbie mnożeń. Metodą binarnego wyszukiwania szukamy wśród wartości $x^s, x^{2s}, x^{4s}, \ldots, x^{2^j s}$ miejsce, gdzie zaczynają się wartości 1, i sprawdzamy, czy bezpośrednio przed nią wystepuje wartość -1.

2.5. Test EQFT

W pracy [DF01] zaproponowano i zanalizowano pewną wariację na temat testu QFT, nazwaną EQFT (Extended QFT). Podobnie jak w teście QFT, operujemy na pierścieniu wielomianów $Z_n[x]/f(x)$, ale tym razem nie losujemy różnych f za każdą iteracją testu, raczej, jak w teście Millera-Rabina zmieniamy element podnoszony do potęgi. Z pozoru może ta zmiana wydawać się drobiazgiem, bo o ile tylko n jest pierwsze, a f jest wielomianem nierozkładalnym, to zawsze $Z_n[x]/f(x) \sim GF(n^2)$ – jest tylko jedno ciało skończone o n^2 elementach. Jednakże, zmiana ta pozwala nam wykorzystywać znalezione pierwiastki z -1 z poprzednich iteracji, a także dobrać wielomian f o wygodnej dla obliczeń postaci.

Rozważmy pierścień $R = Z_n[x]/(x^2 - c)$, gdzie c jest nieduże i spełnia $(\frac{c}{n}) = -1$.

Definicja 2.1 *Określmy sprzężenie jako odwzorowanie* $\overline{\cdot}: R \to R$, $\overline{ax+b} = -ax + b$ *oraz normę* $N: R \to Z_n$, $N(z) = z\overline{z}$. *Sprzężenie i norma są homomorfizmami mulitplikatywnymi.*

Jeśli n jest pierwsze i c nie jest resztą kwadratową, to R jest ciałem izomorficznym z $GF(n^2)$. Wtedy zachodzą następujące własności:

$$z^n = \overline{z}$$

$$z^{(n^2-1)/2} = N(z)^{(n-1)/2} = \left(\frac{N(z)}{n}\right)$$

Test działa w taki sposób, że wybieramy losowo element $z \in R$, taki, że $\left(\frac{N(z)}{n}\right) = 1$. Sprawdzamy wtedy powyższe równości, a potem wykonujemy procedurę podobną do testu Millera-Rabina, ale rozszerzoną o badanie pierwiastków z -1 i pierwiastków trzeciego stopnia z 1.

Zauważmy, że jeśli n jest pierwsze, to w R istnieją dokładnie 3 pierwiastki trzeciego stopnia z jedności, $1, \theta_3, \theta_3^{-1}$, oraz 4 pierwiastki czwartego stopnia, $\pm 1, \pm\theta_4$. Rozkładamy $n^2 - 1 = 2^u 3^v q$, gdzie q nie dzieli się przez 2 i 3. Możemy obliczyć ciąg wartości $z^{2^i 3^v q}$, $0 \leqslant i < u - 1$, i podobnie $z^{2^u 3^j q}$, $0 \leqslant j \leqslant v$. Podczas tych obliczeń możemy znaleźć wartości θ_3, θ_4. Możemy je zapamiętać i użyć w następnej iteracji testu (jako że R się nie zmienia, to i te pierwiastki nie powinny się zmienić). Jeśli znajdziemy więcej „pierwiastków" niż to możliwe dla R będącego ciałem, wtedy na pewno n jest liczbą złożoną. To rozszerzenie nie opiera się na szczególnym rodzaju wykorzystywanego ciała i można też zastosować je do zwykłego testu Millera-Rabina.

W tej samej pracy przeprowadzono analizę tego testu. W pesymistycznym przypadku ograniczono błąd t iteracji do $256/24^{4t}$. Badano też błąd w średnim przypadku, generując losowej liczby losowe k-bitowe przy użyciu t iteracji. Otrzymano wynik:

Twierdzenie 2.13 *Dla* $2 \leqslant t \leqslant k - 1$ *błąd ten jest rzędu* $O(k^{3/2} 2^{(\sigma_t+1)t} t^{-1/2} 4^{-\sqrt{2\sigma_t tk}})$, *gdzie* $\sigma_t \to \lg(24) \approx 9.2$.

Porównując podobne oszacowanie dla błędu testu Millera-Rabina w średnim przypadku pokazane z pracy [DLP93] $p_{k,t} = O(k^{3/2} 2^t t^{-1/2} 4^{-\sqrt{tk}})$, można snuć wniosek, że test EQFT daje nam asymptotycznie efekt 9-krotnego powtarzania testu Millera-Rabina, podczas gdy można go zaimplementować tak, by średni czas działania wynosił około 2 razy tyle co test Millera-Rabina. Nie jest to jednak całkiem jasne, jak w rzeczywistości te testy mają się do siebie. Trudno rozstrzygnąć to eksperymentalnie, gdyż te szanse błędu są naprawdę nieduże i trzeba by przeprowadzić zbyt wiele prób żeby osiągnąć przybliżony wynik.

Rozdział 3

Dowodzenie pierwszości

Probabilistyczne testy pierwszości mylą się rzadko, ale nie gwarantują nam uzyskania poprawnego wyniku. Nie można traktować wyniku takiego testu jako ścisły, matematyczny dowód pierwszości liczby. Istnieją jednak metody, które pozwalają wykazywać pierwszość. Będziemy je nazywać algorytmami dowodzenia pierwszości. Oczywiście, można wykazać pierwszość liczby n sprawdzając po kolei, czy nie dzieli się ona przez kolejne liczby od 2 aż do $\sqrt{n}$, ale znane są efektywniejsze metody, lecz nie tak szybkie jak probabilistyczne testy pierwszości.

Zwykle w procesie dowodzenia pierwszości znajdujemy pewne dane świadczące, w oparciu o pewne twierdzenia matematyczne, że dana liczba jest pierwsza. Takie dane nazywamy certyfikatem pierwszości tej liczby. W niektórych metodach zweryfikowanie certyfikatu wymaga mniej obliczeń niż jego znalezienie. W innych zaś sprawdzenie certyfikatu niesie ze sobą główny koszt obliczeniowy dowodu.

3.1. Test Lucasa

Aby dowieść pierwszości liczby n, możemy skorzystać z tw. Eulera, które mówi, że $a^{\varphi(n)} \equiv 1 \pmod{n}$. Jeśli n jest pierwsze, to $\varphi(n) = n-1$, w przeciwnym przypadku $\varphi(n) < n-1$. Zatem, jeśli znajdziemy takie a, by $a^{n-1} \equiv 1 \pmod{n}$ oraz $a^k \not\equiv 1 \pmod{n}$ dla $0 < k < n-1$, to pokażemy, że n jest pierwsze.

Gdyby miało miejsce $a^k \equiv 1 \pmod{n}$ oraz $a^{n-1} \equiv 1 \pmod{n}$, to wtedy $a^{\gcd(k,n-1)} \equiv 1 \pmod{n}$. Stąd wniosek, że wystarczy sprawdzić, czy $a^{\frac{n-1}{d}} \not\equiv 1 \pmod{n}$ dla wszystkich dzielników pierwszych $d|n-1$. Potrzebny jest rozkład liczby $n-1$ na czynniki pierwsze. Na ogół ciężko jest go znaleźć, ale nie o to nam chodzi – przyjmijmy, że jest nam dany.

Ten test można odrobinę ulepszyć, gdyż można używać osobnych podstaw a dla każdego dzielnika pierwszego $d|n-1$. Zachodzi bowiem tw.

Twierdzenie 3.1 (Lucas) *Niech $n > 1$. Jeśli dla każego dzielnika pierwszego $d|n-1$ istnieje a takie, że $a^{n-1} \equiv 1 \pmod{n}$ oraz $a^{(n-1)/d} \not\equiv 1 \pmod{n}$, to n jest liczbą pierwszą.*

Certyfikat dla liczby n składa się z przedstawienia liczby $n-1$ w postaci iloczynu liczb $n-1 = d_1 d_2 \cdots d_k$, certyfikatu pierwszości dla każdej z liczb $d_1, d_2, \ldots, d_k$, oraz odpowiednich liczb $a_1, a_2, \ldots a_n$ spełniających założenia tw. Lucasa. Ta rekurencyjna definicja jest poprawna, bo liczby $d_i < n$ są coraz mniejsze i oczywiście nie dojdzie do zapętlenia. Znalezienie takiego certyfikatu może być trudne, chyba że $n-1$ jest szczególnej postaci, natomiast jego weryfikacja wymaga $O((\lg n)^4)$ operacji na bitach.

Odnotujmy pokrótce, że istnieje wiele sposobów dowodzenia pierwszości liczb o szczególnych własnościach, na przykład takich, że $n-1$ albo $n+1$ mają szczególnej postaci rozkład

na czynniki pierwsze. Jednym z najsłynniejszych w tej dziedzinie jest test Lucasa-Lehmera, sprawdzający pierwszość liczb Mersenne'a, czyli liczb postaci $2^n - 1$. Testy pierwszości dla liczb specjalnej postaci pozostają poza zakresem niniejszej pracy.

3.2. Metoda krzywych eliptycznych

Test ECPP to dowodzenie pierwszości oparte na krzywych eliptycznych. Krzywa eliptyczna $E_p(a,b)$ to zbiór punktów $(x,y) \in Z_p^2$ spełniających równanie $y^2 = x^3 + ax + b \pmod p$. O ile tylko krzywa nie jest zdegenerowana ($4a^3 + 27b^2 \neq 0$), można wprowadzić na punktach krzywej działanie, które nadaje $E_p(a,b)$ strukturę grupy przemiennej.

Możemy użyć tej grupy do udowodnienia pierwszości liczby p w taki sam sposób jak w teście Lucasa używaliśmy niejawnie grupy Z_p^*. Przewaga krzywych eliptycznych kryje się w tym, że rozmiar tamtej grupy $|Z_p^*| = p-1$ jest stały, natomiast rozmiar grupy $E_p(a,b)$ zawiera się w przedziale

$$p + 1 - 2\sqrt{p} \leqslant |E_p(a,b)| \leqslant p + 1 + 2\sqrt{p}$$

i zmienia się mniej więcej jednorodnie wraz ze zmianą parametrów a, b krzywej. Możliwe zatem, że znajdziemy takie paremtry, by rozmiar grupy był liczbą szczególnej postaci, np. łatwo rozkładalną na czynniki pierwsze. Obliczanie rozmiaru grupy krzywej eliptycznej jest skomplikowane, ale wykonalne.

Krzywe eliptyczne w dowodzeniu pierwszości pierwsi wprowadzili S. Goldwasser i J. Killian [GK86]. Testu ECPP został zaimplementowany m.in. przez A. O. L. Atkina i F. Moraine'a [ECPP] i opisany przez nich w [AM93].

Największa liczba pierwsza udowodniona testem ECPP ma 19524 bity długości (około 3000 cyfr dziesiętnych). Obliczenia trwały przy tym około miesiąca. Jest to rekord wśród metod dowodzenia pierwszości dla liczb ogólnej postaci. Nie znaczy to, że każdą liczbę mniejszej długości da się równie szybko sprawdzić tym testem – czas działania mocno się waha. Bazując na heurystykach i hipotezach przypuszcza się, że złożoność czasowa tego algorytmu wynosi $O((\lg n)^{6+o(1)})$.

3.3. Metoda Adlemana-Pomerance'a-Rumely'ego

Przed metodami oparte na krzywych eliptycznych, najlepszym algorytmem dowodzenia pierwszości był test APR zaproponowany przez Adlemana, Pomerance'a i Rumely'ego [APR83], ulepszony później przez Cohena i H. W. Lenstrę [CL84] i zaimplementowany przez Cohena i A. K. Lenstrę [CL87]. Złożoność czasowa tego testu jest prawie wielomianowa i wynosi $(\lg n)^{O(\lg\lg\lg n)}$. Test ten nie tworzy certyfikatu, który by można było sprawdzić szybciej niż przez powtórzenie wszystkich obliczeń.

Rozdział 4

Wielomianowe dowodzenie pierwszości algorytmem AKS

W tym rozdziale opiszemy algorytm dowodzenia pierwszości Agrawala, Kayala i Saxeny, zwany dalej w skrócie AKS. Świat ujrzał ten algorytm stosunkowo niedawno, bo w sierpniu 2002 w opublikowanej w internecie pracy „PRIMES is in P" [AKS]. Jest to przełomowy wynki z punktu widzenia teorii złożoności obliczeniowej, ponieważ AKS jest pierwszym w pełni deterministycznym wielomianowym testem pierwszości. Co więcej, sam algorytm jest prosty, a dowód jego poprawności wcale nietrudny.

Metoda AKS opisana został przystępnie w pracy [Sm]. Mój opis bazuje na oryginalnym artykule oraz na pracy Bernsteina [Be1], zawierającej dobry przegląd ulepszeń AKS. Wpierw sformułujemy i udowodnimy twierdzenia stanowiące sedno metody AKS. Później, w częsci 4.3, przedstawimy wielomianowy algorytm sprawdzający pierwszość. Ulepszenia i optymalizacje omówimy w podrozdziale 4.5. Następnie, w podrozdziale 4.6, zaprezentujemy inspirowany metodą AKS algorytm Bernsteina dowodzenia pierwszości (z pracy [Be2]).

Phil Carmody prowadził w Internecie stronę z zasobami związanymi z algorytmem AKS ([fatphil.org]) – niestety, autor jest pacyfistą i ostatnio zablokował dostęp do niej z krajów wspierających USA (w tym Polski), pokazując im tylko stosowny komunikat `HTTP 403 No war on Iraq`.

4.1. Matematyczne podstawy metody Agrawala-Kayala-Saxeny

Faktem jest, że dla n pierwszych, to $w(x)^n \equiv w(x^n) \pmod{n}$. W szczególności dla jednomianu $w(x) = x - b$ zachodzi

$$(x-b)^n \equiv x^n - b^n \equiv x^n - b \pmod{n}$$

Takie przystawanie wielomianów nie ma miejsca, gdy n jest liczbą złożoną – w istocie, gdy liczba pierwsza p dzieli n w potędze α, to współczynniki przy x^{kn/p^α} wielomianu $(x-b)^n$ nie są podzielne przez p dla $\gcd(k,n) = 1$. Nie jesteśmy w stanie obliczyć całego wielomianu $(x-a)^n$, gdyż ten ma wykładniczą ilość współczynników. Ale za to możemy sprawdzać naszą równość modulo pewien wielomian wielomianowego stopnia r.

$$(x-a)^n \equiv x^n - a \pmod{n, x^r - 1} \tag{4.1}$$

Wielomian $x^r - 1$ wybrany jest ze względu na swoje szczególne właściwości. Gdybyśmy na jego miejscu wybierali losowy wielomian stopnia r, to otrzymalibyśmy całkiem silny test pro-

babilistyczny, a tak będziemy mogli wykorzystać w dowodzie własności $x^r - 1$. Dodatkowo zyskujemy na tym, że obliczenia modulo $x^r - 1$ przeprowadza się szczególnie łatwo.

Algorytm AKS zasadniczo składa się z dwóch faz: w pierwszej znajdowane są odpowiednie parametry r i s, w drugiej fazie tożsamość 4.1 sprawdzana jest dla s róznych wartości b. Jeśli liczba n przechodzi wszystkie te testy, to musi być potęgą liczby pierwszej $n = p^\alpha$, co możemy sprawdzić wcześniej osobno. Zachodzi bowiem twierdzenie

Twierdzenie 4.1 (Agrawal, Kayal, Saxena) *Niech n jest liczbą całkowitą dodatnią, q i r liczbami pierwszymi takimi, że $q|r-1$ oraz $n^{(r-1)/q} \bmod r \notin \{0,1\}$. Niech S będzie zbiorem s liczb całkowitych takich, że $\gcd(n, b-b') = 1$ dla różnych $b, b' \in S$. Załóżmy jeszcze, że*

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

oraz, że dla każdego $b \in S$ zachodzi w pierścieniu $Z_n[x]/x^r - 1$ równość

$$(x+b)^n \equiv x^n + b$$

Wtedy n jest potegą liczby pierwszej.

Dowód. Idea dowodu zawarta jest w pracy [AKS]. Sformułowanie twierdzenia i zwięzły dowód znajdują się w [Be1].

Na podstawie tego twierdzenia można pokazać wielomianowy deterministyczny algorytm testowania pierwszości. Trzeba przy tym pokazać, że odpowiednie liczby q, r, s istnieją, na dodatek wielomianowej wielkości. W oryginalnym artykule powoływano się na twierdzenie Fouvry'ego [F85], że istnieje wiele liczb pierwszych r takich, że $r-1$ ma dzielnik pierwszy q większy od $r^{2/3}$. Nie jest to łatwe ani eleganckie twierdzenie. Na dodatek opierając się na mocno ugruntowanych hipotezach można się spodziewać istnienia wiele liczb pierszych r takich, że $(r-1)/2$ jest pierwsze, co prowadzi do lepszych oszacowań złożoności algorytmu AKS. Z tego powodu pokażemy od razu nieco lepszy wariant twierdzenia AKS, dzięki czemu nie będzie trzeba później powoływać się na tw. Fouvry'ego.

Twierdzenie 4.2 (Agrawal, Kayal, Saxena, H. W. Lenstra, Jr.) *Niech n będzie liczbą całkowitą dodatnią, r liczbą pierwszą. Niech $v = ord_r(n)$ będzie rzędem n modulo r. Niech S będzie zbiorem s liczb całkowitych takich, że $\gcd(n, b-b') = 1$ dla różnych $b, b' \in S$. Załóżmy jeszcze, że dla każdego d będącego dzielnikiem $\varphi(r)/v$*

$$\binom{s+\varphi(r)-1}{s} \geqslant n^{2d\lfloor\sqrt{\varphi(r)/d}\rfloor}$$

oraz, że dla każdego $b \in S$ zachodzi w pierścieniu $Z_n[x]/x^r - 1$ równość

$$(x+b)^n \equiv x^n + b$$

Wtedy n jest potegą liczby pierwszej.

Zauważmy, że najsilniejsze ograniczenie zachodzi najpewniej dla maksymalnego $d = \varphi(r)/v$ (tak jest jak pominiemy część całkowitą).

Gdy n jest pierwiastkiem pierwotnym modulo r, to $v = \varphi(r)$ i twierdzenie nam się upraszcza:

Twierdzenie 4.3 *Niech n jest liczbą całkowitą dodatnią, r liczbą pierwszą. Niech n jest pierwiastkiem pierwotnym modulo r. Niech S będzie zbiorem s liczb całkowitych takich, że* $\gcd(n, b - b') = 1$ *dla różnych $b, b' \in S$. Załóżmy jeszcze, że*

$$\binom{s + \varphi(r) - 1}{s} \geqslant n^{2\lfloor\sqrt{\varphi(r)}\rfloor}$$

oraz, że dla każdego $b \in S$ zachodzi w pierścieniu $Z_n[x]/x^r - 1$ równość

$$(x + b)^n \equiv x^n + b$$

Wtedy n jest potęgą liczby pierwszej.

4.2. Dowód głównego twierdzenia AKS

Najpierw pokażemy dowód tw. 4.3, czyli prostszej wersji, gdzie zakładamy, że n jest pierwiastkiem pierwotnym modulo r. Załóżmy, że p jest dzielnikiem pierwszym liczby n. Dowód zorganizujemy i podzielimy na pare lematów.

Lemat 4.4 *Istnieją $(i_1, j_1) \neq (i_2, j_2)$: $i_1, j_1, i_2, j_2 \geqslant 0$, takie że dla $t = n^{i_1}p^{j_1}$, $u = n^{i_2}p^{j_2}$ zachodzi $t \equiv u \pmod{r}$, przy czym $|t - u| < n^{2\lfloor\sqrt{\varphi(r)}\rfloor}$*

Dowód lematu. Wiadomo, że $x^t = x^u \pmod{x^r - 1}$ wtedy i tylko wtedy, gdy $t \equiv u \pmod{r}$. Rozważmy wartości $n^i p^j \bmod r$ dla par (i, j) spełniających $0 \leqslant i, j \leqslant \lfloor\sqrt{\varphi(r)}\rfloor$. Tych wartości może być różnych $|Z_r^*| = \varphi(r)$, natomiast par (i, j) jest więcej, bo $(1 + \lfloor\sqrt{\varphi(r)}\rfloor)^2$. Wobec tego z zasady szufladkowej Dirichleta znajdą się różne pary $(i_1, j_1) \neq (i_2, j_2)$ takie, że $n^{i_1}p^{j_1} \equiv n^{i_2}p^{j_2} \pmod{r}$. Oznaczmy $t = n^{i_1}p^{j_1}$ i $u = n^{i_2}p^{j_2}$. Zauważmy, że $1 \leqslant t, u \leqslant n^{2\lfloor\sqrt{\varphi(r)}\rfloor}$, więc $|t - u| < n^{2\lfloor\sqrt{\varphi(r)}\rfloor}$.

Uwaga. Chcemy pokazać, że $t = u$ — wtedy, wobec $i_1 \neq i_2$, n musi być potęgą p.

Lemat 4.5 *Niech G będzie zbiorem wielomianów $\{\prod_{b \in S}(x + b)^{e_b} : e_b \geqslant 0\}$. Niech t, u będą liczbami z poprzedniego lematu. Pokażemy, że dla każdego wielomianu $g \in G$ zachodzi $g^t = g^u$ w $Z_p[x]/x^r - 1$.*

Dowód lematu. Tożsamość $g^t = g^u$ jest multiplikatywna. Wystarczy zatem, że pokażemy ją dla jednomianów $g = x + b$.

Skoro dla $b \in S$

$$(x + b)^n \equiv x^n + b \pmod{n, x^r - 1}$$

to

$$(x + b)^n \equiv x^n + b \pmod{p, x^r - 1}$$

Podstawiając x^{n^i} za x otrzymamy

$$(x^{n^i} + b)^n \equiv x^{n^{i+1}} + b \pmod{p, x^{n^i r} - 1}$$

czyli, ponieważ $x^r - 1 | x^{kr} - 1$,

$$(x^{n^i} + b)^n \equiv x^{n^{i+1}} + b \pmod{p, x^r - 1}$$

a z tego, przez indukcję po i

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

Biorąc pod uwagę jeszcze to, że $w(x^p) \equiv w(x)^p \pmod{p}$, otrzymujemy

$$(x+b)^{n^i p^j} = (x^{n^i} + b)^{p^j} = x^{n^i p^j} + b \pmod{p, x^r - 1}$$

A ponieważ $x^r = 1$ i $t = u \pmod{r}$, to

$$(x+b)^t = x^t + b = x^u + b = (x+b)^u \pmod{p, x^r - 1}$$

Lemat 4.6 *Niech $h(x)$ będzie nierozkładalnym wielomianem, dzielnikiem wielomianu cyklotomicznego $\Phi_r(x)$. Niech G określone jak poprzednio. Wtedy G zawiera conajmniej $\binom{s+\varphi(r)-1}{s}$ różnych modulo $h(x)$ wielomianów.*

Dowód lematu. Każdy element G jest postaci $\prod_{b\in S}(x+b)^{e_b}$ dla pewnego ciągu liczb $(e_b)_{b\in S}$. Rozważmy te ciągi dla których $e_b \geqslant 0$ i $\sum_b e_b < d = \varphi(r)$ – prosta kombinatoryka pokazuje, że jest ich właśnie $\binom{s+d-1}{s}$. Z założenia $\gcd(b-b', n)$ wynika, że wielomiany generowane przez różne ciągi liczb e_b są różne w $Z_p[x]$, bo mają różne pierwiastki, a Z_p jest ciałem.

Pozostaje pokazać, że są też różne w $Z_p[x]/h(x)$. Nie jest to oczywiste, bo maksymalny stopień naszych wielomianów w $Z_p[x]$ wynosi d i może przekroczyć $\deg h$. W tym miejscu w dowodzie twierdzenia 4.1 pokazuje się, że $\deg h \geqslant q$, gdzie q jest specjalnym dzielnikiem $r-1$. Skorzystamy z innej metody, i pokażemy w następnym lemacie, że elementy G stopnia $\leqslant d$ są różne modulo $h(x)$.

Lemat 4.7 *Niech G, h określone jak poprzednio. Niech n jest pierwiastkiem pierwotnym modulo r. Dla $e(x), f(x) \in G$, jeśli $e(x) = f(x)$ w $Z_p[x]/h(x)$, to $\Phi_r(x) | e(x) - f(x)$.*

Jeśli ponadto $\deg e, \deg f < \deg \Phi_r = \varphi(r)$, *to $e(x) = f(x)$ w $Z_p[x]$.*

Dowód lematu. Oznaczmy przez F ciało $Z_p[x]/h(x)$.

Załóżmy że dwa wielomiany $e(x) = \prod_b (x+b)^{e_b}$, $f(x) = \prod_b (x+b)^{f_b}$ są równe $e(x) = f(x)$ w F. Wtedy

$$e^{n^a}(x) = \prod_b (x+b)^{n^a e_b} = \prod_b (x^{n^a} + b)^{e_b} = e(x^{n^a})$$

w F dla $a \geqslant 0$; podobnie $f^{n^a}(x) = f(x^{n^a})$. Wobec tego

$$e(x^{n^a}) = e^{n^a}(x) = f^{n^a}(x) = f(x^{n^a})$$

w F. Rozważmy wielomian $g = e - f$. Jest on wielomianem o współczynnikach z Z_p. Ponieważ naturalnie $Z_p \subset F$, możemy potraktować g jako wielomian o współczynnikach z F, oznaczmy go przez $g(z) \in F[z]$.

Jak pokazaliśmy przed chwilą, pierwiastkami g w ciele F są na pewno elementy z $T = \{x^{n^a} : a \geqslant 0\}$. Skoro F jest ciałem, to $\prod_{t\in T}(z-t) \mid g(z)$. Z założenia n jest pierwiastkiem pierwotnym modulo r, więc $\{n^a \bmod r : a \in Z\} = Z_r^*$, a skoro $x^r = 1 \pmod{h(x)}$, to

$$\{x^{n^a} \in F : a \geqslant 0\} = \{x^c \in F : c \in Z_r^*\}$$

Zauważmy, że $h(x) = 0$ w F, a przecież h nierozkładalny, $h(x) \mid \Phi_r(x) \mid x^r - 1$, więc x jest jednym z pierwiastków r-tego stopnia z jedynki, a x^c dla $c \in Z_r^*$ są pozostałymi pierwiastkami; wszystkie są różne. Można na to spojrzeć tak, że F jest izomorficzne z rozszerzeniem ciała $Z_p(\zeta_r)$, gdzie ζ_r jest pierwiastkiem r-tego stopnia z 1.

W konsekwencji w $F[z]$ zachodzi:

$$\Phi_r(z) = \prod_{c \in Z_r^*} (z - x^c) \mid g(z)$$

Ale e, f i g są wielomianami stopnia mniejszego niż $\varphi(x) = \deg \Phi_r(x)$. Zatem $g = 0$, czyli $e = f$ w $Z_p[x]$.

Dowód. Pozostaje pokazać samo twierdzenie. Znajdujemy z lematu 4.4 odpowiednie u, t oraz nierozkładalny nad Z_p wielomian $h \mid \Phi_r$. Jeśli $u \neq t$, to wielomian $g^u - g^t$ może mieć w ciele $Z_p[x]/h(x)$ najwyżej $|u - t|$ niezerowych pierwiastków, bo jeśli np. $u > t$, to $g^u - g^t = g^t(g^{u-t} - 1)$. Ale wiemy z lematów 4.5, 4.6 i założeń twierdzenia, że jest tych pierwiastków conajmniej

$$|G| \geqslant \binom{s + \varphi(r) - 1}{s} \geqslant n^{2\lfloor\sqrt{\varphi(r)}\rfloor}$$

Tymczasem z lematu 4.4

$$n^{2\lfloor\sqrt{\varphi(r)}\rfloor} > |u - t|$$

Wobec tego $u = t$, czyli $n^{i_1}p^{j_1} = n^{i_2}p^{j_2}$ dla $(i_1, j_1) \neq (i_2, j_2) \Rightarrow i_1 \neq i_2$, czyli

$$n = p^{\frac{j_2 - j_1}{i_1 - i_2}}$$

co należało dowieść. □

Dowód tw. 4.2. Możemy teraz przystąpić do pokazania silniejszej wersji. Dowód będzie przebiegał podobnie jak poprzednio, załóżmy że p jest dzielnikiem pierwszym n.

Jeśli n nie jest pierwiastkiem pierwotnym modulo r, to możliwe, że wśród liczb $n^i p^j \bmod r$ wystąpi mniej wartości. Rozważmy $\langle n, p\rangle$, podgrupę Z_r^* generowaną przez n, p. Jej rozmiar dzieli $|Z_r^*| = \varphi(r)$, przyjmijmy, że $|\langle n, p\rangle| = \varphi(r)/d$. Skoro $v = |\langle n\rangle|$ dzieli $|\langle n, p\rangle|$, to $d \mid \varphi(r)$. Lemat 4.4 można teraz łatwo wzmocnić do

Lemat 4.8 *Istnieją* $(i_1, j_1) \neq (i_2, j_2)$: $i_1, j_1, i_2, j_2 \geqslant 0$, *takie że dla* $t = n^{i_1}p^{j_1}$, $u = n^{i_2}p^{j_2}$ *zachodzi* $t \equiv u \pmod r$ *i* $|t - u| < n^{2\lfloor\sqrt{\varphi(r)/d}\rfloor}$

Cena jaką płacimy za to wzmocnienie jest dużo wyższa. Skoro $\langle n\rangle$ niekoniecznie musi być całą grupą Z_r^*, trudniej będzie przeprowadzić dowody kolejnych lematów. Rozważmy grupę ilorazową $Z_r^*/\langle n, p\rangle$, jej rozmiar wynosi d. Wybierzmy układ d reprezentanów tej grupy $\{m_1, m_2, \ldots, m_d\} \subset Z_r$. Podstawiając x^{m_l} za x w lemacie 4.5 otrzymamy, że do zbióru wielomianów G spełniających $g^t = g^u$ należą też $x^{m_l} - b$ dla $b \in S$ i oczywiście ich wszelakie iloczyny.

Niestety, trudno powiedzieć które iloczyny w G są równe. Dlatego rozważamy układy d wielomianów z G. Podobnie jak poprzednio, dla ciągu liczb $(e_b)_{b \in S}$, $e_b \geqslant 0$, $\sum_b e_b \leqslant \varphi(r)$ tworzymy wielomian $e(x) = \prod_b (x+b)$ i rozważamy uklad wielomianów $(e(x^{m_1}), \ldots, e(x^{m_d})) \in G^d$. Pokażemy, że te układy są różne w $(Z_p[x]/h(x))^d$. Wtedy, zgodnie z założeniami twierdzenia, jest ich conajmniej

$$\binom{s + \varphi(r) - 1}{s} \geqslant n^{2d\lfloor\sqrt{\varphi(r)/d}\rfloor} > |t - u|^d$$

zatem w $F_p[x]/h(x)$ jest więcej niż $|t - u|$ elementów z G.

Lemat 4.9 *Niech* G, h *określone jak powyżej. Dla* $e(x), f(x) \in G$, *jeśli* $e(x^m) = f(x^m)$ *w* $Z_p[x]/h(x)$ *dla wszyskich* $m \in \{m_1, m_2, \ldots, m_d\}$, *to* $\Phi_r(x) | e(x) - f(x)$.

Jeśli ponadto $\deg e, \deg f < \deg \Phi_r = \varphi(r)$, *to* $e(x) = f(x)$ *w* $Z_p[x]$.

Dowód lematu. Podobnie jak w lemacie 4.7, rozważamy wielomian $g = f - e$. Okazuje się, że

$$e(x^{n^i p^j m}) = \prod_b (x^{n^i p^j m} + b)^{e_b} = \prod_b (x^m + b)^{n^i p^j e_b} = e(x^m)^{n^i p^j}$$

$$e(x^{n^i p^j m}) = e(x^m)^{n^i p^j} = f(x^m)^{n^i p^j} = f(x^{n^i p^j m})$$

a zatem $x^{n^i p^j m}$ są pierwiastkami g. Ale liczby $\{n^i p^j m \bmod r\}$ przyjmują wszystkie wartości z Z_r^*, więc możemy dalej użyć metody z lematu 4.7, by pokazać, że

$$\Phi_r(z) = \prod_{c \in Z_r^*} (z - x^c) \mid g(z) = e(z) - f(z)$$

4.3. Algorytm wielomianowy

Opierając się na twierdzeniu 4.2 pokażemy deterministyczny algorytm, który sprawdza czy dana jest liczba pierwsza w czasie wielomianowym. Algorytm ten, zaproponowany przez Lenstrę, jest wariantem oryginalnego. Nie jest najefektywniejszy, ale za to najłatwiej udowodnić jego poprawność i wielomianową złożoność. Algorytm ten wypisuje odpowiedź 1 wtedy i tylko wtedy, gdy wejście jest liczbą pierwszą (w zapisie dziesiątkowym).

Algorytm AKS Lenstry

- Sprawdź, czy wejście jest zapisem dziesiątkowym liczby całkowitej dodatniej n; jeśli nie, to wypisz 0 i zakończ.
- Sprawdź, czy n jest potęgą liczby pierwszej – sprawdź jej pierwiastek kwadratowy, sześcienny, itd. aż do pierwiastka stopnia $\lg n$; jeśli tak, wypisz 0 i zakończ.
- Znajdź najmniejszą liczbę pierwszą r, która nie dzieli liczby N

  $$N = 2n \prod_{i=1}^{4(\lg n)^2} (n^i - 1)$$

  Ponieważ $\lg N < k = (8 + o(1))(\lg n)^5$, oraz iloczyn wszystkich liczb pierwszych mniejszych niż $2k$ jest większy niż 2^k (tw. Czebyszewa), więc $r < 2k$ jest wielomianowej wielkości.
- Sprawdź, czy n jest liczbą pierwszą mniejszą lub równą r; jeśli tak, to wypisz 1 i zakończ.
- Sprawdź, czy n jest podzielne przez liczbę pierwszą mniejszą lub równą r; jeśli tak, to wypisz 0 i zakończ.
- Sprawdź, czy $(x + b)^n = x^n + b \pmod{n, x^r - 1}$ dla $b \in S = \{1, 2, \ldots, r\}$; jeśli nie, wypisz 0 i zakończ.
- Wypisz 1 i zakończ – n musi być pierwsze.

Poprawność ostatniego kroku tego algorytmu wynika z twierdzenia 4.2. Jeśli algorytm dotarł do ostatniego kroku, to n i r są względnie pierwsze, a także wszystkie $b \in S$ są względnie pierwsze z n. Liczba r jest pierwsza, więc $\varphi(r) = r - 1$. Rząd n modulo r wynosi $v > 4(\lg n)^2$. Rozmiar zbioru S wynosi $s = r$. Dla d będącego dzielnikiem $\varphi(r)/v$ zachodzi

$$d \leqslant \varphi(r)/v < \varphi(r)/4(\lg n)^2$$

$$2d\lfloor\sqrt{\varphi(r)/d}\rfloor \leqslant 2d\sqrt{\varphi(r)/d} = \sqrt{4d\varphi(r)} < \varphi(r)/(\lg n)$$
$$n^{2d\lfloor\sqrt{\varphi(r)/d}\rfloor} < n^{\varphi(r)/(\lg n)} = 2^{\varphi(r)}$$

Ale

$$\binom{s+\varphi(r)-1}{s} = \binom{2(r-1)}{r} > 2^{r-1} = 2^{\varphi(r)}$$

czyli spełnione są założnia twierdznia 4.2.

4.4. Efektywna złożoność algorytmu AKS

Algorytm AKS Lenstry, mimo że wielomianowy, nie jest efektywny. Można go optymalizować różnymi sposobami. Jako że najwięcej obliczeń zabiera druga faza algorytmu, czyli sprawdzenie równości wielomianów 4.1, szczególną uwagę należy zwrócić na odpowiedni dobór parametrów r i s. Najlepiej dla kandydatów na r szacować, jakie s jest potrzebne, by móc skorzystać z twierdzenia 4.3 lub 4.1, i wybrać te parametry, by zminimalizować późniejsze obliczenia. Warto też uwzględnić różne wzmocnienia twierdzenia AKS, co skutkuje zmniejszeniem złożoności obliczeniowej.

Nasuwa się pytanie, jaki jest efektywny rząd złożoności czasowej algorytmu AKS. W drugiej fazie algorytmu wykonujemy około $s \lg n$ podnoszeń do kwadratu wielomianów z pierścienia $Z_n[x]/(x^r-1)$, które można zapisać jako liczby o łącznej długości $O(\lg nr)$ bitów. Zakładając użycie szybkiej transformacji Fouriera do mnożenia w pierścieniu $Z_n[x]/(x^r-1)$ w czasie niemal liniowym, wszystkie obliczenia zajmą $O(s \lg n(\lg nr)^{1+o(1)})$. Wynika stąd, że rząd złożoności czasowej algorytmu jest w przybliżeniu proporcjonalny do iloczynu rs.

Wielkość iloczynu rs zależy od tego, jakiego rzędu trzeba dobrać r by najmniejsze s spełniające

$$\binom{s+\varphi(r)-1}{s} \geqslant n^{2\sqrt{\varphi(r)}}$$

było wielomianowej wielkości. Zgrubne oszacowania pokazują, że $r, s \approx (\lg n)^2$. Możemy przybliżyć $\lg \binom{s+\varphi(r)-1}{s} \approx \lg(s^r/r!) \approx r\lg s - r\lg r$ oraz $\lg n^{2\sqrt{\varphi(r)}} \approx 2r^{1/2}\lg n$, więc powinno być

$$r\lg s - r\lg r > 2r^{1/2}\lg n$$
$$\lg s > \lg r + r^{-1/2}\lg n$$

aby s było wielomianowe względem $\lg n$ musi zniknąć ostatni składnik, czyli r musi być rzędu $(\lg n)^2$; wtedy również $s \approx r$ powinno być tego rzędu.

Pytanie, czy możemy znaleźć r wielkości $(\lg n)^2$, takie by n było pierwiastkiem pierwotnym modulo r. Wedle dobrze ugruntowanych hipotezy, odpowiedź na to pytanie jest twierdząca. Każda liczba pierwsza r ma pierwiastek pierwotny. Jesli r ma pierwiastek pierwotny, to ma ich $\varphi(\varphi(r))$, więc szansa że losowo wybrane n jest pierwiastkiem pierwotnym liczby pierwszej r jest całkiem duża, zależy od dzielników liczby $r-1$, im ich mniej tym dla nas lepiej. Na przykład, gdy $r-1=2q$, gdzie q jest pierwsze, to szansa ta jest bliska $1/2$. Takie pary liczb pierwszych $q, 2q+1$ nazywamy liczbami pierwszymi Sofii Germain, wedle hipotezy występują one całkiem często, z gęstością rzędu $(\lg x)^{-2}$. To wystarcza na pewno dla istnienia r, q, s rzędu $(\lg n)^2$ odpowiednich do użycia twierdzenia 4.1.

Znajdując odpowiednie liczby r, s rzędu $O(\lg n)^2$ otrzymujemy złożoność czasową algorytmu AKS $(\lg n)^{6+o(1)}$; nie taką złą na tle innych metod dowodzenia pierwszości, niemniej

jednak obarczoną dużą stałą; w praktyce algorytm AKS, nawet z optymalizacjami, spisuje się gorzej od innych znanych algorytmów dowodzenia pierwszości.

4.5. Dalsze ulepszenia metody AKS

Twierdzenia, na których opiera się algorytm AKS, można poprawić kilkoma sposobami, osłabiając niezbędne oszacowania. W rezultacie poprawiamy złożoność czasową algorytmu (o stałą), ponieważ mniejsze parametry r, s są potrzebne do wykazania twierdzenia, i wtedy mniej mamy obliczeń do wykonania. Większość poprawek dotyczy oszacowań jednego z lematów dowodu.

4.5.1. Poprawki w znajdowaniu u, t

W lemacie 4.4 pokazano, że można znaleźć $u \equiv t \pmod r$ postaci $n^i p^j$, $i, j \geqslant 0$, takie, że $|u - t| < n^{2\lfloor\sqrt{\varphi(r)}\rfloor}$. Możemy to zrobić lepiej.

Zauważmy, że w ciele $Z_p[x]/h(x)$ podnoszenie wielomianu do p-tej potęgi jest operacją odwracalną, bo rozmiar grupy multiplikatywnej tego ciała wynosi $p^{\deg h} - 1$, więc

$$(w(x)^p)^{p^{\deg h - 1}} = w(x)^{p^{\deg h}} = w(x)^{p^{\deg h}-1} w(x) = w(x)$$

a skoro tak, to $g^{tp^k} = g^{up^k} \Rightarrow g^t = g^u$ w tym ciele. Dlatego wystarczy rozważać t, u postaci $(n/p)^i p^j$ (pamiętamy, że n/p jest liczbą całkowitą).

Samo zastąpienie $n^i p^j$ przez $(n/p)^i p^j$ prowadzi od razu do oszacowania $u, t \leqslant n^{\lfloor\sqrt{\varphi(r)}\rfloor}$. Można lepiej.

Lemat 4.10 *Niech p dzielnik pierwszy n, $\gcd(n, r) = 1$. Wśród wartości $\{(n/p)^i p^j : i, j \geqslant 0\}$ znajdziemy dwie u, t przystające do siebie modulo r, odległe od siebie nie więcej niż*

$$|u - t| < n^{\sqrt{\varphi(r)/3}}$$

Dowód.

Rozważmy trójkąt T na płaszczyźnie złożony z punktów (x, y), $x, y \geqslant 0$, ograniczonych przez prostą $(n/p)^x p^y \leqslant M = n^{\sqrt{\varphi(r)/3}}$. Potencjalne pary (i, j) leżą wewnątrz niego. Policzmy pole trójkąta T: jest to trójkąt prostokątny o wierzchołkach w punktach $(0, 0), (a, 0), (0, b)$ spełniających $(n/p)^a = M$ i $p^b = M$. Stąd $a = \log_{(n/p)} M = \frac{\ln M}{\ln(n/p)}$ i $b = \log_p M = \frac{\ln M}{\ln p}$. Z nierówności między średnią geometryczną i harmoniczną

$$|T| = \frac{ab}{2} \geqslant \frac{1}{2}\left(\frac{2}{1/a + 1/b}\right)^2 = 2\left(\frac{\ln M}{\ln(n/p) + \ln p}\right)^2 =$$

$$= 2\left(\frac{\ln M}{\ln n}\right)^2 = 2\left(\log_n M\right)^2 = 2\left(\sqrt{\varphi(r)/3}\right)^2 = \frac{2}{3}\varphi(r)$$

Poszukujemy par $(i, j) \neq (k, l)$, takich, że $(n/p)^i p^j \equiv (n/p)^k p^l \pmod r$, co oznacza, że $(n/p)^{i-k} p^{j-l} \equiv 1 \pmod r$, dla $(i - k, j - l) \neq (0, 0)$.

Rozważmy zbiór $L = \{(i, j) : (n/p)^i p^j \equiv 1 \pmod r\}$. Jest to krata, czyli liniowa podprzestrzeń wymiaru 2. Każda krata charakteryzuje się wyznacznikiem – wyznacznik kraty rozpiętej

w R^n na bazie wektorów $\mathbf{v}_1, \ldots, \mathbf{v}_n \in R^n$ to po prostu wyznacznik macierzy złożonej z tych wektorów

$$\det \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_n \end{bmatrix}$$

Ten wyznacznik to objętość równoległościanu rozpiętego na tych wektorach; można sobie wyobrazić, że charakteryzuje on, jak rzadko na płaszczyźnie położone są punkty z kraty – mówiąc niezbyt ściśle, gdybyśmy zliczyli punkty z kraty L wewnątrz dużego koła o polu A, znalazłoby się tam około $A/\det L$ punktów.

Wyznacznik naszej kraty $\det L$ nie przekracza $\varphi(r)$, ponieważ płaszczyzna Z^2 rozpada się na najwyżej $\varphi(r)$ przesuniętych krat $L(c) = \{(i,j)\colon (n/p)^i p^j \equiv c \pmod r\}$, dla $c \in Z_r^*$.

Skorzystamy z następującego twierdzenia:

Twierdzenie 4.11 (Minkowski) *Niech L jest kratą w R^n. Niech C jest zbiorem wypukłym, środkowosymetrycznym względem punktu 0. Jeśli pole C jest równe conajmniej $2^n \det L$, to w zbiorze C leży przynajmniej jeden niezerowy punkt z L.*

Niech $C = T - T = \{t - t'\colon t, t' \in T\}$. Jest to wypukły i środkowo symetryczny sześciokąt o polu $|C| = 6|T| \geqslant 4\varphi(r) \geqslant 4 \det L$. Z tw. Minkowskiego istnieje niezerowy punkt $(i,j) \in C \cap L$. Bez straty ogólności $i \geqslant 0$ (jeśli $i < 0$ to rozpatrzmy $-(i,j) \in C \cap L$). Jeśli $j > 0$, to $(i,j) \in T$, wtedy kładziemy $u = (n/p)^i p^j$, $t = 1$. W przeciwnym przypadku $(i,0), (0,-j) \in T$ i przyjmujemy $u = (n/p)^i$, $t = p^{-j}$.

4.5.2. Lepsze oszacowania rozmiaru zbioru G

Podstawienie $1/x$ za x

Przypomnijmy, G jest zbiorem generowanym przez iloczyny jednomianów ze zbioru $\{(x + b)\colon b \in S\}$. Niewielkim wysiłkiem możemy podwoić zbiór S, zaliczając do generatorów również jednomiany $\{(x+1/b\colon b \in S\}$. Jeśli bowiem $(x+b)^n = x^n + b$ w $Z_n[x]/(x^r - 1)$, to podstawiając $1/x$ za x otrzymujemy

$$(1/x + b)^n = (1/x)^n + b$$

$$(1 + bx)^n = 1 + bx^n = 1 + b^n x^n = 1 + (bx)^n$$

$$(1/b + x)^n = 1/b^n + x^n = 1/b + x^n$$

Ta sztuczka działa pod warunkiem $b^n = b \pmod n$, co powinno zachodzić dla n liczby pierwszej, – musimy to dodatkowo sprawdzić we wstępnej fazie testu. Ponadto, aby upewnić się, że wielomiany $x+b, x+1/b'$ są względnie pierwsze, musimy sprawdzić, czy $\gcd(n, bb'-1) = 1$ dla wszystkich par różnych $b, b' \in S$.

Ujemne potęgi

Lepsze oszacowanie wielkości G uzyskamy dopuszczając „ujemne" potęgi jednomianów generujących G. Aby móc dzielić przez te jednomiany w pierścieniu $Z_p[x]/\Phi_r(x)$, potrzeba i wystarcza, by te jedomiany były względnie pierwsze z nierozkładalnymi $h(x)$ dzielnikami $\Phi_r(x)$. Znany fakt o wielomianach cyklotomicznych mówi, że $\deg h = ord_r(p)$. Wystarczy zatem, jeśli tylko wybierzemy za p taki dzielnik pierwszy, by $ord_r(p) > 1$. Na pewno takie p istnieje, jeśli tylko zgodnie z założeniami twierdzenia 4.3 n jest pierwiastkiem pierwotnym modulo r.

Ustalmy $d \geqslant 0$. Niech E będzie zbiorem ciągów liczb całkowitych $(e_b)_{b\in S}$ takich, że $\sum_{e_b>0} e_b < \varphi(r) - d$ i $\sum_{e_b<0} |e_b| \leqslant d$. Dla ciągu $(e_b) \in E$ konstruujemy wielomian $\hat{e}(x) = \prod_b (x+b)^{d+e_b}$. Pokażemy, że wielomiany odpowiedające różnym ciągom są różne w $Z_p[x]/\Phi(r)$. Zauważmy, że dla $d = 0$ mamy sytuację taką samą jak w lemacie 4.6, lecz dla $d > 0$ liczba takich ciągów (e_b) może być sporo większa.

Lemat 4.12 *Niech $e, f \in E$, $e \neq f$ będą dwoma różnymi ciągami. Wtedy wielomiany im odpowiadające też są różne $\hat{e}(x) \not\equiv \hat{f}(x)$ w $Z_p[x]/\Phi_r(x)$.*

Dowód lematu. Załóżmy, że $\hat{e}(x) \equiv \hat{f}(x)$ w $Z_p[x]/\Phi_r(x)$. Wtedy przekształcamy:

$$\prod_{b\in S} (x+b)^{d+e_b} \equiv \prod_{b\in S} (x+b)^{d+f_b}$$

$$\prod_{e_b>0} (x+b)^{d+e_b} \prod_{e_b<0} (x+b)^{d+e_b} \equiv \prod_{f_b>0} (x+b)^{d+f_b} \prod_{f_b<0} (x+b)^{d+f_b}$$

$$\prod_{e_b>0} (x+b)^{e_b} \prod_{e_b<0} (x+b)^{e_b} \equiv \prod_{f_b>0} (x+b)^{f_b} \prod_{f_b<0} (x+b)^{f_b}$$

$$\prod_{e_b>0} (x+b)^{e_b} \prod_{f_b<0} (x+b)^{|f_b|} \equiv \prod_{f_b>0} (x+b)^{f_b} \prod_{e_b<0} (x+b)^{|e_b|}$$

Obie strony równości są wielomianami stopnia mniejszego niż $\varphi(r) - d + d = \deg \Phi_r$, więc równość zachodzi również w $Z_p[x]$, a wtedy muszą się zgadzać wykładniki. Dla każdego $b \in S$ zachodzi równość (zapis w notacji Iversona):

$$[e_b > 0]e_b + [f_b < 0]|f_b| = [f_b > 0]f_b + [e_b < 0]|e_b|$$

skąd wynika, że $e_b = f_b$. Co kończy dowód lematu. □

Lemat 4.13 *Liczba ciągów w E wynosi*

$$|E| = \sum_i \binom{s}{i} \binom{d}{i} \binom{s-i+\varphi(r)-1-d}{s-i}$$

można ją oszacować z dołu przez

$$|E| \geqslant \binom{s}{i} \binom{d}{i} \binom{s-i+\varphi(r)-1-d}{s-i}$$

dla wybranego i.

Dowód lematu. Wszystkie ciągi $e_b \in E$ możemy skonstruować następującą procedurą

- ustalamy i liczbę ujemnych wartości e_b,
- wybieramy i elementowy podzbiór $S_- \subset S$; można to zrobić na $\binom{s}{i}$ sposobów,
- wybieramy wartości $e_b < 0$ dla $b \in S_-$ tak, by $\sum_{b\in S_-} |e_b| \leqslant d$; można to zrobić na $\binom{d}{i}$ sposobów,
- wybieramy wartości $e_b \geqslant 0$ dla $b \in S \setminus S_-$ tak, by $\sum_{b\in S\setminus S_-} e_b < \varphi(r) - d$; można to zrobić na $\binom{s-i+\varphi(r)-1-d}{s-i}$ sposobów.

To pokazuje nam równość z lematu. Jest ona niepraktyczna, ciężką wyliczyć całą sumę, dlatego lepiej użyć szacowania jednym składnikiem (wszystkie składniki są nieujemne). Wybierając i maksymalizujące wielkość składnika możemy uzyskać całkiem rozsądne przybliżenie. Można też wybrać kilka wartości i i zsumować je, by uzyskać jeszcze lepsze oszacowanie.
□

Jak podaje Bernstein w [Be1], rozsądne wielkości parametrów jakie dobieramy w trakcie pierwszej fazy usprawnionego algorytmu AKS wynoszą

$$r \geqslant r_0 \approx 0.01(\lg n)^2, d \approx 0.5\varphi(r), i \approx 0.475\varphi(r)$$

odpowiednie $s \approx 5r$ znajdujemy wyszukiwaniem binarnym. Przy takich ustawieniach $rs = (0.00050266\ldots + o(1))(\lg n)^4$, co jest ponad milionkrotnym przypsieszeniem względem szacowania $rs = (1024 + o(1))(\lg n)^4$ z oryginalego algorytmu AKS.

Inne ulepszenia

Możliwe są inne ulepszenia twierdzenia AKS, np. można brać pod uwagę też wielomiany wyższego stopnia niż 1, albo lepiej szacować rozmiar grupy G, jak to zrobił Voloch w [Voloch]. Dobry przegląd tych usprawnień znajduje się w wymienionej już pracy Bernsteina.

4.6. Metoda Bernsteina dowodzenia pierwszości

Na podstawie algorytmu AKS i prac Berrizbeitii [Berriz] Bernstein zaproponował w [Be2] algorytm dowodzenia pierwszości, która działa w oczekiwanym czasie $(\lg n)^{4+o(1)}$. Główny pomysł polega na tym, by sprawdzać równość $(x-b)^n = x^n - b$ w pierścieniu modulo $x^r - a$ zamiast $x^r - 1$. Pozwala to nam użyć w dowodzie nie tylko jednomianów $x - b$, ale też $\zeta x - b, \zeta^2 x - b, \ldots, \zeta^{r-1} x - b$ dla pewnego $\zeta \neq 1$, co zwiększa efektywną wielkość zbioru S aż r razy. Dzięki temu praktycznie wystarczy nawet jedno sprawdzenie, tj. $|S| = 1$. To oczywiście zmniejsza czas działania algorytmu o czynnik rzędu $r = O((\lg n)^2)$.

Niestety, ta metoda wymaga, by r było dzielnikiem $n - 1$, na dodatek wielkości rzędu $(\lg n)^2$. Tak jest dla większości liczb n; jeśli tak nie jest, to można szukać takiej liczby całkowitej $d > 1$, by $n^d - 1$ miało dzielnik r rzędu wielkości $d^2(\lg n)^2$ – można pokazać istnienie takiego d rzędu podwielomianowego $d = \exp(O(\lg\lg\lg n \lg\lg\lg\lg n)) = (\lg n)^{o(1)}$. Sam algorytm i jego dowód poprawności stają się dużo bardziej skomplikowane. Jako podstawową strukturę używa się nie pierścienia Z_n, ale $Z_n[y]/f(y)$ dla $\deg f = d$. W złożoności obliczeniowej algorytmu d występuje w znacznej potędze, ale ponieważ jest podwielomianowej wielkości, nie wpływa to znacząco na teoretyczną złożoność obliczeniową. W praktyce jednak rozsądne jest tylko używanie tego algorytmu dla $d = 1$. Qi Cheng zaproponował [Cheng] wykorzystanie jednej fazy metody ECPP, by zredukować dowodzenie pierwszości n do dowodzenia pierwszości takiej liczby, by $n - 1$ miało pożądany dzielnik i dało się użyć tej metody w prostym przypadku $d = 1$.

4.6.1. Certyfikaty Bernsteina

Zbiór parametrów określających test pierwszości nazywamy certyfikatem. Będziemy się starać używać oznaczeń zbliżonych do tych co poprzednio, raczej niż oryginalnych oznaczeń Bernsteina.

Definicja 4.1 *Niech $n, d, r > 0$ oraz $c, c_- \geqslant 0$ będą liczbami całkowitymi. Niech $f(y) \in Z_n[y]$ jest wielomianem monicznym stopnia d (tj. z współczynnikiem przy y^d równym 1). Oznaczmy przez R pierścień $Z_n[y]/f(y)$. Niech $a \in R$. Niech $S \subset R$. Niech $s = |S|$. Załóżmy, że*

- $r|n^d - 1$,
- $a^{n^d-1} = 1$ *w* R,
- $a^{(n^d-1)/q} - 1$ *odwracalne w* R *dla każdego pierwszego dzielnika* $q|r$,
- *dla każdego* $b \in S$ *odwracalne w* R *są* b *i* $b^r - a$,
- *dla każdych różnych* $b, b' \in S$ *odwracalne w* R *jest* $b^r - (b')^r$,
- $\binom{rs}{c_-}\binom{c}{c_-}\binom{rs-c_-+r-1-c}{r-1-c} \geqslant n^{d\sqrt{r/3}}$,
- $(x-b)^{n^d} = a^{(n^d-1)/r}x - b$ *w pierścieniu* $R[x]/(x^r - a)$ *dla każdego* $b \in S$.

Wtedy $\{d, r, c, c_-, f, a, S\}$ *jest certyfikatem dla* n.

Dla jasności, napiszmy tą definicję dla szczególnego przypadku $d = 1$.

Definicja 4.2 *Niech* $n, r > 0$ *oraz* $c, c_- \geqslant 0$ *będą liczbami całkowitymi. Niech* $S \subset Z_n$. *Niech* $s = |S|$. *Załóżmy, że*

- $r|n - 1$,
- $a^{n-1} = 1 \pmod{n}$,
- $\gcd(n, a^{(n-1)/q} - 1) = 1$ *dla każdego pierwszego dzielnika* $q|r$,
- $\gcd(n, b) = \gcd(n, b^r - a) = 1$ *dla każdego* $b \in S$,
- $\gcd(n, b^r - (b')^r) = 1$ *dla każdych różnych* $b, b' \in S$,
- $\binom{rs}{c_-}\binom{c}{c_-}\binom{rs-c_-+r-1-c}{r-1-c} \geqslant n^{\sqrt{r/3}}$,
- $(x-b)^n = a^{(n-1)/r}x - b$ *w pierścieniu* $Z_n[x]/(x^r - a)$ *dla każdego* $b \in S$.

Wtedy $\{r, c, c_-, a, S\}$ *jest certyfikatem dla* n.

Twierdzenie 4.14 (Bernstein) *Jeśli* n *ma certyfikat* $\{d, r, c, c_-, f, a, S\}$, *spełniający wszystkie założenia definicji 4.1, to* n *jest potęgą liczby pierwszej.*

4.6.2. Dowód twierdzenia Bernsteina

Dowód. Kompletny dowód twierdzenia 4.14 zawarty jest w [Be2]. Dla uproszczenia pokażemy tutaj tylko szkic dowodu dla przypadku $d = 1$. Dowód jest podobny do dowodu twierdzenia AKS i wykorzystuje podobne sztuczki, co i tamten.

Załóżmy, że p jest dzielnikiem pierwszym n. Oznaczmy $\zeta = a^{(n-1)/r} \in Z_p$. Zachodzi $x^n \equiv \zeta x \pmod{p, x^r - a}$. Z własności certyfikatu $\zeta \neq 1$, więcej nawet, $ord(\zeta) = r$. Jako że rząd elementu dzieli rząd grupy, to $r|p - 1$.

Dla każdego $b \in S$, zachodzi $(x-b)^n = a^{(n-1)/r}x - b$ w $Z_n[x]/(x^r - a)$, czyli $(x-b)^n = \zeta x - b$ w $Z_p[x]/(x^r - a)$. Podstawiając $\zeta^m x$ za x otrzymujemy

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

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

bo $\zeta^r = 1$. Przez indukcję dla $i \geqslant 0$

$$(\zeta^m x - b)^{n^i} = \zeta^{m+i} x - b \pmod{p, x^r - a}$$

Wiadomo, że $x^p = \xi x \pmod{p, x^r - a}$ dla $\xi = a^{(p-1)/r} \in Z_p$. Ponieważ $\xi^r = 1$, to $\xi = \zeta^l$ dla pewnego l. Wtedy

$$(\zeta^m x - b)^{n^i p^j} = \zeta^{m+i+jl} x - b \pmod{p, x^r - a}$$

Rozważmy zbiór jednomianów $T = \{\zeta^m x - b : b \in S, m \in Z_r\}$. Wszystkie elementy T są różne i względnie pierwsze (z własności certyfikatu). Rozmiar $|T| = |Z_r||S| = rs$. Dla każdego $g(x) \in T$ zachodzi $(g(x))^{n^i p^j} = g(\zeta^{i+jl} x)$ w $Z_p[x]/(x^r - a)$.

Jeśli $u = (n/p)^i p^j$, $v = (n/p)^{i'} p^{j'}$ i $i + (j-i)l \equiv i' + (j'-i')l \pmod{r}$, to $i + (j+i')l \equiv i' + (j'+i)l \pmod{r}$ i dla każdego $g(x) \in T$ zachodzi

$$(g(x))^{up^{i+i'}} = (g(x))^{n^i p^{j+i'}} = g(\zeta^{i+(j+i')l} x) = g(\zeta^{i'+(j'+i)l} x) = (g(x))^{n^{i'} p^{j'+i}} = (g(x))^{vp^{i+i'}}$$

Niech $h(x) \mid (x^r - a)$ nierozkładalny nad Z_p. Ponieważ podnoszenie wielomianu do p-tej potęgi jest w ciele $Z_p[x]/h(x)$ odwracalne, to dla każdego $g(x) \in T$ zachodzi $g^u = g^v$. Własność ta jest multiplikatywna i spełniać ją będą wszystkie wielomiany G generowane przez iloczyny elementów T.

Możemy znaleźć takie u, v, by $|u - v| < n^{\sqrt{r/3}}$. Niech L będzie kratą

$$L = \{(i, j) \in Z^2 : r \mid i + (j-i)l\}$$

Wyznacznik tej kraty wynosi $\det L = r$. Skorzystamy z twierdzenia Minkowskiego dla sześciokąta wypukłego

$$C = \{(x, y) \in R^2 : |x| \lg(n/p), |y| \lg p, |x \lg(n/p) + y \lg p| \leqslant \sqrt{r/3} \lg n\}$$

Pole C wynosi przynajmniej $4r$, wobec czego istnieje niezerowy punkt $(i, j) \in L \cap C$, $i \geqslant 0$. Jesli $j \geqslant 0$, kładziemy $u = (n/p)^i p^j, v = 1$, w przeciwnym przypadku $u = (n/p)^i, v = p^{-j}$. Z definicji zbioru C mamy $1 \leqslant u, v \leqslant n^{\sqrt{r/3}}$.

Jak zwykle pokażemy, że $|G| > |u - v|$. Rozważamy funkcje $e : T \to Z$, takie że $|\{t \in T : e(t) < 0\}| = c_-$, $\sum_{e(t)<0} |e(t)| \leqslant c$ oraz $\sum_{e(t)>0} e(t) \leqslant r - 1 - c$. Takich funkcji jest $\binom{rs}{c_-}\binom{c}{c_-}\binom{rs-c_-+r-1-c}{r-1-c}$. Pokażemy, że wielomiany zdefiniowane dla tych funkcji wzorem $W(e) = \prod_t t^{e(t)}$ są różne w $Z_p[x]/h(x)$.

Załóżmy, że dla takich funkcji e, f mamy $W(e) = W(f)$ w $Z_p[x]/h(x)$. Wtedy

$$\prod_{t \in T} t^{e(t)} = \prod_{t \in T} t^{f(t)}$$

$$\prod_{t \in T} t^{e(t)[e(t)>0] - f(t)[f(t)<0]} = \prod_{t \in T} t^{f(t)[f(t)>0] - e(t)[e(t)<0]}$$

Oznaczmy te wielomiany A, B. Zachodzi $A(x) = B(x)$ w $Z_p[x]/h(x)$. Zachodzi też

$$A(\zeta^i x) = A^{n^i} = B^{n^i} = B(\zeta^i x)$$

Zatem pierwiastkami wielomianu $A - B$ są $\zeta^i x$, a to jest r różnych pierwiastków. Wielomiany A, B mają stopień najwyżej niż $c + (r - 1 + c) < r$, więc $A = B$ w $Z_p[x]$, a to oznacza, że $e = f$.

Ostatecznie $g^u = g^v$ ma więcej niż $|u - v|$ rozwiązań, stąd $u = v$ i w konsekwnecji $n = p^\alpha$.
□

4.6.3. Algorytm certyfikatów Bernsteina

Twierdzenie Bernsteina o certyfikatach w naturalny sposób prowadzi do algorytmu dowodzenia pierwszości. Można pokazać, że dla liczby pierwszej n da się znaleźć certyfikat w czasie $(\lg n)^{2+o(1)}$. Taki certyfikat można zweryfikować w czasie $(\lg n)^{4+o(1)}$. W praktyce interesujący jest tylko przypadek $d = 1$, ale wtedy ta metoda nie działa efektywnie dla niektórych n. Algorytm ten niestety ma dużą złożoność pamięciową, rzędu $dr \lg n = (\lg n)^3$ bitów.

Przy pomocy prostej implementacji tego algorytmu, Bernstein udowodnił pierwszość liczby $n = 2^+1024 + 643$ dla certyfikatu $\{d = 1, r = 57449, c = 28724, c_- = 16826, a = 2, S = \{1\}\}$. Obliczenia trwały $3.8 * 10^{13}$ cykli procesora, czyli około jednego dnia. To o wiele dłużej niż w przypadku metody ECPP, ale są perspektywy na dalsze optymalizacje tego algorytmu.

Rozdział 5

O hipotezie 4 AKS

W artykule „PRIMES is in P" [AKS] postawiono hipotezę nr 4, której spełnienie prowadziłoby do względnie szybkiego i prostego testu pierwszości.

Hipoteza 5.1 *Jeśli r jest liczbą pierwszą,* $\gcd(n,r) = 1$*, oraz*

$$(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1} \tag{5.1}$$

to n jest liczbą pierwszą lub $n^2 \equiv 1 \pmod{r}$.

Gdyby tak istotnie było, wystarczyłoby dla przetestowania pierwszości zadanej liczby n dobrać takie r, by $n^2 \not\equiv 1 \pmod{r}$, a potem sprawdzić tylko jedno przystawanie wielomianów. Takie r znajdzie się na pewno rzędu $O(\lg n)$, bo $n^2 - 1$ nie może mieć zbyt dużo małych dzielników pierwszych. A dla większości n wystarczą małe wartości r.

Na poparcie tej hipotezy w [AKS] i [BP01] przytaczany jest argument, że sprawdzono ją dla $r \leqslant 100, n \leqslant 10^{10}$ i znaleziono dużo przykładów „potwierdzających" tą hipotezę, tj. takich, że przystawanie wielomianów zachodziło dla n liczby złożonej, ale zawsze wtedy było $n^2 \equiv 1 \pmod{r}$, a zwykle to nawet $n \equiv 1 \pmod{r}$.

W matematyce hipotezy nie stają się bardziej prawdziwe od ich powtarzania; wystarczy jeden kontrprzykład, by obalić nieudowodnioną hipotezę. Z drugiej strony, jest to interesujący fenomen, bo w gruncie rzeczy dziwne w tej hipotezie jest to, że istnieje tak dużo przykładów n złożonych, dla których $(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1}$. Gdyby zamiast $x^r - 1$ wybrać inny (np. losowy) wielomian stopnia r, zachodziłoby to dla niewielu złożonych liczb n.

Zauważmy, że dla $r = 2, 3$ ta hipoteza jest w oczywisty sposób prawdziwa, więc istotne są tylko $r \geqslant 5$.

5.1. Wyjaśnienie fenomenu

Gdy spojrzymy na postać liczb n spełniających hipotezę 5.1, można zaobserwować pewną prawidłowość. Otóż przeważająca wiekszość z nich to liczby Carmicheala o czynnikach pierwszych przystających do 1 modulo r. Na przykład, dla $r = 5$ pasuje $n = 11 * 31 * 61 * 401$. W istocie, zachodzi twierdzenie:

Twierdzenie 5.1 *Niech $n = p_1 p_2 \cdots p_k$ będzie liczbą Carmicheala taką, że $p_i \equiv 1 \pmod{r}$ dla $i = 1, \ldots, k$. Wtedy $n \equiv 1 \pmod{r}$ i zachodzi tożsamość (5.1).*

Dowód. Oczywiście $n \equiv 1 \pmod{r}$ jako iloczyn liczb przystających do 1 modulo r. Zatem

$$x^n - 1 \equiv x - 1 \pmod{n, x^r - 1}$$

czyli musimy pokazać

$$(x-1)^n \equiv x-1 \pmod{n, x^r-1}$$

a to wystarczy pokazać modulo wszystkie dzielniki n

$$(x-1)^n \equiv x-1 \pmod{p_i, x^r-1}$$

Z małego tw. Fermata $(x-1)^p \equiv (x^p-1) \pmod{p}$ dla liczby pierwszej p, więc skoro $p_i \equiv 1 \pmod{r}$, to

$$(x-1)^{p_i} \equiv x^{p_i}-1 \equiv x-1 \pmod{p_i, x^r-1}$$

czyli $(x-1)$ występuje w ciągu $(x-1)^k \bmod p_i, x^r-1$ z okresem p_i-1, tj.

$$(x-1)^{1+k(p_i-1)} \equiv x-1 \pmod{p_i, x^r-1}$$

Ale jeśli n jest liczbą Carmicheala, to z kryterium Korselta $p_i|n-1$, co kończy dowód. □

5.2. Wyjątki od reguły

Pokazane twierdzenie nie da się odwrócić – poza liczbami Carmicheala zdarzają się również inne liczby n spełniające 5.1. Zdefiniujmy okres:

Definicja 5.1 *Okresem* $(x-1)$ *modulo* p, x^r-1 *nazywamy najmniejszą taką liczbę* $t>0$, *że* $(x-1)^{1+t} \equiv (x-1) \pmod{p, x^r-1}$. *Oznaczamy go przez* $\sigma_{p,r}$.

Możemy pokazać, że dla $d = ord_r(p)$ zachodzi $\sigma_{p,r} \mid p^d-1$. Zachodzi bowiem

$$(x-1)^{p^k} \equiv (x^{p^k}-1) \equiv (x^{p^k \bmod r}-1) \pmod{p, x^r-1}$$

a przecież z definicji rzędu $p^d \bmod r = 1$. W dowodzie poprzedniego twierdzenia korzystaliśmy z tego faktu dla $d=1$. Można zaobserwować, że im większe r tym częściej $\sigma_{p,r} = p^d-1$.

Może się zdarzyć, że $\sigma_{p,r}$ jest mniejsze niż p^d-1. Często dzieje się tak dla małych r. Na przykład dla $r=5, d=4$ przeciętnie $\sigma_{p,r} \approx p^{2.5}$, a dla $r=7, d=3$ to już raczej $\sigma_{p,r} \approx p^{3-\varepsilon}$. Dlatego n wcale nie musi być liczbą Carmicheala, może mieć nawet dwa czynniki. Na przykład dla $r=5, n=pq, p=271, q=541$, gdzie $n, p, q \equiv 1 \pmod{r}$ zachodzi $p-1|n-1$, ale nie $q-1|n-1$. Jednakże $\sigma_{q,r} = 270 = \frac{q-1}{2} \mid n-1$ i z tego powodu spełniona jest równość 5.1.

Możemy pokazać ogólniejszą charakteryzację:

Twierdzenie 5.2 *Jeżeli* n *było bezkwadratowe, i dla każdego dzielnika pierwszego* $p|n$ *zachodzi* $n \equiv p^k \pmod{\sigma_{p,r}}$ *dla* k *takiego, że* $p^k \equiv n \pmod{r}$, *to wtedy*

$$(x-1)^n \equiv (x^n-1) \pmod{n, x^r-1}$$

Dowód. Jeśli tak jest, to wtedy

$$(x-1)^n \equiv (x-1)^{p^k} \equiv (x^{p^k}-1) \equiv (x^n-1) \pmod{p, x^r-1}$$

□.

Niestety, nie jest to warunek konieczny, bo zdarza się (bardzo rzadko i nieregularnie), że równość

$$(x-1)^n \equiv (x^{n \bmod r}-1) \pmod{p, x^r-1}$$

zachodzi dla n spoza ciągu $p^k \bmod r$. Nie wiadomo jednak, czy to prowadzi do jakiegoś przykładu n spełniającego 5.1 – stąd problemy z udowodnieniem hipotezy. Wobec tego ograniczmy się tylko do analizy przykładów scharakteryzowanych twierdzeniem 5.2.

Najłatwiej znaleźć liczby n spełniające 5.2, gdy rzędy modulo r dzielników p są niskie. Jasno widać, że im większy rząd $ord_r(p)$ tym większe będą okresy $\sigma_{p,r}$, gdyż wiadomo, że $\sigma_{p,r} \mid p^{ord_r(p)} - 1$. Zauważmy, że gdyby nie szczególna postać wielomianu $x^r - 1$, to wtedy wiedzielibyśmy jedynie, że $\sigma_{p,r} \mid p^r - 1$. A im większe okresy $\sigma_{p,r}$ tym trudniej podać odpowiednią liczbę n. Wiadomo, że istnieje nieskończenie wiele liczb Carmicheala n. Mają one taką własność, że $p-1|n-1$ dla dzielników pierwszych $p|n$. Nie wiadomo zaś, czy istnieją takie liczby, które mają własność $p^d - 1|n-1$ dla wyższych potęg $d > 1$.

W konsekwencji ciężko jest znaleźć przykłady spełniające 5.1 dla $n \not\equiv \pm 1 \pmod r$. Wtedy bowiem któryś z dzielników pierwszych $p|n$ musi mieć rząd modulo r większy od 2. Więcej nawet, nie powinno się zdarzyć, by którykolwiek z dzielników pierwszych $p|n$ spełniał $p \equiv 1 \pmod r$. Jeśli tak jest, to ciąg $\{(x-1)^k \bmod p, x^r - 1\}$ zapętla się po niedużym okresie $p-1$ i najpewniej nie wystąpi w tym ciągu $x^j - 1$ dla $j \neq 1$ (mogłoby tak przypadkiem się zdarzyć, ale to jest chwilowo poza naszymi rozważaniami). Ten sam argument pokazuje też, że gdy dla pewnego $p|n$ zachodzi $p \equiv -1 \pmod r$, to raczej $n \equiv \pm 1 \pmod r$.

To wszystko pokazuje, jak ciężko jest znaleźć regularny przykład, dla którego $n \not\equiv \pm 1 \pmod r$. Niełatwo też o przykład, dla którego niektóre spośród dzielników $p|n$ nie przystają do ± 1 modulo r. Zdarza się tak czasem, na ogół dla małych r. Na przykład dla $r = 5, n = 7 * 17 * 229 * 251$ lub $r = 5, n = 7 * 17 * 19 * 41 * 181$. Okazuje się powiem, że $\sigma_{7,5} = 480$ oraz $\sigma_{17,5} = 2880$, co jest dużo mniejsze od odpowiednio $7^4 - 1$ i $17^4 - 1$.

Obserwacje wskazują, że ewentualny kontrprzykład powinien być liczbą bezkwadratową; ciąg $(x-1)^k \bmod p^2, x^r - 1$ nie wykazuje tendencji do zapętlania się dużo szybciej niż po około $(p(p-1))^r$ krokach.

5.3. W poszukiwaniu kontrprzykładu

Z powodów opisanych wyżej nie jest łatwo ani udowodnić hipotezę 5.1 ani też ją obalić. Zdołamy pokazać, że nie można jej wzmocnić. Jeśli przejrzymy wszystkie przykłady n, r przytoczone w [BP01], to zauważymy, że dla $r \geqslant 5$ zawsze $n \equiv 1 \pmod r$. Czy możemy zatem w hipotezie 5.1 opuścić przypadek $n \equiv -1 \pmod r$? Odpowiedź brzmi: nie.

Skonstruujemy taką liczbę n, która będzie spełniać 5.1 i $n \equiv -1 \pmod r$. Każdy dzielnik pierwszy n też powinien przystawać do -1 modulo r, inaczej napotykamy trudności. Liczba n powinna być bezkwadratowa. Wobec tego n musi mieć nieparzystą liczbę różnych czynników pierwszych, najprościej przyjmijmy, że będą to 3 czynniki pierwsze $n = p_1 p_2 p_3$, $p_i \equiv -1 \equiv n \pmod r$. Aby skorzystać z twierdzenia 5.2, musimy pokazać, że $n \equiv p_i \pmod{\sigma_{p_i,r}}$. Wiemy, że $ord_r(p_i) = 2$, więc $\sigma_{p_i,r} \mid p_i^2 - 1$, ale to nie wystarcza, bo ciężko skonstruować n takie, by $n \equiv p_i \pmod{p_i^2 - 1}$. Zauważmy, że to pociąga za sobą $n \equiv 1 \pmod{p_i}$, więc n byłoby liczbą Carmichaela; dlatego takie liczby można nazwać liczbami Carmicheala 2-giego rzędu. Niewiele wiadomo o liczbach Carmichaela rzędu 2 i wyższych – prawdopodobnie nie istnieją. Szczęśliwie dla nas, okres $\sigma_{p_i,r}$ jest znacznie mniejszy niż $p_i^2 - 1$, a to za sprawą specjalnej postaci wielomianów $x - 1$ i $x^r - 1$.

Twierdzenie 5.3 *Niech $p, r \geqslant 3$ liczby pierwsze, $p \equiv -1 \pmod r$. Wtedy $\sigma_{p,r} \mid 2r(p-1)$, czyli*

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

Dowód. Oznaczmy $p(x) = 1 + x + x^2 + \ldots + x^{r-1}$, $w(x) = (x-1)^{p-1}$. Łatwo widać, że w $Z_p[x]/(x^r - 1)$ zachodzi

$$w(x)(x-1) = (x-1)^{p-1}(x-1) = (x-1)^p = x^p - 1 = x^{r-1} - 1$$

Co możemy powiedzieć o $w(x)$? Wiadomo, że $p(x)(x-1) = 0$, więc również

$$(w(x) + ap(x)) = x^{r-1} - 1$$

Przedstawmy $w(x) = \sum i = 0^{r-1} a_i x^i$. Bez straty ogólności $a_0 = 0$, skąd wynika że $a_{r-1} = -1$ i $a_i = 0$ dla $i = 0, 1, \ldots, r-2$. Ostatecznie $w(x) = ap(x) - x^{r-1}$.

Zatem

$$(x-1)^{2r(p-1)+1} = (ap(x) - x^{r-1})^{2r}(x-1) = (-x^{r-1})^{2r}(x-1) = (x-1)$$

co należało dowieść. □

Podsumowując, poszukujemy liczby $n = p_1 p_2 p_3$, takiej, że $p_i \equiv -1 \pmod{r}$ oraz

$$n \equiv p_i \pmod{2}r(p_i - 1)$$

Jeśli n jest liczbą Carmichaela, to $n \equiv 0 \pmod{p_i - 1}$. Wiemy też, że $n \equiv -1 \pmod{r}$, więc

$$n \bmod 2r(p_i - 1) \in \{p_i, p_i(r+1)\}$$

W rzeczywistości obie te możliwości zdarzają się mniej więcej równie często i średnio co ósma liczba Carmicheala o 3 czynnikach przystających do -1 modulo r spełnia nasze oczekiwania. Najmniejszą taką liczbą dla $r = 5$ jest $n = 3169 * 34849 * 66529$. Liczba ta nie została uwzględniona w wykazie liczb spełniających hipotezę zamieszczonym w [BP01].

Wniosek 5.4 *Dla* $n = 3169 * 34849 * 66529$, $r = 5$, *zachodzi* $(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$ *oraz* $n \equiv -1 \pmod{r}$.

Rozdział 6

Arytmetyka dużych liczb

– tutaj algorytmy szybkiego mnożenia, sprawdzania perfect-powers, w np. GMP – biblioteka GMP – kwestie implementacji AKS – [[???]]

Spis literatury

[CLR] Cormen, T. H., Leiserson, C. E. i Rivest, R. L., 1990 MIT [[???]] *Wprowadzenie do algorytmów.* Wydawnictwa Naukowo-Techniczne, Warszawa 1997

[Koblitz] Koblitz, N. *Wykład z teorii liczb i kryptografii.* Wydawnictwa Naukowo-Techniczne, Warszawa 1995

[AGP94] Alford, W. R., Granville, A., Pomerance, C. *There are infinitely many Carmichael numbers.* W *Ann. of Math.* (2), 139 703–722 (1994)

[Mi76] Miller, G. L. *Riemann's hypothesis and tests for primality.* W *Journal of Computer and System Sciences*, 13(3):300-317 (1976)

[Ra80] Rabin, M. O. *Probabilistic algorithms for testing primality.* W *Journal of Number Theory* **12**, s. 128–138 (1980)

[Ba85] Bach, E. *Analytic methods in the analysis and design of number-theoretic algorithms.* W *ACM Distinguished Dissertations*, The MIT Press, s. xiii+48, Cambridge, MA 1985

[Gr01] Grantham, J. *Frobenius pseudoprimes.* W *Math. Comp.* **70**, s. 873–891 (2001)
`http://www.pseudoprime.com/pseudo1.ps`

[Gr98] Grantham, J. *A probable prime test with high confidence.* W *Journal of Number Theory* **72**, s. 32–47 (1998)
`http://www.pseudoprime.com/pseudo2.ps`

[DF01] Damgård, I. B. i Frandsen, G. S. *An Extended Quadratic Frobenius Primality Test with Average Case Error Estimates.* BRICS Report RS-01-45 (2001)
`http://www.brics.dk/RS/01/45/`

[DLP93] Damgård, I. B., Landrock, P. i Pomerance, C. *Average Case Error Estimates for the Strong Probable Prime Test.* W *Math. Comp.* **61**, s.177–194 (1993)

[KnuthII] Donald E. Knuth [[???]]

[GK86] Goldwasser, S. i Killian, J. *Almost all primes can be quickly certified.* W *„18th Annual Symposium on Foundations of Computer Science" IEEE*, s.316–329, Berkeley, California, 1986

[AM93] Atkin, A. O. L. i Morain, F. *Elliptic curves and primality proving.* W *Math. Comp.*, 61:203 (1993) s.29–68 http://[[???]]

[ECPP] F.Morain, strona implementacji testu ECPP, http://[[???]]

[APR83] Adleman, L. M, Pomerance C. i Rumely R. S. *On distinguishing prime numbers from composite numbers.* W *Ann. Math.* 117:173–206, 1983

[CL84] Cohen, H. i Lenstra, Jr., H. W. *Primality testing and Jacobi sums.* W *Math. Comp.* **42**, s.297–330 (1984)

[CL87] Cohen, H. i Lenstra, A. K. *Implementation of a new primality test.* W *Math. Comp.* **48**, s.103–121 (1987)

[AKS] Agrawal M., Kayal N., Saxena, N. *PRIMES is in P.* preprint (sierpień 2002)
`http://www.cse.iitk.ac.in/users/manindra/primality.ps`

[Sm] Smid M. *Primality testing in polynomial time.* (grudzień 2002)
`http://www.scs.carleton.ca/m̃ichiel/primes.ps.gz`

[Be1] Bernstein, D. J. *Proving primality after Agrawal-Kayal-Saxena.* – szkic (2003)
`http://cr.yp.to/papers/aks.ps`

[Be2] Bernstein, D. J. *Proving primality in essentialy quartic expected time.* (2003)
`http://cr.yp.to/papers/quartic.ps`

[fatphil.org] Carmody, P. *AKS primality proving analyses.* – strona WWW
`http://fatphil.org/maths/AKS/`

[F85] Fouvry, E. *Theoreme de Brun-Titchmarsh; application au theoreme de Fermat.* W *Invent. Math.*, 79:383–407 (1985)

[BP01] Bhattacharjee, R. i Pandey P. *Primality testing. Technical report.* IIT Kanpur, 2001
`http://www.cse.iitk.ac.in/research/btp2001/primality.html`

[Cheng] Qi Cheng *Primality proving via one round in ECPP and one iteration in AKS.* (2003)
`http://www.cs.ou.edu/ qcheng`

[Berriz] Berrizbeitia, P. *Sharpening PRIMES is in P for a large family of numbers.* (2002)
`http://arxiv.org/abs/math.NT/0211334`

[Voloch] Voloch, J. F. *Improvements to AKS.*
`http://?`