УДК 681.322

Р.Б. Попович
Національний університет "Львівська політехніка"
кафедра електронних обчислювальних машин

УДОСКОНАЛЕННЯ АЛГОРИТМУ AKS ДОВЕДЕННЯ ПРОСТОТИ ЦІЛИХ ЧИСЕЛ

Запропоновано перевіряти рівності в алгоритмі AKS не для послідовних цілих чисел, а для цілих чисел, які є послідовними квадратами. У цьому разі число елементів, для яких рівності справедливі, подвоюється.

They suggested to check AKS algorithm equalities not for sequential integers, but for integers that are sequential squares. In that case a number of elements for that equalities are true doubles.

Вступ. У 1976 р. відкрито новий етап розвитку криптографії. Поступ, що відбувся, пов'язаний з іменами американських математиків В.Діффі та М.Хелмана, а також Р.Меркле, які розвинули ідеологію відкритого ключа.

Завдяки цьому з'явився цілком новий клас криптографічних систем, які називають асиметричними або криптосистемами з відкритим ключем. У цих системах для шифрування й дешифрування використовують різні ключі, пов'язані між собою певною залежністю. Ця залежність є такою, що визначити один ключ, знаючи інший, з обчислювального погляду дуже важко. Один з ключів може бути доступним для всіх, і в цьому разі немає проблеми отримання загального ключа для зв'язку.

У разі побудови криптографічних систем з відкритим ключем виникає така задача. Маємо випадкове велике натуральне число n. Треба перевірити, чи n є простим числом. Алгоритми розв'язування цієї задачі називають тестами простоти.

Огляд відомих тестів простоти

Розрізняють два типи тестів прототи [1,2,4,7]: алгоритми доведення простоти та алгоритми доведення складеності.

Кожен із цих двох типів тестів можна виконувати передбачувано (детерміновані алгорими) або залучати під час виконання певну випадковість, як правило, це означає доступ до генератора псевдовипадкових чисел (імовірнісні алгоритми).

Основою сучасних тестів простоти є мала теорема Ферма [5]:

якщо n – просте ціле число, то для будь-якого цілого числа, яке не має спільних дільників з n,

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

У 1983 р., Адлеман, Померанс і Румелі запропонували детермінований алгоритм для тестування простоти (ще його називають циклотомічним методом) [3]. Цей алгоритм виконується за час, який оцінюється величиною $\exp(O(\lg\lg n \lg\lg\lg n))$ квазіполіноміальної складності.

Кохен, Ленстра, Босма, ван дер Хулст та Міхайлеску спростили алгоритм як теоретично, так і алгоритмічно. Цей алгоритм ефективний на практиці, числа, з 2000 десяткових розрядів, можуть бути протестовані за 10^{14} умовних циклів.

Найкращим сьогодні практичним, але не детермінованим алгоритмом доведення простоти довільних чисел вважається метод ECPP, який використовує обчислення на еліптичних кривих над кільцями залишків Z_n. Він був запропонований в роботі Гольдвассер та Кіліана й вдосконалений

Аткіном, Шаллітом [4]. У разі деяких правдоподібних припущеннях про розподіл простих чисел цей алгоритм для будь-якого простого числа n доводить його простоту в середньому за $O(\log^4 n)$. В основі цього алгоритму лежить твердження, в деякому сенсі подібне до малої теореми Ферма. Метод ECPP був використаний для доведення простоти чисел з 5000 десяткових розрядів.

У 2002 М.Агравал, Н.Кайал та Н.Саксена запропонували детермінований поліноміальної складності алгоритм доведення простоти, який не спирається ні на які не доведені припущення [3]. Ідея цього алгоритму – довести простоту за допомогою комбінаторики: якщо можна записати багато елементів простого циклотомічного розширення кільця Z_n цілих чисел за модулем n , то n є степенем простого числа.

Основним результатом роботи Агравала, Каяла і Саксени є доказ того, що задачу про те, чи є ціле число простим, чи ні, можна розв'язати за допомогою детермінованого алгоритму за час, який обмежується поліномом залежно від розміру вхідного значення, без використання будь-яких недоведених математичних припущень.

AKS грунтується на такій простій версії малої теореми Ферма [1]:

Нехай a і p – взаємно прості цілі числа, p > 1. p – просте тоді і тільки тоді, коли

$$(x-a)^p = (x^p-a) \pmod p$$

Перевірка цієї рівності є складною, оскільки є дуже багато коєфіцієнтів, які необхідно перевірити. Ідея Агравала, Каяла і Саксени полягала у використанні простішої умови:

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

для відповідно вибраного r.

Після цього запропоновано низку вдосконалень, які зменшують обчислювальну складність алгоритму. Ці вдосконалення підсумовані в роботах [5–8].

Постановка задачі. Запропоновані вдосконалення алгоритму AKS хоча й дозволили зменшити складність початкового варіанта алгоритму, проте не дозволили довести його до практичної реалізації. Вони, зокрема, не враховують потрібний для виконання обсяг пам'яті. Тому актуальними є подальші вдосконалення алгоритму.

Завданням цієї роботи є дослідження ще одного вдосконалення алгоритму AKS, яке дозволить додатково зменшити обчислювальну складність.

Початковий варіант роботи наведений в [9].

Число AKS рівностей для перевірки

$\varphi(r)$ позначає функцію Ейлера та дорівнює числу цілих чисел, менших від r і взаємно простих з r; $|S|$ – число елементів множини S; $o_r(n)$ – мультиплікативний порядок цілого числа n за модулем цілого числа r.

Лема 1. Нехай n натуральне число. Якщо $|b|<n/2, |b'|<n/2$ для різних цілих b, b' та $b= b' \bmod p$ для деякого нетривіального дільника p числа n, то $p \le \text{нсд}(n, |b-b'|) < n$.

Доведення. Оскільки $b= b' \bmod p$, то $| b-b'|$ ділиться на p. За припущенням леми $|b-b'|<|b|+|b'|<n$ і доведення завершене.

Лема 2. Нехай n натуральне число. Якщо $|b|<\sqrt{n}$,$|b'|<\sqrt{n}$ та $b^{-1}= b' \bmod p$ для деякого нетривіального дільника p числа n, то $p \le \text{нсд}(n, |bb'-1|) < n$.

Доведення. Оскільки $b^{-1}= b' \bmod p$, то $|bb'-1|$ ділиться на p. За припущенням леми $|bb'-1|<|b||b'|+1<n$ і доведення завершене.

Враховуючи лему 1 та лему 2, отримуємо трохи видозмінену версію теореми Бернштейна з роботи [6].

Теорема 1. Нехай n та r натуральні числа. Нехай d, i та j невід'ємні цілі. Нехай S скінченна множина цілих чисел та 0,1,-1 $\notin$S. Припустимо, що n примітивний корінь за модулем $r\geq 3$;

що $|b|<\sqrt{n}$ для всіх $b\in S$;

що нсд(n, $|b-b'|$)=1 для всіх попарно різних b, $b'\in S$

що нсд(n, $|bb'-1|$)=1 для всіх b, $b'\in S$

що $b^{n-1}=1 \bmod n$ для всіх $b\in S$;

що $\binom{2|S|}{i}\binom{d}{i}\binom{2|S|-i}{j}\binom{\varphi(r)-1-d}{j} \geq n^{\lceil\sqrt{\varphi(r)/3}\rceil}$

та що $(x-b)^n=x^n-b \pmod{n,x^r-1}$ для всіх $b\in S$. Тоді n є степенем простого числа.

Звичайно як елементи множини S беруть послідовні цілі числа. Краще брати цілі числа, які послідовно підносять до квадрата, як описано далі.

Лема 3. Нехай $f(x)$ елемент кільця $Z_n[x]/(x^r-1)$. Якщо $(f(x))^n=f(x^n) \pmod{n,x^r-1}$, то $(f(x^i))^n=f(x^{in}) \pmod{n,x^r-1}$ для довільного натурального i.

Доведення. Заміняючи x на x^i (i – довільне натуральне число) у рівності $(f(x))^n=f(x^n) \pmod{n,x^r-1}$ отримуємо $(f(x^i))^n=f(x^{in}) \pmod{n,x^{ir}-1}$. Оскільки x^r-1 ділить $x^{ir}-1$, то остання рівність виконується також за модулем n,x^r-1.

Лема 4. Нехай n примітивний корінь за модулем простого числа $r\geq 3$. Тоді елемент $x-b$ ($b\neq 1$) має мультиплікативний обернений у кільці $Z_n[x]/(x^r-1)$.

Доведення. Досить показати, що x^r-1 не ділиться на $x-b$. Припустимо, що це не так:

$x^r-1=(x-b)(x^{r-1}+a_{r-2}x^{r-2}+\ldots+a_1x+a_0)$. Звідси випливає $a_{r-2}=b$, $a_{r-3}=b$ $a_{r-2}=b^2,\ldots$, $a_0=b$ $a_1=b^{r-1}$, b $a_0=b^r=1 \bmod n$. Оскільки r просте та $b\neq 1$, то r ділить $n-1$. Отже, $n=1 \bmod r$ – суперечність.

Лема 5. Нехай n примітивний корінь за модулем простого числа $r\geq 3$. Якщо $(x-b)^n=x^n-b \pmod{n,x^r-1}$ та $(x-b^2)^n=x^n-b^2 \pmod{n,x^r-1}$, то $(x+b)^n=x^n+b \pmod{n,x^r-1}$.

Доведення. Якщо припущення леми справедливе, то за лемою 3 $(x^2-b^2)^n=x^{2n}-b^2 \pmod{n,x^r-1}$. Значить $(x-b)^n(x+b)^n=(x^n-b)(x^n+b) \pmod{n,x^r-1}$. Домножуючи останню рівність зліва на мультиплікативний обернений елемента $(x-b)^n=x^n-b$, який існує згідно з лемою 4, отримуємо потрібну рівність.

Теорема 2. Нехай n примітивний корінь за модулем простого числа $r\geq 3$. Нехай u натуральне число. Якщо $(x-a^{2^i})^n=x^n-a^{2^i} \pmod{n,\ x^r-1}$ для $i=0,1,\ldots,u$, то $(x+a^{2^i})^n=x^n+a^{2^i} \pmod{n,x^r-1}$ для $i=0,1,\ldots,u-1$.

Доведення. Індукцією по натуральному числу u. Застосовуючи лему 5.

Маючи задане натуральне число n, можна використати теорему 1 та теорему 2 так.

Перевірити чи n є степенем простого числа; якщо так, то n складене число.

Знайти найменше просте число $r\geq 3$ таке, що n примітивний корінь за модулем r.

Вибрати:

– ціле d між 0 та $\varphi(r)-1$;

– ціле i між 0 та d;

– ціле j між 0 та $\varphi(r)-1-d$.

Вибрати натуральне число s таке, що $\binom{2s}{i}\binom{d}{i}\binom{2s-i}{j}\binom{\varphi(r)-1-d}{j} \geq n^{\lceil\sqrt{\varphi(r)/3}\rceil}$.

Визначити множину $S_1=\{2,2^2,2^4,\ldots,\ 2^{2^{u_1}};\ 3,3^2,3^4,\ldots,3^{2^{u_2}};\ 5,5^2,5^4,\ldots,5^{2^{u_3}};\ 6,6^2,6^4,\ldots,\ 6^{2^{u_4}};\ \ ;$ $b,b^2,\ldots,\ b^{2^{u_t}}\}$. Зауважимо, що загальне число елементів множини S_1 дорівнює $\sum_{k=1}^{t}(u_k+1)$.

У цьому разі вибрати натуральні числа t, u_1, u_2,…, u_t , щоб задовольнити такі умови:

– абсолютні значення всіх елементів множини S_1 менші від $\sqrt{n}$;

– всі елементи множини S_1 попарно різні (тобто беремо для послідовного піднесення до квадрата послідовні натуральні числа, за винятком тих, які вже є між степенями попередніх чисел);

– виконується рівність: $\sum_{k=1}^{t}(2u_k+1)=s$.

Перевірити чи нсд(n,b)=1 для всіх $b\in S_1$; якщо ні, n складене число.

Перевірити чи нсд(n, |b-b'|)=1 для всіх попарно різних b, $b'\in S_1$; якщо ні, n складене число.

Перевірити чи нсд (n, b+b')=1 для всіх попарно різних b, $b'\in S_1$; якщо ні, n складене число.

Перевірити чи нсд (n, |b b'-1|)=1 для всіх b, $b'\in S_1$; якщо ні, n складене число.

Перевірити чи нсд (n, b b'+1)=1 для всіх b, $b'\in S_1$; якщо ні, n складене число. Зауважимо, що $(-b)^{-1}\equiv -b^{-1} \bmod p$.

Перевірити чи $b^{n-1}=1 \bmod n$ для всіх $b\in S_1$; якщо ні, n складене число.

Перевірити чи рівності алгоритму AKS $(x-b)^n=x^n-b \pmod{n,x^r-1}$ справедливі для всіх $b\in S_1$; якщо ні, n складене число.

Якщо рівності справедливі для всіх елементів множини S_1 , то за теоремою 2 рівності також виконуються для елементів множини $S_2=\{-2,-2^2,-2^4,\ldots,-2^{2^{u_1-1}};-3,-3^2,-3^4,\ldots,-3^{2^{u_2-1}};-5,-5^2,-5^4,\ldots,-5^{2^{u_3-1}};-6,-6^2,-6^4,\ldots,-6^{2^{u_4-1}};\ldots;-b,-b^2,\ldots,-b^{2^{u_t-1}}\}$. Загальне число елементів множини S_2 дорівнює $\sum_{k=1}^{t}u_k$.

Множина $S=S_1\cup S_2$ має всього $\sum_{k=1}^{t}(2u_k+1)=s$ елементів. Виконані раніше перевірки ґарантують, що умови теореми 1 справедливі для S. Отже, n є простим за теоремою 1.

Відношення $|S|/|S_1|$ є близьким до 2 для великих цілих чисел n.

Зауваження Можна визначити множину S_1 як послідовні квадрати лише олного цілого числа, наприклад 2. Якщо всі елементи цієї множини попарно різні за модулем n , то $|S|=2|S_1|-1$.

Числовий приклад

Було згенеровано випадкове натуральне число з 500 десятковими розрядами та використовуючи найпростіші перевірки (пробні ділення на малі прості числа та проби Ферма) знайдено найближче ймовірно просте число:

n=47940917743537973692644475812229992529786814872499245562292570755330643813134833171
00458499922259011023504448867777071492685879122518530652291843944762804120812191729618
87681039791349635530458534138304162846593055485126172037102380279251953595226831353710
55658904063286578635833582214067827360654259330234894372332159730250159696606450783603
91073101715445822433684928993232433968828438559337786465588280324886300918982672383912
96818317568544802394638532517956101892005378546853479529063224213885215 03

n є примітивним коренем за модулем простого числа r=2755759; $\varphi(r)=o_r(n)$=27555758.

Виберемо для останньої нерівності s=0.0497$\varphi(r)$=136961; i=j=0.047$\varphi(r)$=129520; d=0.5$\varphi(r)$=1377879. У результаті остання нерівність виконується: логарифм за основою 2 лівої частини дорівнює 1581626.22, а логарифм за основою 2 правої частини дорівнює 1581407.72.

Множину S_1 визначаємо так. Оскільки $n<10^{500}=2^{1650}$, то $\sqrt{n}<2^{825}$.

Спочатку беремо натуральне число 2. u_1=9 є найбільшим натуральним числом для 2 таким, що $2^{2^{u_1}}<\sqrt{n}$. Тоді 2, 2^2, 2^4, 2^8, 2^{16}, 2^{32}, 2^{64}, 2^{128}, 2^{256}, $2^{512}\in S_1$.

Далі беремо натуральне число 3. u_2=9 є найбільшим натуральним числом для 3 таким, що $3^{2^{u_2}} < \sqrt{n}$. Тоді 3, 3^2, 3^4, 3^8, 3^{16}, 3^{32}, 3^{64}, 3^{128}, 3^{256}, $3^{512} \in S_1$.

Не беремо натуральне число 4, бо воно вже є серед степенів числа 2. Тобто, як чергове натуральне число беремо 5 і т.д. У такий спосіб беремо t=11076 натуральних чисел.

Останнє натуральне число дорівнює 11207. u_{11076}=5 є найбільшим натуральним числом для 11207 таким, що $11207^{2^{u_{11076}}} < \sqrt{n}$. Тоді 11207, 11207^2, 11207^4, 11207^8, 11207^{16}, $11207^{32} \in S_1$.

Отримали у цьому прикладі $|S_1|$=74023 and $|S|/|S_1|$=1,85.

Отже, для доведення простоти числа n достатньо показати таке:

– що нсд(n, $|b-b'|$)=1 для всіх попарно різних b, $b' \in S_1$;

– що нсд(n, $b+b'$)=1 для всіх попарно різних b, $b' \in S_1$;

– що gcd(n, $|b\ b'-1|$)=1 для всіх b, $b' \in S_1$;

– що gcd(n, $b\ b'+1$)=1 для всіх b, $b' \in S_1$;

– що $b^{n-1} = 1 \bmod n$ для всіх $b \in S_1$;

– що рівності $(x-b)^n = x^n - b \pmod{n, x^r-1}$ виконуються для всіх 74023 елементів множини S_1.

Висновки. Запропоновано перевіряти рівності алгоритму AKS для цілих чисел, які послідовно підносимо до квадрата b, b^2, b^4,…, b^{2^i} .Показано, що тоді рівності справедливі також для елементів $-b$, $-b^2$, $-b^4$,…, $-b^{2^{i-1}}$. Значить, число елементів, для яких рівності виконуються, збільшується майже в два рази. Це означає, що обчислювальна складність етапу перевірки рівностей, який в основному визначає обчислювальну складність алгоритму загалом, зменшується практично вдвічі.

1. Ємець В.Ф., Мельник А.О., Попович Р.Б. Сучасна криптографія: основні поняття. – Львів: БаК, 2003. 2. Шнайер Б. Прикладная криптография. Протоколи, алгоритми, исходные тексти на язике Си. – М.: Триумф, 2003. 3. M. Agrawal, N. Kayal and N. Saxena, PRIMES is in P, Annals of Mathematics, 160 (2004), no. 2, pp. 781–793. 4. A. Granville, It is easy to determine whether a given integer is prime, Bulletin of the American Mathematical Society, 42 (2005), pp. 3–38. 5. D.J. Bernstein, Proving primality in essentially quartic random time, Mathematics of Computation, Volume 76, Number 257, January 2007, pp. 389–403. 6. D. J.Bernstein, Proving primality after Agrawal, Kayal and Saxena. http://cr.yp.to/papers.html#aks. 7. D.J. Bernstein, Distinguishing prime numbers from composite numbers: the state of the art in 2004. http://cr.yp.to/papers.html#prime2004. 8. J.F.Voloch, On some subgroups of the multiplicative group of finite rings, 2003. http://www.ma.utexas.edu/users/voloch/preprint.html. 9. R. Popovych, Improvement to AKS algorithm, Cryptology ePrint Archive, http://eprint.iacr.org/2006/230.