Improvement to AKS algorithm

Roman Popovych

Abstract

We propose to verify the AKS algorithm identities not for sequential integers, but for integers which are sequentially squared. In that case a number of elements, for which the identities are valid, doubles.

1. Introduction

Prime numbers are of fundamental importance in mathematics in general, and cryptography theory in particular. Efficient primality tests are also useful in practice: a number of cryptographic protocols need big prime numbers.

In 2002 M.Agrawal, N.Kayal and N.Saxena presented a deterministic polynomial-time primality testing algorithm which relies on no unproved assumptions [1]. Idea of the algorithm is to prove primality with combinatorics: if one can write down many elements of a prime cyclotomic extension of the ring Z_n of integers modulo n then n is a power of a prime.

After that some improvements were proposed which reduced time complexity of the algorithm. The improvements are summarized in [2].

We offer one more improvement to the AKS algorithm which reduces a time complexity in near two times.

$f(r)$ means Euler's function giving the number of integers less than r and relatively prime to r; $|S|$ - a number of elements of the set S; $o_r(n)$ - a multiplicative order of integer n modulo integer r.

2. The idea

A common way of AKS algorithm application – to verify the correspondent identities for sequential integers b=1, 2,…, l for appropriately chosen l. It was showed in [3] that if such verifications are done then the identities are valid also for multiplicative inverses of verifyed elements. As a result, a number of elements for which the identities are true doubles.

We propose to verify the identities for integers which are sequentially squared b, b^2, b^4,…, b^{2^i} .We show that then the identities are valid also for elements $-b$, $-b^2$, $-b^4$,…, $-b^{2^{i-1}}$. Hence a number of elements for which the identities hold is near two times bigger.

3. Number of AKS identities for verification

Lemma 1 Let n be a positive integer. If $|b|<n/2, |b'|<n/2$ for distinct integers b, b' and $b= b'$ mod p for some non-trivial divisor p of n, then $p=\gcd(n,|b-b'|)<n$.[1]

Proof As $b= b'$ mod p then $|b-b'|$ is divided by p. From the lemma assumption $|b-b'|<|b|+|b'|<n$ and proof is completed.

Lemma 2 Let n be a positive integer. If $|b|<\sqrt{n}$, $|b'|<\sqrt{n}$ and $b^{-1}= b'$ mod p for some non-trivial divisor p of n, then $p=\gcd(n,|bb'-1|)<n$.

Proof As $b^{-1}= b'$ mod p then $|bb'-1|$ is divided by p. From the lemma assumption $|bb'-1|<|b||b'|+1<n$ and proof is completed.

Taking into account lemma 1 and lemma 2 we obtain a slightly modified version of theorem given by D.Bernstein in [2].

Date: 7 July 2006

Theorem 1 Let n and r be positive integers. Let d, i and j be nonnegative integers. Let S be a finite set of integers with $0,1,-1 \notin S$. Assume that n is a primitive root modulo r=3;

that $|b|<\sqrt{n}$ for all $b \in S$;

that $\gcd(n, |b-b'|)=1$ for all distinct b, $b' \in S$

that $\gcd(n, |bb'-1|)=1$ for all b, $b' \in S$

that $b^{n-1}=1 \bmod n$ for all $b \in S$;

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

and that $(x-b)^n=x^n-b \pmod{n, x^r-1}$ for all $b \in S$. Then n is a power of a prime.

Usually one takes sequential integers as elements of the set S.

We propose to take integers which are sequentially squared as described further.

Lemma 3 Let $f(x)$ be an element of the ring $Z_n[x]/(x^r-1)$. If $(f(x))^n=f(x^n) \pmod{n, x^r-1}$, then $(f(x^i))^n=f(x^{in}) \pmod{n, x^r-1}$ for any positive integer i.

Proof Substituting x by x^i (i – any positive integer) in the equality $(f(x))^n=f(x^n) \pmod{n, x^r-1}$ we obtain $(f(x^i))^n=f(x^{in}) \pmod{n, x^{ir}-1}$. As x^r-1 divides $x^{ir}-1$ then last equality holds also modulo n, x^r-1.

Lemma 4 Let n be a primitive root modulo prime number r=3. Then element $x-b$ (b?1) has a multiplicative inverse in the ring $Z_n[x]/(x^r-1)$.

Proof It is sufficient to show that x^r-1 is not divided by $x-b$. Assume that is not the case: $x^r-1=(x-b)(x^{r-1}+a_{r-2}x^{r-2}+\ldots+a_1x+a_0)$. It follows that $a_{r-2}=b$, $a_{r-3}=b\ a_{r-2}=b^2, \ldots, a_0=b\ a_1=b^{r-1}$, $b\ a_0=b^r=1 \bmod n$. As r is prime and b?1 then r divides n-1. Hence $n=1 \bmod r$ – a contradiction.

Lemma 5 Let n be a primitive root modulo prime number r=3. If $(x-b)^n=x^n-b \pmod{n, x^r-1}$ and $(x-b^2)^n=x^n-b^2 \pmod{n, x^r-1}$, then $(x+b)^n=x^n+b \pmod{n, x^r-1}$.

Proof If the assumption of the lemma holds then by lemma 3 $(x^2-b^2)^n=x^{2n}-b^2 \pmod{n, x^r-1}$. Hence $(x-b)^n(x+b)^n=(x^n-b)(x^n+b) \pmod{n, x^r-1}$. Multiplying last equation from the left by multiplicative inverse of $(x-b)^n=x^n-b$, which exists by lemma 4, we obtain the desired equality.

Theorem 2 Let n be a primitive root modulo prime number r=3. Let u be positive integer. If $(x-a^{2^i})^n=x^n-a^{2^i} \pmod{n, x^r-1}$ for i=0,1,…, u then $(x+a^{2^i})^n=x^n+a^{2^i} \pmod{n, x^r-1}$ for i=0,1,…, u-1.

Proof By induction on integer u. Using lemma 5.

One uses theorem 1 and theorem 2 as follows, given a positive integer n.

Check whether n is a perfect power; if so, then n is composite.

Find the smallest prime r=3 such that n is a primitive rot modulo r.

Select:

- an integer d between 0 and $j(r)$-1;
- an integer i between 0 and d;
- an integer j between 0 and $j(r)$-1-d.

Select a positive integer s such that $\binom{2s}{i}\binom{d}{i}\binom{2s-i}{j}\binom{j(r)-1-d}{j} \geq n^{\lceil \sqrt{j(r)/3} \rceil}$.

Define the set $S_1=\{2,2^2,2^4,\ldots, 2^{2^{u_1}}; 3,3^2,3^4,\ldots,3^{2^{u_2}}; 5,5^2,5^4,\ldots,5^{2^{u_3}}; 6,6^2,6^4,\ldots, 6^{2^{u_4}}; \ldots; b,b^2,\ldots, b^{2^{u_t}}\}$. Note that a total number of elements of the set S_1 equals to $\sum_{k=1}^{t}(u_k+1)$.

In that case select positive integers t, u_1, u_2,…, u_t to satisfy the following conditions:

- absolute values of all elements of the set S_1 are smaller than $\sqrt{n}$;
- all elements of the set S_1 are pair wise distinct (that is we take for sequential squaring sequential positive

integers excepting those which are between powers of the previous integers);

- the equality holds: $\sum_{k=1}^{t}(2u_k+1)=s$.

Check whether gcd(n,b)=1 for all $b\in S_1$; if not, n is composite.

Check whether gcd(n, |b-b'|)=1 for all distinct b, $b'\in S_1$; if not, n is composite.

Check whether gcd(n, b+b')=1 for all distinct b, $b'\in S_1$; if not, n is composite.

Check whether gcd(n, |b b'-1|)=1 for all b, $b'\in S_1$; if not, n is composite.

Check whether gcd(n, b b'+1)=1 for all b, $b'\in S_1$; if not, n is composite. Note that $(-b)^{-1}=-b^{-1}$ mod p.

Check whether $b^{n-1}=1$ mod n for all $b\in S_1$; if not, n is composite.

Check whether the AKS algorithm identities $(x-b)^n=x^n-b$ (mod n,x^r-1) are valid for all $b\in S_1$; if not, n is composite.

If the identities are valid for all elements of the set S_1 then by theorem 2 the identities also hold for elements of the set $S_2=\{-2,-2^2,-2^4,\ldots,-2^{2^{u_1-1}};-3,-3^2,-3^4,\ldots,-3^{2^{u_2-1}};-5,-5^2,-5^4,\ldots,-5^{2^{u_3-1}};-6,-6^2,-6^4,\ldots,-6^{2^{u_4-1}};\ldots;-b,-b^2,\ldots,-b^{2^{u_t-1}}\}$. A total number of elements of the set S_2 equals to $\sum_{k=1}^{t}u_k$ .The set $S=S_1\cup S_2$ has totally $\sum_{k=1}^{t}(2u_k+1)=s$ elements. The checks performed before guarantee that conditions of theorem 1 are true for the set S. Hence n is prime by theorem 1.

The ratio $|S|/|S_1|$ is near 2 for big integers n.

Remark One can define the set S_1 as sequential squares of only one integer, for example 2. If all elements of the set are pair wise distinct modulo n then $|S|=2|S_1|-1$.

4. Results of a numerical experiment

We generated a random integer with 500 decimal digits and using the simplest checks (trial divisions by small primes and Fermat trials) found the nearest probably prime integer:

n=47940917743537973692644475812229992529786814872499245562292570755330643813134833171004584999222590110235044488677770714926858791225185306522918439447628041208121917296188768103979134963553045853413830416284659305548512617203710238027925195359522683135371055658904063286578635833582214067827360654259330234894372332159730250159696606450783603910731017154458224336849289932324339688284385593377864655882803248863009189826723839129681831756854480239463853251795610189200537854685347952906322421388521503

n is a primitive root modulo prime r=2755759; $j(r)=o_r(n)$=27555758.

Select for the last inequality s=0.0497 $j(r)$=136961; $i=j$=0.047 $j(r)$=129520; d=0.5 $j(r)$=1377879. As a result the last inequality holds: the base 2 logarithm of left side equals to 1581626.22, and the base 2 logarithm of the right side equals to 1581407.72.

The set S_1 is defined as follows.

As $n<10^{500}=2^{1650}$ then $\sqrt{n}<2^{825}$.

First take integer 2. u_1=9 is the smallest positive integer for integer 2 such that $2^{2^{u_1}}<\sqrt{n}$. Therefore 2, 2^2, 2^4, 2^8, 2^{16}, 2^{32}, 2^{64}, 2^{128}, 2^{256}, $2^{512}\in S_1$.

Next take integer 3. u_2=9 is the smallest positive integer for integer 3 such that $3^{2^{u_2}}<\sqrt{n}$. Therefore 3, 3^2, 3^4, 3^8, 3^{16}, 3^{32}, 3^{64}, 3^{128}, 3^{256}, $3^{512}\in S_1$.

Do not take integer 4 because it is between the powers of integer 2. So take next integer 5 etc.

In such a way we took t=11076 integers.

Last integer equals to 11207. u_{11076}=5 is the smallest positive integer for integer 11207 such that

$11207^{2^{u_{11076}}} < \sqrt{n}$. Therefore 11207, 11207^2, 11207^4, 11207^8, 11207^{16}, $11207^{32} \in S_1$.

We obtained in the example $|S_1|=74023$ and $|S|/|S_1|=1.85$.

Hence to prove that n is prime it is sufficient to show the following:

- that $\gcd(n, |b-b'|)=1$ for all distinct b, $b' \in S_1$;
- that $\gcd(n, b+b')=1$ for all distinct b, $b' \in S_1$;
- that $\gcd(n, |b\ b'-1|)=1$ for all b, $b' \in S_1$;
- that $\gcd(n, b\ b'+1)=1$ for all b, $b' \in S_1$;
- that $b^{n-1}=1 \bmod n$ for all $b \in S_1$;
- that equalities $(x-b)^n=x^n-b \pmod{n, x^r-1}$ hold for all 74023 elements of the set S_1.

References

[1] M. Agrawal, N. Kayal and N. Saxena, PRIMES is in P, 2002. http://www.cse.iitk.ac.in/news/primality.pdf

[2] D.Bernstein, Proving primality after Agrawal, Kayal and Saxena, 2003. http://cr.yp.to/papers.html#aks

[3] J.F.Voloch, On some subgroups of the multiplicative group of finite rings, 2003. http://www.ma.utexas.edu/users/voloch/preprint.html

Department of Computer Engineering
National University Lviv Politechnika, Bandery Str.,12, 79013, Lviv, Ukraine
e-mail: popovych@polynet.lviv.ua