Some remarks and questions about the AKS algorithm and related conjecture

Martin Mačaj

Abstract

We show that AKS-algorithm for primality testing (see [1]) can be modified to run in $\tilde{O}(\log^{7.5} n)$ time. We present some remarks and ask two questions related to this algorithm.

1 Introduction

In August 2002 M. Agrawal, N. Kayal and N. Saxena presented 'a deterministic polynomial-time algorithm that determines whether an input number n is prime or composite' (see [1]). They showed that their algorithm runs in $\tilde{O}(\log^{12} n)$ time and under hypothesis about the density of Sophie Germain primes in $\tilde{O}(\log^6 n)$ time. They also stated conjecture which, if true, enables to make a deterministic primality-testing algorithm running in $\tilde{O}(\log^3 n)$ time.

In second section we ask two question related to this algorithm. In third section we show that it suffices to find r such that order of $n \pmod r$ is greater than $\log^2 n$ and set S of size $\sqrt{r}\log n$. Using Fouvry's result we get $\tilde{O}(\log^{7.5} n)$ time complexity. Last two sections address Question 1 and Question 2, respectively.

We assume that reader is familiar with papers [1] and [3]. We get results modifying proof from these articles so we point only to main differences. log means logarithm with base 2.

2 Questions

Here we ask two questions related to the AKS-algorithm. We present motivation to these questions in later sections.

Question 1 Given a pair of integers n and α what is the best way to find integer r, s.t. order of $n \pmod r$ is $\geq \alpha$? (We are interested in the case $\alpha = \log^2 n$).

Question 2 Denote by PC_n the number of polynomials $f(x) \in \mathbb{Z}[x]$ of degree n which are products of cyclotomic polynomials. The generating function for the sequence $\{\mathrm{PC}_n\}_{n=1}^{\infty}$ is the function

$$\mathrm{PC}(x) = \prod_{k=1}^{\infty} (1 - x^{\varphi(k)})^{-1},$$

where $\varphi(k)$ denotes the Euler totient function. Are there real numbers $a > \frac{1}{2}$ and $A > 1$ such that $\mathrm{PC}_n \geq A^{n^a}$?

3 Introducing order $d_r(n, p)$

In this section we slightly modify Theorem 2 from [3]. This result implies existence of $\tilde{O}(\log^{7.5} n)$ version of AKS.

Let r be an integer and X be a set of positive integers coprime to r. Denote by $d_r(X)$ the order of the subgroup of $(\mathbb{Z}_r^*, \cdot)$ generated by the set X.

Theorem 3.1 *Let n and r be positive integers such that $(r, n) = 1$. Let p be a prime such that $p|n$ and $p \leq \sqrt{n}$. Denote $d = d_r(n, p)$. Let S be a finite set of integers. Assume that $(n, b - b') = 1$ for all distinct $b, b' \in S$; $\binom{d+|S|-1}{|S|-1} \geq n^{(-1+\sqrt{8d+1})/4}$; and that $(x + b)^n = x^n + b \pmod{n, x^r - 1}$ for all $b \in S$. Then n is a power of p.*

We put difference from [3] to following three lemmas:

Lemma 3.2 *Let r, n, p and d be as above. Let $h(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial dividing the rth cyclotomic polynomial $\Phi_r(x)$ and y be a root of $h(x)$. If a polynomial $g(x) \in \mathbb{Z}_p[x]$ satisfies $g(x^{n^a}) = 0$ in $\mathbb{Z}_p[x]/(h(x))$ for every integer a then $g(x)$ has at least d roots in $\mathbb{Z}_p[x]/(h(x))$ (namely $y^{n^u p^v}$, u, $v \in \mathbb{N}$).*

Lemma 3.3 *Let r, n, p, d and S be as above. The set of all products $\prod_{b \in S} (x - b)^{e_b}$ where $\sum_{b \in S} e_b = d$ has $\binom{d+|S|-1}{|S|-1}$ elements.*

Lemma 3.4 *Let r, n, p, and d be as above. Let $n = p^{\alpha}$ (If we assume that $\alpha \notin \mathbb{N}$ then we get $\alpha \notin \mathbb{Q}$). Let $E_c = \{(i, j) \in \mathbb{N}_0 \times \mathbb{Z} \ : \ n^i p^j \in \mathbb{N}$ and $n^i p^j \leq n^c\}$. Then*

1. *The set E_c has more than $\frac{\alpha^2}{2(\alpha-1)} c^2 + \frac{\alpha}{2} c$ elements.*
2. *If $c \geq \frac{1+\sqrt{8d+1}}{4}$ then E_c has more than d elements.*

Proof . 1 Since $n = p^{\alpha}$, the condition $n^i p^j \leq n^c$ is equivalent to the condition $j \leq \lfloor \alpha(c - i) \rfloor$.

If $j \geq -i$ then $n^i p^j \in \mathbb{N}$. Therefore

$$|E_c| \geq \sum_{i=0}^{\infty} \max\{\lfloor \alpha(c - i) \rfloor + i + 1, 0\}.$$

Let $C = \lfloor \frac{\alpha}{\alpha-1} c \rfloor$. If $i \leq C$ then $-i \leq \lfloor \alpha(c-i) \rfloor$ and we get

$$|E_c| \geq \sum_{i=0}^{C} \lfloor \alpha(c-i) \rfloor + i + 1.$$

Let $z_i = 1 + \lfloor \alpha(c-i) \rfloor - \alpha(c-i) > 0$. We get $\lfloor \alpha(c-i) \rfloor + i + 1 = \alpha c - (\alpha-1)i + z_i$ and

$$|E_c| \geq \alpha c(C+1) - \frac{1}{2}(\alpha-1)C(C+1) + \sum_{i=0}^{C} z_i.$$

Let $0 \leq z = \frac{\alpha}{\alpha-1} c - C < 1$ Then

$$|E_c| \geq (\frac{1}{2}\alpha c + \frac{\alpha-1}{2} z)(\frac{\alpha}{\alpha-1} c + 1 - z) + \sum_{i=0}^{C} z_i =$$

$$\frac{\alpha^2}{2(\alpha-1)} c^2 + \frac{\alpha}{2} c + \frac{\alpha-1}{2} z(1-z) + \sum_{i=0}^{C} z_i.$$

Since $0 \leq z(1-z)$ and $z_i > 0$ we have

$$|E_c| > \frac{\alpha^2}{2(\alpha-1)} c^2 + \frac{\alpha}{2} c.$$

2 For $\alpha > 2$ we have $\frac{\alpha^2}{2(\alpha-1)} > 2$ and $\frac{\alpha}{2} > 1$. Hence E_c has more than $2c^2 + c$ elements. $\frac{1+\sqrt{8d+1}}{4}$ is greater root of the polynomial $2x^2 + x - d \in \mathbb{R}[x]$. Thus $2c^2 + c > d$ and $|E_c| > d$. $\Box$

If we use $\binom{2d}{d} \geq 2^d$ we get

Proposition 3.5 *Let n, p, r and d are as above. Let S be a finite set of integers with cardinality $d+1$. Assume that $(n, b-b') = 1$ for all distinct $b, b' \in S$; and that $(x+b)^n = x^n - 1 \pmod{n, x^r - 1}$ for all $b \in S$. If $d \geq \log^2 n$ then n is a power of p.*

Remark. Using bound

$$\binom{2d}{d} \geq \frac{\sqrt{5}}{4} \frac{2^{2d}}{\sqrt{d + \frac{1}{4}}}$$

we can show that if we assume that $n \geq 2^{13}$ then it suffices to take $d \geq \frac{1}{8} \log^2(n)$.

Using $d_r(n) | d_r(n,p)$ and $d_r(n,p) | \phi(r) \leq r-1$ we get

Theorem 3.6 *Let n and r be positive integers such that $d_r(n) \geq \log^2 n$. Let $s = \lceil \sqrt{\frac{r}{2}} \log n \rceil$ Assume that every prime divisor of n is greater than s and that $(x+b)^n = x^n + b \pmod{n, x^r - 1}$ for all $b \in \{0, 1, 2, \ldots s\}$. Then n is a power of a prime.*

Proof . Let $p \leq \sqrt{n}$ be a prime divisor of n. Let $d = d_r(p, n)$. By previous theorem it suffices to show that $\binom{s+d}{s} = \binom{s+d}{d} \geq n^{\sqrt{d/2}} \geq n^{(-1+\sqrt{8d+1})/4}$.

If $d \leq s$ then this follows from $\log^2 n \leq d_r(n) \leq d$.

If $d > s$ then $\log \binom{s+d}{s} \geq \log \binom{2s}{s} \geq s \geq \sqrt{\frac{r}{2}} \log n \geq \sqrt{\frac{d}{2}} \log n = \log n^{\sqrt{d/2}}$.
□

4 How to find required r?

So, for given integer n, we want to find an integer r such that $d_r(n) > \log^2 n$. We also want to find such an r as small as possible and as soon as possible.

If the conjecture about distribution of Sophie Germain primes holds, then it suffice to seek r between co-Sophie Germain primes. What we can do if this conjecture does not hold? Here are some possible ways.

1) PRIMES Copying [1] we can use results from [5], [2] to find a prime r in the range $O(\log^3 n)$ such that $d_r(n)$ has a prime factor $q \geq \log^2 n$.

Remark. If we copy the proof of Lemma 4.2 from [1], we are able to prove that r lies in range $O(\log^{3+\varepsilon} n)$. To lose ε it suffices to bound the number of prime divisors of an integer m by $c \log m / \log \log m$.

As we showed, it is not necessary for $d_r(n)$ to have large prime factor. Thus, it is possible that we can find better r.

2)(SQUAREFREE) COMPOSITES Maybe we can use the Chinese Remainder Theorem to get required r as a product of some small primes.

3) POWERS OF PRIMES If $n \equiv \pm 3 \pmod 8$ then for $r = 2^{\lceil 2 \log \log n \rceil + 2}$ we have $d_r(n) = 2^{\lceil 2 \log \log n \rceil} \geq \log^2 n$ and $r < 8 \log^2 n$. So for half of odd integers we have instantly very small r. So it seems appropriate to seek r between prime powers.

Lemma 4.1 *Let n be an odd integer. Let $\nu_2(n,k)$ be an integer such that $2^{\nu_2(n,k)} || n^{2^k} - 1$. Then*

1. $\nu_2(n,k) = k - 1 + \nu_2(n,1)$,
2. *for $l \geq \nu_2(n,1)$ we have $d_{2^l}(n) = 2^{l+1-\nu_2(n,1)}$.*

Proof .

1. by induction on k. Using $n^{2^{k+1}} - 1 = (n^{2^k} - 1)(n^{2^k} + 1)$ and $2 || n^{2^k} + 1$,
2. follows immediately from 1.

□

Lemma 4.2 *Let p be an odd prime. Let n be an integer coprime to p. Let $\alpha = d_p(n)$ and $m = n^\alpha$. Let $\nu_p(n,k)$ be an integer such that $p^{\nu_p(n,k)} || m^{p^k} - 1$. Then*

1. $\nu_p(n,k) = k + \nu_p(n,0)$,

2. for $l \geq \nu_p(n,0)$ *we have* $d_{p^l}(n) = \alpha p^{l-\nu_p(n,0)}$.

Proof .

1. by induction on k. Using

$$m^{p^{k+1}} - 1 = (m^{p^k} - 1)((m^{p^k})^{p-1} + (m^{p^k})^{p-2} + \cdots + (m^{p^k}) + 1)$$

and

$$p||(m^{p^k})^{p-1} + (m^{p^k})^{p-2} + \cdots + (m^{p^k}) + 1,$$

2. follows immediately from 1.

□

So we can do following: If $n > 2$ is even then it is composite. We find $\nu_2(n,1)$. If $2^{\nu_2(n,1)} \leq \log n$ then we have $r = 2^l$ for some l. Else we look into primes $< \log n$. If $p|n$ then n is composite. We find $\nu_p(n,0)$. If $p^{\nu_p(n,0)} \leq \log n$ we have $r = p^l$ for some l.

If all primes $p < \log n$ fail (**is it possible?**), then n could be suitable for some test based on other tests (see [3] [9]).

(If a prime $p < \log n$ fails then $p^2|n^{d_p(n)} - 1$. For random n this occurs with probability $(p-1)/p^2 < 1/p$. Thus n for which all primes $p < \log n$ fail seems to be very rare.)

5 Conjecture

In [7] authors stated conjecture (in slightly different form):

Conjecture *If n is an integer and r is a prime such that*

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

then n is prime or $n^2 \equiv 1 \pmod r$.

They also showed that if this conjecture holds then there is a practical deterministic polynomial time algorithm for primality testing.

In this section we present a modified version of this conjecture and show that if there is a positive answer to the Question 2 then this modified conjecture is true.

Modified Conjecture *There exists a real number B and b such that following statement is true:*

Let n and r be coprime integers such that

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

Let $p > r$ be a prime dividing n and $d = d_r(n,p)$. If $d \geq B \log^b n$ then n is power of p.

Here we start an attempt to prove this modified conjecture. Main idea lies in following two lemmas:

Lemma 5.1 *Let n and r are coprime integers. Let a be an integer. Assume that $(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$. Then*

1. $(x^a - 1)^n \equiv x^{an} - 1 \pmod{n, x^r - 1}$,
2. *if* $r \not| a$ *then* $\Phi_a^n(x) \equiv \Phi_a(x^n) \pmod{n, \Phi_r(x)}$,
3. *if* $(r, a) = 1$ *then* $\Phi_a^n(x) \equiv \Phi_a(x^n) \pmod{n, \frac{x^r-1}{x-1}}$,
4. *if* $(r, a) = 1$ *then* $\Phi_a^n(x) \equiv \Phi_a(x^n) \pmod{n, x^r - 1} \Leftrightarrow \Phi_a^n(1) \equiv \Phi_a(1^n) \pmod{n}$.

Lemma 5.2 *Let n and r are coprime integers. Let p be a prime such that $p|n$ and $r < p$. Let $d = d_r(n,p)$ and $h(x) \in \mathbb{Z}_p[x]$ be an irreducible divisor of $x^r - 1$. Let S be a subgroup of $((\mathbb{Z}_p[x]/(h(x)))^*, \cdot)$ generated by the set $\{\Phi_a(x) + (h(x));\ r \not| a\}$. Assume that $(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$. Then S has at least $\mathrm{PC}_d - 2$ elements.*

From these two lemmas we get:

Proposition 5.3 *Let n and r are coprime integers. Let $p < \sqrt{n}$ be a prime such that $p|n$ and $r < p$. Let $d = d_r(n,p)$. Assume that $(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$ and $\mathrm{PC}_d > n^{(1+\sqrt{8d+1})/4}$. Then n is a power of p.*

Thus, if answer to Question 2 is positive then Modified Conjecture holds for $b > (a - 1/2)^{-1}$.

References

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

[2] R. C. Baker and G. Harman : The Brun-Titchmarsh Theorem on average. In *Proceedings of a conference in Honor of Heini Halberstam, Volume 1,* pages 39-103, 1996.

[3] D. Bernstein : An exposition of the Agrawal-Kayal-Saxena primality proving theorem. http://cr.yp.to/papers.html

[4] P. Berrizbeitia : Sharpening *Primes is in P* for a large family of numbers. http://xxx.langl.gov/pdf/math.nt/0211334

[5] R. Bhattacharjee and P. Pandey : Primality testing. http://www.cse.iitk.ac.in/research/btp2001/primality.html.

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

[7] N. Kayal and N. Saxena : Towards a deterministic polynomial-time test. http://www.cse.iitk.ac.in/btp2002/primality.html.

[8] J. F. Voloch : On some subgroups of the multiplicative group of finite rings.

[9] P. Berrizbeitia, T. G. Berry and J. Tena-Ayuso : A Generalization of the Proth Theorem. http://www.ldc.usb.ve/ berry/preprints.html.

Authors' address:
Comenius University
Department of Algebra and Number Theory
Mlynská dolina
842 15 Bratislava, Slovakia
e-mail: Martin.Macaj@fmph.uniba.sk