A note on Agrawal conjecture

Roman Popovych

Abstract. We prove that Lenstra proposition suggesting existence of many counterexamples to Agrawal conjecture is true in a more general case. At the same time we obtain a strictly ascending chain of subgroups of the group $(Z_p[X]/(C_r(X)))^*$ and state the modified conjecture that the set $\{X\text{-}1, X\text{+}2\}$ generate big enough subgroup of this group.

1 Introduction

Prime numbers are of fundamental importance in mathematics in general: there are few better known or more easily understood problems in pure mathematics than the question of rapidly determining whether a given number is prime or composite. 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 [1] presented a deterministic polynomial-time algorithm AKS that determines whether an input number is prime or composite. It was proved [4] that AKS algorithm runs in $O^{\sim}((\log n)^{7.5})$ time. H.Lenstra and C.Pomerance [4] gave a significantly modified version of AKS with $O^{\sim}((\log n)^6)$ running time.

In the paper we do not consider randomozed primality proving algorithm which was introduced by P.Berrizbeitia and investigated by Q.Cheng, D.Bernstein, P.Mihailescu-R.Avanzi [2].

The note concerns Agrawal conjecture. The conjecture was given in [2] and verified for $r<100$ and $n<10^{10}$ in [3].

Conjecture. *If r is a prime number that does not divide n and if* $(X\text{-}1)^n \equiv X^n\text{-}1 \pmod{n, X^r\text{-}1}$, *then either n is prime or* $n^2 \equiv 1 \pmod{r}$.

If Agrawal conjecture were true, this would improve the polynomial time complexity of the AKS primality testing algorithm from $O^{\sim}((\log n)^6)$ to $O^{\sim}((\log n)^3)$.

H.Lenstra and C.Pomerance [4] gave a heuristic argument which suggests that the above conjecture is false. However, M.Agrawal, N. Kayal and N. Saxena [1] pointed out that some variant of the conjecture may still be true (for example, if we force $r>\log n$).

In this paper we prove that proposition (H.Lenstra) from [4] suggesting existence of many counterexamples to the Agrawal conjecture is true in a more general case. We also give some modified conjecture and arguments that this conjecture may be true.

Date: December 30, 2008

2 Preliminaries

Z_n denotes a ring of numbers modulo n. Recall that if p is prime and $h(X)$ is a polynomial of degree d and irreducible in Z_p then $Z_p[X]/(h(X))$ is a finite field of order p^d. We will use the notation $f(X)=g(X)$ (mod n, $h(X)$) to represent the equation $f(X)=g(X)$ in the ring $Z_n[X]/(h(X))$.

We use the symbol $O^{\sim}(t(n))$ for $O(t(n)\cdot\text{poly}(\log t(n)))$ where $t(n)$ is any function of n. We use log for base 2 logarithm.

N and Z denote the set of natural numbers and integers respectively. (a,b) denotes the greatest common divisor of integers a and b. Given $r\in N$, $a\in Z$ with $(a,r)=1$ the order of a modulo r is the smallest number k such that $a^k=1$ (mod r). It is denoted $O_r(a)$. For $r\in N$, $\varphi(r)$ is Euler's totient function giving the number of numbers less than r that are relatively prime to r. It is easy to see that $O_r(a) | \varphi(r)$ for any a, $(a,r)=1$.

$(u_1,\ldots, u_k)$ denotes the group generated by elements $u_1,\ldots, u_k$. A^* denotes the group of units of the ring A.

AKS algorithm basis consists in the following reasoning [1]. Let n is arbitrary integer for which it is necessary to determine whether it is prime or composite. For this purpose we verify the equalities $(X+a)^n\equiv X^n+a$ in the ring $Z_n[X]/(X^r-1)$ for numbers $l=1,\ldots,a$. We choose as power r of the polynomial X^r-1 the smallest r, that satisfies the condition $O_r(n)>\log^2 n$. The number of equalities is equal to $l=\left\lfloor \sqrt{\varphi(r)}\log n \right\rfloor$.

Then we consider the subgroup A of the group Z_r^*, generated by elements n and p. Assume that $|A|=t$.

We also consider the subgroup G of the group $U=(Z_p[X]/(h(X)))^*$ (p is prime divisor of n, $h(X)$ is irreducible over Z_p divisor of X^r-1), generated by the set of elements $X+a$, $a=0,\ldots,l$.

As $t<\varphi(r)$, $l<t$, then creating products of at most $l+1$ polynomials of the form $X+a$ and proving that they are different in U , we obtain the lower bound $|G|\geq 2^{l+1}$ (note that it is possible to obtain more accurate bound).

If p is not a power of n, then one can also obtain an upper bound for $|G|$. For this goal we consider the set $I=\{(n/p)^i p^j | 0\leq i,j\leq \lfloor\sqrt{t}\rfloor\}$. I consists of $\left(\lfloor\sqrt{t}\rfloor+1\right)^2>t$ different numbers. As $|G|=t$ then at least two numbers in I coincide modulo r: $\alpha=\beta$ mod r. Then $(X+a)^{\alpha}=X^{\alpha}+a=X^{\beta}+a=(X+a)^{\beta}$. Hence, $(X+a)^{\alpha-\beta}=1$ and $|G|$ divides $\alpha-\beta$. So $|G|<\alpha<(\frac{n}{p}\cdot p)^{\lfloor\sqrt{t}\rfloor}\leq n^{\lfloor\sqrt{t}\rfloor}$

As $t>\log^2 n$ then $|G|\geq 2^{l+1}\geq 2^{\lfloor\sqrt{t}\log n\rfloor+1}>n^{\lfloor\sqrt{t}\rfloor}$ and we come to contradiction.

So the idea of AKS algorithm proof consists in the following: to show that the set of elements $X+a$ generates "big enough" subgroup in the group $(Z_p[X]/(h(X)))^*$.

From this point of view it is possible to interpret the Agrawal conjecture in the following way. If the identity $(X\text{-}1)^n \equiv X^n\text{-}1 \pmod{n, X^r\text{-}1}$ holds then the set that consists of unique element X-1 generates big enough subgroup.

In this paper we generalize H.Lenstra proposition which indicates that the set $\{X\text{-}1\}$ very likely does not generate big enough subgroup. At the same time we obtain a chain of subgroups $(X)\subset(X+1)\subset(X\text{-}1)\subset(X\text{-}1,\ X+2)$ and state the conjecture that the set $\{X\text{-}1,\ X+2\}$ generate big subgroup. The goal of future work is to clear up this question: what minimal set of elements one have to take to generate big enough subgroup. Primality proving algorithm running time depends on a number of elements of the set.

We will need the following simple fact.

Lemma 2.1. *(1) $n\text{-}p^i$ for any integer i is divided by p-1 if and only if $p\text{-}1|n\text{-}1$.*

(2) $n\text{-}p^i$ for any integer i is divided by p+1 if and only if $p+1|n+1$.

Proof. (1) The equality $n\text{-}p^i=(n\text{-}1)\text{-}(p^i\text{-}1)$ holds. Since $p\text{-}1|p^i\text{-}1$, $n\text{-}p^i$ is divided by p-1 if and only if $p\text{-}1|n\text{-}1$.

(2) The equality $n\text{-}p^i=(n+1)\text{-}(p^i+1)$ holds. Since $p+1|p^i+1$, $n\text{-}p^i$ is divided by p+1 if and only if $p+1|n+1$. □

3 Suggesting existence of counterexamples

Proposition 3.1. *Let $p_1,\ldots,p_k$ be* k *pairwise distinct prime integers, and let $n= p_1\ldots p_k$, r is prime number, p_i is primitive modulo r for all i. If for all i* exist such integers a_i that $n \equiv p_i^{a_i} \bmod 2r(p_i^{(r-1)/2}-1)$*, then*

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

Proof. Polynomials X-1 and $C_r(X)=X^{r-1}+X^{r-2}+\ldots+X+1$ are coprime in the polynomial ring $Z_n[X]$. Hence, in order to prove the identity $(X\text{-}1)^n \equiv X^n\text{-}1 \pmod{n, X^r\text{-}1}$ it suffices to prove that

$(X\text{-}1)^n \equiv X^n\text{-}1 \pmod{n, C_r(X)}$

The Chinese remainder theorem gives the following isomorphism:

$$Z_n[X]/(C_r(X)) \cong \prod_{i=1}^{k} Z_{p_i}[X]/(C_r(X))$$

Each factor ring $R_i = Z_{p_i}[X]/(C_r(X))$ is a field since each prime p_i is primitive modulo r ($O_r(p_i)=p_i\text{-}1$) and thus the polynomial $C_r(X)$ is irreducible in $Z_{p_i}[X]$.

It therefore suffices to prove the identity

$$(X\text{-}1)^n \equiv X^n\text{-}1 \pmod{p_i, C_r(X)} \qquad (3.1)$$

for each p_i.

By assumption $n \equiv p_i^{a_i} \bmod r$ for some integer a_i. Therefore $X^n \equiv X^{p_i^{a_i}}$ modulo X^r-1 and so modulo $C_r(X)$.

Since R_i is a field {p_i is prime}, the identity

$$(X-1)^{p_i^{a_i}} \equiv X^{p_i^{a_i}} - 1(\operatorname{mod} p_i, C_r(X)) \tag{3.2}$$

holds for the integer a_i.

p_i is primitive modulo r , $p_i^{r-1} \equiv 1 \bmod r$ and $p_i^{(r-1)/2} \equiv -1 \bmod r$ (since r is prime number).

Thus $(X-1)^{p_i^{(r-1)/2}} \equiv X^{-1} - 1$ and $(X-1)^{p_i^{(r-1)/2}} \equiv -X^{-1}(X-1)$ in the field R_i. Hence the order of X-1 in R_i divides $2r(p_i^{(r-1)/2} - 1)$. By assumption $n \equiv p_i^{a_i} \bmod 2r(p_i^{(r-1)/2} - 1)$ and thus $(X-1)^n \equiv (X-1)^{p_i^{a_i}}$.

Since left and right parts of identities (3.1), (3.2) coincides and identity (3.2) holds, then identity (3.1) also holds. □

In the case r=5 we obtain the following proposition.

Proposition 3.2. *Let $p_1,\dots,p_k$ be* k *pairwise distinct prime integers and let $n= p_1\dots p_k$. Suppose that*

1) k is odd

2) p_i mod 5∈{2,3} for i=1,…,k;

3) p_1 mod 16∈{3,5,11,13};

for i=2,…,k: if $p_i \equiv p_1$ mod 5 then $p_i \equiv p_1$ mod 16, otherwise $p_i \equiv p_1^3 \bmod 16$;

4) p_i-1|n-1 for i=1,…,k;

5) p_i+1|n+1 for i=1,…,k.

Then $(X-1)^n \equiv X^n-1$ (mod n,X^5-1) and $n^2 \neq 1$ mod 5.

Proof. Even number of factors p_i that equal to 2 or 3 modulo 5 gives 1 or -1 modulo 5. Indeed, if p_i mod 5≡2 and p_j mod 5≡2 then p_ip_j mod 5≡-1. If p_i mod 5≡2 and p_j mod 5≡3 then p_ip_j mod 5≡1. If p_i mod 5≡3 and p_j mod 5≡3 then p_ip_j mod 5≡-1.

Odd number (≥3) of factors p_i that equal to 2 or 3 modulo 5 gives 2 or 3 modulo 5. Hence $n^2 \neq 1$ mod 5.

According to proposition 3.1 it suffices to show that for each i exists such integer a_i that the identity $n \equiv p_i^{a_i} \bmod 10(p_i^2 - 1)$ is true.

There are two different variants of $10(p_i^2 - 1)$ factoring into 4 pairwise coprime factors depending on the value p_i mod 16:

- if p_i mod 16 $\in \{3,11\}$ then $10(p_i^2 - 1) = 5(16)\left(\frac{p_i - 1}{2}\right)\left(\frac{p_i + 1}{4}\right)$

- if p_i mod 16 $\in \{5,13\}$ then $10(p_i^2-1) = 5(16)\left(\frac{p_i-1}{4}\right)\left(\frac{p_i+1}{2}\right)$

In both cases it suffices to show that exists such integer a_i that the identity $n \equiv p_i^{a_i} \bmod 10(p_i^2-1)$ is true modulo each factor.

Let us consider the first case.

If $n \equiv p_i$ mod 5, then $a_i=1$, $n \equiv p_i$ mod 16 by assumption 3, $n \equiv p_i$ mod $(p_i-1)/2$ by lemma (2.1) and assumption 4, $n \equiv p_i$ mod $(p_i+1)/4$ by lemma (2.1) and assumption 5.

If $n \not\equiv p_i$ mod 5, then $a_i=3$ (since $2 \equiv 3^3$ mod 5 and $3 \equiv 2^3$ mod 5), $n \equiv p_i^3$ mod 5, $n \equiv p_i^3$ mod 16 by assumption 3 ($11 \equiv 3^3$ mod 16, $3 \equiv 11^3$ mod 16, $13 \equiv 5^3$ mod 16, $5 \equiv 13^3$ mod 16), $n \equiv p_i^3$ mod $(p_i-1)/2$ by lemma (2.1) and assumption 4, $n \equiv p_i^3$ mod $(p_i+1)/4$ by lemma (2.1) and assumption 5.

In the second case the proof is analogous. □

Note that in the proof of proposition 3.2 an order of element X-1 in the ring $Z_{p_i}[X]/(C_r(X))$ divides $10(p_i^2-1)$ for any prime divisor p_i of n.

Remark. Proposition 3.2 is also true in the case p_1 mod 32 $\in \{7,9,23,25\}$; for $i=2,\dots,k$: if $p_i \equiv p_1$ mod 5 then $p_i \equiv p_1$ mod 32, otherwise $p_i \equiv p_1^3 \bmod 32$.

Proposition (H.Lenstra) from [4] is a partial case of proposition 3.2.

By proposition 3.2, we have a heuristic which suggests the existence of many counterexamples [4] to the Agrawal conjecture. But no counterexample is yet known.

4 Chain of subgroups

Since, very likely, the Agrawal conjecture is not true it is natural to modify it slightly to obtain a version that may still be true.

Number n is assumed to be primitive mod r. Note that element X-1 is a unit in the ring $Z_p[X]/(C_r(X))$.

Proposition 4.1 *If $(X-1)^n \equiv X^n-1$ (mod n, X^r-1), then $(X) \subset (X+1) \subset (X-1)$ is a strictly ascending chain of subgroups of the group $(Z_p[X]/(C_r(X)))^*$ for any prime divisor p of n.*

Proof. As $(X-1)^n \equiv X^n-1$ (mod n, X^r-1), then $(X-1)^n \equiv X^n-1$ (mod p, $C_r(X)$). Since n is primitive mod r there exist such integer a that $n^a \equiv 2$ (mod r). Then $(X-1)^{n^a} = X^2-1 = (X-1)(X+1)$. So $X+1 = (X-1)^{n^a} \in (X-1)$ and $(X+1) \subseteq (X-1)$.

As $X+1 \in (X-1)$ and $(X-1)^n \equiv X^n-1$ (mod p, $C_r(X)$), then $(X+1)^n \equiv X^n+1$ (mod p, $C_r(X)$).

Since n is primitive mod r there exist such integer c that $n^c \equiv r-1$ (mod r). Then

$(X+1)^{n^c} = X^{n^c} + 1 = X^{r-1} + 1 = X^{-1} + 1 = X^{-1}(X+1)$. Recall that $X^r=1$. Hence, $(X+1)^{n^c-1} = X^{-1}$ (mod p, $C_r(X)$). So $(X^{-1})\subseteq(X+1)$. As groups (X^{-1}) and (X) coincide then $(X)\subseteq(X+1)$.

Since $(X)=\{1, X,\ldots, X^{r-1}\}$ it is clear that element $X+1\notin(X)$ and $(X)\subset(X+1)$.

To prove that $(X+1)\subset(X-1)$ let us consider an automorphism σ of the ring $Z_p[X]/(C_r(X))$ sending X to X^{-1}. Assume $(X+1)^V=X-1$ (mod p, $C_r(X)$) for some integer V.

Recall that $X+1$ and $X-1$ are units and so $[\sigma(X+1)]^{-1}$ and $[\sigma(X-1)]^{-1}$ exist. Consider $(X+1)[\sigma(X+1)]^{-1}=(X+1)[X^{-1}(1+X)]^{-1}=X$ and $(X-1)[\sigma(X-1)]^{-1}=(X-1)[-X^{-1}(X-1)]^{-1}=-X$. Then $X^V=-X$ – a contradiction.

So, the chain of groups $(X)\subset(X+1)\subset(X-1)$ is strictly ascending. □

Hence, if $(X-1)^n\equiv X^n-1$ (mod n, X^r-1) then an order of element $X-1$ in the group $(Z_p[X]/(C_r(X)))^*$ is a product of three numbers: an order of group (X) that equals to r, an index of subgroup (X) in group $(X+1)$ and an index of subgroup $(X+1)$ in group $(X-1)$.

Proposition 4.2. *If p is prime and $a\neq 0,-1,1$ mod p, then element $X+a\notin(X-1)$ in the group $(Z_p[X]/(C_r(X)))^*$.*

Proof. Assume that $(X-1)^V=X+a$ (mod p, X^r-1). Again let us consider an automorphism σ of the ring $Z_p[X]/(C_r(X))$ sending X to X^{-1}. Then we have $(X+a)\ [\sigma(X+a)]^{-1}=(X-1)^V[\sigma((X-1)^V)]^{-1}$, $(X+a)[X^{-1}+a]^{-1}=(-X)^V$, $X+a=(-1)^V X^{V-1}+(-1)^V aX^V$. Since $(-1)^V\neq a$ then $X=(-1)^V X^{V-1}$, $V-1\equiv 1$ mod r, $V\equiv 2$ mod r. From the other hand $a=(-1)^V aX^V$, $V\equiv 0$ mod r – a contradiction. □

Hence, we have the following strictly ascending chain of groups $(X)\subset(X+1)\subset(X-1)\subset(X-1, X+2)$.

Moreover, for $r=5$ we have the following proposition.

Proposition 4.3. *If prime number p is not equal to 2,3,5,11,19 and $p^2\neq 1$ mod 5, then an order of element $X+2$ in the field $Z_p[X]/(C_5(X))$ does not divide $10(p^2-1)$.*

Proof. It is easy to verify that $(X+2)(X^3-X^2+3X-5)=-11$ (mod $p,C_5(X)$), so element $-11^{-1}(X^3-X^2+3X-5)$ is a multiplicative inverse of $X+2$ in the field $Z_p[X]/(C_5(X))= Z_p[X]/(X^4+X^3+X^2+X+1)$. We have

$(X+2)^{p^2} \equiv X^{-1}+2 = X^{-1}(2X+1)$ (as p is prime) and

$$(X+2)^{p^2-1} \equiv -11^{-1}X^{-1}(2X+1)(X^3-X^2+3X-5) = -11^{-1}X^{-1}(-3X^3+3X^2-9X-7)$$

Therefore $(X+2)^{10(p^2-1)} \equiv 11^{-10}(\text{-3X}^3+3\text{X}^2\text{-9X-7})^{10} \equiv$

$$\equiv -11^{-10}(19486165920X^3+26683280040X^2+22802637960X+29275201379)$$

Factorization of polynomial coefficients of non-zero powers of X is as follows:
19486165920=2·2·2·2·2·3·5·13·19·164357; 26683280040=2·2·2·3·5·19·167·70079; 22802637960=2·2·2·3·3·5·19·67·49757.

Since p does not divide the greatest common divisor of the coefficients (equals to $2\cdot 2\cdot 2\cdot 3\cdot 5\cdot 19$) then the coefficients are not simultaneously equal to 0 modulo p. Hence, the polynomial $(X+2)^{10(p^2-1)}$ is not equal to 1. □

5 Conclusion

In this paper we generalize H.Lenstra proposition which indicates that the set $\{X\text{-}1\}$ very likely does not generate big enough subgroup in the group $(Z_p[X]/(C_r(X)))^*$.

At the same time we obtain a strictly ascending chain of subgroups $(X)\subset(X+1)\subset(X-1)\subset(X-1,\ X+2)$ of this group and state the modified conjecture that the set $\{X-1, X+2\}$ generate big subgroup.

These arguments suggest that the following variant of the Agrawal conjecture may be true:

Modified conjecture. *If r is a prime number that does not divide n,*
if $(X-1)^n \equiv X^n-1 \pmod{X^r-1, n}$ *and if* $(X+2)^n \equiv X^n+2 \pmod{X^r-1, n}$*,*
then either n is prime or $n^2 \equiv 1 \pmod{r}$*.*

Acknowledgements. I would like to thank Hendrik W.Lenstra for reading a draft version of this paper and providing valuable comments.

References

[1] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, Annals of Mathematics, 160 (2004), pp. 781–793.
[2] D.J.Bernstein, *Proving primality in essentially quartic random time*, Math. of Computations, v.76, No. 257, 2007, pp. 389-403.
[3] R. Bhattacharjee and P. Pandey, *Primality testing*, IIT Kanpur, 2001. Available at `http://www.cse.iitk.ac.in/research/btp2001/primality.html`.
[4] A.Granville, *It is easy to determine whether a given integer is prime*, Bullletin of the American Math. Society, v.42, No. 1, 2005, pp. 3-38.
[5] N. Kayal and N. Saxena, *Towards a deterministic polynomial-time test*, IIT Kanpur, 2002. Available at `http://www.cse.iitk.ac.in/research/btp2002/primality.html`.
[6] H.W.Lenstra,Jr. and C.Pomerance, *Remarks on Agrawal's conjecture*, 2003. Available at `http://www.aimath.org/WWN/primesinp/articles/html/50a`.

Roman Popovych, Department of Computer Science and Engineering,
National University Lviv Politechnika, Bandery Str.,12, 79013, Lviv, Ukraine
E-mail: popovych@polynet.lviv.ua