ISSN 2075-9827 http://www.journals.pu.if.ua/index.php/cmp
Carpathian Math. Publ. 2013, **5** (2), 310–314 Карпатські матем. публ. 2013, Т.5, №2, С.310–314
doi:10.15330/cmp.5.2.310-314

POPOVYCH R.

LOWER BOUNDS ON THE ORDERS OF SUBGROUPS CONNECTED WITH AGRAWAL CONJECTURE

Explicit lower bounds are obtained on the multiplicative orders of subgroups of a finite field connected with primality proving algorithm.

Key words and phrases: primality proving, finite field, multiplicative order.

Lviv Polytechnic National University, 12 Bandera str., 79013, Lviv, Ukraine
E-mail: rombp07@gmail.com

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 n is prime or composite. It was proved [4] that AKS algorithm runs in $(\log n)^{7,5+o(1)}$ time. H.Lenstra and C.Pomerance [5] gave a significantly modified version of AKS with $(\log n)^{6+o(1)}$ running time.

Probabilistic versions of AKS are also known [3] with $(\log n)^{4+o(1)}$ time complexity. The Agrawal conjecture [1, 4] was proposed for further improvement of AKS running time. A heuristic argument was given [5] which suggests that the above conjecture is false. However, it was pointed out [1] that some variant of the conjecture may still be true. A modified conjecture is given in [7]. A strongly ascending chain of subgroups of the multiplicative group of a finite field appears in this conjecture.

Using results from [8], we obtain in this paper lower bounds on the orders of these subgroups.

1 PRELIMINARIES

Let q be a power of an odd prime number p, and F_q be a finite field with q elements. We use F_q^* to denote the multiplicative group of F_q. A partition of an integer C is a sequence of non-negative integers $u_1, ..., u_C$ such that $\sum_{j=1}^{C} ju_j = C$. $U(C)$ denotes the number of the partitions of C. $U(C, d)$ denotes the number of such partitions of C, for which $u_1, ..., u_C \leq d$, i.e., each part

УДК 512.624
2010 *Mathematics Subject Classification:* 11T30.

appears no more than d times. $\langle v_1, ..., v_k\rangle$ denotes the group generated by elements $v_1, ..., v_k$, and $G \times H$ — the direct product of groups G and H. $|G|$ denotes the multiplicative order of the group G.

Let q be a primitive root modulo r, that is the multiplicative order of q modulo r equals to $r-1$. Set $F_q(\theta) = F_{q^{r-1}} = F_q[x]/\Phi_r(x)$, where $\Phi_r(x) = x^{r-1} + x^{r-2} + ... + x + 1$ is the r-th cyclotomic polynomial and $\theta = x \ (mod\ \Phi_r(x))$. It is clear that the equality $\theta^r = 1$ holds. The element $\beta = \theta + \theta^{-1}$ is called a Gauss period of type $((r-1)/2, 2)$. It generates normal base over F_q [2].

The following strongly ascending chain of subgroups of the multiplicative group appears (if to take $q = p$ is a prime number and $r < p$) in the modified conjecture [7]:

$$\langle\theta\rangle \subset \langle\theta+1\rangle \subset \langle\theta-1\rangle \subset \langle\theta-1, \theta+2\rangle .$$

It was shown in [2], that the order of Gauss period β is at least $U((r-3)/2, p-1)$. In [8, Theorem 1], this result was improved and generalized, i.e. the following theorem was proved.

Theorem 1. *Let q be a power of an odd prime number p, $r = 2s+1$ be a prime number coprime with q, q be a primitive root modulo r, θ generates the extension $F_q(\theta) = F_{q^{r-1}}$, e be any integer, f be any integer coprime with r, a be any non-zero element in the finite field F_q. Then*
(a) $\theta^e(\theta^f + a)$ has the multiplicative order at least $U(r-2, p-1)$,
(b) $(\theta^{-f} + a)(\theta^f + a)$ for $a^2 \neq \pm 1$ has the multiplicative order at least $U((r-3)/2, p-1)$ and this order divides $q^{(r-1)/2} - 1$,
(c) $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$ for $a^2 \neq 1$ has the multiplicative order at least $U((r-3)/2, p-1)$ and this order divides $q^{(r-1)/2} + 1$,
(d) $\theta^e(\theta^f + a)$ for $a^2 \neq \pm 1$ has the multiplicative order at least $[U((r-3)/2, p-1)]^2/2$.

We take to the end of the paper that $q = p > 3$ is a prime number and $r < p$.

Explicit lower bounds on the orders of subgroups connected with Agrawal conjecture in terms of p and r are of special interest. That is why we use in this paper Theorem 1 and some known estimate from [6] to derive explicit lower bounds on the multiplicative orders of $\langle\theta+1\rangle$, $\langle\theta-1\rangle$ and $\langle\theta-1, \theta+2\rangle$.

If $C < d$, then clearly $U(C, d) = U(C)$. Explicit lower bound on $U(C)$ for all integers C is proposed in [6]. According to [6, Theorem 4.2], the following inequality holds for all integers C:

$$U(C) > \frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{C}\right)}{13C}. \quad (1)$$

2 LOWER BOUNDS ON THE ORDERS

We obtain in this section lower bounds on the orders of subgroups connected with Agrawal conjecture. First of all, it is clear that $|\langle\theta\rangle| = r$.

Lemma 2.1. $\langle\theta+1\rangle = \langle\theta\rangle \times \langle\theta+\theta^{-1}\rangle$.

Proof. Let us show first that $\langle\theta^2+1\rangle = \langle\theta+1\rangle$. Since p is primitive modulo r, an integer i exists such that $p^i \equiv 2\ mod\ r$. Then $(\theta+1)^{p^i} = \theta^2 + 1 (mod\ p, \Phi_r(\theta))$. Analogously an integer j exists such that $p^j \equiv 2^{-1}\ mod\ r$. Then we have $(\theta^2+1)^{p^j} = \theta + 1 (mod\ p, \Phi_r(\theta))$.

Now we show that $\langle\theta\rangle \cdot \left\langle \theta+\theta^{-1} \right\rangle = \left\langle \theta^2+1 \right\rangle$. Indeed, $\theta(\theta+\theta^{-1}) = \theta^2+1$ and the inclusion $\langle\theta\rangle \cdot \left\langle \theta+\theta^{-1} \right\rangle \supseteq \left\langle \theta^2+1 \right\rangle$ is obvious. As $\theta \in \langle\theta+1\rangle = \left\langle \theta^2+1 \right\rangle$, $\theta^{-1}(\theta^2+1) = \theta+\theta^{-1} \in \left\langle \theta^2+1 \right\rangle$ and we have the inclusion $\langle\theta\rangle \cdot \left\langle \theta+\theta^{-1} \right\rangle \subseteq \left\langle \theta^2+1 \right\rangle$.

To prove that the intersection of $\langle\theta\rangle$ and $\left\langle \theta+\theta^{-1} \right\rangle$ equals to the trivial subgroup, consider the automorphism σ of the field $F_p(\theta)$, which sends θ to θ^{-1}. For every element $a \in F_p(\theta)$ we take $t(a) = a \cdot (\sigma(a))^{-1}$. It is clear that $t(ab) = t(a)t(b)$ and $t(a^i) = [t(a)]^i$. Then it is easy to obtain $t((\theta+\theta^{-1})^u) = 1$ and $t(\theta^c) = \theta^{2c}$. Suppose $\theta^c = (\theta+\theta^{-1})^u$ for some integers c, u. Use for $\alpha = \theta^c$ and $\beta = (\theta+\theta^{-1})^u$ the fact that $\alpha = \beta$ implies $t(a) = t(b)$. Then $\theta^{2c} = 1$, and therefore c is divided by r and $\theta^c = 1$.

Hence, the result follows. □

As a consequence of Lemma 2.1, we have the following more precisely specified chain of subgroups:

$$\langle\theta\rangle \subset \langle\theta\rangle \times \left\langle \theta+\theta^{-1} \right\rangle = \langle\theta+1\rangle \subset \langle\theta-1\rangle \subset \langle\theta-1, \theta+2\rangle .$$

Theorem 2. *The Gauss period $\beta = \theta+\theta^{-1}$ has the multiplicative order larger than*

$$\frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)}$$

and this order divides $p^{(r-1)/2}-1$.

Proof. Since

$$(\theta+\theta^{-1})^{p^{(r-1)/2}-1} = (\theta^{p^{(r-1)/2}} + \theta^{-p^{(r-1)/2}})(\theta+\theta^{-1})^{-1} = (\theta^{-1}+\theta)(\theta+\theta^{-1})^{-1} = 1,$$

the multiplicative order of β divides $p^{(r-1)/2}-1$.The fact that the order of $\beta = \theta+\theta^{-1} = \theta^{-1}(\theta^2+1)$ is at least $U(r-2, p-1)$ follows from Theorem 1, part (a).

Since $p > r$, we have $r-2 < p$ and $U(r-2, p-1) = U(r-2)$. Then it follows from inequality (1) that the multiplicative order $L_1(r)$ of $\beta = \theta+\theta^{-1} = \theta^{-1}(\theta^2+1)$ satisfies the bound

$$L_1(r) \geq U(r-2, p-1) = U(r-2) > \frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)}.$$

□

We obtain from Lemma 2.1 and Theorem 2 the following explicit lower bound.

Corollary 2.1. $|\langle\theta+1\rangle| > \frac{r}{13(r-2)} \exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)$.

Since $\langle\theta+1\rangle \subset \langle\theta-1\rangle$, the following result is clear.

Lemma 2.2. $|\langle\theta-1\rangle| \geq 2|\langle\theta+1\rangle|$.

Remark. *The order of element $\theta+1$ in the case $r = 5$ and $p \equiv 2 \mod r$ divides $2r(p+1)$, because $(\theta+1)^{p+1} = (\theta^p+1)(\theta+1) = (\theta^2+1)(\theta+1) = \theta^3+\theta^2+\theta+1 = -\theta^4$, and the order of $-\theta^4$ equals to $2r$. On the other hand, one can show that $(\theta-1)^{2r(p+1)} \neq 1$.*

Taking into account Corollary 2.1 and Lemma 2.2, we have the following lower bound.

Corollary 2.2. $|\langle\theta-1\rangle| > \frac{2r}{13(r-2)}\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)$.

Now we are ready to give the lower bound on the order of $\langle\theta-1,\theta+2\rangle$.

Theorem 3. $|\langle\theta-1,\theta+2\rangle| > \frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot(1+\frac{\sqrt{2}}{2})\sqrt{r-3}\right)}{169(r-2)(r-3)}$.

Proof. Recall that the order of $F^*_{p^{r-1}}$ equals to $p^{r-1}-1 = (p^{(r-1)/2}-1)(p^{(r-1)/2}+1)$. The factors $p^{(r-1)/2}-1$ and $p^{(r-1)/2}+1$ have the greatest common divisor 2, since their sum equals to $2p^{(r-1)/2}$.

Consider the subgroup of $F^*_{p^{r-1}}$ generated by $\theta-1$ and $\theta+2$. This subgroup contains two subgroups: first one is generated by $\beta=\theta+\theta^{-1}$ (because $\langle\theta-1\rangle$ contains $\langle\theta+1\rangle$, and $\langle\theta+1\rangle$ contains $\langle\theta+\theta^{-1}\rangle$), and second one — by $\gamma=(\theta-2)^{p^{(r-1)/2}-1}=(\theta^{-1}-2)(\theta-2)^{-1}$.

According to Theorem 2, β has the order that divides $p^{(r-1)/2}-1$ and is at least

$$\frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)}.$$

As $2^2\neq 1(mod\ p)$, according to Theorem 1, part (c) (if to put $e=0$, $f=1$), the γ has the order that divides $p^{(r-1)/2}+1$ and is at least $U((r-3)/2,p-1)$.

Construct the element

$$\delta=\begin{cases}\beta^2\gamma, & \text{if } \rho_2(p^{(r-1)/2}-1)=2,\\ \beta\gamma^2, & \text{if } \rho_2(p^{(r-1)/2}+1)=2.\end{cases}$$

Obviously the group $\langle\theta-1,\theta+2\rangle$ contains the subgroup generated by δ. If

$$\rho_2(p^{(r-1)/2}-1)=2,$$

then $(p^{(r-1)/2}-1)/2$ is odd and coprime with $p^{(r-1)/2}+1$. Clearly the order of β^2 is a divisor of $(p^{(r-1)/2}-1)/2$. Hence, in this case, we have the following direct product of subgroups $<\delta>=<\beta^2>\times<\gamma>$.

If $\rho_2(p^{(r-1)/2}+1)=2$, then $(p^{(r-1)/2}+1)/2$ is odd and coprime with $p^{(r-1)/2}-1$. Clearly the order of γ^2 is a divisor of $(p^{(r-1)/2}+1)/2$. Hence, in this case, we have the following direct product of subgroups $<\delta>=<\beta>\times<\gamma^2>$.

In both cases, the order of δ is the product of orders of β and γ divided by 2.

Since $(r-3)/2<p$, we have $U((r-3)/2,p-1)=U((r-3)/2)$. Applying to $U((r-3)/2)$ the inequality (1), we obtain that the multiplicative order $L_2(r)$ of δ satisfies the bound

$$\begin{aligned}L_2(r) &\geq \frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)}\cdot U((r-3)/2)/2\\ &> \frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)}U((r-3)/2)/2 > \frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot(1+\frac{\sqrt{2}}{2})\sqrt{r-3}\right)}{169(r-2)(r-3)}.\end{aligned}$$

This finishes the proof. □

REFERENCES

[1] Agrawal M., Kayal N., Saxena N. *PRIMES is in P*. Annals of Mathematics 2004, **160** (2), 781–793. doi: 10.4007/annals.2004.160.781

[2] Ahmadi O., Shparlinski I.E., Voloch J.F. *Multiplicative order of Gauss periods*. Intern. J. Number Theory 2010, **6** (4), 877–882. doi:10.1142/S1793042110003290

[3] Bernstein D.J. *Proving primality in essentially quartic random time*. Math. Comp. 2007, **76** (257), 389–403.

[4] Granville A. *It is easy to determine whether a given integer is prime*. Bull. Amer. Math. Soc. 2005, **42** (1), 3–38. doi:10.1090/S0273-0979-04-01037-7

[5] Lenstra H.W. Jr., Pomerance C. *Remarks on Agrawal's conjecture*. In: Proc. ARCC workshop "Future directions in algorithmic number theory", Palo Alto, USA, March 24–28, 2003, The American Institute of Mathematics. http://www.aimath.org/WWN/primesinp/primesinp.pdf

[6] Maróti A. *On elementary lower bounds for the partition function*. Integers: Electronic J. Comb. Number Theory 2003, **3** (A10).

[7] Popovych R. *A note on Agrawal conjecture*. Cryptology ePrint Archive 2009. http://eprint.iacr.org/2009/008

[8] Popovych R. *Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$*. Finite Fields Appl. 2012, **18** (4), 700-710. doi:10.1016/j.ffa.2012.01.003

Received 10.01.2013

Попович Р. *Нижні оцінки для порядків підгруп, пов'язаних з гіпотезою Агравала* // Карпатські математичні публікації. — 2013. — Т.5, №2. — C. 310–314.

Отримано нижні оцінки для мультиплікативних порядків підгруп скінченого поля, пов'язаних з алгоритмом доведення простоти числа.

Ключові слова і фрази: нижні оцінки, скінченне поле, мультиплікативний порядок.

Поповыч Р. *Нижние оценки для порядков подгрупп, связанных с гипотезой Агравала* // Карпатские математические публикации. — 2013. — Т.5, №2. — C. 310–314.

Получены нижние оценки для порядков подгрупп конечного поля, связанных с алгоритмом доказательства простоты числа.

Ключевые слова и фразы: нижние оценки, конечное поле, мультипликативный порядок.