ВІСНИК НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
"ЛЬВІВСЬКА ПОЛІТЕХНІКА"
"Фізико-математичні науки"
№804, 2014, с. 108–111

JOURNAL OF LVIV POLYTECHNIC
NATIONAL UNIVERSITY
"Physical and mathematical sciences"
№804, 2014, p. 108–111

ПРО ПІДГРУПИ МУЛЬТИПЛІКАТИВНОЇ ГРУПИ ОДНОГО КЛАСУ СКІНЧЕННИХ ПОЛІВ

Попович Р. Б.

Національний університет "Львівська політехніка"
вул. С. Бандери 12, 79013, Львів, Україна

(Отримано 25 вересня 2014 р.)

Розглянуто підгрупи мультиплікативної групи одного класу скінченних полів, пов'язані з алгоритмом AKS тестування простоти.

Ключові слова: скінченне поле, мультиплікативна група.

2000 MSC: 11T30

УДК: 512.624

Вступ

Прості числа мають фундаментальне значення в математиці загалом: є небагато краще відомих або легших для розуміння проблем у чистій математиці, ніж питання швидкого визначення є дане число простим чи складеним. Ефективні тести простоти також необхідні в прикладних застосуваннях: у низці криптографічних протоколів використовують великі прості числа.

У 2002 р. М. Агравал, Н. Кайал, Н. Саксена [1] представили детермінований поліноміальний алгоритм AKS, який визначає вхідне число n простим чи складеним. Доведено [3], що AKS виконується за час $(\log n)^{7.5+o(1)}$. Х. Ленстра та К. Померанс [4] дали істотно змінену версію AKS з часом виконання $(\log n)^{6+o(1)}$. Відомі також імовірнісні варіанти AKS [2] з часом виконання $(\log n)^{4+o(1)}$. Для подальшого покращення оцінки часу виконання було зроблене таке припущення [1], яке часто називають гіпотезою Агравала: якщо r просте число, яке не ділить n, та якщо $(X-1)^n = X^n - 1(mod\ n, X^r-1)$, то або n просте або $n^2 \equiv 1(mod\ r)$.

Якщо ця гіпотеза виявиться справедливою, то це покращить оцінку часу виконання алгоритму AKS до $(\log n)^{3+o(1)}$. Гіпотеза перевірена для $r < 100$ та $n < 10^{10}$ [1]. У [4] дається евристичний аргумент, який припускає, що наведена гіпотеза хибна. Проте, в [4] зауважено, що певний варіант гіпотези може все ж бути правильним (наприклад, якщо приймемо $r > \log n$).

У роботі розглядаємо підгрупи мультиплікативної групи відповідних скінченних полів.

I. Підґрунтя алгоритму AKS тестування простоти та постановка задачі

N та Z позначають відповідно множини натуральних та цілих чисел. (a,b) позначає найбільший спільний дільник чисел a та b. Якщо $r \in N$, $a \in Z$ та $(a,r) = 1$,то порядок a за модулем r – це таке найменше k, що $a^k \equiv 1(mod\ r)$. Його позначаємо $O_r(a)$. Для $r \in N$, $\varphi(r)$ є функцією Ейлера, яка дає кількість чисел, менших від r і взаємно простих з r. Легко бачити, що $O_r(a)|\varphi(r)$ для будь-якого a, $(a,r) = 1$.

$\langle u_1, ..., u_k\rangle$ позначає групу, породжену елементами $u_1, ..., u_k$. A^* позначає групу одиниць кільця A. Z_n позначає кільце цілих чисел за модулем n. Нагадаємо, що коли p просте та $h(X)$ нерозкладний над Z_p поліном степеня d, то $Z_p[X]/h(X)$ – скінченне поле з p^d елементів [5, 6]. Ми будемо використовувати позначення $f(X) = g(X)(mod\ n, h(X))$ для подання рівняння $f(X) = g(X)$ в кільці $Z_n[X]/h(X)$. log позначатиме логарифм за основою 2.

В основі алгоритму AKS лежать такі міркування [1]. Нехай n довільне ціле, для якого слід визначити: воно просте чи складене. Для цього перевіряємо рівності $(X+a)^n \equiv X^n + a$ в кільці $Z_n(X)/(X^r-1)$ для чисел $a = 1, ..., l$. Як степінь r полінома $X^r - 1$ вибираємо найменше r, що задовольняє умову $O_r(n) > \log^2 n$. Число рівнянь $l = \left\lfloor \sqrt{\varphi(r)} \log n \right\rfloor$. Розглядаємо підгрупу A групи Z_r^*, породжену елементами n та p. Припустимо, що $|A| = t$.

Також розглядаємо підгрупу G групи $U=(Z_p[X]/h(X))^*$ (p – простий дільник n, $h(X)$ – нерозкладний над Z_p дільник X^r-1), породжену множиною елементів $X + a, a = 0, ..., l$. Оскільки $t<\varphi(r), l<t$, то утворюючи добутки щонайбільше $l+1$ поліномів виду $X + a$ та показуючи, що вони різні в U, ми отримуємо нижню границю $|G| \geq 2^{l+1}$.

Якщо n не є степенем p, можна отримати також верхню границю для $|G|$. З цією метою розглядаємо множину $I = \{(n/p)^i p^j | 0 \leq i, j \leq \lfloor\sqrt{t}\rfloor\}$. I містить $\left(\lfloor\sqrt{t}\rfloor + 1\right)^2 > t$ різних чисел. Оскільки $|A| = t$, то принаймні два числа з I співпадають за модулем r: $\alpha \equiv \beta mod\ r$. Тоді $(X+a)^\alpha \equiv X^\alpha + a \equiv X^\beta + a \equiv (X+a)^\beta$. Значить, $(X+a)^{\alpha-\beta} = 1$ та $\alpha - \beta$ ділить $|G|$. Отже, $|G| < \alpha < (\frac{n}{p} \cdot p)^{\lfloor\sqrt{t}\rfloor} \leq n^{\lfloor\sqrt{t}\rfloor}$. Так як $t > \log^2 n$,

то $|G| \geq 2^{l+1} \geq 2^{\lfloor\sqrt{t}\log n\rfloor+1} > n^{\lfloor\sqrt{t}\rfloor}$ і ми отримуємо суперечність.

Отже, ідея алгоритму AKS полягає в такому: показати, що множина елементів $X + a$ породжує "достатньо велику" підгрупу групи $(Z_p[X]/h(X))^*$. З цього погляду можна трактувати гіпотезу Аггравала в такий спосіб. Якщо рівність $(X-1)^n = X^n - 1(mod\ n, X^r - 1)$ виконується, то множина, що складається з одного елемента $X-1$, породжує достатньо велику підгрупу.

Враховуючи наведене, важливою задачею є розгляд властивостей підгруп мультиплікативної групи скінченних полів вигляду $Z_p[X]/h(X)$, де p – просте число, $h(X)$ – нерозкладний над Z_p дільник полінома $X^r - 1$. Як правило, в алгоритмі AKS вибирають $h(X) = (X^r-1)/(X-1)$. Такі поля називають розширеннями простого поля Z_p на основі циклотомічних поліномів.

В остаточному підсумку бажано з'ясувати таке питання: яку мінімальну множину елементів слід взяти, щоб утворити достатньо велику підгрупу. Час виконання алгоритму доведення простоти залежить від кількості елементів цієї множини.

II. Підгрупа, породжена елементом $X-1$

Спочатку доведемо такий допоміжний результат.

Лема 1. *(1) $n - p^i$ для будь-якого цілого i ділиться на $p-1$ тоді і тільки тоді, коли $p-1|n-1$.*

(2) $n - p^i$ для будь-якого цілого i ділиться на $p+1$ тоді і тільки тоді, коли $p+1|n+1$.

□ *Доведення.* (1) Справедлива рівність $n - p^i = (n-1)-(p^i-1)$. Оскільки $p-1|p^i-1$, $n-p^i$ ділиться на $p-1$ тоді і тільки тоді, коли $p-1|n-1$.

(2) Справедлива рівність $n-p^i = (n+1)-(p^i+1)$. Оскільки $p+1|p^i+1$, $n-p^i$ ділиться на $p+1$ тоді і тільки тоді, коли $p+1|n+1$. ■

Наведені нижче теореми 1 та 2 описують властивості підгрупи $\langle X-1\rangle$.

Теорема 1. *Нехай $p_1, ..., p_k$ – попарно різні прості числа, $n = p_1...p_k$, r – просте число, p_i примітивне за модулем r для $i = 1, ..., k$. Якщо для кожного $i = 1, ..., k$ існує таке ціле число a_i, що $n \equiv p_i^{a_i}(mod\ 2r(p_i^{(r-1)/2} - 1))$, то*

$$(X-1)^n = X^n - 1(mod\ n, X^r - 1).$$

□ *Доведення.* Поліноми $X-1$ та $C_r(X) = X^{r-1} + X^{r-2} + ... + X + 1$ взаємно прості в кільці поліномів $Z_n[X]$. Тому, щоб довести рівність $(X-1)^n = X^n - 1(mod\ n, X^r - 1)$ досить довести, що

$$(X-1)^n = X^n - 1(mod\ n, C_r(X)).$$

За китайською теоремою про залишки маємо такий ізоморфізм:

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

Кожне фактор-кільце $R_i = Z_{p_i}[X]/C_r(X)$ є полем, оскільки кожне просте число p_i примітивне за модулем r ($O_r(p_i) = r-1$) , і, значить, поліном $C_r(X)$ нерозкладний над $Z_{p_i}[X]$ [5]. Тобто досить довести рівність

$$(X-1)^n = X^n - 1(mod\ p_i, C_r(X)) \qquad (1)$$

для кожного p_i.

За припущенням $n \equiv p_i^{a_i}(mod\ 2r(p_i^{(r-1)/2} - 1))$ для деякого цілого a_i, і тому $n \equiv p_i^{a_i}(mod\ r)$. Тоді $X^n \equiv X^{p_i^{a_i}}$ за модулем p_i і, отже, за модулем $C_r(X)$.

Оскільки R_i поле, то виконується рівність

$$(X-1)^{p_i^{a_i}} \equiv X^{p_i^{a_i}} - 1(mod\ p_i, C_r(X)) \qquad (2)$$

Оскільки p_i примітивне за модулем r , то $p_i^{r-1} \equiv 1(mod\ r)$ та $p_i^{(r-1)/2} \equiv -1(mod\ r)$(бо r – просте число). Тоді $(X-1)^{p_i^{(r-1)/2}} \equiv X^{-1}-1$ та $(X-1)^{p_i^{(r-1)/2}-1} \equiv -X^{-1}$ в полі R_i. Оскільки $(-X^{-1})^{2r} = 1$, то порядок $X-1$ в R_i ділить $2r(p_i^{(r-1)/2} - 1)$. За припущенням $n \equiv p_i^{a_i}(mod\ 2r(p_i^{(r-1)/2}-1))$ і тому $(X-1)^n \equiv (X-1)^{p_i^{a_i}}$. Оскільки відповідно ліві та праві частини рівнянь 1 та 2 співпадають і рівняння 2 виконується, то рівняння 1 також виконується. ■

Застосовуючи теорему 1 для випадку $r = 5$, отримуємо таку теорему.

Теорема 2. *Нехай $p_1, ..., p_k$ попарно різні прості числа і нехай $n = p_1...p_k$. Припустимо, що справедливі такі умови:*

(1) k – непарне

(2) $p_i(mod\ 5) \in \{2, 3\}$ для $i = 1, ..., k$;

(3) $p_1(mod\ 16) \in \{3, 5, 11, 13\}$ та для $i = 2, ..., k$ виконується: якщо $p_i \equiv p_1(mod\ 5)$, то $p_i \equiv p_1(mod\ 16)$, в іншому разі $p_i \equiv p_1^3(mod\ 16)$;

(4) $p_i - 1|n-1$ для $i = 1, ..., k$;

(5) $p_i + 1|n+1$ для $i = 1, ..., k$.

Тоді $(X-1)^n = X^n - 1(mod\ n, X^5 - 1)$ та $n^2 \equiv 1(mod\ 5)$.

□ *Доведення.* Парне число дільників p_i, які дорівнюють 2 або 3 за модулем 5, дають 1 або -1 за модулем 5. Дійсно, якщо $p_i(mod\ 5) \equiv 2$ та $p_j(mod\ 5) \equiv 2$, то $p_ip_j(mod\ 5) \equiv -1$. Якщо $p_i(mod\ 5) \equiv 2$ та $p_j(mod\ 5) \equiv 3$, то $p_ip_j(mod\ 5) \equiv 1$. Якщо $p_i(mod\ 5) \equiv 3$ та $p_j(mod\ 5) \equiv 3$, то $p_ip_j(mod\ 5) \equiv -1$.

Непарне число (принаймні три) дільників p_i, які дорівнюють 2 або 3 за модулем 5 дають 2 або 3 за модулем 5. Значить, $n^2 \neq 1(mod\ 5)$. За теоремою 1 досить показати, що для кожного i існує таке ціле a_i, що рівність $n \equiv p_i^{a_i}(mod\ 10(p_i^2 - 1))$ справедлива.

Відомі два різних варіанти розкладу $10(p_i^2 - 1)$ на 4 попарно взаємно простих множники залежно від значення $p_i(mod\ 16)$:

– якщо $p_i(mod\ 16) \in \{3,11\}$, то $10(p_i^2-1) = 5\cdot 16\cdot \frac{p_i-1}{2}\cdot\frac{p_i+1}{4}$;

– якщо $p_i(mod\ 16) \in \{5,13\}$, то $10(p_i^2-1) = 5\cdot 16\cdot \frac{p_i-1}{4}\cdot\frac{p_i+1}{2}$.

В обидвох випадках досить показати існування такого цілого a_i, що рівність $n \equiv p_i^{a_i}(mod\ 10(p_i^2-1))$ справедлива за модулем кожного дільника.

Розглянемо перший випадок.

Якщо $n \equiv p_i(mod\ 5)$, то $a_i = 1$, $n \equiv p_i(mod\ 16)$ за умовою (3), $n \equiv p_i(mod\ (p_i-1)/2)$ за лемою 1 та умовою (4), $n \equiv p_i(mod (p_i+1)/4)$ за лемою 1 та умовою (5).

Якщо $n \not\equiv p_i(mod\ 5)$, то $a_i = 3$ (оскільки $2 \equiv 3^3 mod\ 5$ та $3 \equiv 2^3 mod\ 5$), $n \equiv p_i^3(mod\ 5)$, $n \equiv p_i^3(mod\ 16)$ за умовою (3), ($11 \equiv 3^3(mod\ 16)$, $3 \equiv 11^3(mod\ 16)$,$13 \equiv 5^3(mod\ 16)$,$5 \equiv 13^3(mod\ 16)$), $n \equiv p_i^3(mod\ (p_i-1)/2)$ за лемою 1 і умовою (4), $n \equiv p_i^3(mod\ (p_i+1)/4)$ за лемою 1 та умовою (5).

У другому випадку доведення аналогічне. ■

Зауважимо, що теорема 2 також правильна у випадку, якщо умову (3) замінити на таку:

(3′) $p_1(mod\ 32) \in \{7,9,23,25\}$ та для $i = 2,...,k$ виконується: якщо $p_i \equiv p_1(mod\ 5)$, то $p_i \equiv p_1(mod\ 32)$, в іншому випадку $p_i \equiv p_1^3(mod\ 32)$. Аналогічні умови можна записати, заміняючи 32 на більші степені двійки.

Також слід зауважити, що порядок групи $(Z_{p_i}[X]/C_r(X))^*$ дорівнює $(p_i^2-1)(p_i^2+1)$. Виконується умова $10|p_i^2+1$. Порядок елемента $X-1$ з теореми 2 в групі $(Z_{p_i}[X]/C_r(X))^*$ ділить $10(p_i^2-1)$ для будь-якого простого дільника p_i числа n.

Теорема 2 узагальнює твердження з роботи [4]. Згідно з нею можна шукати контрприклади [4] для гіпотези Агравала при $r = 5$. Враховуючи теорему 1, це можна робити і для $r > 5$. У доповнення до обчислювальних результатів з [1] гіпотезу перевірено для $r = 5$ та $10^{100} < n < 10^{100} + 10^5$ [8]. Ні один контрприклад поки що не знайдено.

III. Ланцюг підгруп мультиплікативної групи

Число n припускаємо примітивним за модулем r. Зауважимо, що для $p|n$ елемент $X-1$ є одиницею в кільці $Z_p[X]/(C_r(X))$.

Теорема 1. *Якщо* $(X-1)^n = X^n - 1(mod\ n, X^r-1)$, *то* $\langle X\rangle \subset \langle X+1\rangle \subset \langle X-1\rangle$ *строго зростаючий ланцюг підгруп групи* $(Z_p[X]/C_r(X))^*$ *для будь-якого простого дільника* p *числа* n.

□ *Доведення.* Оскільки $(X-1)^n = X^n - 1(mod\ n, X^r-1)$, то $(X-1)^n = X^n - 1(mod\ p, C_r(X))$. Оскільки n примітивне за модулем r, існує таке ціле a, що $n^a \equiv 2(mod\ r)$. Тоді $(X-1)^{n^a} = X^2-1 = (X-1)(X+1)$. Значить, $X+1 = (X-1)^{n^a-1} \in \langle X-1\rangle$ та $\langle X+1\rangle \subseteq \langle X-1\rangle$.

Оскільки $X+1 \in \langle X-1\rangle$ та $(X-1)^n = X^n - 1(mod\ p, C_r(X))$, то $(X+1)^n = X^n + 1(mod\ p, C_r(X))$.

Оскільки n примітивне за модулем r, існує таке ціле c, що $n^c \equiv r-1(mod\ r)$. Тоді $(X+1)^{n^c} = X^{n^c}+1 = X^{r-1}+1 = X^{-1}+1 = X^{-1}(X+1)$. Нагадаємо, що $X^r = 1$. Звідси, $(X+1)^{n^c-1} = X^{-1}(mod\ p, C_r(X))$. Тоді $\langle X^{-1}\rangle \subseteq \langle X+1\rangle$. Оскільки групи $\langle X^{-1}\rangle$ та $\langle X\rangle$ співпадають, то $\langle X\rangle \subseteq \langle X+1\rangle$. Оскільки $\langle X\rangle = \{1, X, ..., X^{r-1}\}$, зрозуміло, що $X+1 \notin \langle X\rangle$ та $\langle X\rangle \subset \langle X+1\rangle$.

Для доведення $\langle X+1\rangle \subset \langle X-1\rangle$ розглянемо автоморфізм σ кільця $Z_p[X]/(C_r(X))$, який відображає X в X^{-1}. Припустимо $(X+1)^V = X-1(mod\ p, C_r(X))$ для деякого цілого V. Скористаємось для $\alpha = (X+1)^V$ та $\beta = X-1$ тим фактом, що з $\alpha = \beta$ випливає $\alpha\cdot(\sigma(\alpha))^{-1} = \beta\cdot(\sigma(\beta))^{-1}$.

Зауважимо, що $X+1$ та $X-1$ є одиницями, і тому $[\sigma(X+1)]^{-1}$ та $[\sigma(X-1)]^{-1}$ існують. Маємо $(X+1)[\sigma(X+1)]^{-1} = (X+1)[X^{-1}(X+1)]^{-1} = X$ та $(X-1)[\sigma(X-1)]^{-1} = (X-1)[-X^{-1}(X-1)]^{-1} = -X$. Тоді $X^V = -X$– суперечність.

Отже, ланцюг підгруп $\langle X\rangle \subset \langle X+1\rangle \subset \langle X-1\rangle$ є строго зростаючим. ■

Теорема 2. *Якщо* p *– просте та* $a \not\equiv 0, 1, -1(mod\ p)$, *то* $X+a \notin \langle X-1\rangle$ *в групі* $(Z_p[X]/C_r(X))^*$.

□ *Доведення.* Припустимо $(X-1)^V = X + a(mod\ p, C_r(X))$. Знову розглянемо автоморфізм σ кільця $Z_p[X]/(C_r(X))$, який переводить X в X^{-1}. Тоді маємо

$$(X+a)[\sigma(X+a)]^{-1} = (X-1)^V[\sigma((X-1)^V)]^{-1},$$

$$(X+a)[X^{-1}+a)]^{-1} = (-X)^V,$$

$$X+a = (-1)^V(-X)^{V-1} + (-1)^V aX^V.$$

Якщо $X = (-1)^V aX^V$, то $(-1)^V \neq a$, що неможливо. Тоді $X = (-1)^V X^{V-1}$, $V-1 \equiv 1(mod\ r)$, $V \equiv 2(mod\ r)$. З іншого боку, $a = (-1)^V aX^V$, $V \equiv 0(mod\ r)$ – суперечність. ■

Враховуючи теорему 1 та 2, маємо такий строго зростаючий ланцюг підгруп

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

Більше того, для $r = 5$ справедлива така теорема.

Теорема 3. *Якщо просте число* p *не дорівнює 2,3,5,11,19 та* $p^2 \neq 1(mod\ 5)$, *то порядок елемента* $X+2$ *в полі* $Z_p[X]/(C_5(X))$ *не ділить* $10(p^2-1)$.

□ *Доведення.* Легко перевірити, що $(X+2)\times(X^3-X^2+3X-5) \equiv -11(mod\ p, C_5(X))$, тобто елемент $-11^{-1}(X^3-X^2+3X-5)$ є мультиплікативним оберненим для $X+2$ в полі

$Z_p[X]/(C_5(X)) = Z_p[X]/(X^4+X^3+X^2+X+1)$. Маємо $(X+2)^{p^2} \equiv X^{-1}+2 = X^{-1}(2X+1)$ та

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

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

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

$$+22802637960X + 29275201379).$$

Розклад на прості множники коефіцієнтів полінома при ненульових степенях X є таким:

$$19486165920 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 13 \cdot 19 \cdot 164357;$$

$$26683280040 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 19 \cdot 167 \cdot 70079;$$

$$22802637960 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 19 \cdot 67 \cdot 49757.$$

Оскільки p не ділить найбільший спільний дільник коефіцієнтів (який дорівнює $2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 19$), то ці коефіцієнти одночасно не дорівнюють нулю за модулем p. Значить, поліном $(X+2)^{10(p^2-1)}$ не дорівнює 1. ■

Доведені теореми 1, 2 та 3 дають змогу припустити, що такий варіант гіпотези Аггравала може бути правильним: якщо r просте число, яке не ділить n, якщо $(X-1)^n = X^n - 1(mod\ n, X^r - 1)$ і якщо $(X+2)^n = X^n + 2(mod\ n, X^r - 1)$, то або n просте або $n^2 \equiv 1(mod\ r)$.

На завершення зауважимо, що, використовуючи результати з [7], можна отримати експоненційну нижню оцінку для числа елементів підгрупи $\langle X+1 \rangle$.

Література

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

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

[3] *Granville A.* It is easy to determine whether a given integer is prime // Bull. Amer. Math. Soc., **42** (1). – 2005. – P. 3–38.

[4] *Lenstra H.W., Jr., Pomerance C.* Remarks on Agrawal's conjecture // http:// www.aimath.org/ WWN/ primesinp/ articles/ html/ 50a, 2003.

[5] *Lidl R., Niederreiter H.* Finite Fields. – Cambridge University Press, Cambridge, 1997. – 755 p.

[6] *Mullen L., Panario D.* Handbook of finite fields. – CRC Press, London, 2013. – 1068 p.

[7] *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ // Finite Fields Appl., **18** (4). – 2012. – P. 700–710.

[8] *Popovych R., Popovych B.* On Agrawal conjecture // Int. Conf. dedicated to the 120th anniversary of S. Banach, Lviv, Ukraine, 17–21 Sept. 2012. – 261 p.

О ПОДГРУППАХ МУЛЬТИПЛИКАТИВНОЙ ГРУППЫ ОДНОГО КЛАССА КОНЕЧНЫХ ПОЛЕЙ

Поповыч Р. Б.

Национальный университет "Львівська политэхника"
ул. С. Бандеры, 12, 79013, Львов, Украина

Рассмотрено подгруппы мультипликативной группы одного класса конечных полей, связанных с алгоритмом AKS тестирования простоты.

Ключевые слова: конечное поле, мультипликативная группа.

2000 MSC: 11T30

УДК: 512.624

ON SUBGROUPS OF MULTIPLICATIVE GROUP OF ONE CLASS OF FINITE FIELDS

Popovych R. B.

Lviv Polytechnic National University
12, S. Bandery Str., Lviv, 79013, Ukraine

We consider subgroups of the multiplicative group of one class of finite fields connected with the primality testing AKS algorithm.

Key words: finite field, multiplicative group.

2000 MSC: 11T30

UDK: 512.624