УДК 512.713

АНАЛОГ КРИТЕРИЯ МИЛЛЕРА В ДЕДЕКИНДОВЫХ КОЛЬЦАХ С КОНЕЧНОЙ НОРМОЙ

М.М. Васьковский, Н.В. Кондратёнок

Белорусский государственный университет, Минск, Беларусь
vaskovskii@bsu.by, nkondr2006@rambler.ru

Найдены новые классы дедекиндовых колец с конечной нормой, в которых выполняется аналог критерия Миллера, а также получен эффективный алгоритм тестирования простоты идеалов, являющийся аналогом вероятностного теста Миллера-Рабина. В предположении справедливости расширенной гипотезы Римана доказан аналог теоремы Анкени, с помощью которой получено усиление аналога критерия Миллера, приводящее к детерминированному полиномиальному алгоритму тестирования простоты идеалов.

***Ключевые слова*:** дедекиндово кольцо; простые идеалы; критерий Миллера; тест на простоту.

AN ANALOGUE OF THE MILLER CRITERION IN DEDEKIND DOMAINS WITH A FINITE NORM PROPERTY

M.M. Vaskouski, N.V. Kondratyonok

Belarusian State University, Minsk, Belarus

There are found new classes of Dedekind domains with a finite norm property such that an analogue of the Miller criterion is valid in these domains, and an analogue of the Miller-Rabin algorithm for testing ideals primality is obtained. Assuming validity of the extended Riemann hypothesis, an analogue of Ankeny's theorem is proved that allows to obtain a strengthening of Miller's criterion analogue providing to a deterministic polynomial algorithm for testing the primality of ideals.

***Keywords*:** Dedekind domain; prime ideals; miller criterion; simplicity test; primality test.

Введение

Начиная со второй половины XX века начала активно развиваться информатика и криптография, что привело к увеличению активности работы в области алгоритмической теории чисел со стороны ведущих математиков. В частности, были получены принципиально новые критерии простоты, приводящие к эффективным алгоритмам тестирования простоты и генерации больших простых чисел. В 1980 году, опираясь на результат Г. Миллера [1], М.О. Рабиным [2] был получен безусловный полино-

миальный вероятностный алгоритм тестирования простоты, названный алгоритмом Миллера-Рабина. В предположении справедливости расширенной гипотезы Римана в работе [3] была доказана теорема, позволяющая получить детерминированный вариант алгоритма Миллера-Рабина. Алгоритм Миллера-Рабина играет ключевую роль при генерации ключей для RSA-криптосистемы.

Задача проверки на простоту существенно усложняется при переходе от целых чисел к более общим алгебраическим структурам. В работе [4] был получен полиномиальный детерминированный алгоритм проверки на простоту в конечнопорожденных дедекиндовых кольцах. В работе М.М. Васьковского, Н.В. Кондратёнка и Н.П. Прохорова [5] был разработан подход, позволяющий переносить доказательства ряда известных критериев простоты на различные алгебраические структуры. В 2020 году в работе Н.П. Прохорова [6] были доказаны новые критерии простоты в кольцах целых алгебраических чисел. В настоящей статье доказывается аналога критерия Миллера в некотором классе дедекиндовых колец, а также приводится соответствующий алгоритм тестирования простоты идеалов.

1. Основные результаты

Пусть R дедекиндово кольцо. Нормой $Nm(\mathfrak{n})$ идеала $\mathfrak{n} \subset R$ называется мощность факторкольца $R/\mathfrak{n}$. Говорят, что дедекиндово кольцо R является дедекиндовым кольцом с конечной нормой (finite norm property), если для любого собственного идеала $\mathfrak{n} \subset R$ факторкольцо $R/\mathfrak{n}$ конечно. Далее в работе будем рассматривать только дедекиндовы кольца с конечной нормой. Пусть $a, b \in R$ и $\mathfrak{n} \subseteq R$. Будем говорить, что a сравнимо с b по модулю $\mathfrak{n}$ и писать $a \equiv b(mod\ \mathfrak{n})$, если $a - b \in \mathfrak{n}$.

Определение 1. [7, с. 285] Функцией Эйлера нетривиального идеала $\mathfrak{n} \subset R$ называется функция

$$\varphi(\mathfrak{n}) = \left|I_{R/\mathfrak{n}}\right|.$$

Определение 2. Элемент $a \in R$ будем называть квадратичным вычетом по модулю идеала $\mathfrak{n}$, если существует $b \in R$, что $b^2 \equiv a(mod\ \mathfrak{n})$.

Для простого идеала $\mathfrak{p}$ и $a \in I_{R/\mathfrak{p}}$ определим символ Лежандра следующим образом

$$\left(\frac{a}{\mathfrak{p}}\right) = \begin{cases} 1, \text{если } a \text{ квадратичный вычет по модулю } \mathfrak{p}, \\ -1, \text{иначе.} \end{cases}$$

Для нетривиального идеала $\mathfrak{n} = \mathfrak{p}_1 \dots \mathfrak{p}_k$ и $a \in I_{R/\mathfrak{n}}$ определим символ Якоби следующим образом

$$\left(\frac{a}{\mathfrak{n}}\right) = \left(\frac{a}{\mathfrak{p}_1}\right) \dots \left(\frac{a}{\mathfrak{p}_k}\right).$$

Пусть K является полем частных R. Пусть расширение $L \supset K$ конечное, сепарабельное и нормальное расширение, а $Gal(L/K)$ является абелевой. Положим S алгебраическое замыкание R в L.

Определение 3. Пусть $\mathfrak{p}$ простой идеал кольца R. Рассмотрим идеал $\mathfrak{p}S$, который он генерирует в кольце S. Рассмотрим его факторизацию на простые идеалы

$$\mathfrak{p}S = \prod\nolimits_{\mathfrak{q}} \mathfrak{q}^{e_{\mathfrak{q}}},$$

где произведение берется по всем простым идеалам кольца S и $e_{\mathfrak{q}} > 0$ только для конечного количества простых $\mathfrak{q}$.

Если $e_{\mathfrak{q}} > 0$ для некоторого $\mathfrak{q}$, то говорят, что $\mathfrak{q}$ лежит над (lie over, lie above) простым идеалом $\mathfrak{p}$. Число $e_{\mathfrak{q}}$ из разложения называется индексом разветвления (ramification index) $\mathfrak{q}$.

Если для простого идеала $\mathfrak{p} \subseteq R$ выполнено $e_{\mathfrak{q}} > 1$ для некоторого $\mathfrak{q} \subseteq R$, то говорят, что идеал $\mathfrak{p}$ ветвится в L. Если идеал $\mathfrak{p}S$ простой в S, то говорят, что $\mathfrak{p}$ инертный (inert). Если для всех $\mathfrak{q}$ выполняется или $e_{\mathfrak{q}} = 0$, или $e_{\mathfrak{q}} = 1$, то говорят, что $\mathfrak{p}$ полностью разлагается (splits completely) в L.

Определение 4. Пусть $\mathfrak{p}$ простой идеал кольца R, не ветвящийся в L и пусть $\mathfrak{P} = \mathfrak{p}S$ соответствующий идеал в S. Тогда существует единственный такой элемент $\sigma \in Gal(L/K)$, что для любого $\alpha \in L$ выполнено $\sigma(\alpha) \equiv \alpha^{Nm(\mathfrak{p})} (mod\ \mathfrak{P})$. Этот элемент называют символом Артина идеала $\mathfrak{p}$.

Определение 5. Пусть $\phi: Gal(L/K) \to I_{\mathbb{C}}$ гомоморфизм. Рассмотрим функцию

$$\chi(\mathfrak{p}) = \begin{cases} \phi\left(\sigma_{\mathfrak{p}}\right), \text{если } \mathfrak{p} \text{ не ветвится}, \\ 0, \text{иначе}, \end{cases}$$

где $\mathfrak{p}$ простой и $\sigma_{\mathfrak{p}}$ символ Артина идеала $\mathfrak{p}$. Используя мультипликативность, эту функцию можно определить для всех идеалов R. Полученную функцию χ будем называть характером. Характер, принимающий только значения 0 и 1, называется главным.

Определение 6. Будем говорить, что характер χ задан по модулю идеала $\mathfrak{f} \subset R$, если для всех идеалов $\mathfrak{n} \subseteq R$, из сравнения $\mathfrak{n} \equiv 1 (mod\ \mathfrak{f})$ следует равенство $\chi(\mathfrak{n}) = 1$.

Определение 7. Пусть характер χ задан на множестве идеалов кольца R, не является главным и определен по модулю идеала $\mathfrak{n} \subset R$. Через $\mathfrak{p}_\chi$ обозначим идеал минимальной нормы, для которого $\chi\left(\mathfrak{p}_\chi\right) \neq 0, 1$.

Определение 8. Пусть R дедекиндово кольцо с полем частных K и L расширение поля K степени не меньше 2. Будем говорить, что кольцо R удовлетворяет условию A для идеала $\mathfrak{n}$, если существует многочлен f_R, что для любого характера χ, не являющегося главным и определенного по модулю $\mathfrak{n}$, выполнено

$$Nm(\mathfrak{p}_\chi) \leq f_R(\log Nm(\mathfrak{n})).$$

Замечание. Из работы [8] следует, что, если расширенная гипотеза Римана выполнена, то условие A выполнено для всех колец $\mathcal{O}_K$ целых алгебраических чисел числового поля K и $f_{\mathcal{O}_K}(x) = 12\mathrm{x}^2 + 12\log^2 \Delta_K$.

Замечание. Из работы [3] следует, что, если обобщенная гипотеза Римана выполнена, то условие A выполнено для кольца целых чисел и $f_{\mathbb{Z}}(x) = 2x^2$.

Предложение 1. Пусть кольцо R удовлетворяет условию A. Пусть $\chi: I_{R/\mathfrak{n}} \to G$ нетривиальный гомоморфизм. Тогда существует идеал $\mathfrak{a}$ взаимнопростой с $\mathfrak{n}$ и такой, что $\chi(\mathfrak{a}) \neq 1$ и $Nm(\mathfrak{a}) \leq f_R(\log Nm(\mathfrak{n}))$.

Доказательство. Из условия предложения следует, что подгруппа $\chi(I_{R/\mathfrak{n}}) \subseteq G$ нетривиальная. Рассмотрим нетривиальный характер $\xi: \chi(I_{R/\mathfrak{n}}) \to I_{\mathbb{C}}$. Очевидно, что $\xi \circ \chi: I_{R/\mathfrak{n}} \to I_{\mathbb{C}}$ является нетривиальным характером группы $I_{R/\mathfrak{n}}$.

Из определения условия A следует, что существует простой $\mathfrak{a}$ взаимнопростой с $\mathfrak{n}$ и такой, что $(\xi \circ \chi)(\mathfrak{a}) \neq 1$ и $Nm(\mathfrak{a}) \leq f_R\big(\log\big(Nm(\mathfrak{n})\big)\big)$. Из того, что $(\xi \circ \chi)(\mathfrak{a}) \neq 1$ следует, что $\chi(\mathfrak{a}) \neq 1$.

Предложение 2. Пусть идеал $\mathfrak{p}$ простой с нечетной нормой. Тогда сравнение $x^{Nm(\mathfrak{p})-1} \equiv 1 (mod\ \mathfrak{p}^2)$ имеет не более $Nm(\mathfrak{p}) - 1$ решений относительно $x \in I_{R/\mathfrak{p}^2}$.

Доказательство. Из теоремы Эйлера [7, с. 285] следует, что сравнение $x^{Nm(\mathfrak{p})-1} \equiv 1 (mod\ \mathfrak{p})$ имеет ровно $Nm(\mathfrak{p}) - 1$ решений относительно $x \in I_{R/\mathfrak{p}}$.

Заметим, что все решения сравнения $x^{Nm(\mathfrak{p})-1} \equiv 1 (mod\ \mathfrak{p}^2)$ имеют вид $a + \mathfrak{p}\mathfrak{t}$, где $x \in I_{R/\mathfrak{p}}$, $\mathfrak{t} \in R/\mathfrak{p}$ и a является решением сравнения $x^{Nm(\mathfrak{p})-1} \equiv 1 (mod\ \mathfrak{p})$. Подставим этот вид в сравнение, раскроем скобки и получим сравнение $\mathfrak{p}\mathfrak{t}(Nm(\mathfrak{p}) - 1)a^{Nm(\mathfrak{p})-2} \equiv 1 - a^{Nm(\mathfrak{p})-1} (mod\ \mathfrak{p}^2)$. Так как $\Big((Nm(\mathfrak{p}) - 1)a^{Nm(\mathfrak{p})-2}, \mathfrak{p}\Big) = 1$, то это сравнение имеет ровно одно решение при фиксированном a. Следовательно, исходное сравнение имеет не более $Nm(\mathfrak{p}) - 1$ решений относительно $x \in I_{R/\mathfrak{p}^2}$.

Из рассуждений работы [6] вытекает следующий аналог критерия Эйлера для дедекиндовых колец с конечной нормой.

Утверждение 2. Пусть $\mathfrak{n}$ – нетривиальный идеал нечетной нормы дедекиндового кольца R. Тогда $\mathfrak{n}$ – простой идеал тогда и только тогда, когда для любого $a \in I_{R/\mathfrak{n}}$ выполнено $a^{\frac{Nm(\mathfrak{n})-1}{2}} \equiv \left(\frac{a}{\mathfrak{n}}\right) (mod\ \mathfrak{n})$.

Теорема 1. Пусть $\mathfrak{n}$ – нетривиальный идеал нечетной нормы дедекиндового кольца R. Пусть $Nm(\mathfrak{n}) - 1 = 2^t u$, $(u, 2) = 1$. Тогда $\mathfrak{n}$ – простой идеал тогда и только тогда, когда для любого $a \in I_{R/\mathfrak{n}}$, $a^u \not\equiv 1 (\mathrm{mod}\ \mathfrak{n})$ существует $k \in \{0, \dots, t-1\}$, такое что $a^{2^k u} \equiv -1 (\mathrm{mod}\ \mathfrak{n})$.

Пусть кольцо R факториальное и удовлетворяет условию А. Тогда $\mathfrak{n}$ – простой идеал тогда и только тогда, когда для любого $a \in I_{R/\mathfrak{n}}$, $Nm(a) \leq f_R\big(Nm(a)\big)$, $(a, \mathfrak{n}) = 1$, $a^u \not\equiv 1 (\mathrm{mod}\ \mathfrak{n})$ существует $k \in \{0, \dots, t-1\}$, такое что $a^{2^k u} \equiv -1 (\mathrm{mod}\ \mathfrak{n})$.

Доказательство. Докажем первую часть теоремы. Предположим, что $\mathfrak{n}$ – простой идеал. Рассмотрим произвольный $a \in I_{R/\mathfrak{n}}$, $a^u \not\equiv 1 (\mathrm{mod}\ \mathfrak{n})$. Из теоремы Эйлера следует, что $a^{2^t u} = a^{\varphi(\mathfrak{n})} \equiv 1 (\mathrm{mod}\ \mathfrak{n})$. Раскладываем на множители и получаем, что выполнено $(a^u - 1)(a^u + 1)(a^{2u} + 1) \dots \left(a^{2^{t-1} u} + 1\right) \equiv 0 (\mathrm{mod}\ \mathfrak{n})$. Из того, что $a^u \not\equiv 1 (\mathrm{mod}\ \mathfrak{n})$ следует, что $a^{2^k u} + 1 \equiv 0 (\mathrm{mod}\ \mathfrak{n})$ для некоторого $k \in \{0, \dots, t-1\}$. Это завершает доказательство необходимости.

Предположим, что $\mathfrak{n}$ – не простой идеал. Пусть $\mathfrak{n}$ раскладывается в произведение простых идеалов следующим образом $\mathfrak{n} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$. Так как норма простого идеала примарная, то обозначим $Nm(\mathfrak{p}_i) = q_i^{f_i}$, где q_i – простой в $\mathbb{Z}$.

Пусть существует такой $j \in \{1, \dots, r\}$, что $\alpha_j > 1$ в разложении $\mathfrak{n}$ на множители. Из теоремы Коши для групп и свойств функции Эйлера следует, что существует $a \in I_{R/\mathfrak{n}}$ порядка q_j. Так как $u \not\equiv 0 \big(mod\ q_j\big)$, то $a^u \not\equiv 1 (mod\ \mathfrak{n})$. Следовательно, существует число $k \in \{0, \dots, t-1\}$, такое что выполнено сравнение $a^{2^k u} \equiv -1 (\mathrm{mod}\ \mathfrak{n})$. Тогда $a^{2^{k+1} u} \equiv 1 (\mathrm{mod}\ \mathfrak{n})$. Значит выполнено $2^{k+1} u \equiv 0 \big(mod\ q_j\big)$. Из последнего сравнения следует, что $Nm(\mathfrak{n}) - 1 \equiv 0 \big(mod\ q_j\big)$, что невозможно.

Следовательно, $\alpha_j = 1$ для любого $j \in \{1, \dots, r\}$. Так как $\mathfrak{n}$ – составное, то $r \geq 2$. Из аналога Китайской теоремы об остатках и того, что элемент -1 имеет порядок 2 в каждой группе $I_{R/\mathfrak{p}_j}$ следует, что существует по крайней мере $2^r - 1 \geq 3$ элемента $I_{R/\mathfrak{n}}$ порядка 2. Пусть $a \not\equiv \pm 1 (mod\ \mathfrak{n})$ является произвольным элементом порядка 2 в группе $I_{R/\mathfrak{n}}$. Из того, что $(u, 2) = 1$ следует, что $a^u \equiv a \not\equiv \pm 1 (mod\ \mathfrak{n})$. Таким образом, существует

$k \in \{0, \dots, t-1\}$, такое что верно $a^{2^k u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$. Это противоречит тому, что порядок a равен 2. Это завершает доказательство достаточности.

Теперь докажем вторую часть теоремы. Необходимость следует из доказанного ранее. Предположим, что $\mathfrak{n} \in R^* \setminus I_R$ составной идеал нечетной нормы и для любого $a \in I_{R/\mathfrak{n}}$, $Nm(a) \leq f_R\big(Nm(a)\big)$, $(a, \mathfrak{n}) = 1$, $a^u \not\equiv 1 (\mathrm{mod}\, \mathfrak{n})$ существует $k \in \{0, \dots, t-1\}$, такое что $a^{2^k u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$.

Предположим, что существует такой простой идеал $\mathfrak{p}$, что $\mathfrak{p}^2 | \mathfrak{n}$. Рассмотрим такое отображение $\chi: I_{R/\mathfrak{p}^2} \to I_{R/\mathfrak{p}^2}$, что для всех $a \in I_{R/\mathfrak{p}^2}$ выполнено $\chi(a) = a^{Nm(\mathfrak{p})-1}$. Из предложения 2 следует, что это нетривиальный гомоморфизм. Тогда, из предложения 1, получаем, что существует такой элемент $a \in I_{R/\mathfrak{p}^2}$, что $a^{Nm(\mathfrak{p})-1} \not\equiv 1 (mod\ \mathfrak{p}^2)$.

Предположим, что $a^{Nm(\mathfrak{n})-1} \equiv 1 (mod\ \mathfrak{n})$. Тогда $a^{Nm(\mathfrak{n})-1} \equiv 1 (mod\ \mathfrak{p}^2)$. Тогда $ord_{R/\mathfrak{p}^2}(a) | Nm(\mathfrak{n}) - 1$ и $ord_{R/\mathfrak{p}^2}(a) | \varphi(\mathfrak{p}^2)$. Из этого следует, что $ord_{R/\mathfrak{p}^2}(a) | Nm(\mathfrak{p}) - 1$. Это противоречит выражению $a^{Nm(\mathfrak{p})-1} \not\equiv 1 (mod\ \mathfrak{p}^2)$.

Следовательно, не существует такой простой идеал $\mathfrak{p}$, что $\mathfrak{p}^2 | \mathfrak{n}$. Пусть $\mathfrak{p}$ и $\mathfrak{q}$ различные простые делители $\mathfrak{n}$. Обозначим $v_2(n)$ максимальную степень двойки, делящую $n \in \mathbb{Z}$. Не нарушая общности, предположим, что $v_2(Nm(\mathfrak{p}) - 1) \geq v_2(Nm(\mathfrak{q}) - 1)$. Пусть

$$\mathfrak{d} = \begin{cases} \mathfrak{pq}, \text{если } v_2(Nm(\mathfrak{p}) - 1) = v_2(Nm(\mathfrak{q}) - 1), \\ \mathfrak{p}, \text{если } v_2(Nm(\mathfrak{p}) - 1) > v_2(Nm(\mathfrak{q}) - 1). \end{cases}$$

Рассмотрим такое отображение $\xi: I_{R/\mathfrak{n}} \to I_{R/\mathfrak{n}}$, что для всех $a \in I_{R/\mathfrak{n}}$ выполнено $\xi(a) = \left(\frac{a}{\mathfrak{d}}\right)$. Это отображение является нетривиальным гомоморфизмом. Тогда, из предложения 1, получаем, что существует такой элемент $a \in I_{R/\mathfrak{n}}$, что $\left(\frac{a}{\mathfrak{d}}\right) \not\equiv 1 (mod\ \mathfrak{n})$.

Положим $b = a^u$. Тогда $\left(\frac{b}{\mathfrak{d}}\right) = -1$. Следовательно, $b \not\equiv 1 (mod\ \mathfrak{d})$. Пусть $j \in \mathbb{Z}$ минимальное число, для которого $a^{2^j u} \equiv -1 (mod\ \mathfrak{n})$. Тогда $ord_{R/\mathfrak{p}}(b) = ord_{R/\mathfrak{q}}(b) = 2^{j+1}$.

Рассмотрим два случая. Пусть $v_2(Nm(\mathfrak{p}) - 1) > v_2(Nm(\mathfrak{q}) - 1)$. Тогда $ord_{R/\mathfrak{q}}(b) = 2^{j+1} | \varphi(\mathfrak{q}) = Nm(\mathfrak{q}) - 1$. Следовательно, $ord_{R/\mathfrak{p}}(b) = 2^{j+1} | (Nm(\mathfrak{p}) - 1)/2$. Получаем, что $\left(\frac{b}{\mathfrak{d}}\right) = \left(\frac{a}{\mathfrak{p}}\right) = -1$ и $b^{(Nm(\mathfrak{p})-1)/2} \equiv 1 (mod\ \mathfrak{p})$. Это противоречит критерию Эйлера.

Пусть $v_2(Nm(\mathfrak{p}) - 1) = v_2(Nm(\mathfrak{q}) - 1)$. Тогда $\left(\frac{b}{\mathfrak{d}}\right) = \left(\frac{b}{\mathfrak{p}}\right)\left(\frac{b}{\mathfrak{q}}\right) = -1$. Следовательно, один из множителей равен -1. Пусть $\left(\frac{b}{\mathfrak{p}}\right) = -1$ и $\left(\frac{b}{\mathfrak{q}}\right) = 1$.

Из критерия Эйлера следует, что $b^{(Nm(\mathfrak{q})-1)/2} \equiv 1(mod\ \mathfrak{q})$ и $ord_{R/\mathfrak{p}}(b) = ord_{R/\mathfrak{q}}(b) | (Nm(\mathfrak{q})-1)/2$. Тогда $ord_{R/\mathfrak{p}}(b) | (Nm(\mathfrak{p})-1)/2$. Следовательно, $b^{(Nm(\mathfrak{p})-1)/2} \equiv 1(mod\ \mathfrak{p})$, что противоречит предположению $\left(\frac{b}{\mathfrak{p}}\right) = -1$.

Аналог алгоритма Миллера-Рабина. Пусть дан идеал $\mathfrak{n} \subset R$. Необходимо определить является ли он простым.

1. Найти $\mathfrak{u}, t \in \mathbb{N}$, что $Nm(\mathfrak{n}) - 1 = 2^t u$ и $(2, u) = 1$;
2. Выбрать случайный $a \in I_{R/\mathfrak{n}}$ и вычислить $r_0 \equiv a^u (mod\ \mathfrak{n})$;
3. Если $r_0 = 1$, то вернуть "неизвестно" и завершить алгоритм;
4. Для k от 0 до t выполнить:
   a. Если $r_k = -1$, то вернуть "неизвестно" и завершить алгоритм;
   b. Вычислить $r_{k+1} \equiv r_k^2 (mod\ \mathfrak{n})$;
5. Вернуть "$\mathfrak{n}$ не простой" и завершить алгоритм.

Замечание. Аналог алгоритма Миллера-Рабина является вероятностным. Если был получен ответ "неизвестно", то можно выполнить алгоритм еще раз.

Библиографические ссылки

1. Miller G. Riemann’s Hypothesis and Tests for Primality // Journal of Computer and System Sciences. 1976. № 13(3). P. 300–317.
2. Rabin M.O. Probabilistic Algorithm for Testing Primality // Journal of number theory. 1980. № 12. P. 128–138.
3. Ankeny N.C. The least quadratic non-residue // Ann. of Math. 1952. P. 65–72.
4. Dandan Huang, Yingpu Deng Algorithm for computing the factor ring of an ideal in Dedekind domain with finite rank. Science China Mathematics. 2017. № 61. P. 783-796.
5. Vaskouski M., Kondratyonok N., Prochorov N. Primes in quadratic unique factorization domains // Journal of Number Theory. 2016. № 168. P. 101–116.
6. Прохоров Н.П. Вероятностный и детерминированный аналоги алгоритма Миллера-Рабина для идеалов колец целых алгебраических элементов конечных расширений поля Q // Известия Национальной академии наук Беларуси. Серия физико-математических наук. 2020. № 56. С. 144–156.
7. Petukhova K.A., Tronin S.N. RSA Cryptosystem for Dedekind Rings // Lobachevskii Journal of Mathematics. 2016. № 37. P. 284–287.
8. Bach E. Explicit bounds for primality testing and related problems // Mathematics of Computation. 1990. P. 355–380.