ISSN 1561-8323 (print)
УДК 511.622

Поступило в редакцию 18.09.2017
Received 18.09.2017

М. М. Васьковский, Н. В. Кондратёнок, Н. П. Прохоров

Белорусский государственный университет, Минск, Республика Беларусь

АНАЛОГ ТЕСТА СОЛОВЕЯ–ШТРАССЕНА В КВАДРАТИЧНЫХ ЕВКЛИДОВЫХ КОЛЬЦАХ

(Представлено академиком Н. А. Изобовым)

Аннотация. В произвольных квадратичных евклидовых кольцах построен аналог теста Соловея–Штрассена. Доказано, что построенный аналог теста Соловея–Штрассена позволяет показать, что число N является составным с вероятностью не менее 0,5 за полиномиальное время относительно битовой длины числа N. В тесте Соловея–Штрассена ключевую роль играет вычисление символа Якоби. В работе построен эффективный алгоритм для его вычисления в квадратичных факториальных кольцах. Ключевой идеей доказательства является сведение символа Якоби в квадратичных факториальных кольцах к символу Якоби в целых числах.

Ключевые слова: евклидово кольцо, простые числа, символ Якоби, тест на простоту

Для цитирования: Васьковский, М. М. Аналог теста Соловея–Штрассена в квадратичных евклидовых кольцах / М. М. Васьковский, Н. В. Кондартёнок, Н. П. Прохоров // Докл. Нац. акад. наук Беларуси. – 2017. – Т. 61, № 5. – С. 28–32.

Maksim M. Vaskouski, Nikita V. Kondratyonok, Nikolai P. Prochorov

Belarusian State University, Minsk, Republic of Belarus

ANALOGUE OF THE SOLOVAY–STRASSEN PRIMALITY TEST IN QUADRATIC EUCLIDEAN DOMAINS

(Communicated by Academician Nikolai A. Izobov)

Abstract. An analogue of the Solovay–Strassen primality test in general quadratic Euclidean domains is obtained. We prove that the obtained primality test allows us to prove that N is composite and has a probability of no less than 0.5 in polynomial time with respect to a bit size of the number N. The main part of the Solovay-Strassen primality test analogue is the calculation of the Jacobi symbol. The efficient algorithm for its computing in quadratic unique factorization domains is constructed. The main idea of the proof is to reduce the Jacobi symbol to that in integers.

Keywords: Euclidean domain, primes, Jacobi symbol, primality test

For citation: Vaskouski M. M., Kondratyonok N. V., Prochorov N. P. Analogue of the Solovay–Strassen primality test in quadratic Euclidean domains. *Doklady Natsional'noi akademii nauk Belarusi = Doklady of the National Academy of Sciences of Belarus*, 2017, vol. 61, no. 5, pp. 28–32 (in Russian).

Многие криптосистемы с открытым ключом (RSA, Рабина, Блюма–Гольдвассер и др.) используют в качестве ключей большие простые числа [1, гл. 14, 15]. В связи с этим возникает необходимость строить эффективные алгоритмы тестирования чисел на простоту. В основе любого алгоритма тестирования на простоту лежит некоторый критерий простоты числа. Проверка всех условий критерия простоты гарантирует достоверное знание, является ли число простым, но без предположения о справедливости расширенной гипотезы Римана требует, как правило, экспоненциального числа операций относительно длины числа (в том числе тесты Соловея–Штрассена и Миллера–Рабина [2, гл. 5; 3, гл. 2]). На практике проверяют лишь часть условий критерия, что даёт возможность с некоторой положительной вероятностью доказать, что число является составным. Тест Соловея–Штрассена основан на следующем критерии Эйлера простоты: «натуральное число $n > 1$ является простым тогда и только тогда, когда для любого целого a, взаимно простого с n, выполняется сравнение $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n)$» и позволяет с вероятностью не менее 0,5 доказать, что число является составным, за полиномиальное относительно длины

числа n время. Отметим, что в [4–6] построен и исследован аналог RSA-криптосистемы в квадратичных факториальных кольцах, доказана возможность эффективной реализации в квадратичных евклидовых кольцах, а в [5] доказаны аналоги критериев Эйлера и Миллера в квадратичных факториальных кольцах, предложена эффективная реализация аналога теста Миллера–Рабина в мнимых квадратичных евклидовых кольцах.

Цель работы – построение аналога теста Соловея–Штрассена в произвольных квадратичных евклидовых кольцах. В первом параграфе мы построим эффективный алгоритм вычисления символа Якоби в квадратичных евклидовых кольцах. Во втором параграфе, опираясь на аналог критерия Эйлера [5] и эффективный алгоритм вычисления символа Якоби, мы получаем аналог теста Соловея–Штрассена тестирования простоты в квадратичных евклидовых кольцах, позволяющий доказать, что число N является составным с вероятностью не менее 0,5 за полиномиальное число двоичных операций относительно битовой длины N.

Пусть $m \neq 1$ – целое число, свободное от квадратов. Обозначим через O_K кольцо целых алгебраических элементов квадратичного поля $K=\mathbb{Q}(\sqrt{m})$. Пусть $\omega=\sqrt{m}$, если $m \equiv 2,3 (\mathrm{mod}\ 4)$, и $\omega=\frac{1+\sqrt{m}}{2}$, если $m \equiv 1 (\mathrm{mod}\ 4)$, а $\mathrm{disk}(K)=(\omega-\overline{\omega})^2$ – дискриминант поля K, где $\overline{\omega}$ – сопряженное к ω. Будем предполагать, что O_K – факториальное кольцо. Известно, что $O_K=\mathbb{Z}\oplus\mathbb{Z}[\omega]$ [7, с. 44]. Обозначим через $O_K^{\times}$ множество всех обратимых элементов O_K с нулем. Пусть $a+b\sqrt{m}\in O_K$, через $Nm(a+b\sqrt{m})=a^2-mb^2$ обозначим норму в O_K, обозначим $\left|a+b\sqrt{m}\right|_m=a^2+/m/b^2$. Элемент $a \in O_K$ называется простым, если для любого представления $a = pq$, $p, q \in O_K$, хотя бы одно из чисел p, q обратимо в мультипликативной группе кольца O_K. Пусть $\mathcal{P}_K$ множество всех простых элементов O_K. Обозначим $\mathcal{P}_{1,K}=\{p\in\mathcal{P}_K \mid Nm(p)=\pm 2 \text{ или } p=2\varepsilon, \varepsilon\in O_K^{\times}\}$. Для каждого $N\in O_K\setminus O_K^{\times}$ обозначим через $O_{K,N}$ и $O_{K,N}^{\times}$ аддитивную группу вычетов по модулю N и мультипликативную группу вычетов по модулю N соответственно.

Для простого числа $p \in O_K$ с нечетной нормой и $a \in O_K$, взаимно простого с p, определяем символ Лежандра $\left[\frac{a}{p}\right]$ равным 1, если в кольце O_K разрешимо сравнение $x^2 \equiv a (\mathrm{mod}\ p)$, и равным –1 в противном случае. Для любого $N \in O_K$ с нечетной нормой и $a \in O_K$, взаимно простого с N, определяем символ Якоби $\left[\frac{a}{N}\right]$ как произведение символов Лежандра $\prod_{k=1}^{n}\left[\frac{a}{p_k}\right]$, где $N=\prod_{k=1}^{n}p_k$, p_k – простые числа кольца O_K (полагаем $\left[\frac{a}{N}\right]=1$, если N – обратимый элемент кольца O_K). Для взаимно простых нечетного $b \in \mathbb{Z}$ и целого $a \in \mathbb{Z}$ через $\left(\frac{a}{b}\right)$ будем обозначать символ Якоби в кольце $\mathbb{Z}$.

Эффективный алгоритм вычисления символа Якоби.

П р е д л о ж е н и е 1. *Пусть* $a \in O_K$, $\beta \in \mathbb{Z}$ *взаимно простые. Если* β *нечетное, то* $\left[\frac{\alpha}{\beta}\right]=\left(\frac{Nm(\alpha)}{\beta}\right)$; *если* $Nm(\alpha)$ *нечетное, то* $\left[\frac{\beta}{\alpha}\right]=\left(\frac{\beta}{Nm(\alpha)}\right)$.

Д о к а з а т е л ь с т в о. Пусть $\alpha=\prod_{k=1}^{n}p_k$, $\beta=\prod_{j=1}^{m}q_j$, p_k – простые числа кольца O_K либо элементы $O_K^{\times}$, q_j – простые числа кольца $\mathbb{Z}$ либо ± 1, тогда $\left[\frac{\alpha}{\beta}\right]=\prod_{j=1}^{m}\prod_{k=1}^{n}\left[\frac{p_k}{q_j}\right]$, $\left[\frac{\beta}{\alpha}\right]=\prod_{j=1}^{m}\prod_{k=1}^{n}\left[\frac{q_j}{p_k}\right]$. В силу мультипликативности нормы в кольце O_K достаточно доказать, что для любых k, j выполняются равенства $\left[\frac{p_k}{q_j}\right]=\left(\frac{Nm(p_k)}{q_j}\right)$, $\left[\frac{q_j}{p_k}\right]=\left(\frac{q_j}{Nm(p_k)}\right)$. Не нарушая общности, можно считать, что q_j из первого равенства и p_k из второго равенства не являются обратимыми соответственно в $\mathbb{Z}$ и O_K.

Докажем второе равенство. Согласно критерию Эйлера [5], имеем $\left[\frac{q_j}{p_k}\right]=q_j^{\frac{Nm(p_k)-1}{2}} (\mathrm{mod}\ p_k)$. Если $p_k \in \mathbb{Z}$, то $Nm(p_k)=p_k\overline{p}_k$ является простым числом в $\mathbb{Z}$ [5] и тогда по критерию Эйлера

$\left(\frac{q_j}{Nm(p_k)}\right) \equiv q_j^{\frac{Nm(p_k)-1}{2}} (\mathrm{mod}\, p_k\overline{p}_k)$. Если $\left(\frac{q_j}{Nm(p_k)}\right)=1$, то $q_j^{\frac{Nm(p_k)-1}{2}} \equiv 1(\mathrm{mod}\, p_k)$, т. е. $\left[\frac{q_j}{p_k}\right]=1$. Если $\left(\frac{q_j}{Nm(p_k)}\right)=-1$, то $q_j^{\frac{Nm(p_k)-1}{2}} \equiv -1(\mathrm{mod}\, p_k)$ и тогда $\left[\frac{q_j}{p_k}\right]=-1$. Предположим, что $p_k \in \mathbb{Z}$, тогда $\left(\frac{q_j}{Nm(p_k)}\right)=\left(\frac{q_j}{p_k^2}\right)=1$ и $\left[\frac{q_j}{p_k}\right] \equiv q_j^{\frac{p_k^2-1}{2}} = \left(q_j^{\frac{p_k+1}{2}}\right)^{p_k-1} \equiv 1(\mathrm{mod}\, p_k)$ в силу малой теоремы Ферма.

Докажем первое равенство. Предположим, что q_j является простым в O_K, тогда из [7, предложения 2.1 и 2.21] вытекает справедливость равенства $p_k^{q_j} \equiv \overline{p}_k (\mathrm{mod}\, q_j)$. Согласно критерию Эйлера, имеем $\left[\frac{p_k}{q_j}\right] \equiv p_k^{\frac{q_j^2-1}{2}} (\mathrm{mod}\, q_j)$, $\left(\frac{Nm(p_k)}{q_j}\right) \equiv (p_k\overline{p}_k)^{\frac{q_j-1}{2}} (\mathrm{mod}\, q_j)$. Таким образом, $\left[\frac{p_k}{q_j}\right] \equiv \left(\frac{Nm(p_k)}{q_j}\right)(\mathrm{mod}\, q_j)$, и как следствие $\left[\frac{p_k}{q_j}\right]=\left(\frac{Nm(p_k)}{q_j}\right)$. Предположим, что q_j не является простым в O_K. Если $q_j = q^2$, где q – некоторое простое в O_K, то согласно [7, предложение 2.1] выполняется $q_j|\mathrm{disk}(K)$, и как следствие $q_j|m$. Пусть $p_k = a + b\sqrt{m}$, тогда $4Nm(p_k) \equiv (2a)^2 (\mathrm{mod}\ q_j)$. Поэтому $\left(\frac{Nm(p_k)}{q_j}\right)=1=\left[\frac{p_k}{q}\right]\left[\frac{p_k}{q}\right]=\left[\frac{p_k}{q_j}\right]$. Остаётся рассмотреть случай $q_j = q\overline{q}$ для некоторого простого $q \in O_K$. Используя уже доказанное второе равенство настоящего предложения, имеем

$$\left[\frac{p_k}{q_j}\right]=\left[\frac{p_k}{q}\right]\left[\frac{p_k}{\overline{q}}\right]=\left[\frac{p_k}{q}\right]\left[\frac{\overline{p}_k}{q}\right]=\left[\frac{Nm(p_k)}{q}\right]=\left(\frac{Nm(p_k)}{Nm(q)}\right)=\left(\frac{Nm(p_k)}{q_j}\right).$$

Предложение доказано.

Т е о р е м а 1. *Для любых взаимно простых* $\alpha = a + b\omega$, $\beta = c + d\omega \in O_K$, *таких, что* $|Nm(\beta)|$ *нечетно и больше 1, выполняется равенство* $\left[\frac{\alpha}{\beta}\right]=\left(\frac{Nm(\alpha)}{g}\right)\left(\frac{d_1^2 a - bc_1d_1}{Nm(\beta_1)}\right)$, *где* $\beta_1 = \beta / g$, $c_1 = c / g$, $d_1 = d / g$, $g = (c, d) \in \mathbb{N}$.

Д о к а з а т е л ь с т в о. Докажем, что $(d_1, \beta_1) = 1$. Предположим противное, т. е. существует простое $p \in O_K$ такое, что $p|d_1$, $p|\beta_1 = c_1 + d_1\omega$. Если $p \in \mathbb{Z}$, то $p|c_1$, что противоречит условию $(c_1, d_1) = 1$. Следовательно, $p \in O_K \setminus \mathbb{Z}$. Отсюда вытекает, что $p_1 = Nm(p)$ делит d_1 и делит $Nm(\beta_1) = c_1^2 + c_1d_1(\omega + \overline{\omega}) + d_1^2\omega\overline{\omega}$. Так как p_1 простое в $\mathbb{Z}$, то p_1 делит c_1, что противоречит условию $(c_1, d_1) = 1$.

Используя предложение 1, получаем

$$\left[\frac{\alpha}{\beta}\right]=\left[\frac{\alpha}{g}\right]\left[\frac{\alpha}{\beta_1}\right]=\left(\frac{Nm(\alpha)}{g}\right)\left[\frac{a+b\omega}{c_1+d_1\omega}\right]=\left(\frac{Nm(\alpha)}{g}\right)\left[\frac{d_1}{\beta_1}\right]\left[\frac{d_1a+d_1b\omega}{c_1+d_1\omega}\right]=$$
$$\left(\frac{Nm(\alpha)}{g}\right)\left[\frac{d_1}{\beta_1}\right]\left[\frac{d_1a-c_1b}{\beta_1}\right]=\left(\frac{Nm(\alpha)}{g}\right)\left[\frac{d_1^2a-d_1c_1b}{\beta_1}\right]=\left(\frac{Nm(\alpha)}{g}\right)\left(\frac{d_1^2a-bc_1d_1}{Nm(\beta_1)}\right),$$

что и требовалось доказать.

Теперь сформулируем алгоритм вычисления символа Якоби $\left[\frac{\alpha}{\beta}\right]$ для взаимно простых $\alpha = a + b\omega$, $\beta = c + d\omega \in O_K$, таких, что $|Nm(\beta)|$ нечетное и больше 1.

А л г о р и т м 1. Входные данные: $\alpha = a + b\omega$, $\beta = c + d\omega \in O_K$ такие, что $|Nm(\beta)|$ нечетное и больше 1. Выходные данные: значение символа Якоби $\left[\frac{\alpha}{\beta}\right]$.

Ш а г 1. Вычислить $g = (c, d)$, $A = Nm(\alpha)$, $B = Nm(\beta_1)$, $C = d_1^2a - bc_1d_1$, где $\beta_1 = \frac{\beta}{g} = c_1 + d_1\omega$.

Ш а г 2. Вычислить значение символа Якоби $\left[\frac{\alpha}{\beta}\right]$ по формуле $\left[\frac{\alpha}{\beta}\right]=\left(\frac{A}{g}\right)\left(\frac{C}{B}\right)$, используя алгоритм вычисления символа Якоби в кольце целых чисел.

З а м е ч а н и е 1. Корректность работы алгоритма вытекает из теоремы 1, при этом временная сложность алгоритма 1 определяется сложностью алгоритма Евклида и алгоритма вычисления символа Якоби в кольце целых чисел, т. е. составляет $O(\log^2 N)$ двоичных операций, где $|\alpha|_m \le N$, $|\beta|_m \le N$.

Аналог теста Соловея–Штрассена в кольце O_K. В дальнейшем будем предполагать, что кольцо O_K является евклидовым относительно нормы $Nm(a)=a\overline{a}$.

П р е д л о ж е н и е 2 [6]. *Если кольцо O_K является евклидовым, то операции сложения, умножения, деления с остатком в кольце O_K имеют такую же сложность, как и в кольце целых чисел, т. е. для любого натурального N и любых $a, b \in O_K$, $|a|_m \le N$, $|b|_m \le N$, любая из указанных операций над числами a, b может быть выполнена за $O(f(N))$ битовых операций, где $f(n)$ – оценка числа битовых операций, необходимых для выполнения аналогичной операции в кольце целых чисел над любыми числами $c, d \in \mathbb{Z}$, $|c| \le \sqrt{N}$, $|d| \le \sqrt{N}$.*

П р е д л о ж е н и е 3 [5]. *Пусть $N \in O_K \setminus O_K^\times$ не делится ни на какое простое $p \in \mathcal{P}_{1,K}$. Число N является простым в O_K тогда и только тогда, когда для любого $a \in O_{K,N}^\times$ выполняется сравнение* $a^{\frac{|Nm(N)|-1}{2}} \equiv \left[\frac{a}{N}\right] (\mathrm{mod}\, N)$.

З а м е ч а н и е 2. Число $N \in O_K \setminus O_K^\times$ будем называть псевдопростым по основанию $a \in O_{K,N}^\times$, если выполняется сравнение из предложения 3. Легко видеть, что множество $H_{K,N}$ всех $a \in O_{K,N}^\times$, для которых N является псевдопростым по основанию a, образует подгруппу группы $O_{K,N}^\times$. Если $N \in O_K \setminus O_K^\times$ не является простым, то из предложения 3 вытекает, что $H_{K,N}$ – собственная подгруппа группы $O_{K,N}^\times$ и согласно теореме Лагранжа выполняется неравенство $|H_{K,N}| \le |O_{K,N}^\times| / 2$.

Следующий алгоритм является аналогом теста Соловея–Штрассена в кольце O_K.

А л г о р и т м 2 (проверка простоты в кольце O_K). Входные данные: число $N \in O_K \setminus O_K^\times$.

Ш а г 1. Проверить наличие делителей из $\mathcal{P}_{1,K}$ числа N.

Если $Nm(N)$ нечетно, то делителей из $\mathcal{P}_{1,K}$ нет, в этом случае перейти к шагу 2.

Если $Nm(N)$ четно и $|Nm(N)| > 4$, то ответ: «N – составное».

Если $|Nm(N)| = 4$ и $\mathrm{disk}(K) \equiv 5 (\mathrm{mod}\ 8)$, то ответ: «$N$ – простое».

Если $|Nm(N)| = 4$ и $\mathrm{disk}(K) \not\equiv 5 (\mathrm{mod}\ 8)$, то ответ: «$N$ – составное».

Если $|Nm(N)| = 2$, то ответ: «N – простое».

Ш а г 2. Выбрать случайное $a \in O_{K,N}^\times$ и вычислить $(a, N) = d$.

Если $|Nm(d)| > 1$, то ответ: «N – составное».

Если $|Nm(d)| = 1$, то проверить справедливость сравнения $a^{\frac{|Nm(N)|-1}{2}} \equiv \left[\frac{a}{N}\right] (\mathrm{mod}\, N)$.

Если данное сравнение не выполняется, то ответ: «N – составное». В противном случае ответ: «неизвестно» и необходимо повторить шаг 2 алгоритма с другим значением a.

Корректность работы алгоритма вытекает из [7, предложение 2.1] и предложения 3, а из замечания 2 вытекает справедливость следующей теоремы.

Т е о р е м а 2. *Пусть $N \in O_K$ – составное число, тогда разовое применение алгоритма 2 дает ответ «N – составное» с вероятностью не менее 0,5.*

Т е о р е м а 3. *Временная сложность алгоритма 2 составляет $O(\log^3 |N|_m)$ двоичных операций.*

Д о к а з а т е л ь с т в о. Из предложения 2 вытекает, что $a^{\frac{|Nm(N)|-1}{2}} (\mathrm{mod}\, N)$ можно найти с помощью бинарного алгоритма возведения в степень за $O(\log^3 |N|_m)$ двоичных операций.

Так как кольцо O_K является евклидовым, то существует постоянная $\alpha_K < 1$ такая, что для любых $a, b \in O_K$ найдутся $q, r \in O_K$, удовлетворяющие условиям $a = bq + r$ и $|Nm(r)| \le \alpha_K |Nm(b)|$ [6; 8]. Отсюда и из предложения 2 вытекает, что наибольший общий делитель (a, N) можно найти

с помощью алгоритма Евклида за $O(\log^3|N|_m)$ двоичных операций. Согласно замечанию 1 символ Якоби $\left[\frac{a}{N}\right]$ можно вычислить за $O(\log^2|N|_m)$ двоичных операций. Таким образом, сложность алгоритма 2 составляет $O(\log^3|N|_m)$ двоичных операций, что и требовалось доказать.

Список использованных источников

1. Криптология / Ю. С. Харин [и др.]. – Минск: БГУ, 2013. – 511 с.

2. Введение в теоретико-числовые методы криптографии / М. М. Глухов [и др.]. – СПб.: Лань, 2011. – 401 с.

3. Kranakis, E. Primality and cryptography / E. Kranakis. – New Haven: Yale University, 1986. – 235 p.

4. Vaskouski, M. Analogue of the RSA-cryptosystem in quadratic unique factorization domains / M. Vaskouski, N. Kondratyonok // Доклады Национальной академии наук Беларуси. – 2015. – Vol. 59, N 5. – P. 18–23.

5. Vaskouski, M. Primes in quadratic unique factorization domains / M. Vaskouski, N. Kondratyonok, N. Prochorov // J. Number Theory. – 2016. – Vol. 168. – P. 101–116. doi.org/10.1016/j.jnt.2016.04.022

6. Васьковский, М. М. Полиномиальная эквивалентность вычисления функции Эйлера RSA-модуля и поиска секретного ключа в квадратичных евклидовых кольцах / М. М. Васьковский // CSIST'16. Международный конгресс по информатике: Информационные системы и технологии: материалы международного конгресса. – Минск: БГУ, 2016. – С. 427–430.

7. Lemmermeyer, F. Reciprocity laws: from Euler to Eisenstein / F. Lemmermeyer. – Springer, 2000. – 514 p.

8. Vaskouski, M. Shortest division chains in unique factorization domains / M. Vaskouski, N. Kondratyonok // J. Symbolic Computation. – 2016. – Vol. 77. – P. 175–188. doi.org/10.1016/j.jsc.2016.02.003

References

1. Kharin Yu. S., Agievich S. V., Vasil'ev D. V., Matveev G. V. *Cryptology.* Minsk, Belarusian State University, 2013. 511 p. (in Russian).

2. Glukhov M. M., Kruglov I. A., Pichkur A. B., Cheremushkin A. V. *Introduction to number theoretical methods in cryptography*. Saint-Petersburg, Lan' Publ., 2011. 401 p. (in Russian).

3. Kranakis E. *Primality and cryptography*. New Haven, Yale University, 1986. 235 p.

4. Vaskouski M., Kondratyonok N. Analogue of the RSA-cryptosystem in quadratic unique factorization domains. *Doklady Natsional'noi akademii nauk Belarusi = Doklady of the National Academy of Sciences of Belarus*, 2015, vol. 59, no. 5, pp. 18–23. (in Russian).

5. Vaskouski M., Kondratyonok N., Prochorov N. Primes in quadratic unique factorization domains. *Journal of Number Theory*, 2016, vol. 168, pp. 101–116. doi.org/10.1016/j.jnt.2016.04.022

6. Vaskouski M. M. Polynomial equivalence of computing Euler's function from RSA modulus and searching for private key in Euclidean quadriatic domains. *CSIST'16. Mezhdunarodnyi kongress po informatike: Informatsionnye sistemy i tekhnologii: materialy mezhdunarodnogo kongressa* [CSIST'16. International congress on computer science: information systems and technologies: Proceedings of the International Scientific Congress]. Minsk, Belarusian State University, 2016, pp. 427–430 (in Russian).

7. Lemmermeyer F. *Reciprocity laws: from Euler to Eisenstein*. Springer, 2000. 514 p.

8. Vaskouski M., Kondratyonok N. Shortest division chains in unique factorization domains. *Journal of Symbolic Computation*, 2016, vol. 77, pp. 175–188. doi.org/10.1016/j.jsc.2016.02.003

Информация об авторах

Васьковский Максим Михайлович – доцент. Белорусский государственный университет (пр. Независимости, 4, 220030, Минск, Республика Беларусь). E-mail: vaskovskii@bsu.by.

Кондратёнок Никита Васильевич – студент. Белорусский государственный университет (пр. Независимости, 4, 220030, Минск, Республика Беларусь). E-mail: nkondr2006@rambler.ru.

Прохоров Николай Петрович – студент. Белорусский государственный университет (пр. Независимости, 4, 220030, Минск, Республика Беларусь). E-mail: nprohorovminsk@mail.ru.

Information about the authors

Vaskouski Maksim Mihailovich – Assistant Professor. Belarusian State University (4, Nezavisimosti Ave., 220030, Minsk, Republic of Belarus). E-mail: vaskovskii@bsu.by.

Kondratyonok Nikita Vasilyevich – Student. Belarusian State University (4, Nezavisimosti Ave., 220030, Minsk, Republic of Belarus). E-mail: nkondr2006@rambler.ru.

Prochorov Nikolai Petrovich – Student. Belarusian State University (4, Nezavisimosti Ave., 220030, Minsk, Republic of Belarus). E-mail: nprohorovminsk@mail.ru.