Науковий часопис НПУ імені М.П.Драгоманова. Серія 1. Фізико-математичні науки
Київ: НПУ імені М.П. Драгоманова. — 2015, № 17.— С. 60–69.

УДК 519.41/47

Функція Ойлера на множині $\mathbb{Z}\left[\sqrt{d}\,\right]$ та її застосування

О. О. Требенко, Н.М. Цибульська
(Національний педагогічний університет імені М. П. Драгоманова, Київ, Україна)

Анотація. В роботі розглядається функція Ойлера $\varphi(n)$ на множині $\mathbb{Z}\left[\sqrt{d}\,\right]$, де $d \neq 1$ – вільне від квадратів ціле число. Отримані теоретичні результати доповнено програмною реалізацією алгоритму знаходження значення функції Ойлера для елемента n в кільці $\mathbb{Z}\left[\sqrt{d}\,\right]$. Запропоновано ввести в розгляд розширений алгоритм RSA для елементів кільця $\mathbb{Z}\left[\sqrt{d}\,\right]$.

Ключові слова: кільця цілих алгебраїчних чисел, кільця $\mathbb{Z}\left[\sqrt{d}\,\right]$, функція Ойлера $\varphi(n)$ на множині $\mathbb{Z}\left[\sqrt{d}\,\right]$, розширений алгоритм RSA для елементів кілець $\mathbb{Z}\left[\sqrt{d}\,\right]$.

Abstract. Described in the work of H. Elkamchouchi, K. Elshenawy i H. Shaban and also in the Koval's PhD "Security systems based on Gaussian integers: analysis of basic operations and time complexity of secret transformations" is an RSA-algorithm over the field of Gaussian Integers which uses Euler function for elements of the ring of Gaussian Integers $\mathbb{Z}[i]$. An Euler function for Gaussian Integers is explored in the Cross'es work.

This paper generalises the mentioned results for the case of the principal ideal ring $\mathbb{Z}\left[\sqrt{d}\,\right]$ where $d \neq 1$ is an arbitrary squarefree integer. Remark that by $\mathbb{Z}[\sqrt{d}]$ we mean a minimal ring, containing the ring $\mathbb{Z}$ and the element $\sqrt{d}$, i.e. the ring

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}.$$

A notion of Euler function $\varphi(n)$ for the element $n \in \mathbb{Z}\left[\sqrt{d}\,\right]$ is introduced and a formula to calculate its values is found.

Obtained theoretical results are complemented by a software implementation of the algorithm for finding values of the Euler function for the given element n of the ring $\mathbb{Z}\left[\sqrt{d}\,\right]$.

Introduced also is an extended RSA algorithm for elements of the ring $\mathbb{Z}\left[\sqrt{d}\,\right]$.

The results can be used in further studies on algebraic number theory and theory of rings. Developed software will be used for specialists in the field of abstract algebra and applications.

Keywords: rings of integers of algebraic number fields, rings $\mathbb{Z}\left[\sqrt{d}\,\right]$, the Euler function on the set $\mathbb{Z}\left[\sqrt{d}\,\right]$, extended RSA algorithm for elements of rings $\mathbb{Z}\left[\sqrt{d}\,\right]$.

Mathematics Subject Classification (2010): 11R04, 11R11, 11Y40, 11Y70

Вступ

Останніми десятиліттями дослідження алгоритмічних питань теорії чисел переживають період бурхливого розвитку, в першу чергу, завдяки запитам криптографії та широкому розповсюдженню ЕОМ. Стрімкий розвиток сучасних технологій та розширення меж використання комп'ютерних мереж зумовили появу якісно нових хакерських атак, які становлять загрозу безпеці інформації. У зв'язку із цим перед сучасною наукою надзвичайно актуальним постає питання про необхідність пошуку нових альтернативних методів шифрування, які б не вимагали великих затрат часу і були більш криптостійкими і безпечними.

Одним із таких альтернативних алгоритмів шифрування міг би бути алгоритм RSA для елементів кілець $\mathbb{Z}[\sqrt{d}\,]$.

Слід зауважити, що суттєвим недоліком відомих сьогодні методів криптоаналізу системи RSA є необхідність працювати з матрицями великого розміру. Іншим можливим підходом до шифрування інформації в RSA є використання функції Ойлера. За такого підходу немає потреби використовувати суперкомп'ютер.

В роботі H. Elkamchouchi, K. Elshenawy і H. Shaban [1], а також у докторській дисертації A. Koval на тему "Security systems based on Gaussian integers: analysis of basic operations and time complexity of secret transformations" [2] розглядається алгоритм RSA для цілих гаусових чисел, який використовує функцію Ойлера для елементів кільця $\mathbb{Z}[i]$. Сама ж функція Ойлера для цілих гаусових чисел досліджується в роботі Cross (1983) [3].

В даній роботі функція Ойлера $\varphi(n)$ розглядається на множині

$$\mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} | \, a, b \in \mathbb{Z}\},$$

де $d \neq 1$ – вільне від квадратів ціле число і $\mathbb{Z}[\sqrt{d}\,]$ – кільце головних ідеалів.

Робота складається з трьох частин. У першій її частині введено поняття функції Ойлера $\varphi(n)$ для елемента $n \in \mathbb{Z}[\sqrt{d}\,]$ та знайдено формулу для обчислення її значення. В другій частині запропоновано програмну реалізацію алгоритму знаходження значення функції Ойлера для елемента $n \in \mathbb{Z}[\sqrt{d}\,]$. У третій частині введено в розгляд розширений алгоритм RSA для елементів кілець $\mathbb{Z}[\sqrt{d}\,]$.

В роботі використовуються наступні позначення: K^* – мультиплікативна група кільця K; $|G|$ – порядок групи G; $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ – кільце класів лишків за модулем n. Інші позначення стандартні.

1. Функція Ойлера $\varphi(n)$ на множині $\mathbb{Z}[\sqrt{d}\,]$

На множині $\mathbb{Z}[\sqrt{d}\,]\backslash\{0\}$ введемо в розгляд функцію $\varphi(n)$, значення якої для елемента $n \in \mathbb{Z}[\sqrt{d}\,]$ дорівнює кількості елементів кільця, попарно не конгруентних між собою за модулем n і взаємно простих із n, і назвемо її *функцією Ойлера*.

Лема 1. *Нехай* $\mathbb{Z}[\sqrt{d}\,]$ *– кільце головних ідеалів,* $n \in \mathbb{Z}[\sqrt{d}\,]\backslash\{0\}$, $G_n = \left\{\overline{g} = g + \langle n\rangle |\ g \in \mathbb{Z}[\sqrt{d}\,], (g,n) \sim 1\right\}$. *Тоді* $G_n = \left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*$, *де* $\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*$ *– мультиплікативна група кільця* $\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle$.

Доведення. Розглянемо фактор-кільце кільця $\mathbb{Z}[\sqrt{d}\,]$ за ідеалом $I = \langle n\rangle$:

$$\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle = \left\{\overline{g} |\ g \in \mathbb{Z}[\sqrt{d}\,]\right\}.$$

Виділимо в множині $\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle$ підмножину G_n таких елементів $\overline{g}$, що $(g,n) \sim 1$.

Оскільки $\mathbb{Z}[\sqrt{d}\,]$ є кільцем головних ідеалів, то для довільного елемента $\overline{g} \in G_n$ існують елементи $u, v \in \mathbb{Z}[\sqrt{d}\,]$ такі, що $gu + nv = 1$, а значить, $\overline{gu + nv} = \overline{1}$, звідси $\overline{g} \cdot \overline{u} = \overline{1}$, тобто $\overline{g} \,|\, \overline{1}$ в $\mathbb{Z}[\sqrt{d}\,]$. Отже, множина G_n складається з дільників одиниці кільця $\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle$, тому $G_n \subseteq \left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*$. Якщо ж $\overline{g} \in \left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*$, то існує елемент $\overline{u} \in \left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*$, для якого $\overline{g} \cdot \overline{u} = \overline{1}$. Тоді $gu \equiv 1 (\mathrm{mod}\langle n\rangle)$, а значить $qu - 1 \in \langle n\rangle$, тобто існує $v \in \mathbb{Z}[\sqrt{d}\,]$, для якого $gu + nv = 1$, звідки $(g,n) \sim 1$. Таким чином, $\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^* \subseteq G_n$ і $G_n = \left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*$. □

Наслідок 1. *Нехай кільце* $\mathbb{Z}[\sqrt{d}\,]$, *де* $d \neq 1$ *– вільне від квадратів ціле число, є кільцем головних ідеалів і нехай* $n \in \mathbb{Z}[\sqrt{d}\,]\backslash\{0\}$. *Тоді* $\varphi(n) = |G_n| = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*\right|$.

Доведення. Зрозуміло, що $\varphi(n) = |G_n|$, де $G_n = \left\{\overline{g} = g + \langle n\rangle |\ g \in \mathbb{Z}[\sqrt{d}\,], (g,n) \sim 1\right\}$, але тоді із твердження 1 $\varphi(n) = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*\right|$. □

Твердження 1. *Нехай кільце* $\mathbb{Z}[\sqrt{d}\,]$, *де* $d \neq 1$ *– вільне від квадратів ціле число, є кільцем головних ідеалів. Тоді функція Ойлера на множині* $\mathbb{Z}[\sqrt{d}\,]\backslash\{0\}$ *– мультиплікативна.*

Доведення. Для функції Ойлера на $\mathbb{Z}[\sqrt{d}\,]$ маємо:

1. Нехай $n = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$. За наслідком 1 із леми 1 $\varphi(n) = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*\right|$, тому $\varphi(n) > 0$.

2. Нехай $n_1, n_2 \in \mathbb{Z}[\sqrt{d}\,]\backslash\{0\}$, $(n_1, n_2) \sim 1$ і $n = n_1 \cdot n_2$. За наслідком 1 із леми 1, $\varphi(n_1) = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n_1\rangle\right)^*\right|$, $\varphi(n_2) = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n_2\rangle\right)^*\right|$, $\varphi(n) = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*\right|$. Оскільки $(n_1, n_2) \sim 1$, то, за твердженням 2 [5, С.352] і лемою 1 [6, С.460], $\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^* = \left(\mathbb{Z}[\sqrt{d}\,]/\langle n_1\rangle\right)^* \times \left(\mathbb{Z}[\sqrt{d}\,]/\langle n_2\rangle\right)^*$,
тому $\left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*\right| = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n_1\rangle\right)^*\right| \cdot \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n_2\rangle\right)^*\right|$, звідки $\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2)$.

Отже, $\varphi(n)$ – мультиплікативна функція за означенням [4, С.59]. □

Задамо відображення $f\colon \mathbb{Z}[\sqrt{d}\,]\backslash\{0\} \to \mathbb{N}$ наступним чином: $f(a+b\sqrt{d}) = |a^2 - b^2 d|$.

Теорема 1. *Нехай кільце $\mathbb{Z}[\sqrt{d}\,]$, де $d \neq 1$ – вільне від квадратів ціле число, є кільцем головних ідеалів і нехай $n = \varepsilon \cdot q_1^{k_1} \cdot q_2^{k_2} \cdot \ldots \cdot q_r^{k_r} \in \mathbb{Z}[\sqrt{d}\,] \setminus \{0\}$, де $\varepsilon | 1$, елементи q_i – прості в $\mathbb{Z}[\sqrt{d}\,]$ для всіх $i \in \overline{1,r}$, причому $q_i \nsim q_j$ при $i \neq j$. Тоді*

$$\varphi(n) = f(n) \cdot \left(1 - \frac{1}{f(q_1)}\right) \cdot \left(1 - \frac{1}{f(q_2)}\right) \cdot \ldots \cdot \left(1 - \frac{1}{f(q_r)}\right).$$

Доведення. Якщо $n = \varepsilon$ – дільник одиниці в $\mathbb{Z}[\sqrt{d}\,]$, то

$$\varphi(n) = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle n\rangle\right)^*\right| = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle \varepsilon\rangle\right)^*\right| = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\mathbb{Z}[\sqrt{d}\,]\right)^*\right| = 1.$$

Водночас $f(\varepsilon) = 1$, оскільки для елемента $\varepsilon = a + b\sqrt{d}$ оберненим буде або елемент $a - b\sqrt{d}$, або елемент $-a + b\sqrt{d}$, значить, добуток елемента $a + b\sqrt{d}$ і оберненого до нього елемента ($a - b\sqrt{d}$ або $-a + b\sqrt{d}$) дорівнює 1, але цей добуток – рівний $|a^2 - b^2 d|$, тому $|a^2 - b^2 d| = 1$. Отже, $\varphi(\varepsilon) = f(\varepsilon)$ і для $n = \varepsilon$ теорема є справедливою.

Нехай n не є дільником одиниці в $\mathbb{Z}[\sqrt{d}\,]$ і $n = \varepsilon \cdot q_1^{k_1} \cdot q_2^{k_2} \cdot \ldots \cdot q_r^{k_r}$ – канонічний розклад елемента n в $\mathbb{Z}[\sqrt{d}\,]$, $k_i \geq 1$ для всіх $i \in \overline{1,r}$. В силу мультиплікативності функції Ойлера на $\mathbb{Z}[\sqrt{d}\,]$ (твердження 1):

$$\varphi(n) = \varphi(\varepsilon) \cdot \varphi\left(q_1^{k_1}\right) \cdot \ldots \cdot \varphi\left(q_r^{k_r}\right).$$

Тоді, враховуючи наслідок 1 із леми 1, матимемо:

$$\varphi(n) = \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle q_1^{k_1}\rangle\right)^*\right| \cdot \ldots \cdot \left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle q_r^{k_r}\rangle\right)^*\right|. \tag{1}$$

Нехай q^k – довільний елемент із елементів $q_i^{k_i}$ ($i \in \overline{1,r}$). За теоремою 3 [7, С. 225], елемент q задовольняє одну з умов:

1) $q = \varepsilon \cdot 2$, якщо $d \equiv 1 (\mathrm{mod} 4)$;

2) $q = \varepsilon \cdot a$, де a – просте непарне число, $a \nmid d$ і $\left(\frac{d}{a}\right) = -1$;

3) $q = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$, якщо $(a, b) = 1$ і $|a^2 - b^2 d|$ – просте число.

Знайдемо порядки груп $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q_r^{k_r}\rangle\right)^*$ для кожного із випадків 1)-3). Оскільки $\langle \varepsilon \cdot q^k\rangle = \langle q^k\rangle$ для довільного $\varepsilon | 1$, то достатньо розглянути наступні випадки:

1. $q = 2$ при $d \equiv 1 (\mathrm{mod} 4)$ або q – просте непарне число, $q \nmid d$ і $\left(\frac{d}{q}\right) = -1$.

2. $q = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$, де $(a, b) = 1$ і $f(q) = |a^2 - b^2 d|$ – просте число.

Покажемо, що в кожному із даних випадків

$$\left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^k\rangle\right)^*\right| = (f(q))^k \cdot \left(1 - \frac{1}{f(q)}\right).$$

1. Нехай $q = 2$ при $d \equiv 1 (\mathrm{mod}\, 4)$ або q – просте непарне число, $q \nmid d$ і $\left(\frac{d}{q}\right) = -1$. За твердженням 1, елемент $\overline{x}$ кільця $\mathbb{Z}[\sqrt{d}\,]/\langle q^k\rangle$ є дільником одиниці тоді і лише тоді, коли $(x, q^k) \sim 1$ (тобто $\overline{x} \in G_{q^k}$, де $G_{q^k} = \left\{\overline{g} = q + \langle q^k\rangle |\ g \in \mathbb{Z}[\sqrt{d}\,], (g, q^k) \sim 1\right\}$).

Нехай $M = \left\{\overline{y_1 + y_2\sqrt{d}} = y_1 + y_2\sqrt{d} + \langle q^k\rangle |\ y_1 + y_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,], 0 \leq y_1 \leq q^k - 1 \wedge 0 \leq y_2 \leq q^k - 1 \wedge \left((y_1, q^k) = 1 \vee (y_2, q^k) = 1\right)\right\}$. Доведемо, що $G_{q^k} = M$.

Нехай $\overline{x} \in G_{q^k}$ і $\overline{x} = \overline{x_1 + x_2\sqrt{d}}$ – такий запис $\overline{x}$, що x_1, x_2 – найменші можливі цілі невід'ємні числа. За твердженням 1, $G_{q^k} = \left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^k\rangle\right)^*$, тому, очевидно, $0 \le x_1 \le q^k - 1$, $0 \le x_2 \le q^k - 1$. Оскільки елемент $\overline{x}$ належить до G_{q^k}, то $(x_1 + x_2\sqrt{d}, q^k) \sim 1$. Якщо $x_1 \vdots q$ і $x_2 \vdots q$, то $(x_1 + x_2\sqrt{d}, q^k) \nsim 1$, але це не так. Тому або $x_1 \not\vdots q$, або $x_2 \not\vdots q$. Отже, $(x_1, q^k) = 1$ або $(x_2, q^k) = 1$. Таким чином, $\overline{x} \in M$. В силу довільності вибору елемента $\overline{x}$ з G_{q^k}, маємо $G_{q^k} \subseteq M$. Навпаки, нехай $\overline{x} = \overline{x_1 + x_2\sqrt{d}} \in M$, тоді $0 \le x_1, x_2 \le q^k - 1$ і $(x_1, q^k) = 1$ або $(x_2, q^k) = 1$. Припустимо, що $(x_1 + x_2\sqrt{d}, q^k) \nsim 1$. Оскільки q – простий в $\mathbb{Z}\left[\sqrt{d}\,\right]$ елемент, то звідси випливає, що $x_1 + x_2\sqrt{d} \vdots q$, тобто $x_1 + x_2\sqrt{d} = q(u + v\sqrt{d})$ для деякого $u + v\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\,\right]$. Тоді $x_1 = qu$, $x_2 = qv$. Тобто $x_1 \vdots q$ і $x_2 \vdots q$, що суперечить вибору $\overline{x}$ в M. Отже, $(x_1 + x_2\sqrt{d}, q^k) \sim 1$, а значить, $\overline{x} \in G_{q^k}$ і $M \subseteq G_{q^k}$. Таким чином, $G_{q^k} = M$.

Для спрощення підрахунку кількості елементів в множині M, кожен її елемент $\overline{a + b\sqrt{d}}$ зображатимемо у вигляді пари (a, b). Розмістимо пари (a, b) у формі таблиці:

$(0,0)$	$(q,0)$	...	...	$(0,1)$	$(q,1)$	...	...	...	$(0, q^k-1)$	(q, q^k-1)	...	...
$(1,0)$	$(q+1,0)$	...	...	$(1,1)$	$(q+1,1)$	...	...	...	$(1, q^k-1)$	$(q+1, q^k-1)$	...	...
$(2,0)$	$(q+2,0)$	...	...	$(2,1)$	$(q+2,1)$	...	...	...	$(2, q^k-1)$	$(q+2, q^k-1)$	...	...
...	...	...	...	...	...	...	...	...	...	...	...	...
$(q-1,0)$	$(2q-1,0)$	...	$(q^k-1,0)$	$(q-1,1)$	$(2q-1,1)$	...	$(q^k-1,1)$	...	$(q-1, q^k-1)$	$(2q-1, q^k-1)$	...	(q^k-1, q^k-1)

В даній таблиці всі пари (a, b), для яких $(a, q^k) \ne 1$ і $(b, q^k) \ne 1$ знаходяться в першому рядку. Далі, якщо b – фіксоване, то пар (a, b), в яких $(a, q^k) \ne 1$, є рівно q^{k-1}, а саме: (q, b), (q^2, b), ..., (q^{k-1}, b). Кількість елементів $b \in \overline{0, q-1}$ таких, що $(b, q^k) \ne 1$, також дорівнює q^{k-1}, а саме: q, q^2, ..., q^{k-1}. Тоді кількість пар (a, b) даної таблиці таких, що $(a, q^k) \ne 1$ і $(b, q^k) \ne 1$, дорівнює $q^{k-1} \cdot q^{k-1} = q^{2(k-1)}$. Всього в таблиці є q^{2k} пар, тому пар (a, b) в розглядуваній таблиці таких, що $(a, q^k) = 1$ або $(b, q^k) = 1$, є рівно $q^{2k} - q^{2(k-1)}$.

Оскільки $G_{q^k} = M$, то із твердження 1

$$\left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^k\rangle\right)^*\right| = \left|G_{q^k}\right| = q^{2k} - q^{2(k-1)} = (q^2)^k \cdot \left(1 - \frac{1}{q^2}\right) = (f(q))^k \cdot \left(1 - \frac{1}{f(q)}\right).$$

2. Нехай $q = a + b\sqrt{d}$, де $(a, b) = 1$ і $f(q) = |a^2 - b^2 d|$ – просте число. Для доведення рівності $\left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^k\rangle\right)^*\right| = (f(q))^k \cdot \left(1 - \frac{1}{f(q)}\right)$ в цьому випадку використаємо метод математичної індукції.

Перевіримо справедливість твердження при $k = 1$. Оскільки $(a, b) = 1$, то за теоремою 1 [7] $\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q\rangle \cong \mathbb{Z}_p$, де $p = f(q)$, тобто $\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q\rangle$ – поле з p елементів, його мультиплікативна група $\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^k\rangle\right)^*$ має порядок $p - 1$. Отже, $\left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q\rangle\right)^*\right| = p - 1 = p \cdot \left(1 - \frac{1}{p}\right) = f(q) \cdot \left(1 - \frac{1}{f(q)}\right)$. Таким чином, при $k = 1$ твердження справедливе.

Припустимо справедливість твердження при $k = n$:

$$\left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^n\rangle\right)^*\right| = (f(q))^n \cdot \left(1 - \frac{1}{f(q)}\right),$$

і доведемо при $k = n+1$: $\left|\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^*\right| = (f(q))^{n+1} \cdot \left(1 - \frac{1}{f(q)}\right)$. Розглянемо відображення ψ: $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^* \to \left(\mathbb{Z}[\sqrt{d}\,]/\langle q^n\rangle\right)^*$ за правилом: $\psi(x+y\sqrt{d}+\langle q^{n+1}\rangle) = x + y\sqrt{d} + \langle q^n\rangle$. Покажемо, що ψ – гомоморфізм групи $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^*$ на групу $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^n\rangle\right)^*$.

Нехай $x + y\sqrt{d} + \langle q^{n+1}\rangle \in \left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^*$. Знайдемо образ елемента $x + y\sqrt{d} + \langle q^{n+1}\rangle$: $\psi(x+y\sqrt{d}+\langle q^{n+1}\rangle) = x+y\sqrt{d}+\langle q^n\rangle$. Зрозуміло, що образ $\psi(x+y\sqrt{d}+\langle q^{n+1}\rangle)$ існує і єдиний. Залишається показати, що $x + y\sqrt{d} + \langle q^n\rangle = \psi(x + y\sqrt{d} + \langle q^{n+1}\rangle)$ належить до $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^n\rangle\right)^*$. Але це випливає з того, що якщо $x + y\sqrt{d} + \langle q^{n+1}\rangle$ є дільником одиниці в $\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle$, то за твердженням 1 $(x + y\sqrt{d}, q^{n+1}) \sim 1$, а значить, зрозуміло, і $(x + y\sqrt{d}, q^n) \sim 1$, тому $x + y\sqrt{d} + \langle q^n\rangle$ є дільником одиниці в $\mathbb{Z}[\sqrt{d}\,]/\langle q^n\rangle$. Навпаки, для довільного елемента $x + y\sqrt{d} + \langle q^n\rangle$ із $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^n\rangle\right)^*$, прообраз $x + y\sqrt{d} + \langle q^{n+1}\rangle$ в $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^*$ існує завжди.

Доведемо, що операція множення зберігається. Нехай $x_1+y_1\sqrt{d}+\langle q^{n+1}\rangle$, $x_2+y_2\sqrt{d}+$ $+\langle q^{n+1}\rangle$ – довільні два елементи групи $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^*$. Тоді

$$\psi\left((x_1 + y_1\sqrt{d} + \langle q^{n+1}\rangle)(x_2 + y_2\sqrt{d} + \langle q^{n+1}\rangle)\right) =$$

$$= \psi\left(x_1x_2 + y_1y_2d + (x_1y_2 + y_1x_2)\sqrt{d} + (x_1 + y_1\sqrt{d} + x_2 + y_2\sqrt{d})\langle q^{n+1}\rangle + (\langle q^{n+1}\rangle)^2\right) =$$

$$= \psi\left(x_1x_2 + y_1y_2d + (x_1y_2 + y_1x_2)\sqrt{d} + \langle q^{n+1}\rangle\right) = x_1x_2+y_1y_2d+(x_1y_2+y_1x_2)\sqrt{d}+\langle q^n\rangle =$$

$$= (x_1 + y_1\sqrt{d} + \langle q^n\rangle)(x_2 + y_2\sqrt{d} + \langle q^n\rangle) = \psi(x_1 + y_1\sqrt{d} + \langle q^{n+1}\rangle)\psi(x_2 + y_2\sqrt{d} + \langle q^{n+1}\rangle).$$

Таким чином, відображення ψ: $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^* \to \left(\mathbb{Z}[\sqrt{d}\,]/\langle q^n\rangle\right)^*$ є гомоморфізмом.

Знайдемо ядро гомоморфізму ψ. Ядро $\mathrm{Ker}\psi$ складається із всіх елементів $x+y\sqrt{d}+$ $\langle q^{n+1}\rangle$ групи $\left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^*$, для яких $\psi(x+y\sqrt{d}+\langle q^{n+1}\rangle) = 1+0\sqrt{d}+\langle q^n\rangle$, тобто $x + y\sqrt{d} + \langle q^n\rangle = 1 + 0\sqrt{d} + \langle q^n\rangle$. Зрозуміло, що остання рівність можлива лише у випадку, коли $x + y\sqrt{d} \equiv 1(\mathrm{mod}\ \langle q^n\rangle)$. Отже,

$$\mathrm{Ker}\psi = \left\{x + y\sqrt{d} + \langle q^{n+1}\rangle \in \left(\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle\right)^* | x + y\sqrt{d} \equiv 1(\mathrm{mod}\ \langle q^n\rangle)\right\}.$$

Знайдемо порядок ядра $\mathrm{Ker}\psi$.

Нехай $x + y\sqrt{d} + \langle q^{n+1}\rangle \in \mathrm{Ker}\psi$, тоді $\psi(x + y\sqrt{d} + \langle q^{n+1}\rangle) = 1 + \langle q^n\rangle$, тобто $x + y\sqrt{d} + \langle q^n\rangle = 1 + \langle q^n\rangle$. Звідси, $x + y\sqrt{d} \equiv 1(\mathrm{mod}\ \langle q^n\rangle)$, а значить, $x + y\sqrt{d} = 1 + t \cdot q^n$ для деякого $t \in \mathbb{Z}[\sqrt{d}\,]$. Отже, порядок ядра $\mathrm{Ker}\psi$ дорівнює кількості різних класів лишків фактор-кільця $\mathbb{Z}[\sqrt{d}\,]/\langle q^{n+1}\rangle$ виду $1+t\cdot q^n+\langle q^{n+1}\rangle$, де $t \in \mathbb{Z}[\sqrt{d}\,]$. Покажемо,

що їх є стільки, скільки існує попарно не конгруентних за ідеалом $\langle q\rangle$ елементів $t \in \mathbb{Z}\left[\sqrt{d}\,\right]$. Дійсно, нехай $1 + t \cdot q^n + \langle q^{n+1}\rangle = 1 + s \cdot q^n + \langle q^{n+1}\rangle$, тоді $1 + t \cdot q^n \equiv 1 + s \cdot q^n (\mathrm{mod}\,\langle q^{n+1}\rangle)$, тобто $t \cdot q^n \equiv s \cdot q^n (\mathrm{mod}\,\langle q^{n+1}\rangle)$, звідки $t \equiv s (\mathrm{mod}\,\langle q\rangle)$. Навпаки, якщо $t \equiv s (\mathrm{mod}\,\langle q\rangle)$, то $t - s \in \langle q\rangle$, тобто $t - s \vdots q$, а значить, $(1 + t \cdot q^n) - (1 + s \cdot q^n) = (t-s)q^n \vdots q^{n+1}$, звідки $1+t\cdot q^n \equiv 1+s\cdot q^n (\mathrm{\ mod}\,\langle q^{n+1}\rangle)$ і $1+t\cdot q^n+\langle q^{n+1}\rangle = 1+s\cdot q^n+\langle q^{n+1}\rangle$.

Кількість таких попарно не конгруентних за ідеалом $\langle q\rangle$ елементів $t \in \mathbb{Z}\left[\sqrt{d}\,\right]$ дорівнює числу класів лишків фактор-кільця $\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q\rangle$. В силу теореми 1 [7, С. 220] $\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q\rangle \cong \mathbb{Z}_p$, де $p = f(q)$, тому $|\mathrm{Ker}\psi| = f(q)$.

Далі, за основною теоремою гомоморфізму груп,

$$\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^{n+1}\rangle\right)^* / \mathrm{Ker}\psi \cong \left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^n\rangle\right)^*,$$

а значить,

$$\left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^{n+1}\rangle\right)^*\right| = \left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^{n}\rangle\right)^*\right| \cdot |\mathrm{Ker}\psi| = \left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^{n}\rangle\right)^*\right| \cdot f(q).$$

Але за індуктивним припущенням $\left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^{n}\rangle\right)^*\right| = (f(q))^n \cdot \left(1 - \dfrac{1}{f(q)}\right)$, отже,

$$\left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^{n+1}\rangle\right)^*\right| = (f(q))^n \cdot \left(1 - \frac{1}{f(q)}\right) \cdot f(q) = (f(q))^{n+1} \cdot \left(1 - \frac{1}{f(q)}\right).$$

В силу принципу математичної індукції, для довільного $q = a + b\sqrt{d}$, де $(a, b) = 1$ і $f(q) = |a^2 - b^2 d|$ – просте число, справедливо $\left|\left(\mathbb{Z}\left[\sqrt{d}\,\right]/\langle q^{k}\rangle\right)^*\right| = (f(q))^k \cdot \left(1 - \dfrac{1}{f(q)}\right)$ для будь-якого $k \in \mathbb{N}$.

Таким чином, для довільного простого в $\mathbb{Z}\left[\sqrt{d}\,\right]$ елемента q,

$$\varphi(q^k) = (f(q))^k \cdot \left(1 - \frac{1}{f(q)}\right).$$

Тоді з рівності (1) отримаємо:

$$\varphi(n) = f(n) \cdot \left(1 - \frac{1}{f(q_1)}\right) \cdot \left(1 - \frac{1}{f(q_2)}\right) \cdot \ldots \cdot \left(1 - \frac{1}{f(q_r)}\right).$$

□

2. Програмна реалізація алгоритмів

На основі отриманих авторами теоретичних результатів та процедур *SGInorm*, *SGIiselementof*, *SGIrem*, *SGIquo*, *SGIareassociated*, *SGImod*, *SGIgcd*, *SGIfactors*, *SGIfactor*, *SGIisprime* [8] в СКМ Maple розроблено процедуру *SGIphi* для знаходження значення функції Ойлера для елемента $u \in \mathbb{Z}\left[\sqrt{d}\,\right]$:

```
SGIphi :=proc(u, d)
local f;
 if nargs ≠ 2 then
  error "wrong number of arguments"
```

```
  elif SGIiselementof(u, d) = false then
    error "wrong type of arguments"
  end if;
  if SGInorm(u, d) = 1 then
    1
  elif SGIisprime(u, d) = true then
    SGInorm(u, d) − 1;
    if evalb(hastype(u, ‘ + ‘) = false) then
      u^2 − 1
    else
      abs(radnormal(op(1, u)^2 − op(2, u)^2)) − 1
    end if;
  else
    f := op(2, SGIfactors(u, d));
    SGInorm(u, d) ∗ convert(map(proc(x)1 − 1/SGInorm(op(1, x), d)end proc, f), ‘ ∗ ‘)
  end if;
end proc:
```

3. Алгоритм RSA для елементів кільця $\mathbb{Z}[\sqrt{d}\,]$

Отримані теоретичні результати дають можливість ввести в розгляд алгоритм RSA для елементів кілець головних ідеалів $\mathbb{Z}[\sqrt{d}\,]$.

Опис алгоритму

Нагадаємо, що RSA є широко використовуваним алгоритмом, який побудований на складності факторизації цілих чисел.

Традиційний RSA алгоритм для цілих чисел має наступний вигляд:

Алгоритм 1

Ключ генерації: Згенерувати два великих простих числа p і q. Обчислити $n = p \cdot q$ та $\varphi(n) = (p-1)(q-1)$. Вибрати випадкове ціле число e так, що $1 < e < \varphi(n)$ і $(e, \varphi(n)) = 1$. Обчислити $h = e^{-1} (\mathrm{mod}\ \varphi(n))$. Пара n і e є відкритим ключем, а h – закритий ключ.

Шифрування: Маючи повідомлення m (представлене у вигляді цілого числа), обчислити зашифрований текст $c = m^e (\mathrm{mod}\ n)$.

Розшифровування: Обчислити оригінальне повідомлення $m = c^h (\mathrm{mod}\ n)$.

Аналогічний алгоритм RSA для елементів кілець головних ідеалів $\mathbb{Z}[\sqrt{d}\,]$ матиме наступний вигляд:

Нехай кільце $\mathbb{Z}[\sqrt{d}\,]$, де $d \neq 1$ – вільне від квадратів ціле число, є кільцем головних ідеалів.

Алгоритм 2

Ключ генерації: Згенерувати два великих простих елементи P і Q кільця $\mathbb{Z}\left[\sqrt{d}\,\right]$. Обчислити $N = P \cdot Q$ та $\varphi(N) = \varphi(P) \cdot \varphi(Q)$. Вибрати випадкове ціле число e так, що $1 < e < \varphi(N)$ і $(e, \varphi(N)) = 1$. Обчислити $h = e^{-1}(\mathrm{mod}\ \varphi(N))$. Трійка N, e і d є відкритим ключем, а h – закритий ключ.

Шифрування: Маючи повідомлення M (представлене як елемент кільця $\mathbb{Z}\left[\sqrt{d}\,\right]$), обчислити зашифрований текст $C = M^e(\mathrm{mod}\ N)$.

Розшифровування: Обчислити оригінальне повідомлення $M = C^h(\mathrm{mod}\ N)$.

Розглянемо приклад застосування наведеного алгоритму.

Приклад застосування алгоритму

Ключ генерації: Розглянемо два прості елементи $P = 581 + 209\sqrt{2}$, $Q = 53$ кільця $\mathbb{Z}\left[\sqrt{2}\,\right]$. Знайдемо $N = P \cdot Q$,

$$\varphi(N) = (f(P) - 1)(f(Q) - 1) = (581^2 - 209^2 \cdot 2 - 1)(53^2 - 1) = 702555984.$$

Виберемо $e = 818741$, $h = e^{-1}(\mathrm{mod}\ \varphi(N)) = 818741^{-1}(\mathrm{mod}\ 702555984 = 121296605)$. Відкритим ключем є $N = 30793 + 11077\sqrt{2}$; $e = 818741$.

Шифрування: Припустимо, що відкритий текст $M = 7 + \sqrt{2}$.
$C = M^e \bmod N = (7 + \sqrt{2})^{818741}(\mathrm{mod}\ 30793 + 11077\sqrt{2}) = 16513 + 26215\sqrt{2}$.
Розшифровування:
$M = C^h \bmod N = (16513 + 26215\sqrt{2})^{121296605}(\mathrm{mod}\ 30793 + 11077\sqrt{2}) = 7 + \sqrt{2}$.

Аналіз алгоритму

У [2] показано, що такий алгоритм RSA, розширений на кільце $\mathbb{Z}[i]$ цілих гаусових чисел, може бути більш стійким, ніж традиційний RSA алгоритм лише якщо p – просте число, $p \equiv 3(\mathrm{mod}4)$. Водночас, для цього необхідно, щоб злам RSA був не настільки складним, як розкладання на множники. Хоча і в цьому випадку, невідомо, чи буде насправді розширений алгоритм більш захищеним.

Виникає питання: чи буде більш стійким алгоритм RSA для деяких кілець головних ідеалів $\mathbb{Z}\left[\sqrt{d}\,\right]$ і, якщо так, то які прості елементи слід брати. Дане питання вимагає подальших досліджень фахівців з інформаційної безпеки.

4. Висновки і перспективи подальших досліджень

В роботі розглянуто функцію Ойлера $\varphi(n)$ на множині $\mathbb{Z}\left[\sqrt{d}\,\right]\backslash\{0\}$, де $d \neq 1$ – вільне від квадратів ціле число. Отримані теоретичні результати доповнено програмною реалізацією алгоритму знаходження значення функції Ойлера для елемента n в кільці $\mathbb{Z}\left[\sqrt{d}\,\right]$. Запропоновано ввести в розгляд розширений алгоритм RSA для елементів кільця $\mathbb{Z}\left[\sqrt{d}\,\right]$. Водночас, залишається відкритим питання, чи буде запропонований алгоритм RSA більш стійким, ніж традиційний, і якщо так, то в яких випадках.

Література

[1] *H. Elkamchouchi, K. Elshenawy, and H. Shaban.* Extended Psa Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers // Proceedings of the 8th International Conference on Communication Systems. — 2002. — P. 91-95.

[2] *Koval A.* Security systems based on Gaussian integers: analysis of basic operations and time complexity of secret transformations: a Dissertation Doctor of Philosophy in Computer Science: August 2011 / Koval Aleksey; Faculty of New Jersey Institute of Technology. — New Jersey, 2011. — 153 p.

[3] *Cross J.* The Euler φ-function in the Gaussian integers // Am. Math. Mon. 90. — 1983. — P. 518-528.

[4] *Требенко Д.Я., Требенко О.О.* Алгебра і теорія чисел Ч.1. — К.: НПУ імені М.П. Драгоманова, 2009. — 420 с.

[5] *Винберг Э.Б.* Курс алгебры. Электронное издание. — М: МЦНМО, 2014. — 590 с.

[6] *Завало С.Т.* Курс алгебри. — К.: Вища школа, 1985. — 503 с.

[7] *Trebenko O.O., Tsybulska N.M.* Prime elements of rings $\mathbb{Z}[\sqrt{d}\,]$ // Науковий часопис НПУ імені М.П.Драгоманова. Серія 1. Фізико-математичні науки: Зб. наукових праць. — Київ: НПУ імені М.П.Драгоманова, 2014. — №16 (1). — С. 219-227.

[8] *Trebenko O.O., Tsybulska N.M.* QuadraticInt — a Maple package for working with elements of $\mathbb{Z}[\sqrt{d}\,]$ [Electronic resourse] / Oxana O. Trebenko, Natalia M. Tsybulska // Maplesoft, a division of Waterloo Maple Inc.. — Electronic data. — [Waterloo, ON Canada: Maplesoft application center, 2017]. — 53 p. — Access mode: World Wide Web: maplesoft.com/applications/view.aspx?SID=154235 (viewed on May 2, 2017). — Title from the screen.