УДК 519.6

Рябухо О.М., Пащенко З.Д., Стьопкін А.В., Дегтярьов Я.А.

[1] *кандидат фізико-математичних наук, доцент, «КДМТУ»*

[2] *кандидат фізико-математичних наук, доцент кафедри методики навчання математики та методики навчання інформатики, ДВНЗ «ДДПУ»*

[3] *кандидат фізико-математичних наук, доцент кафедри методики навчання математики та методики навчання інформатики, ДВНЗ «ДДПУ»*

[4] *студент фізико-математичного факультету, ДВНЗ «ДДПУ»*

e-mail: rom.olena@gmail.com, pashchenko_zd@i.ua, stepkin.andrey@ukr.net

ГАУСОВІ ЧИСЛА КАРМАЙКЛА

Узагальнене поняття псевдопростого числа на кільце цілих гаусових чисел. Сформульовані вимоги до алгоритму знаходження гаусових чисел Кармайкла.

Ключові слова: *прості числа, псевдопрості числа, гаусові числа, числа Кармайкла.*

Вступ

В середині 70-х років минулого століття відбувся прорив в сучасній криптографії. В 1976 р. в роботі Вайтфілда Діффі та Мартіна Геллмена «Нові напрямки в криптографії» вперше були сформульовані принципи обміну зашифрованою інформацією без обміну таємним ключем. Невдовзі Рон Рівест, Аді Шамір і Леонард Адлеман побудували систему RSA, першу криптосистему з відкритим ключем, стійкість якої базувалась на проблемі факторизації великих простих чисел.

Для перевірки простоти найбільш широко використовуються так звані «ймовірнісні» алгоритми, які майже точно розпізнають прості числа, але мають певний недолік. Після позитивного проходження числом тесту, залишається імовірність того, що воно насправді складене. Такі складені натуральні числа, що мають деякі властивості простих чисел і успішно проходять тести на простоту називають псевдопростими числами. Існування псевдопростих чисел перешкоджає роботі алгоритмів, які використовують ті чи інші властивості простих чисел.

Майже всі відомі тести простоти базуються на наступній теоремі:

Теорема 1. (мала теорема Ферма) *Якщо* $n \in N$, *просте, то*

$$\forall x < n, \quad x^{n-1} \equiv 1 (mod\, n)$$

Якщо n не є простим, то умови теореми можуть виконуватись, хоча це малоймовірно.

Означення 1. *Якщо n — непарне число, і n не є простим, x ціле число, $НСД(n,x)=1$ і виконуються умови малої теореми Ферма, то n називається псевдопростим числом за основою b.*

Узагальнимо поняття псевдопростого числа на кільце цілих гаусових чисел. Для довільного $z \in Z[i]$ можна визначити множину остач r_i, яка будується таким чином: всі ці залишки знаходяться всередині квадрату, дві вершини якого — т. $(0,0)$ і т. (a,b). Якщо цілі точки попадають на сторони квадрата, то ми включаємо їх в множину, якщо вони попадають на «нижні» сторони квадрата. Кількість остач — a^2+b^2. За допомогою переносу квадрата (множення на гаусове число) можна отримати довільну точку площини, крім точок всередині квадрата.

Множина остач є областю цілості, порядок кожного елемента a^2+b^2. Тому малу теорему Ферма можна узагальнити:

Теорема 2. *Якщо $z \in Z[i]$ — просте в $Z[i]$, то $\forall r \in R(z)$ (множина остач)*

$$r^{a^2+b^2-1} \equiv 1 (mod\, a+bi)$$

Означення 2. *Якщо z — ціле гаусове число, яке не є простим, r — ціле гаусове число і виконуються умови теореми 5, то z називається гаусовим псевдопростим числом за основою r.*

Основна частина

Гаусовим числом Кармайкла називається таке не просте число $z = z_1 + z_2 i \neq 0$, $z_1, z_2 \in \mathbb{Z}$, що

$$(*) \qquad \forall a \in \mathbb{Z}[i] \quad a^{z_1^2+z_2^2-1} \equiv 1 (mod\, z).$$

Зрозуміло, що для перевірки виконання цієї умови достатньо розглянути всі числа a, що $|a| < |z|$, тобто ті, що на комплексній площині належать внутрішній частині кола з центром в початку координат з радіусом $t = |z| = \sqrt{z_1^2+z_2^2}$. Зауважимо, що найменші за модулем гаусові числа $2, 1+i, 1+2i, 2+i$ – прості. Тоді $z \neq 2, 1+i, 1+2i, 2+i \Rightarrow |z| > \sqrt{1^2+2^2} > 2$.

Задача полягає в побудові алгоритму знаходження гаусових чисел Кармайкла та його програмній реалізації, яка повинна містити процедури піднесення комплексного числа до натурального степеня та знаходження остачі від ділення на гаусові числа.

В результаті проведених досліджень були сформульовані вимоги до алгоритму знаходження гаусових чисел Кармайкла.

По-перше, достатньо перевіряти числа z, що знаходяться в першій чверті комплексної площини: $z_1 \geqslant 1, z_2 \geqslant 0$, оскільки всі інші числа мають вигляд – z, $\pm iz$ а остачі від ділення на них не змінюються:

$$\forall b = zq + r, |r| < |z| \quad \Rightarrow \quad b = (-z)(-q) + r, \quad b = (\pm zi)(\mp qi) + r.$$

Тобто, якщо $b \equiv 1(mod\, z)$, то $b \equiv 1(mod\, -z)$, $b \equiv 1(mod\, \pm iz)$. Маємо

Твердження 1. *Якщо $z \in \mathbb{Z}$ задовольняє умову (*), то $-z, \pm iz$ задовольняє умову (*).*

По-друге, достатньо розглянути всі гаусові числа a, що належать внутрішній частині вказаного кола і знаходяться в першій чверті комплексної площини: $a = a_1 + a_2 i, 0 < a_1 < t, 0 \leqslant a_2 < t$. Це пов'язано з тим, що решту чисел із інших чвертей ми можемо одержати множенням a на -1, $\pm i$. Тоді, якщо $a^{t^2-1} = a^{z_1^2+z_2^2-1} \equiv 1(mod\, z)$, то $(-a)^{t^2-1} \equiv (-1)^{t^2-1}(mod\, z)$, $(\pm ia)^{t^2-1} \equiv (\pm i)^{t^2-1}(mod\, z)$. Тому числа $-a, \pm ia$ задовольняють умову (*), якщо степінь $t^2 - 1 = z_1^2 + z_2^2 - 1$ ділиться на 4, а це можливо лише коли z_1 і z_2 мають різну парність:

$$t^2 - 1 = (2k_1)^2 + (2k_2 + 1)^2 - 1 = 4k_1^2 + 4k_2^2 + 4k_2 \equiv 0(mod\, 4).$$

Тоді $(-a)^{t^2-1} \equiv 1(mod\, z)$ і $(\pm ia)^{t^2-1} \equiv 1(mod\, z)$. В протилежному випадку числа $-a$, $\pm ia$ цю умову не задовольняють і число $z = z_1 + z_2 i$ не є числом Кармайкла, а, тим більше, не є простим числом. Отже, маємо також наступні твердження.

Твердження 2. *Число $z = z_1 + z_2 i$ може бути числом Кармайкла або простим, якщо z_1 і z_2 мають різну парність.*

Твердження 3. *Число $z = z_1 + z_2 i$ може бути простим або числом Кармайкла, якщо $z_1^2 + z_2^2 \equiv 1(mod\, 4)$.*

По-третє, неповна частка та остача в кільці цілих гаусових чисел визначається не однозначно. Тому умова $b \equiv 1(mod\, z)$ означає, що $b = zq + 1$ або $b = zq_1 + r$, $|r| < |z|$, де $q1 \neq q$, $r = 1 + pz \neq 1$. Проведемо дослідження, для яких p число r буде остачею, конгруентною 1. Зауважимо, що $|r| < |z| \Rightarrow |r|^2 < |z|^2$.

Модуль суми не перевищує різницю модулів: $|r| = |1 + pz| > |pz| - 1$. Так як $|p| \geqslant 1$, $|z| > 2$, то $|pz| > 2 \Rightarrow |pz| - 1 > 1 > 0 \Rightarrow |z| > |r| > |pz| - 1 \Rightarrow$ $\Rightarrow |p| \cdot |z| < |z| + 1 < 2 \cdot |z| \Rightarrow |p| < 2$. Цій умові можуть задовольняти $p = \pm 1, \pm i, \pm(1 + i), \pm(1 - i)$. Безпосередньою перевіркою перевіряємо можливі значення p в залежності від z.

Нехай $p = \pm 1$. Тоді

$$|1 \pm (z_1 + z_2 i)|^2 < |z|^2 \Rightarrow (1 \pm z_1)^2 + z_2^2 < z_1^2 + z_2^2 \Rightarrow 1 < \mp 2 z_1$$

Так як $z_1 \geqslant 1$, то остання нерівність виконується при $p = -1$.

Нехай $p = \pm i$. Тоді

$$|1 \pm i(z_1 + z_2 i)|^2 < |z|^2 \Rightarrow (1 \mp z_2)^2 + z_2^2 < z_1^2 + z_2^2 \Rightarrow 1 < \pm 2 z_2.$$

Так як $z_2 > 0$, то остання нерівність виконується при $p = i$.

Нехай $p = \pm(1 + i)$. Тоді

$|1 \pm (1 + i)(z_1 + z_2 i)|^2 < |z|^2 \Rightarrow (1 \pm (z_1 - z_2))^2 + (z_1 + z_2)^2 < z_1^2 + z_2^2 \Rightarrow$ $\Rightarrow (1 \pm (z_1 - z_2))^{2^2} < -2 z_1 \cdot z_2 \leqslant 0$ – суперечність для довільного z.

Нехай $p = \pm(1 - i)$. Тоді

$|1 \pm (1 - i)(z_1 + z_2 i)|^2 < |z|^2 \Rightarrow (1 \pm (z_1 + z_2))^2 \mp (z_1 - z_2)^2 < z_1^2 + z_2^2 \Rightarrow$ $\Rightarrow (1 \pm (z_1 + z_2))^2 < \pm 2 z_1 \cdot z_2$

З останньої нерівності $p \neq -(1 - i)$, бо ліворуч додатне, а праворуч від'ємно число: $z_1 \geqslant 1, z_2 \geqslant 0 \Rightarrow -2 z_1 z_2 < 0$. Отримаємо умови для z при $p = 1 - i$.

$$\Rightarrow (1 + (z_1 + z_2))^2 < 2 z_1 \cdot z_2 \Rightarrow (z_1 + z_2) < 1 + (z_1 + z_2) < \sqrt{2 z_1 \cdot z_2} \Rightarrow$$

$$\Rightarrow \frac{(z_1 + z_2)}{2} < \frac{1}{\sqrt{2}} \sqrt{z_1 \cdot z_2} \leqslant \frac{1}{\sqrt{2}} \frac{(z_1 + z_2)}{2}.$$

Остання нерівність враховує співвідношення середнього арифметичного та середнього геометричного, а з неї випливає $1 < \frac{1}{\sqrt{2}}$ – суперечність. Тому $p \neq 1 - i \ \ \forall z$.

Підсумовуючи викладене, маємо

Твердження 4. *Якщо число z задовольняє умову $z_1 \geqslant 1$ і $z_2 \geqslant 0$ і $b \equiv 1 (mod\ z)$, то остача від ділення b на z дорівнює $r = 1$, або $r = 1 - z = (1 - z_1) - i z_2$, або $r = 1 + iz = 1 - z_2 + i z_1$.*

Саме результат цього твердження необхідно врахувати при складанні алгоритму програми для знаходження чисел Кармайкла. Це викликано тим, що процедура знаходження частки від ділення використовує функцію «округлити», а тоді остача від ділення може знаходитись за межами першої чверті комплексної площини.

Висновки

Узагальнене поняття псевдопростого числа на кільце цілих гаусових чисел. Сформульовані вимоги до алгоритму знаходження гаусових чисел Кармайкла.

Література

1. *Alford W.R.* There are Infinitely Many Carmichael Numbers / W.R. Alford, A. Granville; C. Pomerance // Annals of Mathematics. — 1994. — №139. — P. 703–722.
2. *Agrawal M.* Primes is in P / M. Agrawal, N. Kayal, N. Saxena // Annals of Mathematics. — 2004. — №160. — P. 781–793.
3. *Василенко О.Н.* Современные способы проверки простоты чисел / О.Н. Василенко // Кибернетический сборник. — 1988. — №25. — С. 162–187.
4. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. — М.: МЦНМО, 2006. — 336 с.
5. *Дикарев С.С.* Исследование алгоритмов генерации простых чисел / С.С. Дикарев, Е.Н. Рябухо, Т.В. Турка // Молодой ученый, 2015. — №10. — С. 6–9.
6. *Ноден П.* Алгебраическая алгоритмика (с упражнениями и решениями): Пер. с франц. / П. Ноден, К. Китте. — М.: Мир, 1999. — 720 с.
7. *Рябухо О.М.* Дослідження імовірнісних алгоритмів тестування простоти чисел / О.М. Рябухо, Т.В. Турка // Збірник наукових праць фізико-математичного факультету ДДПУ. — 2013. — Випуск 3. — С. 60 – 67.

Ryabukho O.M., Pashchenko Z.D., Stopkin A.V., Dehtiarov Ya. A.
Donbas State Pedagogical University, Sloviansk, Ukraine.

GAUSSIAN CARMICHAEL NUMBER

A generalized notion of a pseudo-prime number on a ring of entire Gaussian numbers. The requirements for the algorithm for finding Carmichael Gaussian numbers are formulated.

Keywords: *prime numbers, pseudo-prime number, Gaussian numbers, Carmichael numbers.*