УДК 512.552.3, 511.14

Пащенко З.Д., Плахотя О.В.

[1] *канд. фіз.-мат. наук, доцент кафедри алгебри, СДПУ*

[2] *студентка 5 курсу фізико-математичного факультету, СДПУ*

e-mail: kafedra_algebry_sdpu@mail.ru

РЕШЕТО ЕРАТОСФЕНА ДЛЯ ГАУСОВИХ ЧИСЕЛ

Побудовано аналог відомого решета Ератосфена для гаусових чисел. Описано його алгоритм. В якості прикладу знайдено всі прості гаусові числа, модуль яких не перевищує 12. Наведено приклад побудови канонічного розкладу гаусового числа.

Ключові слова: *гаусові числа, решето Ератосфена, прості числа, асоційовані числа, канонічний розклад*

Вступ

В теорії факторіальних кілець основним є питання канонічного розкладу елементів. Для цього досліджуються оборотні та прості елементи.

Відомо, що всі евклідові кільця є факторіальними. Достатньо дослідженим є евклідове кільце Z цілих чисел. Його оборотними елементами є числа 1 і -1, всі прості додатні числа p знаходяться за допомогою відомого решета Ератосфена, а тому всі прості числа будуть $\pm p$.

Нагадаємо, що решето Ератосфена використовується для знаходження простих чисел, що не перевищують n. Викреслювання складених чисел закінчується, коли процес доходить до простого числа, що перевищує $\sqrt{n}$. Канонічний розклад натурального числа a знаходиться відбором простих дільників числа a.

Евклідове кільце многочленів над полем раціональних чисел не має такої процедури, яка б дозволяла перевіряти незвідність многочленів, якщо їх степені $n \geq 5$. Тому задача знаходження канонічного розкладу не завжди розв'язна.

Множина цілих гаусових чисел $Z[i] = \{a+bi | a, b \in Z\}$ утворює евклідове кільце, у якого $\delta(a+bi) = \sqrt{a^2+b^2}$, тобто $\delta(z) = |z|$. Нас цікавить питання про можливість знаходження канонічного розкладу довільного гаусового числа. Дослідження ведуться по аналогії з кільцем цілих чисел.

В кільці гаусових чисел оборотними є числа $1, i, -1, -i$. Якщо p – простий елемент кільця $Z[i]$, який знаходиться в першій чверті комплексної пло-

© Пащенко З.Д., Плахотя О.В., 2012

щини, то всі асоційовані з ним числа, $pi\,, -p\,, -pi$ – також прості, і будуть знаходитись у другій, третій, четвертій чверті відповідно, оскільки множенню на $i\,, -1\,, -i$ відповідає поворот на кути $\frac{\pi}{2}\,, \pi\,, \frac{3\pi}{2}$ відповідно.

Тому достатньо знайти всі прості числа, що знаходяться в першій чверті. Для цього побудовано аналог решета Ератосфена для гаусових чисел, суть якого викладена в цій статті.

Основна частина

Теоретичною основою для побудови аналогу решета Ератосфена для гаусових чисел є наступні теореми:

Теорема 1. *Модуль меншого за модулем дільника цілого гаусового числа z не перевищує $\sqrt{|z|}$.*

Доведення. Нехай $z_1 \in Z[i]$ – менший за модулем дільник z, тоді

$$\exists z_2 \in Z[i]: \quad |z_2| \geq |z_1| \ \text{ і } \ z = z_1 \cdot z_2.$$

А значить $|z| = |z_1| \cdot |z_2|$.

Якщо $|z_1| > \sqrt{|z|}$, то $|z_2| = \frac{|z|}{|z_1|} < \frac{|z|}{\sqrt{|z|}} = \sqrt{|z|} < |z_1|$. Тобто маємо, що $|z_2| < |z_1|$, що суперечить умові. □

Наслідком цієї теореми є наступна теорема:

Теорема 2. *Якщо гаусове число z не ділиться ні на яке просте число модуля меншого, ніж $\sqrt{|z|}$, то z – просте.*

Зауважимо, що всі числа першої четверті комплексної площини $Z[i]$, які діляться на $p = c + di$, мають вигляд:

$$(tc + t_1|p|^2) + (td + t_2|p|^2)i, \quad t \in N, \quad t_1, t_2 \in Z_0.$$

Крім того, якщо $p \in Z$, то $(a + bi) \vdots p$, якщо $a = p \cdot t_1$ і $b = p \cdot t_2$, $t_1, t_2 \in N$.

Зауваження 1. *Числа першої чверті, кратні $c + di\,, d \neq 0$, знаходяться зліва, справа, зверху та знизу з кроком $c^2 + d^2$ від чисел вигляду $ct + dti$, $t \in N$, тобто кроком кратності є квадрат модуля числа $c + di$.*

Зауваження 2. *Числа першої чверті, кратні $c\,, c \in N$, мають вигляд $ct_1 + dt_2 i\,, t_1, t_2 \in N_0$, тобто кроком кратності є модуль числа c.*

Знайдемо всі прості цілі гаусові числа, модуль яких не перевищує заданого числа n (аналог решета Ератосфена).

1. Розглянемо всі гаусові числа $a+bi$ першої чверті ($a>0$, $b\geq 0$) такі, що $\sqrt{a^2+b^2}\leq n$.

Будемо їх розташовувати у вигляді таблиці, яка відповідає зображенню комплексних чисел на комплексній площині. Якщо їх розташовувати в порядку зростання модуля, то їх можна записати так:

$1,\ 1+i,\ 2,\ 1+2i,\ 2+i,\ 2+2i,\ 3,\ 1+3i,\ 3+i,\ 2+3i,\ 3+2i,\ \ldots$.

Решето Ератосфена для гаусових чисел починається із найменших за модулем чисел $\neq 1$. Очевидно, що найменше за модулем гаусове число – $1+i$, тому за Теоремою 2 воно просте.

Таким чином, викреслюємо всі гаусові числа, що діляться на $1+i$: спочатку викреслюємо всі числа вигляду $(1+i)k$, $k\in Z$, далі вправо, вліво, вверх, вниз від вже викреслених чисел вигляду $(1+i)k$, $k\in Z$ викреслюємо кожне друге число, так як $|1+i|^2=2$. Викреслюються числа: $2,\ 2+2i,\ 1+3i,\ 3+i,\ \ldots$.

2. Всі числа $z\in Z_I[i]$, $z\neq 1+i$ з найменшим модулем, що залишились не викресленими, є простими. А саме: $1+2i$ і $2+i$.

Вибираємо число $1+2i$ і викреслюємо всі числа, що діляться на нього. Викреслюємо всі числа вигляду $(1+2i)m$, $m\in Z$. Знаходимо квадрат модуля числа $1+2i$: $|1+2i|^2=1+2^2=5$. Далі вправо, вліво, вверх, вниз викреслюємо кожне п'яте число (так як $|1+2i|^2=5$), починаючи від вже викреслених вигляду $(1+2i)m$, $m\in Z$. Викреслюються числа: $3+i,\ 2+4i,\ 5,\ 4+3i,\ 3+6i,\ 1+7i,\ \ldots$.

Вибираємо число $2+i$ і викреслюємо всі числа, що діляться на нього (аналогічно). Викреслюються числа: $1+3i,\ 4+2i,\ 5,\ 3+4i,\ 2+6i,\ 6+3i,\ 5+5i,\ \ldots$.

3. З чисел, що залишились не викресленими, вибираємо найменше за модулем, воно буде простим. Це число 3, $|3|=3$. Вибираємо число 3 і викреслюємо всі числа, що діляться на нього.

Спочатку викреслюємо всі числа вигляду $3\cdot c$, $c\in N$, далі по вертикалі, починаючи від вже викреслених чисел вигляду $3\cdot c$, $c\in N$, викреслюємо кожне третє число (так як $|3|=3$). Викреслюються числа: $3+3i,\ 6,\ 3+6i,\ 6+3i,\ 6+6i,\ 9,\ 3+9i,\ 9+3i,\ \ldots$.

4. Далі вибираємо найменші за модулем числа серед тих, що залишились не викресленими, і викреслюємо їм кратні і т.д.

Процес продовжуємо до тих пір, доки модуль не викреслених чисел, крім знайдених простих, не буде перевищувати число $\sqrt{n}$. Всі ці не викреслені

числа доповнюють множину простих чисел, модуль яких не перевищує n.

Наведемо приклад знаходження всіх простих гаусових чисел, модуль яких не перевищує 12.

Використовуємо аналог решета Ератосфена для гаусових чисел. Процес будемо продовжувати до тих пір, доки модуль не викреслених чисел не буде перевищувати $\sqrt{12}$.

1. Зобразимо у вигляді таблиці всі гаусові числа $a+bi$ першої чверті ($a>0$, $b\geq 0$) такі, що $\sqrt{a^2+b^2}\leq 12$.

~~$1+11i$~~	~~$2+11i$~~	~~$3+11i$~~	$4+11i$	$5+11i$						
$1+10i$	~~$2+10i$~~	$3+10i$	~~$4+10i$~~	~~$5+10i$~~	~~$6+10i$~~					
~~$1+9i$~~	~~$2+9i$~~	~~$3+9i$~~	$4+9i$	~~$5+9i$~~	~~$6+9i$~~	~~$7+9i$~~				
~~$1+8i$~~	~~$2+8i$~~	$3+8i$	~~$4+8i$~~	$5+8i$	~~$6+8i$~~	$7+8i$	~~$8+8i$~~			
~~$1+7i$~~	$2+7i$	~~$3+7i$~~	~~$4+7i$~~	~~$5+7i$~~	~~$6+7i$~~	~~$7+7i$~~	$8+7i$	~~$9+7i$~~		
$1+6i$	~~$2+6i$~~	~~$3+6i$~~	~~$4+6i$~~	$5+6i$	~~$6+6i$~~	~~$7+6i$~~	~~$8+6i$~~	~~$9+6i$~~	~~$10+6i$~~	
~~$1+5i$~~	$2+5i$	~~$3+5i$~~	$4+5i$	~~$5+5i$~~	$6+5i$	~~$7+5i$~~	$8+5i$	~~$9+5i$~~	~~$10+5i$~~	
$1+4i$	~~$2+4i$~~	~~$3+4i$~~	~~$4+4i$~~	$5+4i$	~~$6+4i$~~	~~$7+4i$~~	~~$8+4i$~~	$9+4i$	~~$10+4i$~~	$11+4i$
~~$1+3i$~~	$2+3i$	~~$3+3i$~~	~~$4+3i$~~	~~$5+3i$~~	~~$6+3i$~~	~~$7+3i$~~	$8+3i$	~~$9+3i$~~	$10+3i$	~~$11+3i$~~
$1+2i$	~~$2+2i$~~	$3+2i$	~~$4+2i$~~	$5+2i$	~~$6+2i$~~	$7+2i$	~~$8+2i$~~	~~$9+2i$~~	~~$10+2i$~~	~~$11+2i$~~
$1+i$	$2+i$	~~$3+i$~~	$4+i$	~~$5+i$~~	$6+i$	~~$7+i$~~	~~$8+i$~~	~~$9+i$~~	$10+i$	~~$11+i$~~
1	~~2~~	3	4	~~5~~	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~

2. Викреслюємо всі числа, що діляться на перше просте число $1+i$, кроком кратності є число 2.

3. З тих, що залишились не викресленими, вибираємо найменші за модулем: $1+2i$ і $2+i$. Викреслюємо всі числа, що діляться на прості числа $1+2i$ і $2+i$. Кроком кратності є число 5.

4. З чисел, що залишились не викресленими, вибираємо найменше за модулем. Це число 3. Виділяємо число 3 і викреслюємо всі числа, що діляться на нього.

5. З чисел, що залишились не викресленими, вибираємо найменші за модулем. Це числа: $2+3i$, $3+2i$. Але $|2+3i|=|3+2i|=\sqrt{13}$, а $\sqrt{13}>\sqrt{12}$, тобто процес викреслювання закінчено і всі числа, що залишились не викресленими у визначеному діапазоні, є простими.

Отже, простими числами, модуль яких не перевищує 12, є: $1+i$, $1+2i$, $2+i$, 3, $2+3i$, $3+2i$, $1+4i$, $4+i$, $2+5i$, $5+2i$, $1+6i$, $6+i$, $4+5i$, $5+4i$, 7, $2+7i$, $7+2i$, $5+6i$, $6+5i$, $3+8i$, $8+3i$, $5+8i$, $8+5i$, $4+9i$, $9+4i$, $1+10i$, $10+i$, $3+10i$, $10+3i$, 11, $7+8i$, $8+7i$, $4+11i$, $11+4i$.

Ці прості гаусові числа розташовані в порядку зростання модуля, і стає очевидним, що не всі прості числа кільця Z є простими в кільці $Z[i]$. Наприклад, 2 і 5 не є простими в $Z[i]$, тоді як 3, 7, 11 – прості як в Z, так і в $Z[i]$.

Решето Ератосфена є зручним оператором для знаходження канонічного розкладу гаусових чисел. Наприклад, $z = 89 + 86i$. $|z| = 17\sqrt{53} < 123$, $\sqrt{|z|} < 12$, тобто всі його прості дільники знаходяться серед чисел, знайдених у попередньому прикладі: $1+i$, $1+2i$, $2+i$, 3, $2+3i$, $3+2i$, $1+4i$, $4+i$, $2+5i$, $5+2i$, $1+6i$, $6+i$, $4+5i$, $5+4i$, 7, $2+7i$, $7+2i$, $5+6i$, $6+5i$, $3+8i$, $8+3i$, $5+8i$, $8+5i$, $4+9i$, $9+4i$, $1+10i$, $10+i$, $3+10i$, $10+3i$, 11, $7+8i$, $8+7i$, $4+11i$, $11+4i$.

Звичайним перебором цих чисел знайдемо прості дільники z. Першим таким дільником виявляється $4+i$: $z = (4+i)(x+yi)$. Цей дільник перевіряємо на кратність: z ділиться на $(4+i)^2$, і z не ділиться на $(4+i)^3$ – тобто кратність 2: $z = (4+i)^2(7+2i)$. Оскільки $7+2i$ – просте гаусове число, $z = (4+i)^2(7+2i)$ - канонічних розклад гаусового числа z.

Висновки

Побудовано алгоритм знаходження простих гаусових чисел, модуль яких не перевищує довільного взятого додатнього числа. Це дає можливість створити процедуру перевірки на простоту чи складеність довільного гаусового числа, а також забезпечує цілковиту розв'язність задачі знаходження канонічного розкладу гаусових чисел.

Література

[1] *Крутецкий Р.О.* Алгебра и арифметика комплексных чисел : пособие для учителей средних школ / Р.О. Крутецкий, Д.К. Фадеев. – Л.: Учпедгиз, ленинградское отделение, 1939. – 186 с.

[2] *Костюкова Н.И.* Комбинаторные алгоритмы для программистов : [електронний ресурс]. – Режим доступу : `http://www.intuit.ru/department/algorithms/algocombi/6/2.html`

[3] *Требенко Д.Я.* Алгебра і теория чисел / Д.Я. Требенко, О.О. Требенко. – К.: НПУ імені М.П. Драгоманова, 2006. – Ч 1. – 400 с.

[4] *Виноградов И.М.* Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981. – 176 с.

[5] *Завало С.Т.* Алгебра и теория чисел / С.Т. Завало, В.Н. Костарчук, Б.И. Хацет. – К.: Вища школа, 1974. – Ч 1. – 400 с.