О функции Эйлера колец вычетов гауссовых целых чисел

Г. Юргин

1 Введение

В теории чисел огромную роль играет *функция Эйлера* φ, ставящая в соответствие натуральному числу $m > 1$ количество обратимых элементов кольца вычетов $\mathbb{Z}_m$, т.е. $\varphi(m) := |\mathbb{Z}_m^*|$. Представляется естественным изучить обобщения функции Эйлера на различные другие кольца. В работе [1] были изучены т.н. *матричные функции Эйлера*, ставящие в соответствие натуральному числу $m > 1$ количество обратимых матриц в кольцах $\mathrm{GL}(2, \mathbb{Z}_m)$ и $\mathrm{SL}(2, \mathbb{Z}_m)$.

Целью данной работы является изучение функции Эйлера алгебраических расширений колец вычетов $\mathbb{Z}_m$.

Пусть α является корнем многочлена $Q \in \mathbb{Z}[x]$ степени n и не является корнем никакого многочлена меньшей степени. Обозначим через $\mathbb{Z}[\alpha]$ множество чисел вида

$$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \ldots + a_1\alpha + a_0,$$

где $a_i \in \mathbb{Z}$. На эти числа легко распространяются операции сложения и умножения. Частным случаем таких множеств являются числа вида $a + b\sqrt{-1}$, известные как *гауссовы целые числа*.

Аналогично, через $\mathbb{Z}_m[\alpha]$ будем обозначать множество чисел вида

$$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \ldots + a_1\alpha + a_0,$$

где все $a_i \in \mathbb{Z}_m$, причем m взаимно просто со старшим коэффициентом Q (мы будем считать, что это условие выполнено везде далее).

Определение 1. Через $\varphi_\alpha(m)$ обозначим количество необратимых элементов кольца $\mathbb{Z}_m[\alpha]$, т.е. $\varphi_\alpha(m) := |\mathbb{Z}_m[\alpha]^*|$.

В работе доказаны основные свойства функции Эйлера $\varphi_\alpha(m)$, вычислены ее значения и исследован рост в среднем функции Эйлера $\varphi_\iota(m)$ колец вычетов гауссовых целых чисел $\mathbb{Z}_m[i]^*$. Также в работе исследуются обобщения алгебраических расширений колец вычетов по модулям гауссовых целых чисел, вычисляется соответствующая им функция Эйлера и исследуется ее асимптотика.

2 Конкретные примеры

Прежде всего приведем конкретные примеры вычислений значений функции Эйлера некоторых расширений колец вычетов $\mathbb{Z}_m$.

2.1 Случай $\alpha = \sqrt{2}$

Пусть α — корень многочлена $x^2 - 2$. Тогда

$$\mathbb{Z}_m[\alpha] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}_m\}.$$

Сложение и умножение таких чисел будет выглядеть следующим образом:

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2},$$
$$(a+b\sqrt{2})\cdot(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}.$$

Значения $\varphi_{\sqrt{2}}(m)$ для разных m приведены в таблице (во второй строке — число элементов в кольце $\mathbb{Z}_m[\sqrt{2}]$. В первую строку включены только те числа, по модулю которых 2 — квадратичный вычет, т. к. в этом случае x^2-2 неприводим над $\mathbb{Z}_m$).

m	3	5	9	11	13	15	19	25	27	53	65	99
m^2	9	25	81	121	169	225	361	625	729	2809	4225	9801
$\varphi_{\sqrt{2}}(m)$	8	24	72	120	168	192	360	600	648	2808	4032	8640

2) Пусть α — корень многочлена $3x^2+x-1$. Тогда сложение элементов, как и в случае 1), происходит покоэффициентно. А чтобы вычислить произведение двух элементов, можно их перемножить как многочлены от α, а потом избавиться от слишком больших степеней α, пользуясь тем, что $3\alpha^2+\alpha-1=0$. Например, по модулю 5

$$(2\alpha+1)(\alpha+3)=2\alpha^2+7\alpha+3=-3\alpha^2-3\alpha-2=-(3\alpha^2+\alpha-1)-2\alpha-3=3\alpha+2.$$

Замечание 1. Условие взаимной простоты m и старшего коэффициента важно, т. к. иначе возникают трудности при умножении. Например, если в примере выше положить $m=9$, то уже не ясно, как избавиться от члена $2\alpha^2$.

3 Свойства функции Эйлера $\varphi_\alpha(m)$

В этом разделе мы докажем основные свойства функции Эйлера $\varphi_\alpha(m)$. Они сформулированы в следующей теореме.

Теорема 1. *Имеют место следующие свойства*

1. *Если α является корнем многочлена n-й степени, неприводимого над $\mathbb{Z}_p$, где p — простое, то $\varphi_\alpha(m)=p^n-1$, т.е. $\mathbb{Z}_p[\alpha]$ является полем.*

2. *Если k и m — натуральные взаимно простые числа, причем α является корнем многочлена, неприводимого над $\mathbb{Z}_p$ для всех p, являющихся простыми делителями k или m, то*

   $$\varphi_\alpha(k)\cdot\varphi_\alpha(m)=\varphi_\alpha(km)$$

   (свойство мультипликативности).

3. *Если $m=p_1^{\gamma_1}\cdot\ldots\cdot p_t^{\gamma_t}$ — натуральное число и его разложение на простые, причем α является корнем многочлена n-й степени, неприводимого над $\mathbb{Z}_{p_i}$ для всех i, то*

   $$\varphi_\alpha(m)=m^n\prod_{i=1}^{t}\left(1-\frac{1}{p_i^n}\right).$$

Доказательство. Доказываем от противного. Пусть в $\mathbb{Z}_p[\alpha]$ существует необратимый элемент a, отличный от нуля. Пусть X — множество всех элементов, делящихся на a, и в нём x элементов. Пусть Y — множество всех элементов, дающих 0 при умножении на a, и в нём y элементов. Ясно, что число элементов в $\mathbb{Z}_p[\alpha]$ равно p^n.

Лемма 1.1. $xy = p^n$.

Доказательство леммы 1.1. Рассмотрим граф, в котором вершинами являются элементы $\mathbb{Z}_m[\alpha]$, а рёбрами соединены те и только те элементы, разность которых лежит в Y (в частности, из каждой вершины идёт ребро в себя). Тогда если ребро есть между z_1 и z_2 и между z_2 и z_3 , то оно есть и между z_1 и z_3, т. к. если $z_1 - z_2 \in Y$ и $z_2 - z_3 \in Y$, то и $z_1 - z_2 - (z_2 - z_3) = z_1 - z_3 \in Y$. Значит, наш граф состоит из нескольких клик. Ясно, что $\mathbb{Z}_m[\alpha]$ - группа по сложению, откуда степень каждой вершины y. Значит, в каждой клике y вершин. Теперь покажем, что число клик равно x. Если взять два элемента z_1 и z_2 из одной клики, то $z_1 - z_2 \in Y \Rightarrow a(z_1 - z_2) = 0 \Rightarrow az_1 = az_2$. Если z_1 и z_2 - из разных клик, то $a(z_1 - z_2) \neq 0 \Rightarrow az_1 \neq az_2$. Значит, число клик равно количеству различных чисел вида az, а это и есть x. Т. е. вершины графа разбились на x клик по y вершин в каждой, т. е. $xy = p^n$. Лемма 1 доказана.

Следствие леммы 1.1. $y = p^k$, $x = p^{n-k}$ при каком-то натуральном $k : n \geq k \geq 0$. Более того, модно утверждать, что $n > k > 0$. Ведь 0 и a принадлежат X, т. е. $x > 1 \Rightarrow k \neq n$. В Y есть элемент, отличный от 0 (иначе все числа вида az были бы различны, т. е. среди них была бы 1 и a был бы обратим). Получаем $k \neq 0$

Лемма 1.2. При $k - 1 \geq s \geq 0$ существует хотя бы $p^{k-s} - 1$ ненулевых элементов Y, у которых s старших коэффициентов равны 0.

Доказательство леммы 1.2. Докажем лемму индукцией по s. База: $s = 0$. в N всего p^k элементов, значит, хотя бы $p^k - 1$ ненулевых элементов. Переход: предположим, что в N существует $p^{k-s} - 1$ ненулевых элементов, у которых s старших коэффициентов равны 0 ($s < k-1$). Среди них найдутся либо $p^{k-s-1}-1$ элементов с нулевым $s+1$-ым с конца коэффициентом, либо p^{k-s-1} элементов с одним и тем же $s + 1$-ым с конца коэффициентом. В первом случае утверждение леммы для выполнено. Во втором случае возьмём один из этих элементов и вычтем из него остальные. Мы получим $p^{k-s-1} - 1$ чисел, у которых $s + 1$ старший коэффициент равен 0, при этом все полученные числа тоже принадлежат Y. Т. е. утверждение леммы выполнено. Лемма 2 доказана.

Следствие леммы 1.2. Существует элемент β_1, лежащий в Y, у которого $k - 1$ старший коэффициент равен нулю (т. к. положив в лемме 2 $s = k-1$ получаем, что таких хотя бы $p-1$).

Лемма 1.3. Существует элемент β_1 , лежащий в X, у которого $n - k - 1$ старший коэффициент равен нулю.

Доказательство леммы 3. Заметим, что если элементы z_1 и z_2 принадлежат X, то их разность тоже принадлежит X (т. к. существуют элементы z_1' и z_2' такие, что $z_1 = z_1'az_2 = z_2'a \Rightarrow z_1 - z_2 = (z_1' + z_2')a \Rightarrow z_1 - z_2 \in X$). Теперь можно провести рассуждения, аналогичные рассуждениям в выводе леммы 2 и следствия из неё и получить лемму 3.

Завершим доказательство теоремы 1. Рассмотрим β_1 и β_2 как многочлены от α над $\mathbb{Z}_p$. Произведение $\beta_1\beta_2$ - это многочлен степени не выше n. Подберём константу q так, чтобы коэффициенты при n-й степени у многочленов $Qq\beta_1\beta_2$ были равны. Тогда $q\beta_1\beta_2 - Q$ является многочленом степени не более $n - 1$. Но если мы рассмотрим β_1 и β_2 как элементы $\mathbb{Z}_p[\alpha]$, то получим $\beta_1\beta_2 = 0$ (т. к. β_1 и β_2 лежат в Y и X соответственно, откуда для какого-то элементаβ_2' выполнено $\beta_1\beta_2 = \beta_1 a\beta_2' = 0\beta_2' = 0$). Значит,$q\beta_1\beta_2 - P$ является как многочлен тождественным нулём, откуда Q приводим над $\mathbb{Z}_p$, что и требовалось доказать.

Замечание 2. Случай, когда Q неприводим над $\mathbb{Z}_m$, для нас более интересен, т. к. если Q можно разложить в произведение нескольких неприводимых сомножителей, то можно считать корнем одного из них.

Прежде чем переходить к доказательству свойств 2 и 3, докажем важное следствие свойства 1.

Лемма. *В условиях свойства 3 элемент* $z = a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \ldots + a_1\alpha + a_0$ *обратим тогда и только тогда, когда НОД*$(a_0, a_1, \ldots, a_{n-1}, m) = 1$.

Доказательство леммы. $\boxed{\Rightarrow}$ Если НОД$(a_0, a_1, \ldots, a_{n-1}, m) > 1$, то существует индекс i такой, что все коэффициенты делятся на p_i. Но тогда у любого элемента, полученного умножением z на произвольный элемент, все коэффициенты также будут делиться на p_i. Значит, элемент z необратим.

$\boxed{\Leftarrow}$ Случай 1: $m = p^\gamma$, где p — простое. От противного. Если z необратим, то из принципа Дирихле существуют различные $z_1 z_2 : zz_1 = zz_2, ..z(z_1 - z_2) = 0, a = z_1 - z_2 \neq 0$. Пусть s - минимальная степень вхождения простого множителя в коэффициенты z ($a' \neq 0 \Rightarrow s < k$). Тогда можно za представить в виде $p^s aa'$, причём в a' существует коэффициент, не кратный p. Отсюда в aa' существует коэффициент, не кратный p. (так как можно a и a' рассмотреть по модулю p: $a \neq 0 \pmod p$,$a' \neq 0 \pmod p$, тогда из теоремы 1 $aa' \neq 0 \pmod p$). Но это значит, что $p^s aa' \neq 0$. Противоречие. Случай 2: $m = p_1^{\gamma_1} p_2^{\gamma_2} ... p_t^{\gamma_t}$. Пускай для элемента z выполнено $(a_0, a_1, ..., a_{n-1}, m) = 1$. Тогда из случая 1 для любого i найдётся элемент $z^i : zz^i \equiv 1 \pmod{p_i}$. При этом каждый коэффициент у z^i задан с точностью до остатка по модулю p_i . По китайской теореме об остатках можно подобрать коэффициенты так, чтобы для полученного элемента z' было выполнено $zz' \equiv 1 \pmod{p_i^{\gamma_i}}$ для всех i. Но это значит, что $zz' = 1 \pmod m$, т. е. z обратим, что и требовалось. □

Теперь можно перейти к доказательству теорем 2 и 3.

Доказательство теоремы 2. Из следствия теоремы 1 видно, что элемент z обратим по модулю mk тогда и только тогда, когда он обратим по модулю m и по модулю k. По китайской теореме об остатках каждый коэффициент в точности задаётся остатками по модулю m и k, т. е. элемент в точности задаётся двумя наборами остатков (по модулю m и по модулю k для каждого коэффициента). Число способов выбрать остатки по модулю m так, чтобы элемент был обратим по модулю m, равно $\varphi_\alpha(k)$, по модулю k - оно равно $\varphi_\alpha(m)$, значит, всего имеем $\varphi_\alpha(k)\varphi_\alpha(m)$ обратимых элементов по модулю mk, что и требовалось доказать.

Доказательство теоремы 3. Случай 1. $m = p^\gamma$, где p - простое. Из следствия теоремы 1 элемент необратим тогда и только тогда, когда все его коэффициенты делятся на p. Всего есть n коэффициентов и по $p^{\gamma-1}$ способов выбрать каждый так, чтобы он делился на p. Значит необратимых элементов $p^{(\gamma-1)n}$, а обратимых $p^{\gamma n} - p^{(\gamma-1)n} = m^n(1 - \frac{1}{p^n})$

Случай 2.$m = p_1^{\gamma_1} p_2^{\gamma_2} ... p_t^{\gamma_t}$ Из свойства мультипликативности получаем

$$\varphi_\alpha(m) = m^n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i^n}\right),$$

что и требовалось доказать. □

4 Функция Эйлера колец вычетов гауссовых чисел

Наша цель — получить формулу роста в среднем функции $\varphi_i m$. Для этого изучим функцию $\varphi_\iota(m)$ для всех натуральных m.

Сначала напомним следующее

Определение 2. *Нормой числа* $z := a + bi$ *по модулю* m будем называть число $N(z) := a^2 + b^2 \pmod m$.

Утверждение. Если $a+bi$ - хороший элемент, $c+di$ и $e+fi$ - произвольные элементы, причем $(a+bi)(c+di)=(a+bi)(e+fi)$, то $c+di=e+fi$.

Доказательство. $(a+bi)(c+di)=(a+bi)(e+fi) \Rightarrow a(c-e)+b(d-f)=0a(d-f)-b(c-e)=0$ (здесь и далее во всем доказательстве все равенства по модулю m). Произведём замену: $c-e=s$; $d-f=t$. Тогда $as+bt=0(1)at-bs=0(2) \Rightarrow as+b^2t=0a^2t-abs=0$ Складывая два последних равенства, получаем $t=0$ (т. к. a^2+b^2 взаимно просто с m). Подставляя $t=0$ в (1) и (2), имеем $as=0bs=0 \Rightarrow a^2s=0b^2s=0 \Rightarrow s(a^2+b^2)=0 \Rightarrow s=0$ То есть $s=0t=0 \Rightarrow c=ed=f \Rightarrow c+di=e+fi$ □

Предложение. *Элемент $\alpha \in \mathbb{Z}_m[i]$ обратим тогда и только тогда, когда $N(\alpha)$ и m взаимно просты.*

Доказательство. 1) Часть «И только тогда». Если у элемента α норма не взаимно проста с m, то из мультипликативности нормы для любого элемента β $N(\alpha\beta)$ тоже не взаимно проста с m. Но $N(1)=1$ взаимно проста с m, значит, $\alpha\beta \neq 1$ 2) Часть "Тогда". Пусть элемент α хороший. Умножим каждый элемент $\mathbb{Z}_m[m]$ на α . Из утв. 5.1 в полученном наборе элементов любые два элемента различны. Значит, в нём каждый элемент встречается ровно по одному разу, т. е. в нём есть и 1. Значит, α обратим. □

Оказывается, что формулы для значений функции Эйлера $\varpi_\iota(m)$ различаются в зависимости от того, какие именно простые делители входят в m. Для удобства обозначим через $\mathbb{P}_1$ (соответственно $\mathbb{P}_{-1}$) множество всех простых чисел, дающих остаток 1 (соответственно -1) при делении на 4.

Предложение. *1. Если $p \in \mathbb{P}_1$, то*

$$\varphi_i(p^\alpha)=p^{2\alpha}\left(1-\frac{1}{p}\right)^2.$$

2. Если $p \in \mathbb{P}_{-1}$, то

$$\varphi_i(p^\alpha)=p^{2\alpha}\left(1-\frac{1}{p^2}\right).$$

3. Имеет место равенство

$$\varphi_i(2^\alpha)=2^{2\alpha-1}.$$

Доказательство. 1. Рассмотрим элемент $a+bi$. Из предложения 4 следует, что он обратим тогда и только тогда, когда его норма не делится на p. Посчитаем, при каких a сколько существует значений b таких, что a^2+b^2 делится на p.

1) Пусть a делится на p. В этом случае a^2+b^2 делится на p тогда и только тогда, когда b делится на p. Среди чисел от 0 до $p^\alpha-1$ есть $p^{\alpha-1}$ чисел, кратных p, значит, в случае 1) получаем $p^{2\alpha-2}$ обратимых элементов.

2) Пусть a не делится на p. Тогда нам надо, чтобы b^2 было сравнимо с $-a^2$ по модулю p. Остаток $-a^2$ является квадратичным вычетом по модулю p, так как p даёт остаток 1 при делении на 4. Отсюда следует, что уравнение $b^2 \equiv -a^2 \pmod{p}$ имеет ровно два решения среди чисел от 0 до $p-1$. Значит, среди чисел от 0 до $p^\alpha-1$ оно имеет ровно $2p^{\alpha-1}$ решений. В то же время среди чисел от 0 до $p^\alpha-1$ существует ровно $p^\alpha-p^{\alpha-1}$ значений a, не кратных p, поэтому случай 2) дает $2p^{\alpha-1}(p^\alpha-p^{\alpha-1})$ различных необратимых элементов.

Итого мы имеем

$$2p^{\alpha-1}(p^\alpha-p^{\alpha-1})+p^{2\alpha-2}=2p^{2\alpha-1}-p^{2\alpha-2}$$

необратимых элементов. Всего элементов $p^{2\alpha}$, значит, обратимых ровно

$$p^{2\alpha} - 2p^{2\alpha-1} + p^{2\alpha-2} = p^{2\alpha}\left(1 - \frac{1}{p}\right)^2.$$

2. Если p простое и даёт остаток -1 при делении на 4, то -1 является квадратичным невычетом по модулю p, поэтому этот пункт следует из теоремы 1.

3. Рассмотрим элемент $a+bi$. Среди чисел от 0 до $2^\alpha - 1$ чётных и нечётных поровну. Поэтому одинакова вероятность четырёх исходов:

1) a и b чётны;

2) a и b нечётны;

3) a чётно, b нечётно;

4) a нечётно, b чётно.

Из предложения 4 следует, что элемент $a + b$ обратим тогда и только тогда, когда имеют место исходы 3) или 4). Значит, обратимых элементов ровно половина, т.е. $2^{2\alpha-1}$. □

Из доказательства теоремы 1 сразу следует, что функция Эйлера φ_ι мультипликативна. Таким образом, мы немедленно получаем

Следствие. *Имеет место формула*

$$\varphi_i(m) = \varepsilon(m) \cdot m^2 \cdot \prod_{p_k \in \mathbb{P}_{-1}} \left(1 - \frac{1}{p_k^2}\right) \cdot \prod_{q_l \in \mathbb{P}_1} \left(1 - \frac{1}{q_l}\right)^2.$$

Здесь $\varepsilon(m) = 1$, если m нечётно, и $\varepsilon(m) = \frac{1}{2}$, если m чётно, а произведения ведутся по всем простым делителям числа m.

5 Рост в среднем функции Эйлера φ_ι

В этом разделе мы изучим рост функции Эйлера φ_ι.

Отметим, что функция Эйлера растет крайне нерегулярно. Поэтому говорить о ее асимптотике нельзя. Однако можно «сгладить» скачки функции Эйлера, если рассмотреть ее средние арифметические. Это приводит нас к следующему понятию.

Определение 3. Будем говорить, что две функции f, $g\colon \mathbb{Z}_m[i] \to \mathbb{N}$ *одинаково растут в среднем*, если

$$\frac{\sum_{m \leqslant M} f(m)}{\sum_{m \leqslant M} g(m)} \to 1 \quad \text{при } M \to \infty.$$

Обозначать это будем следующим образом: $f \mathrel{\widehat{\sim}} g$.

Теперь сформулируем основную теорему этого раздела.

Теорема 2. *Имеет место следующая асимптотика в среднем:*

$$\varphi_\iota(m) \mathrel{\widehat{\sim}} cm^2, \quad \text{где } c := \frac{3}{4} \prod_{p \in \mathbb{P}_{-1}} \left(1 - \frac{1}{p^3}\right) \cdot \prod_{q \in \mathbb{P}_1} \left(1 - \frac{2}{q^2} + \frac{1}{q^3}\right) \approx 0,6498.$$

Доказательство. Будем трёхмерные вектора вида (a, b, m), такие, что $a \geq 0$, $b \geq 0$, $m > a$ и $m > b$, называть правильными. Сопоставим правильному вектору вида (a, b, m) элемент $a + bi$ гауссова кольца вычетов $\mathbb{Z}_m[i]$. Тогда каждому элементу каждого множества вида $\mathbb{Z}_m[i]$ будет сопоставлен ровно один правильный вектор. Будем называть правильный вектор (a, b, m)

необратимым по простому модулю p, если a^2+b^2 и m делятся на p. Будем называть правильный вектор (a,b,m) необратимым, если существует простое p, по модулю которого он необратим. Из предложения 4 следует, что правильный вектор соответствует обратимому элементу тогда и только тогда, когда сам вектор обратим.

Лемма. *Если m делится на p, то число элементов с нормой, не кратной p, равно $p^{2\alpha}\sigma(p)$, где $\sigma(p)=\left(1-\frac{1}{p}\right)^2$, если p даёт остаток -1 при делении на 4, $\sigma(p)=1-\frac{1}{p^2}$, если p даёт остаток 1 при делении на 4, и $\sigma(p)=\frac{1}{2}$, если $=2$.*

Доказательство леммы 5. Из предложения 4 следует, что если $m=p^\alpha$, то доля элементов с нормой, кратной p, равна $\frac{1}{\sigma(m)}$. Если же $m=p^\alpha t$, где t и p взаимно просты, то доля элементов с нормой, кратной , будет такой же (это следует из китайской теоремы об остатках). Значит, число элементов с нормой, кратной , равно $p^{2\alpha}\sigma(p)$, что и требовалось. □

Из леммы 5 получаем, что если m делится на p, то существует ровно $p^2(1-\sigma(p))$ правильных векторов, необратимых по модулю p и имеющих третью координату m. Если же m на делится на p, то правильных векторов, необратимых по модулю p и имеющих третью координату m не существует. Всего правильных векторов с третьей координатой с ровно m^2. Отсюда вероятность выбрать вектор, необратимый по модулю , при случайном выборе правильного вектора, равна

$$\lim_{n\to\infty}\frac{p^2(1-\sigma(p))+(2p)^2(1-\sigma(p))+\ldots+(np)^2(1-\sigma(p))}{1^2+2^2+\ldots+(np)^2}=$$
$$=\lim_{n\to\infty}p^2(1-\sigma(p))\frac{1^2+2^2+\ldots+n^2}{1^2+2^2+\ldots+(np)^2}=\lim_{n\to\infty}p^2(1-\sigma(p))\frac{n^3/3}{n^3p^3/3}=\frac{1-\sigma(p)}{p}. \quad (1)$$

Значит, вероятность выбрать таким образом вектор, обратимый по модулю p, составляет

$$1-\frac{1-\sigma(p)}{p}.$$

Ясно, что эти события при разных независимы, поэтому вероятность P выбрать обратимый вектор равна

$$\prod_{p\in\mathbb{P}}\left(1-\frac{1-\sigma(p)}{p}\right)=\frac{3}{4}\prod_{p\in\mathbb{P}_{-1}}\left(1-\frac{1}{p^3}\right)\cdot\prod_{q\in\mathbb{P}_1}\left(1-\frac{2}{q^2}+\frac{1}{q^3}\right).$$

Но при любом m среди m^2 хороших векторов вида (a,b,m) существует ровно $\varphi_i(m)$ обратимых. Поэтому

$$P=\lim_{n\to\infty}\frac{\varphi_\iota(1)+\varphi_\iota(2)+\ldots+\varphi_\iota(n)}{1^2+2^2+\ldots+n^2}$$

Значит,

$$\lim_{n\to\infty}\frac{\varphi_\iota(1)+\varphi_\iota(2)+\ldots+\varphi_\iota(n)}{1^2+2^2+\ldots+n^2}=\frac{3}{4}\prod_{p\in\mathbb{P}_{-1}}\left(1-\frac{1}{p^3}\right)\cdot\prod_{q\in\mathbb{P}_1}\left(1-\frac{2}{q^2}+\frac{1}{q^3}\right).$$

□

6 Продолженная функция Эйлера и ее свойства

В предыдущих разделах была рассмотрена функция Эйлера расширений колец вычетов от натуральных аргументов. В этой части мы рассмотрим продолжение функции Эйлера гауссовых колец вычетов по модулям произвольных целых гауссовых чисел.

Пусть z — гауссово целое число. Все точки на комплексной плоскости, соответствующие числам, кратным z, образуют квадратную решетку. Квадраты, из которых состоит решетка, будем называть её элементарными ячейками. Условимся, что точка, лежащая линиях сетки, принадлежит той ячейке, в которую попадает ее образ при прибавлении к ней числа $\varepsilon z(i+1)$ при малых ε.

Определение 4. *Вычетами по модулю z* будем называть все гауссовы целые числа, лежащие в одной ячейке с числом 0. Через $\mathbb{Z}_z[i]$ обозначим кольцо вычетов по модулю z. *Функцией Эйлера* $\varphi_i(z)$ от произвольного гауссова целого числа z будем называть функцию, сопоставляющую z число обратимых элементов множества $\mathbb{Z}_z[i]$.

Отметим следующее известное

Предложение. *Неприводимыми в $\mathbb{Z}[i]$ являются те и только те числа, которые удовлетворяют одному из следующих свойств:*

1) Норма числа равна 2.

2) Норма числа равна простому числу из $\mathbb{P}_1$.

3) Число является действительным простым числом из $\mathbb{P}_{-1}$.

Предложение. *Во множестве $\mathbb{Z}_z[i]$ ровно $N(z)$ элементов.*

Доказательство. Элементарная ячейка решетки, соответствующая z, является квадратом с площадью $N(z)$. По формуле Пика $N(z) = a + b/2 - 1$, где строго внутри ячейки лежит ровно a целочисленных точек, а на ее границе лежит ровно b целочисленных точек. Но ячейке принадлежат все точки строго внутри нее, одна ее вершина и точки на двух ее сторонах, не являющиеся вершинами. Легко видеть, что это в точности $a + b/2 - 1$ точек. То есть число точек, принадлежащих ячейке, равно $N(z)$, что и требовалось. □

Предложение. *Пусть дано неприводимое число $p \in \mathbb{Z}[i]$, пусть гауссово целое $z \in \mathbb{Z}[i]$ кратно p. Тогда доля элементов $\mathbb{Z}_z[i]$, кратных p, равна $\frac{1}{N(p)}$.*

Доказательство. Элементарная ячейка решетки Z, соответствующей числу z, является квадратом с площадью $N(z)$. Элементарная ячейка решетки P, соответствующей числу p, является прямоугольником с площадью $N(p)$. Каждый узел Z является также узлом P, значит, при совмещении двух ячеек P при помощи параллельного переноса совмещаются все находящиеся в них узлы P. То есть внутри разных ячеек Z поровну узлов P.

Пусть в одной ячейке Z содержится t узлов P. Возьмем какую-нибудь ячейку Z и сопоставим каждому узлу P внутри этой ячейки ячейку решетки P, крайним узлом которой этот узел является. Суммарная площадь всех сопоставленных ячеек равна $tN(p)$.

Возьмем теперь множество S ячеек Z, образующих большой прямоугольник $s \times s$ ячеек и сделаем такое же сопоставление для каждой ячейки из S. Ясно, что отношение суммарной площади ячеек множества S к суммарной площади всех сопоставленных ячеек стремится к 1 при $s \to \infty$. Отношение этих площадей равно $\frac{s^2 N(z)}{s^2 tN(p)} = \frac{N(z)}{tN(p)}$, поэтому $t = \frac{N(z)}{N(p)}$.

Доля элементов $\mathbb{Z}_z[i]$, кратных p, равна отношению числа узлов P в ячейке Z к числу всех точек в ячейке Z, то есть $\frac{t}{N(z)} = \frac{1}{N(p)}$, что и требовалось. □

На функции, определенные на $\mathbb{Z}[i]$, естественным образом обобщается понятие роста в среднем. А именно, будем говорить, что функции f, $g\colon \mathbb{Z}[i] \to \mathbb{N}$ *одинаково растут в среднем*, если

$$\lim_{n\to\infty} \frac{\sum_{N(z)<n} f(z)}{\sum_{N(z)<n} g(z)} = 1.$$

Основная теорема данной работы формулируется следующим образом.

Теорема 3. *Имеет место асимптотика в среднем*

$$\varphi_\iota(z) \widehat{\sim} CN(z), \quad \text{где } C := \frac{3}{4} \prod_{p \in \mathbb{P}_{-1}} \left(1 - \frac{1}{p^4}\right) \cdot \prod_{q \in \mathbb{P}_1} \left(1 - \frac{1}{q^2}\right)^2 \approx 0,6637.$$

Доказательство. Будем рассматривать пары вида (z, r), где z является гауссовым целым числом, а r является элементом множества $\mathbb{Z}_z[i]$. Будем говорить, что пара (z, r) обратима, если r обратим в $\mathbb{Z}_z[i]$.

Пусть гауссово целое число p неприводимо. Будем говорить, что пара (z, r) необратима по модулю p, если z и r кратны p. Пара обратима тогда и только тогда, когда она обратима по модулю всех неприводимых p. Через $T(p)$ обозначим вероятность того, что случайно выбранная пара окажется необратима по модулю p.

Всего пар с первым элементом z ровно $N(z)$. Если z не кратно p, то неприводимых по модулю p пар с первым элементом z не существует. Если z кратно p, то по предложению 6 неприводимых по модулю пар с первым элементом z будет $\frac{N(z)}{N(p)}$.

Доля гауссовых целых z, кратных p, среди всех гауссовых целых чисел равна $\frac{1}{N(p)}$. При этом рост в среднем величины $N(z)$ одинаков для z, кратных p, и для z, не кратных p. Отсюда получаем $T(p) = \frac{1}{N^2(n)}$.

Вероятность того, что случайно выбранная пара окажется обратима по модулю p, равна $1 - T(p) = 1 - \frac{1}{N^2(p)}$. События «выпадение пары, обратимой по модулю» при разных неприводимых p независимы. Значит вероятность выбрать обратимую пару при случайной выборке равна

$$\prod_{p \in \mathbb{P}[i]} \left(1 - \frac{1}{N^2(p)}\right)$$

По предложению 6 это произведение равно

$$\frac{3}{4} \prod_{q \in \mathbb{P}_1} \left(1 - \frac{1}{q^2}\right)^2 \cdot \prod_{q \in \mathbb{P}_{-1}} \left(1 - \frac{1}{q^4}\right).$$

Но число обратимых пар с первым элементом z равно в точности $\varphi_i(z)$. Значит, вероятность выбрать обратимую пару при случайной выборке равна

$$\lim_{n \to \infty} \frac{\sum_{N(z)<n} \varphi_i(z)}{\sum_{N(z)<n} N(z)}.$$

Отсюда получаем, что

$$\lim_{n \to \infty} \frac{\sum_{N(z)<n} \varphi_i(z)}{\sum_{N(z)<n} N(z)} = \frac{3}{4} \prod_{q \in \mathbb{P}_1} \left(1 - \frac{1}{q^2}\right)^2 \prod_{q \in \mathbb{P}_{-1}} \left(1 - \frac{1}{q^4}\right)$$

□

Автор благодарит П.В. Бибикова за постановку задачи и внимание к работе.

Список литературы

[1] Байгушев Д. *О росте в среднем матричной функции Эйлера*// Труды Казанского математического общества им. Н.И. Лобачевского, – **28**, – 2013

[2] Винберг Э.Б. *Курс алгебры.* – М.: Изд-во "Факториал Пресс", 2001. – 544с.

[3] Арнольд В.И. *Группы Эйлера и арифметика геометрических прогрессий.* – М.: МЦНМО, 2003. – 44с.