XVIII Республиканский Турнир Юных Математиков

Задача №11. Деление с остатком

Лицей БГУ - №1

Автор: Пчелинцев Илья
Научный руководитель: Шабан Светлана

Аннотация

Полностью решены пункты 1-3, 5 исходной постановки задачи. В пункте 4 приведены алгоритмы деления для всех отрицательных и большей части от возможных положительных значений d. Предложено множество обобщений, перечисленных в пункте 6.

Минск, 2016

Оглавление

1. Общие свойства допустимых множеств с делением

Пусть K – допустимое множество с функцией f, на котором имеет место деление с остатком. Пусть также в K нет делителей нуля. Если не делать этого допущения, то операция деления не будет определена однозначно. Например, можно взять $Z_4 = \{0,1,2,3\}$ (кольцо вычетов по модулю 4) и $f(x) = x$. Нетрудно убедится, что это допустимое множество, на котором имеет место деление с остатком. Однако $2 = 2 \cdot 3$ и $2 = 2 \cdot 1$. Значит $\frac{2}{2}$ не определено однозначно.

Докажем несколько общих теорем.

1.1 Преобразование функции f

Преобразуем функцию f. Пусть f не принимает значение n. Тогда рассмотрим новую функцию f':

$$f'(x) = \begin{cases} f(x), & \text{если } f(x) < n \\ f(x) - 1, & \text{если } f(x) > n \end{cases}$$

Ясно, что если $f(a) \geq f(b)$, то $f'(a) \geq f'(b)$, и если $f(a) > f(b)$, то $f'(a) > f'(b)$. Значит K с функцией f' также допустимо и на нем имеет место деление с остатком.

Будем повторять это преобразование, пока f не станет сюрьективной. Теперь можем считать, что f принимает все значения.

1.2 Несколько простых утверждений

Утверждение 0. Если a делится на b, то $\frac{a}{b}$ определено однозначно.

Доказательство. Пусть существуют два корня уравнения $a = xb$. Обозначим их x и x'. Тогда:

$$0 = a - a = xb - x'b = b(x - x')$$

Так как в K нет делителей нуля и b не ноль, то $x - x' = 0$. Противоречие с тем, что x и x' различные. ■

Утверждение 1. $x \neq 0 \Rightarrow f(x) \geq 1$

Доказательство. Пусть $f(x) = 0$. Поделим x на x: $x = x \cdot k + r$, где $f(r) < f(x) = 0$. Но f принимает только неотрицательные значения. Противоречие. Значит $f(x) \geq 1$. ■

Утверждение 2. $f(1) = 1$.

Доказательство. $x \neq 0 \Rightarrow f(x) = f(1 \cdot x) \geq f(1)$. Учитывая, что f сюрьективна и $f(1) \geq 1$ (утверждение 1), $f(1) = 1$. ■

Утверждение 3. $f(x) = 0 \Leftrightarrow x = 0$.

Доказательство. f сюрьективна, значит существует x, такой что $f(x) = 0$. Для любого ненулевого x $f(x) \geq 1$. Следовательно, $x = 0$. ■

1.3 Наибольший общий делитель

Определение. $\text{НОД}(a, b)$ – элемент из K, который делит a и b, с наибольшим значением f от него.

Пусть x делит a. Тогда $f(\mathrm{a}) = f(x \cdot k) \geq f(x)$, то есть $f(x)$ ограничено. Значит, НОД существует. Однако НОД может быть не единственен. В таком случае под $\text{НОД}(a, b)$ будем иметь в виду один из НОДов.

Алгоритм Евклида. Пусть дана пара элементов из K (a, b) и при этом $f(a) \geq f(b)$. Пусть c – остаток от деления a на b. Текущую пару заменяем на (b, c). Повторяем алгоритм пока один из элементов в паре не станет нулем.

Теорема 1. Алгоритм Евклида конечен и ненулевой элемент в последней паре есть $\text{НОД}(a, b)$.

Доказательство. Поделим a на b с остатком:

$$a = b \cdot k + c, f(c) < f(b) \tag{1}$$

Таким образом, за один ход мы уменьшаем значение f от одного из чисел. Значит, когда-то f от одного из чисел будет равна 0. Из утверждения 3 следует, что это число само является нулем. Поэтому алгоритм конечен.

Покажем, что любой $\text{НОД}(a, b)$ является также и $\text{НОД}(c, b)$ и наоборот. Из (1) видно, что $\text{НОД}(a, b)$ делит c и делит b по определению. Значит $f\big(\text{НОД}(a, b)\big) \leq f(\text{НОД}(c, b))$. Аналогично $\text{НОД}(c, b)$ делит a и b и $f\big(\text{НОД}(a, b)\big) \geq f(\text{НОД}(c, b))$. Получаем $f\big(\text{НОД}(a, b)\big) = f(\text{НОД}(c, b))$, что и есть определение НОД.

Докажем, что ненулевой элемент в последней паре является НОДом последней пары. Другими словами $\text{НОД}(x, 0) = x$. Ясно, что x делит x и ноль. Пусть существует y делящий x и 0 и $f(y) > f(x)$. Тогда $f(x) = f(ky) \geq f(y)$. Противоречие. ■

Теорема 2. Существуют $x, y \in K$ такие, что $\text{НОД}(a, b) = xa + yb$.

Доказательство. Выполним алгоритм Евклида для a и b, запоминая пару на каждом ходу. Покажем, что если Теорема 2 верна для одной пары, то она верна и для предыдущей. Пусть перед парой (b, c) была пара (a, b) и существуют x и y, такие что:

$$\text{НОД}(a,b) = \text{НОД}(b,c) = xb + yc$$

Из определения алгоритма Евклида:

$$a = b \cdot k + c, f(c) < f(b) \tag{1}$$

Теперь можем представить $\text{НОД}(a,b)$ как необходимо: $\text{НОД}(a,b) = (x - yk)b + ya$.

Легко проверить теорему 2 для последней пары $(y,0)$: $\text{НОД}(y,0) = y = y \cdot 1 + 0 \cdot 0$. Значит, она верна и для первой пары. ■

1.4 Основная теорема арифметики

Определение. Назовем элемент x из K единичным, если $f(x) = 1$. Ненулевой неединичный элемент из K назовем простым, если оно делится только на единичные элементы, на себя и на произведение себя на единичные элементы. Ненулевой элемент из K назовем составным, если он не единичный и не простой. Эквивалентное определение составного элемента — ненулевой элемент, который можно представить в виде произведения двух не единичных элементов из K.

Утверждение 3. Пусть p – простое и p делит ab. Тогда p делит a или b (или и a, и b).

Доказательство. Пусть p не делит а. Покажем $f(\text{НОД}(a,p)) = 1$. Допустим обратное: $f\big(\text{НОД}(a,p)\big) > 1$. Тогда $\text{НОД}(a,p)$ делит p, а значит $\text{НОД}(a,p) = up$, где $f(u) = 1$. Также $\text{НОД}(a,p) = up$ делит a. Значит и p делит a. Но по предположению p не делит a. Противоречие.

По теореме 2 существуют x и y такие что

$$xa + yp = 1$$

$$xab + ypb = b$$

xab и ybp делятся на p. Значит и b делится на p. ■

Утверждение 3'. Пусть p – простое и p делит $a_1 a_2 \dots a_n$. Тогда p делит a_i.

Доказательство. Докажем индукцией по n. База $n = 2$ проверена в утверждении 3. Пусть верно для n. Докажем, что верно и для $n + 1$. p делит $(a_1 a_2 \dots a_n)a_{n+1}$. Применим утверждение 3 для чисел $a_1 a_2 \dots a_n$ и a_{n+1}. Если p делит $a_1 a_2 \dots a_n$, то по предположению индукции оно делит одно из a_i. Иначе p делит a_{n+1}. ■

Утверждение 4. Если b составной элемент, а a ненулевой, то $f(ab) > f(a)$.

Доказательство. $f(ab) \geq f(a)$. Достаточно показать, что $f(ab)$ не может быть равно $f(a)$. Пусть это так. Разделим с остатком a на ab:

$$a = kab + r, f(r) < f(ab) = f(a)$$
$$r = a - kab$$
$$f(r) = f\big(a(1 - kb)\big) \geq f(a)$$

($1 - kb \neq 0$, так как иначе $1 = f(1) = f(kb) \geq f(b) \geq 2$)

Но $f(a) > f(r)$. Противоречие. ■

Основная теорема арифметики. Любой ненулевой элемент K единственным образом представляется как произведение простых с точностью до перестановки и домножения на единичные элементы.

Доказательство. Пусть x ненулевой элемент из K. Докажем теорему индукцией по $f(x)$.

База: $f(x) = 1$. Пусть k делитель x. Тогда $1 = f(x) = f(kt) \geq f(k)$. То есть все делители x являются единичными и сам x единичный. Что и требовалось доказать.

Шаг: пусть утверждение верно для всех x таких что $f(x) < n$. Докажем для n. Пусть существует элемент α для которого $f(\alpha) = n$. Покажем, что x можно представить как произведение простых. Если α простое, то разложение уже есть. Если α составное, то $\alpha = ab$ где $f(a), f(b) > 1$. Согласно утверждению 4 $f(\alpha) = f(ab) > f(a), f(b)$. По предположению индукции a и b можно представить как произведение простых. Значит и $ab = \alpha$ можно.

Докажем теперь что это разложение единственно. Пусть существуют два различных разложения α на простые множители $\alpha = p_1 p_2 \dots p_n = p'_1 p'_2 \dots p'_m$. p_1 делит $p'_1 p'_2 \dots p'_m$, и по утверждению 3' p_1 делит p'_i. Можем переобозначить индексы и считать, что p_1 делит p'_1. То есть $p'_1 = u p_1$, где u единичный элемент. Рассмотрим новое число $\beta = p_2 \dots p_n = u p'_2 \dots p'_m$. $f(\beta) < f(\alpha)$ по утверждению 4. Значит, по предположению индукции β единственным образом представляется как произведение простых с точностью до перестановки и домножения на единичные элементы. Следовательно, $p_2 \dots p_n$ и $u p'_2 \dots p'_m$ есть два одинаковых разложения. Из этого и $p'_1 = u p_1$ следует, что $p_1 p_2 \dots p_n$ и $p'_1 p'_2 \dots p'_m$ есть два одинаковых разложения на простые. ■

1.4 Наименьшее общее кратное

Определение. $\text{НОК}(a, b)$ есть элемент который делится на a и на b с наименьшем значение f от него.

Теорема 3. $\text{НОК}(a,b) = \frac{ab}{\text{НОД}(a,b)}$.

Доказательство. Обозначим $\text{НОД}(a,b) = d$, $\text{НОК}(a,b) = m$. Тогда $a = xd$ и $b = yd$. Ясно, что $f(\text{НОД}(x,y)) = 1$ (иначе $\text{НОД}(x,y)d$ делил бы a и b и $f(\text{НОД}(x,y)d) > f(d)$, что противоречит выбору $d = \text{НОД}(a,b)$).

Покажем $f(m) \geq f(xyd)$. a и b делят m. Значит,

$$m = ak = bl = xdk = ydl$$
$$xk = yl$$

Из основной теоремы арифметики и $\text{НОД}(x,y) = 1$ следует, что x делит l. Таким образом:

$$m = ydl = yd(xt)$$
$$f(m) = f(ydxt) \geq f(yxd)$$

Ясно, что $\frac{ab}{\text{НОД}(a,b)} = xyd$ делится на a и на b. ■

2. Общие свойства квадратичных расширений целых чисел

Введем для удобства новые обозначения, отличные от данных в условии задачи:

$$\mathbb{Z}[\alpha] = \{a + b\alpha: a, b \in \mathbb{Z}\}$$
$$\mathbb{Q}[\alpha] = \{a + b\alpha: a, b \in \mathbb{Q}\}$$

Через O_K обозначим подмножество множества K, в котором каждый элемент является корнем многочлена второй степени с целыми коэффициентами и старшим коэффициентом равным 1. В этих обозначения $O_{\mathbb{Q}[\sqrt{d}]}$ это $\mathbb{Z}[\sqrt{d}]$ в обозначениях из условия задачи.

Далее будем считать, что d - целое число, которое не делится на квадрат простого числа.

Утверждение 2.0 Если $a, b \neq 0 \in \mathbb{Q}[\sqrt{d}]$, то и $\frac{a}{b} \in \mathbb{Q}[\sqrt{d}]$

Доказательство. $\frac{a}{b} = \frac{x+y\sqrt{d}}{x'-y'\sqrt{d}} = \frac{(x'-y'\sqrt{d})(x+y\sqrt{d})}{x'^2-dy'^2} \in \mathbb{Q}[\sqrt{d}]$ ($x'^2 \neq dy'^2$, так как d не делится на квадрат простого) ■

Пусть $x = a + b\sqrt{d}$ и принадлежит $O_{\mathbb{Q}[\sqrt{d}]}$.

Определение. $\bar{x} = a - b\sqrt{d}$ (x сопряженное)

Утверждение 2.1. Пусть $b \neq 0$. Тогда x является корнем только одного многочлена второй степени с целыми коэффициентами и старшим коэффициентом равным 1: $x^2 - 2ax + a^2 - db^2$. Если $b = 0$, то x это целое число и является корнем того же уравнения, но не только его.

Доказательство. Пусть x корень уравнения $x^2 + px + q = 0$, где p и q целые. У этого уравнения есть два корня. Второй обозначим за y. По теореме Виета:

$$-p = x + y = a + b\sqrt{d} + y$$

Чтобы p было целым $y = -b\sqrt{d} + c$, где c рациональное. По теореме Виета:

$$q = xy = \left(a + b\sqrt{d}\right)\left(c - b\sqrt{d}\right) = ac - b^2d + (bc - ab)\sqrt{d}$$
$$= ac - b^2d + b(c - a)\sqrt{d}$$

1) $b \neq 0$. Чтобы q было целым $b(c - a) = 0$. Так как $b \neq 0$, то $c = a$.

Тогда $p = -x - y = -2a$ и $q = xy = a^2 - db^2$. Что и требовалось.

2) $b = 0$. Тогда $-p = a + c$ и $q = ac$. Пусть $a = \frac{s}{t}$, где s и t взаимно простые целые числа. Если $a = 0$ то утверждение верно. Будем считать, что это не так.

$$c = \frac{q}{a} = \frac{qt}{s}$$
$$-p = a + c = \frac{s}{t} + \frac{qt}{s} = \frac{s^2 + qt^2}{ts}$$
Так как $\frac{s^2+qt^2}{ts}$ целое, то t делит $s^2 + qt^2$. Значит, t делит s. Так как t и s взаимно просты, то $t = 1$. Следовательно, x целое число.

Нетрудно убедиться, что x это корень $x^2 - 2ax + a^2 - db^2 = (x-a)^2 = 0$. Но x может быть и корнем других многочленов второй степени с целыми коэффициентами и старшим коэффициентом равным 1. Например $(x-a)(x-a-1) = 0$. ■

Теорема 2.1 Если $d \equiv 1\ (mod\ 4)$, то $O_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Если $d \neq 1\ (mod\ 4)$, то $O_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\sqrt{d}]$.

Доказательство. Пусть $(a + b\sqrt{d})\ \epsilon\ O_{\mathbb{Q}[\sqrt{d}]}$ и является корнем $x^2 + px + q = 0$, где p и q целые. По формуле корней квадратного уравнения
$$a + b\sqrt{d} = \frac{-p + \sqrt{p^2 - 4q}}{2}$$
Значит, $a = \frac{a'}{2}$ и $b = \frac{b'}{2}$, где a’ и b’ целые числа.

Из утверждения 2.1:
$$q = a^2 - db^2 = \frac{a'^2 - db'^2}{4} \Rightarrow a'^2 - db'^2 \equiv 0(mod4) \qquad (1)$$
а) Пусть $d \equiv 1\ (mod\ 4)$.
$$a'^2 - db'^2 \equiv a'^2 - b'^2 = (a' - b')(a' + b') \equiv 0(mod4)$$
Что равносильно тому, что a' и b' имеют одинаковую четность. При этом $-p = a + b = \frac{a'+b'}{2}$ является целым числом. Ясно, что все числа вида $\frac{a+b\sqrt{d}}{2}$, где a и b целые числа одинаковой четности, принадлежат $O_{\mathbb{Q}[\sqrt{d}]}$ и только такие принадлежат.
$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\frac{1+\sqrt{d}}{2} : a, b\ \epsilon\ \mathbb{Z}\right\} = \left\{\frac{(2a+b) + b\sqrt{d}}{2} : a, b\ \epsilon\ \mathbb{Z}\right\}$$
Понятно, что $2a + b$ и b независимо пробегают все пары целых чисел одинаковой четности. Что и требовалось доказать.

б) Пусть $d \neq 1\ (mod\ 4)$. Тогда $d \neq 0\ (mod\ 4)$ (иначе d делилось бы на квадрат простого). Перебором остатков можно убедиться, что $x^2 \equiv 0$ или $1(\ mod\ 4)$. Перебирая остатки по модулю 4 у d, a' и b' в (1) получаем, что a' и b' должны быть четные. Значит a и b целые числа. Ясно, что все числа вида $a+b\sqrt{d}$, где a и b целые числа, принадлежат $O_{\mathbb{Q}[\sqrt{d}]}$ и только такие принадлежат. Следовательно $O_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\sqrt{d}]$. ■

Утверждение 2.2. $\overline{(a+b\sqrt{d})(c+d\sqrt{d})} = \overline{(a+b\sqrt{d})} \cdot \overline{(c+d\sqrt{d})}$

Доказательство. $\overline{xy} = \overline{(a+b\sqrt{d})(c+d\sqrt{d})} = \overline{ac+bdd+(bc+ad)\sqrt{d}} = ac+bdd-(bc+ad)\sqrt{d} = \left(a-b\sqrt{d}\right)\left(c-d\sqrt{d}\right) = \overline{(a+b\sqrt{d})} \cdot \overline{(c+d\sqrt{d})}$ ■

Определение. Норма числа x это $N(x) = x\bar{x} = a^2 - db^2$

Утверждение 2.3. $N\left(\left(a+b\sqrt{d}\right)\left(c+e\sqrt{d}\right)\right) = N\left(a+b\sqrt{d}\right)N\left(c+e\sqrt{d}\right)$

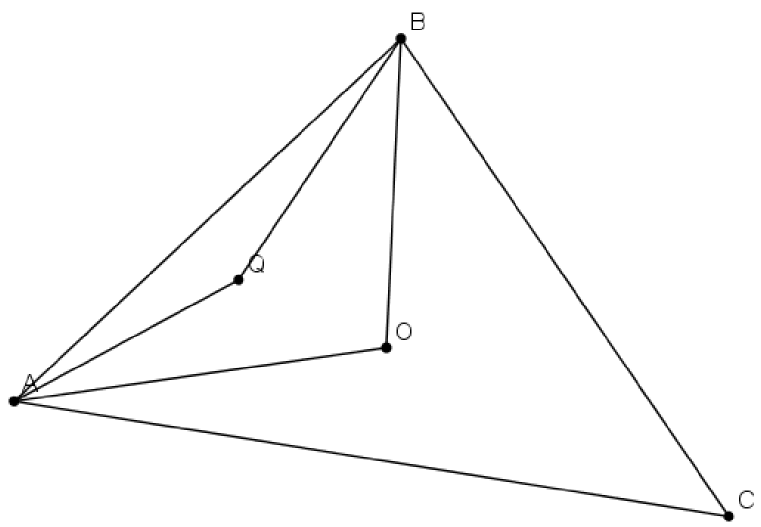
Доказательство. $N\left(\left(a+b\sqrt{d}\right)\left(c+e\sqrt{d}\right)\right) = \left(a+b\sqrt{d}\right)\left(c+e\sqrt{d}\right) \cdot$
$\cdot\, \overline{\left(a+b\sqrt{d}\right)\left(c+e\sqrt{d}\right)} = \left(a+b\sqrt{d}\right)\overline{\left(a+b\sqrt{d}\right)}\left(c+e\sqrt{d}\right)\overline{\left(c+e\sqrt{d}\right)} = N\big(a+$
$+b\sqrt{d}\big)N\left(c+e\sqrt{d}\right)$ ■

Определение. Для множества $\mathbb{Q}\left[\sqrt{d}\right]$ обозначим через $\beta_{\mathbb{Q}[\sqrt{d}]}$ наименьшее действительное число, для которого верно следующее утверждение:

для любого x из $\mathbb{Q}\left[\sqrt{d}\right]$ существует y из $O_{\mathbb{Q}[\sqrt{d}]}$ такой что $N(x-y) \leq \beta_{\mathbb{Q}[\sqrt{d}]}$

Лемма. Пусть дан не тупоугольный треугольник ABC с радиусом описанной окружности R и точка Q внутри его. Тогда $\min(QA, QB, QC) \leq R$.

Доказательство. Обозначим через O центр описанной окружности треугольника ABC. Так как ABC не тупоугольный O лежит внутри или на границе ABC. Можем без ограничения общности считать, что Q лежит внутри или на границе треугольника ABO (который может быть отрезком). По известному неравенству:



$$QA + QB \leq OA + OB = 2R$$

Откуда следует, что $QA \leq R$ или $QB \leq R$. ■

Теорема 2.3 Пусть d натуральное число. Тогда:

$$\beta_{\mathbb{Q}[\sqrt{-d}]} = \begin{cases} \dfrac{(d+1)^2}{16d}, & \text{если} \quad -d \equiv 1 (mod\, 4) \\ \dfrac{d+1}{4}, & \text{если} \quad -d \not\equiv 1 (mod\, 4) \end{cases}$$

Доказательство. Любому комплексному числу $x + yi$ будем ставить в соответствие точку на плоскости (x, y). Ясно, что $N\big((x + yi) - (x' + y'i)\big) = (x - x')^2 + (y - y')^2$ есть квадрат расстояния между точками (x, y) и (x', y').

Тогда $\beta_{\mathbb{Q}[\sqrt{-d}]}$ можно определить как наименьшее действительное число, для которого выполнено следующее: для любого x из $\mathbb{Q}[\sqrt{-d}]$ существует y из $O_{\mathbb{Q}[\sqrt{-d}]}$ такой, что квадрат расстояния между x и y не больше $\beta_{\mathbb{Q}[\sqrt{-d}]}$.

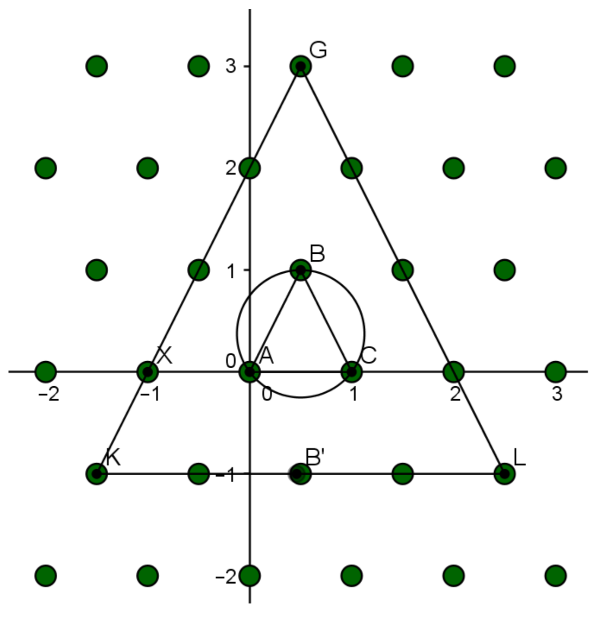
Решим задачу для произвольной целочисленной решетки, а потом подставим $O_{\mathbb{Q}[\sqrt{-d}]}$. Пусть даны два не коллинеарных комплексных числа z_1 и z_2 такие, что треугольник с вершинами 0, z_1 и z_2 не является тупоугольным. Рассмотрим множество:

$$A = \{az_1 + bz_2 : a, b \in \mathbb{Z}\}$$

Будем называть A решёткой, порождённой векторами z_1 и z_2.

Отметим все точки из A на плоскости. Проведем через каждый элемент A две прямые: одну параллельную z_1, а другую параллельную z_2. Получим решетку из равных параллелограммов. Далее проведем прямую через точки z_1 и z_2. Через каждую точку из A проведем прямую параллельную этой. Теперь плоскость разбилась на равные не тупоугольные треугольники (ячейки). Обозначим радиус описанной окружности этого треугольника R.

Пусть x комплексное число. Точка x попадает внутрь или на границу какой-то из ячеек. По лемме одно из расстояний до вершин этой ячейки не превосходит R.



Покажем, что ближайшие элементы из A для центра описанной окружности O одной из ячеек это ее вершины. Пусть O центр описанной окружности треугольника ABC. Рассмотрим треугольник KLM с вершинами в узлах решетки подобный ABC и содержащий ABC строго внутри (см. рис.). Опишем около ABC окружность. Так как $\angle ABC = \angle AB'C \leq 90°$, то B' не лежит строго внутри описанной окружности ABC.

Следовательно $OB' \leq OB$. Ясно, что X не лежит внутри окружности. Итак, описанная окружность треугольника ABC лежит строго внутри треугольника KLM. Следовательно, ближайшая точка из A для O находится на расстоянии R.

Значит, для любой из точек плоскости найдется элемент из A на расстоянии не больше R. Это утверждение неверно для любой другой меньшей константы. Когда $A = O_{\mathbb{Q}[\sqrt{-d}]}$ это и есть определение $\sqrt{\beta_{\mathbb{Q}[\sqrt{-d}]}}$.

а) $-d \not\equiv 1 (mod\ 4)$. Тогда по теореме 2.1:

$$O_{\mathbb{Q}[\sqrt{-d}]} = \mathbb{Z}\left[\sqrt{-d}\right] = \left\{a + b\sqrt{-d}: a, b \in \mathbb{Z}\right\} = \left\{a + b\sqrt{d} \cdot i: a, b \in \mathbb{Z}\right\}$$

Значит эта решетка порождена 1 и $\sqrt{d} \cdot i$. Треугольник с вершинами 0, 1, $\sqrt{d} \cdot i$ прямоугольный и его радиус описанной окружности равен половине гипотенузы равен $\sqrt{\frac{1+d}{4}}$. Следовательно, $\beta_{\mathbb{Q}[\sqrt{-d}]} = \frac{1+d}{4}$.

б) $-d \equiv 1\ (mod\ 4)$. Тогда по теореме 2.1:

$$O_{\mathbb{Q}[\sqrt{-d}]} = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{-d}}{2}\right): a, b \in \mathbb{Z}\right\}$$

Значит, эта решетка порождена 1 и $\frac{1+\sqrt{-d}}{2}$. Треугольник с вершинами 0, 1, $\frac{1+\sqrt{-d}}{2}$ равнобедренный остроугольный. Действительно, при $d = 3$ угол при вершине $\frac{1+\sqrt{-d}}{2}$ равен $60°$, а с ростом d только уменьшается. Нетрудно убедится, что точка $\frac{1}{2} + \frac{d-1}{4d} i$ равноудалена от 0, 1, $\frac{1+\sqrt{-d}}{2}$. Значит, она является центром описанной окружности треугольника. Радиус этой окружности $\sqrt{\frac{(1+d)^2}{16d}}$. Следовательно, $\beta_{\mathbb{Q}[\sqrt{-d}]} = \frac{(1+d)^2}{16d}$. ■

Теорема 2.4 Пусть α не рациональный корень многочлена с целыми коэффициентами: $x^2 + px + q = 0$. Пусть $0 \neq x = a + b\alpha \in \mathbb{Z}[\alpha]$. Тогда количество классов эквивалентности в $\mathbb{Z}[\alpha]$, по отношению $a - b$ делится на x, равно $|a^2 - abp + b^2 q|$.

Доказательство. Заметим, что $\alpha = \frac{-p \pm \sqrt{p^2-4q}}{2}$. Так как α иррационально, то $\sqrt{p^2 - 4q}$ иррационально.

Для каждого $c + d\alpha$ на плоскости отметим точку с координатами (c, d). Рассмотрим множество всех кратных x:

$$A = \{(c + d\alpha)(a + b\alpha): c, d \epsilon \mathbb{Z}[\alpha]\}$$
$$= \{c(a + b\alpha) + d(-bq + (a - bp)\alpha): c, d \epsilon \mathbb{Z}[\alpha]\}$$

Соответствующее A множество точек на плоскости это решетка порожденная векторами $\overrightarrow{(a, b)}$ и $\overrightarrow{(-bq, a - bp)}$. Площадь одной ячейки-параллелограмма это

$$S = \left| det \begin{pmatrix} a & -bq \\ b & a - bp \end{pmatrix} \right| = |a^2 - abp + b^2 q|$$

Покажем, что $S \neq 0$. Это значит, что векторы $\overrightarrow{(a, b)}$ и $\overrightarrow{(-bq, a - bp)}$ не коллинеарны. Пусть $S = 0$. Тогда $a^2 - abp + b^2 q = 0$. Так как $0 \neq x$, то $a \neq 0$ или $b \neq 0$.

1) Пусть $a \neq 0$. Тогда $1 - \frac{b}{a} p + \left(\frac{b}{a}\right)^2 q = 0$

$$\frac{b}{a} = \frac{-p \pm \sqrt{p^2 - 4q}}{2q}$$

Что противоречит тому, что $\frac{b}{a} \epsilon \mathbb{Q}$

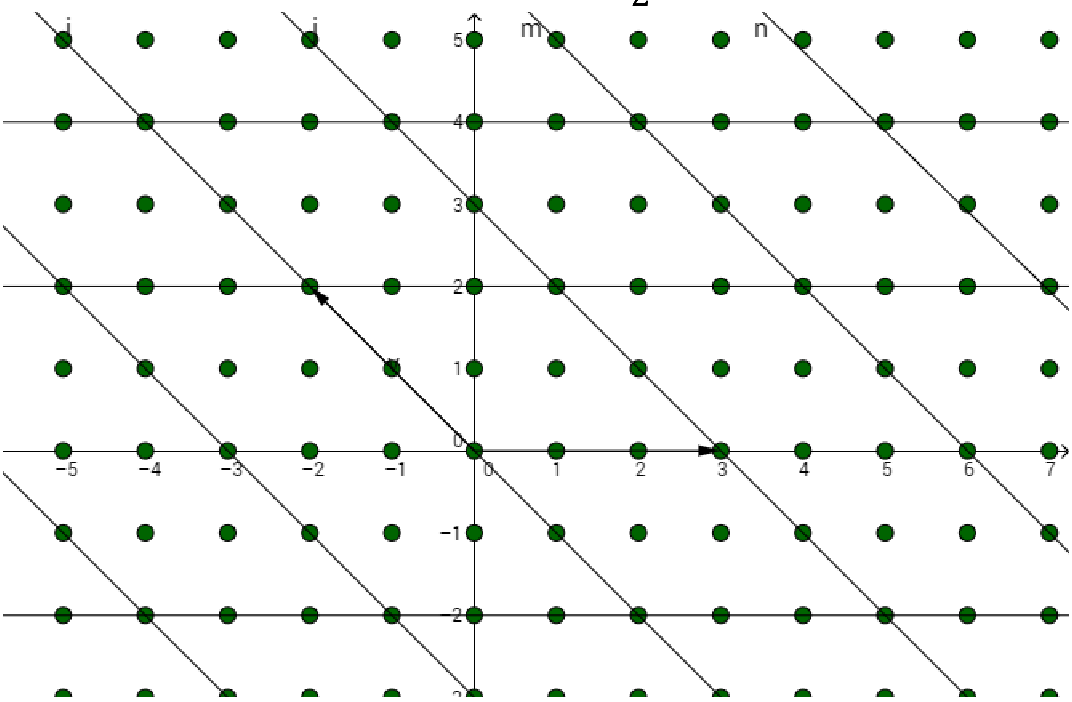
2) Пусть $b \neq 0$. Тогда $\left(\frac{a}{b}\right)^2 - q \frac{a}{b} + p = 0$

$$\frac{a}{b} = \frac{q \pm \sqrt{p^2 - 4q}}{2}$$

Что противоречит тому, что $\frac{b}{a} \epsilon \mathbb{Q}$

По формуле Пика:

$$S = N + \frac{B - 2}{2}$$



Где N – количество целых точек строго внутри ячейки, B – количество целых точек на границе ячейки. Так как ячейка это параллелограмм противолежащие стороны равны и параллельны, значит S это количество целых точек строго внутри ячейки и на векторах $\overrightarrow{(a,b)}$ и $\overrightarrow{(-bq,a-bp)}$ не включая точки (a,b) и $(-bq,a-bp)$. Обозначим множество этих точек C. Ясно, что

$$C=\{x(a,b)+y(-bq,a-bp):0\leq x,y<1\}\cap\mathbb{Z}^2$$

Покажем, что любые два элемента из C не принадлежат одному классу эквивалентности. Допустим противное. То есть $y,z\,\epsilon\,C$ и $z-y\,\epsilon\,A$. Ясно, что все элементы C единственным образом раскладываются по базису $\overrightarrow{(a,b)}$ и $\overrightarrow{(-bq,a-bp)}$:

$$z=z_1(a,b)+z_2(-bq,a-bp)$$
$$y=y_1(a,b)+y_2(-bq,a-bp)$$

при этом $0\leq z_1,z_2,y_1,y_2<1$, так как z и y внутри параллелограмма на векторах $\overrightarrow{(a,b)}$ и $\overrightarrow{(-bq,a-bp)}$.

$$z-y=(z_1-y_1)(a,b)+(z_2-y_2)(-bq,a-bp)$$

Так как $x-y\,\epsilon\,A$, то z_1-y_1 и z_2-y_2 целые числа. Учитывая

$$-1<z_1-y_1<1$$
$$-1<z_2-y_2<1$$

Получаем $z_1-y_1=0=z_2-y_2$. Но тогда $x=y$. Противоречие.

Пусть $z=z_1(a,b)+z_2(-bq,a-bp)$ и $y=y_1(a,b)+y_2(-bq,a-bp)$ – целочисленные точки. Ясно, что $z-y$ делится на $a+b\alpha$ только когда $z_1-y_1\in\mathbb{Z}$ и $z_2-y_2\in\mathbb{Z}$. Чтобы z было эквивалентно y, нужно чтобы $\{z_1\}(a,b)+\{z_2\}(-bq,a-bp)=\{y_1\}(a,b)+\{y_2\}(-bq,a-bp)$. Заметим, что $\{z_1\}(a,b)+\{z_2\}(-bq,a-bp)=x-[z_1](a,b)+[z_1](-bq,a-bp)\in\mathbb{Z}^2$. Значит, $(\{z_1\}(a,b)+\{z_2\}(-bq,a-bp))\in$ C.

Таким образом, классов эквивалентности ровно $|a^2-abp+b^2q|$. ■

Применим теорему 2.4 для множества $O_{\mathbb{Q}[\sqrt{d}]}=\mathbb{Z}[\alpha]$. Мы знаем, что $\sqrt{d}$ это корень $x^2-d=0$, а $\frac{1+\sqrt{d}}{2}$ корень $x^2-x-\frac{d-1}{4}=0$. Легко проверить, что в любом случае количество классов эквивалентности по модулю $a+b\alpha$ равно $N(a+b\alpha)$.

Это аналогично случаю целых чисел, где количество классов эквивалентности по модулю q равно $|q|$.

3 Решение задачи

Пункт 1

С Z все понятно.

$$Z[i] = O_{\mathbb{Q}[\sqrt{-1}]}$$

$$Z[\omega] = Z\left[\frac{-1+\sqrt{-3}}{2}\right] = Z\left[\frac{1+\sqrt{-3}}{2}\right] = O_{\mathbb{Q}[\sqrt{-3}]}$$

Поэтому будем решать задачу для общего случая $O_{\mathbb{Q}[\sqrt{d}]}$. Явный вид $O_{\mathbb{Q}[\sqrt{d}]}$ предоставлен в теореме 2.1. Пусть $O_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\alpha]$.

Пункт 2

Докажем теперь, что $O_{\mathbb{Q}[\sqrt{d}]}$ является допустимым.

1) $0, 1 \epsilon O_{\mathbb{Q}[\sqrt{d}]}$

2) Пусть $a, b \epsilon O_{\mathbb{Q}[\sqrt{d}]}$. Ясно, что $a+b, a-b \epsilon O_{\mathbb{Q}[\sqrt{d}]}$.

Заметим, что $\sqrt{d}$ и $\frac{1+\sqrt{d}}{2}$ (когда $d \equiv 1 (mod\ 4)$) являются корнями следующих уравнений второй степени с целыми коэффициентами соответственно: $x^2 = d$ и $x^2 = x + \frac{d-1}{4}$. Поэтому при перемножении чисел a и b слагаемое с α^2 можно заменить на выражение с меньшей степенью α. А значит $ab \epsilon O_{\mathbb{Q}[\sqrt{d}]}$.

3) $f(a+b\sqrt{d}\,) = \left|N(a+b\sqrt{d}\,)\right| = |a^2 - db^2|$. Согласно утверждению 2.1 $a^2 - db^2$ это последний коэффициент многочлена, корнем которого является $a + +b\sqrt{d}$. Значит, $|a^2 - db^2|$ - целое неотрицательное число.

Покажем, что $N(x) = 0 \Rightarrow x = 0$. Пусть это не так. $x = a + b\sqrt{d}$. Тогда или a, или b не равно 0. А из $|a^2 - db^2| = 0 \Rightarrow a^2 = db^2$ следует, что ни a ни b не равно 0. Поэтому можем поделить на b^2: $d = \left(\frac{a}{b}\right)^2$ что противоречит тому, что d не делится на квадрат простого.

Пусть $y \epsilon O_{\mathbb{Q}[\sqrt{d}]}$. Значит если x ненулевой элемент, то $N(x) \neq 0$ и можем записать:

$$|N(xy)| = |N(x)| \cdot |N(y)| \geq |N(y)|$$

что и требовалось доказать.

Посчитаем $f\left(a + b\,\frac{1+\sqrt{d}}{2}\right) = f\left(\frac{2a+b}{2} + \frac{b}{2}\sqrt{d}\right) = \left|\left(\frac{2a+b}{2}\right)^2 - d\left(\frac{b}{2}\right)^2\right| = \left|a^2 + ab + \frac{-d+1}{4}b^2\right|$.

Пункт 3

Докажем для начала равносильность возможности деления в $O_{\mathbb{Q}[\sqrt{d}]}$ следующему:

для любого $x \epsilon \mathbb{Q}\left[\sqrt{d}\right]$ существует $y \epsilon O_{\mathbb{Q}[\sqrt{d}]}$ такой что $|N(x-y)| < 1$ (1)

Выведем утверждение (1) из возможности деления. Ясно, что любой $x \epsilon \mathbb{Q}\left[\sqrt{d}\right]$ можно представить в виде $\frac{a+b\alpha}{c}$ где a, b, c целые числа. Поделим с остатком $a + b\alpha$ на c: $a + b\alpha = cz + r, f(r) < f(c)$

$$f(a + b\alpha - cz) < f(c)$$

$$\frac{f(a + b\alpha - cz)}{f(c)} < 1$$

$$f\left(\frac{a + b\alpha}{c} - z\right) < 1$$

Что и требовалось доказать.

Докажем в другую сторону. То есть из (1) выведем возможность деления. Пусть хотим поделить a на b, $a, b \epsilon O_{\mathbb{Q}[\sqrt{d}]}$. Для числа $\frac{a}{b}$ (которое принадлежит $\mathbb{Q}\left[\sqrt{d}\right]$ согласно утверждению 2.0) найдется $q \epsilon O_{\mathbb{Q}[\sqrt{d}]}$такой что

$$f\left(\frac{a}{b} - q\right) < 1$$

$$f(a - qb) < f(b)$$

Тогда q это неполное частное, а $a - qb$ остаток при делении а на b. Таким образом два определения равносильны.

Теперь ясно, что деление с остатком возможно в $O_{\mathbb{Q}[\sqrt{d}]}$ тогда и только тогда $\beta_{\mathbb{Q}[\sqrt{d}]} < 1$.

Для $d < 0$ можно воспользоваться теоремой 2.3. Легко получить, что деление возможно только в $\mathbb{Q}\left[\sqrt{-1}\right], \mathbb{Q}\left[\sqrt{-2}\right], \mathbb{Q}\left[\sqrt{-3}\right], \mathbb{Q}\left[\sqrt{-7}\right], \mathbb{Q}\left[\sqrt{-11}\right]$.

Рассмотрим $d > 0$. Нам потребуется следующая теорема, доказанная в [1]:

Теорема. Пусть дана функция $f(x, y) = ax^2 + bxy + cy^2$, где $a, b, c \epsilon \mathbb{Q}$, которая принимает как положительные, так и отрицательные значения. Тогда существуют $x_0, y_0 \epsilon \mathbb{Q}$ такие что для любых $x, y \epsilon \mathbb{Z}$ выполнено:

$$|f(x_0 + x, y_0 + y)| \geq \frac{\sqrt{b^2 - 4ac}}{48}$$

Пусть $a + b\alpha \epsilon O_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\alpha]$. Рассмотрим $f(x, y) = N(x + \alpha y)$.

1) $d \equiv 2 \text{ или } 3 (mod\ 4), \alpha = \sqrt{d}$

$$f(x, y) = N\left(x + \sqrt{d}y\right) = x^2 - dy^2$$

Заметим, что $f(0,1) < 0$ и $f(1,0) > 0$. Значит, можем применить теорему. То есть существуют $x_0, y_0 \in \mathbb{Q}$ такие что для любых $x, y \in \mathbb{Z}$ выполнено

$$|f(x_0 + x, y_0 + y)| = \left|N\left(x_0 + x + \sqrt{d}(y_0 + y)\right)\right| = \left|N\left(x_0 + \sqrt{d}y_0 - \left(-x - \sqrt{d}y\right)\right)\right|$$
$$\geq \frac{\sqrt{4d}}{48} = \frac{\sqrt{d}}{24}$$

Следовательно, $\beta_{\mathbb{Q}[\sqrt{d}]} \geq \frac{\sqrt{d}}{24}$. Получаем, что при $d \geq 24^2$ в $O_{\mathbb{Q}[\sqrt{d}]}$ деление невозможно.

2) $d \equiv 1 (mod\ 4)$, $\alpha = \frac{1+\sqrt{d}}{2}$

$$f(x,y) = N\left(x + \frac{1+\sqrt{d}}{2}y\right) = x^2 + xy + \frac{-d+1}{4}y^2$$

Заметим, что $f(0,1) < 0$ и $f(1,0) > 0$. Значит, можем применить теорему. То есть существуют $x_0, y_0 \in \mathbb{Q}$ такие что для любых $x, y \in \mathbb{Z}$ выполнено

$$|f(x_0 + x, y_0 + y)| = \left|N\left(x_0 + x + \frac{1+\sqrt{d}}{2}(y_0 + y)\right)\right|$$
$$= \left|N\left(x_0 + \frac{1+\sqrt{d}}{2}y_0 - \left(-x - y\frac{1+\sqrt{d}}{2}\right)\right)\right| \geq \frac{\sqrt{d}}{48}$$

Следовательно, $\beta_{\mathbb{Q}[\sqrt{d}]} \geq \frac{\sqrt{d}}{48}$. Получаем, что при $d \geq 48^2$ в $O_{\mathbb{Q}[\sqrt{d}]}$ деление невозможно.

Согласно [2] деление возможно только при $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$.

Пункт 4

Алгоритм 1 (работает для $-8 < d < 4$)

Пусть в допустимом множестве $O_{\mathbb{Q}[\sqrt{d}]}$ можно делить.

Хотим поделить a на b. Поделим a на b как в утверждении 2.0:

$$\frac{a}{b} = s + t\sqrt{d}$$

Если $d \equiv 1 (mod\ 4)$, то заменим s на $s + \frac{t}{2}$, а t на $\frac{t}{2}$. Тогда получим:

$$\frac{a}{b} = s + t\frac{\left(1 + \sqrt{d}\right)}{2}$$

Таким образом, в любом случае имеем:

$$\frac{a}{b} = s + t\alpha$$

Округлим s и t до ближайшего целого. То есть возьмем целые c и e такие что:

$$|s-c| \le \frac{1}{2}, |t-e| \le \frac{1}{2}$$

Докажем, что число $c + e\alpha$ является неполным частным, а $a - bc$ остатком при делении a на b. Для этого достаточно показать:

$$f(a-bc) < f(b) \Leftrightarrow f\left(\frac{a}{b} - c\right) < 1 \Leftrightarrow f(s + t\alpha - c) < 1 \Leftrightarrow$$
$$f\big((s-c) + (t-e)\alpha\big) < 1$$

1) $d \equiv 1(mod\ 4)$. $\alpha = \frac{1+\sqrt{d}}{2}$

$$f\left((s-c) + (t-e)\frac{1+\sqrt{d}}{2}\right) = \left|(s-c)^2 + (s-c)(t-e) + \frac{-d+1}{4}(t-e)^2\right|$$

Учитывая $|s-c| \le \frac{1}{2}, |t-d| \le \frac{1}{2}$, получаем:

$$\left|(s-c)^2 + (s-c)(t-e) + \frac{-d+1}{4}(t-e)^2\right|$$
$$\le |(s-c)^2| + |(s-c)(t-e)| + \left|\frac{-d+1}{4}(t-e)^2\right| \le \frac{1}{2} + \frac{1-d}{16}$$

В этом случае d может быть равно только -3 или -7. Поэтому:

$$f\left((s-c) + (t-e)\frac{1+\sqrt{d}}{2}\right) \le \frac{1}{2} + \frac{1-d}{16} \le 1$$

Равенство достигается только когда $s-c$ и $t-e$ одного знака, $d = 7$ и $(s-c)^2 = (t-e)^2 = \frac{1}{4}$. В этом случае мы заменяем c на $c+1$ или $c-1$ так, чтобы $|s-c|$ осталось $\frac{1}{2}$, а знак $s-c$ поменялся. Тогда:

$$f\left((s-c) + (t-e)\frac{1+\sqrt{d}}{2}\right) = \left|(s-c)^2 + (s-c)(t-e) + \frac{-d+1}{4}(t-e)^2\right|$$
$$= \frac{1}{4} - \frac{1}{4} + \frac{7+1}{4} \cdot \frac{1}{4} = \frac{1}{2} < 1$$

2) $d \ne 1(mod\ 4)$. $\alpha = \sqrt{d}$

$$f\left((s-c) + (t-e)\sqrt{d}\right) = |(s-c)^2 - d(t-e)^2|$$

Учитывая $|s-c| \le \frac{1}{2}, |t-e| \le \frac{1}{2}$ получаем:

$$|(s-c)^2 - d(t-e)^2| \le |(s-c)^2| + |-d| \cdot |(t-e)^2| \le \frac{|d|}{4} + \frac{1}{4}$$

В пункте 3 было получено, что в этом случае d может быть только $2, 3, -1$ или -2. Поэтому $f\left((s-c)+(t-e)\sqrt{d}\right) \le \frac{3}{4}+\frac{1}{4}=1$. Равенство может достигается только в случае $d=3$ и $(s-c)^2=(t-e)^2=\frac{1}{4}$, но в этом случае:

$$f\left((s-c)+(t-e)\sqrt{d}\right)=|(s-c)^2-d(t-e)^2|=\frac{1}{2}$$

Значит $f\left((s-c)+(t-e)\sqrt{d}\right)<1$.

Алгоритм 2 (работает для $d=-11$)

В этом случае алгоритмом 1 делить не всегда получится. Хотим поделить a на b.Так же как и в алгоритме 1 определим s, t, но c и e по-другому:

$$c=[s], e=[t]$$

Тогда $A=\{(\mathrm{c}+e\alpha)b, (\mathrm{c}+1+e\alpha)b, (\mathrm{c}+(e+1)\alpha)b, (\mathrm{c}+1+(e+1)\alpha)b\}$ являются вершинами параллелограмма, в целочисленной решетке порожденной b и αb, который содержит a. Из рассуждений теоремы 2.2 следует, что от точки а до одной из точек A квадрат расстояния меньше 1. Значит, эта точка есть неполное частное. Теперь легко найти остаток.

Алгоритм 3 (работает для $d=2,3,6,7$)

Пусть хотим поделить с остатком a на b. Пусть $\frac{a}{b}=p+q\sqrt{d}$. Будем искать целые x, y такие что

$$\left|N\left(\frac{a}{b}-x-y\sqrt{d}\right)\right|=\left|N\left(p-x+(q-y)\sqrt{d}\right)\right|=|(p-x)^2-d(q-y)^2|<1 \qquad (1)$$

$x+y\sqrt{d}$ будет неполным частным.

Сделаем замену $p\to\epsilon p+u$, $x\to\epsilon x+u$, где $\epsilon=1$ или -1 и u целое число такие что $0\le\epsilon p+u\le\frac{1}{2}$. При такой замене уравнение (1) не изменилось. Аналогичную замену сделаем для q и y. Теперь можем считать, что $0\le p, q\le\frac{1}{2}$.

Покажем, что одна из пар $(x, y)=\{(0{,}0), (1{,}0), (-1{,}0)\}$ подходит. Пусть это не так. То есть для каждой из пар $|(p-x)^2-d(q-y)^2|\ge 1$. Значит, выполнены три условия:

1) $p^2-dq^2\ge 1$ или $p^2-dq^2\le -1$

2) $(p-1)^2-dq^2\ge 1$ или $(p-1)^2-dq^2\le -1$

3) $(p+1)^2-dq^2\ge 1$ или $(p+1)^2-dq^2\le -1$

Из 1) следует, что p и q не оба нули. Учитывая это, первая часть условия 2) не выполняется. Значит, выполнена вторая. Пусть верна первая часть условия 3). Комбинируя это с условием 2

$$(p+1)^2-1-(p-1)^2\ge(p+1)^2-dq^2\ge 1 \qquad (2)$$

$$p \geq \frac{1}{2} \Rightarrow p = \frac{1}{2}$$

(2) можно переписать так

$$\frac{5}{4} = -1 + (p+1)^2 \geq dq^2 \geq 1 + (p-1)^2 = \frac{5}{4}$$

Значит $dq^2 = \frac{5}{4}$ или $d(2q)^2 = 5 \Rightarrow d|5 \Rightarrow d = 1 \text{ или } 5$, что невозможно. Таким образом, первая часть условия 3) не выполняется и верна вторая часть:

$$2 \leq (p+1)^2 + 1 \leq dq^2$$
$$d \geq 8$$

Но в этом алгоритме $d < 8$. Противоречие. Значит одна из пар $(x, y) = \{(0,0), (1,0), (-1,0)\}$ подходит и обратными заменами можем получить начальное $x + y\sqrt{d}$.

Алгоритм 4 (работает для $d = 5, 13, 17, 21, 29$)

Будем действовать аналогично предыдущему алгоритму. Пусть хотим поделить с остатком a на b. Пусть $\frac{a}{b} = p + q\frac{1+\sqrt{d}}{2}$. Будем искать целые x, y такие что

$$\left|N\left(\frac{a}{b} - x - y\frac{1+\sqrt{d}}{2}\right)\right| = \left|N\left(p - x - \frac{y}{2} + \left(q - \frac{y}{2}\right)\sqrt{d}\right)\right| =$$
$$= \left|\left(p - x - \frac{y}{2}\right)^2 - d\left(q - \frac{y}{2}\right)^2\right| = \left|\left(p - x - \frac{y}{2}\right)^2 - \frac{d}{4}(2q - y)^2\right| < 1$$

Заменим $2q$ на q.

$$\left|N\left(\frac{a}{b} - x - y\frac{1+\sqrt{d}}{2}\right)\right| = \left|\left(p - x - \frac{y}{2}\right)^2 - \frac{d}{4}(q - y)^2\right|$$

Заменим (p, x, q, y) на $(\epsilon p + u, \epsilon x + u, \epsilon q, \epsilon y)$ где $\epsilon = \pm 1$ так чтобы $0 \leq \epsilon p + u \leq \frac{1}{2}$. Можем считать, что $0 \leq r \leq \frac{1}{2}$.

Заменим (p, x, q, y) на $(p, x - v, q + 2v, y + 2v)$, так чтобы $-1 \leq q + 2v \leq 1$. Можем считать, что $-1 \leq q \leq 1$.

Если $q < 0$, то заменим (p, x, q, y) на $(p, x + y, -q, -y)$. Можем считать, что $0 \leq q \leq 1$.

Если $\frac{1}{2} \leq q \leq 1$, то заменим (p, x, q, y) на $\left(\frac{1}{2} - p, -x, 1 - q, 1 - y\right)$. Можем считать, что $0 \leq q \leq \frac{1}{2}$.

Покажем, что одна из пар $(x, y) = \{(0,0), (1,0), (-1,0)\}$ подходит. Пусть это не так. То есть для каждой из пар $\left|\left(p - x - \frac{y}{2}\right)^2 - \frac{d}{4}(q - y)^2\right| \geq 1$. Значит, выполнены три условия:

1) $p^2 - \frac{d}{4}q^2 \geq 1$ или $p^2 - \frac{d}{4}q^2 \leq -1$

2) $(p-1)^2 - \frac{d}{4}q^2 \geq 1$ или $(p-1)^2 - \frac{d}{4}q^2 \leq -1$

3) $(p+1)^2 - \frac{d}{4}q^2 \geq 1$ или $(p+1)^2 - \frac{d}{4}q^2 \leq -1$

Условия аналогичны предыдущему алгоритму. Если первая часть условия 3) верна, то можно получить

$$\frac{d}{4}q^2 = \frac{5}{4}$$

$$q^2 = \frac{5}{d}$$

Так как d не делится на квадрат простого, то $d = 5$ и $q = 1$. Противоречие с выбором $q \leq \frac{1}{2}$.

Значит вторая часть условия 3) верна и

$$2 \leq (p+1)^2 + 1 \leq \frac{\mathrm{d}}{4}q^2$$

$$d \geq 32$$

Но в этом случае $d < 32$. Противоречие. Значит одна из пар $(x, y) = \{(0,0), (1,0), (-1,0)\}$ подходит и обратными заменами можем получить начальное $x + y\sqrt{d}$.

Пункт 5

Числа n и n-1, где n целое всегда принадлежат $O_{\mathbb{Q}[\sqrt{d}]}$. Поделим n-1 на n:

$$n - 1 = 0n + n - 1, f(n-1) < f(n)$$

$$f(n-1) \leq \alpha_{O_{\mathbb{Q}[\sqrt{d}]}} f(n)$$

$$\left|\left(1 - \frac{1}{n}\right)^2\right| = f\left(\frac{n-1}{n}\right) \leq \alpha_{O_{\mathbb{Q}[\sqrt{d}]}}$$

При достаточно большом n $\left(1 - \frac{1}{n}\right)^2$ может быть насколько угодно близко к 1. Поэтому $\alpha_{O_{\mathbb{Q}[\sqrt{d}]}} \geq 1$. С другой стороны $\alpha_{O_{\mathbb{Q}[\sqrt{d}]}} = 1$ подходит.

Следуя рассуждениям доказательства равносильности иного определения деления из пункта 3 легко видеть, что $\beta_{\mathbb{Q}[\sqrt{d}]}$ можно считать наименьшей константой такой, что для любых ненулевых $a, b \in O_{\mathbb{Q}[\sqrt{d}]}$ ***существует*** такой остаток r при делении a на b, что $f(r) \leq \beta_{Q[\sqrt{d}]} f(b)$.

Исходя из различных значений констант α и β их определения не эквивалентны. Это значит, что деление с остатком в рассматриваемых множествах не единственно. Действительно можно несколькими способами поделить $-1+4i$ на $2+i$ в $O_{\mathbb{Q}[\sqrt{-1}]}$:

$$-1+4i=(2+i)(2i)+1=(2+i)(1+2i)+(-1-i)=(2+i)(i)+2i$$

Пункт 6

По ходу решения было сделано множество обобщений, особенно в разделах 1 и 2. Перечислим основные полученные свойства допустимых множеств с делением:

1) верна основная теорема арифметики

2) работает алгоритм Евклида для нахождения НОД

3) верна формула для поиска НОК

Основные результаты в исследовании множеств $O_{\mathbb{Q}[\sqrt{d}]}$:

1) описан вид

2) доказана мультипликативность нормы

3) вычислена константа β для отрицательного d и оценена для положительного d

4) доказано, что количество классов эквивалентности по любому модулю z это $|N(z)|$. Это число является количеством классов остатков если в $O_{\mathbb{Q}[\sqrt{d}]}$ можно делить.

Таким образом, множество $O_{\mathbb{Q}[\sqrt{d}]}$ обладает многими свойствами присущими целым числа.

Литература

[1] J. W. S. Cassels, The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms

[2] Euclidean domain – Norm-Euclidean fields https://en.wikipedia.org/wiki/Euclidean_domain#Norm-Euclidean_fields

[3] G. H. Hardy, E. M. Wright, An Introduction to the theory of numbers