Георгий Потошин, 2024

Алгебра I, листочек 5

1. **Опишите все простые и максимальные идеалы в кольцах $\mathbb{Z}/n\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ – поле.**

   Как мы видели оба эти кольца – кольца главных идеалов. Первое, так как это фактор кольца главных идеалов, а второе целостное и имеет деление с остатком, а значит КГИ, тогда дальше все идеалы главные.

   $\Bbbk[x]$ целостно и КГИ, а значит все простые идеалы – главные идеалы неприводимых элементов. Тогда это описание сводится к описанию всех неприводимых элементов, в $\mathbb{C}$ неприводимы например только полиномы степени 1. Так как $\Bbbk[x]$ целостное кольцо главных идеалов, то простые идеалы максимальны. Так как для простых идеалов верно $(a) \subseteq (p)$, а значит $p = au$, но так как p неприводим и a не обратим, то обратим u, а значит $(a) = (p)$.

   Кольцо $\mathbb{Z}/(n)$ в общем случае не целостно. Посмотрим на каноническую проекцию $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/(n)$. Так как прообразы простых идеалов просты, то как минимум нужно рассматривать образы простых из $\mathbb{Z}$. Пусть $(p) \subset \mathbb{Z}$ – простой идеал, тогда $\pi[(p)] = ([1])$, если $p \wedge n = 1$ и $\pi[(p)] = ([p])$ – собственный идеал фактор кольца в противном. Покажем, что во втором случае мы получим простой идеал. Если $p = ab + m$, то ab делится на p, а значит на простое p делится и один из множителей. Это означает, что $([p])$ – простое. Так мы получили, что все простые идеалы имеют вид $([p])$, где p прост и делит n. Каждый простой идеал в данном случаем будет максимальным, так как они образы максимальных из $\mathbb{Z}$ при сюрьективном гомоморфизме, то есть, если $([a]) \subseteq ([p])$, то $(a) = (p)$ по максимальности второго, а тогда и $([a]) = ([p])$.

2. **Элемент x кольца A называется простым, если порожденный им идеал (x) прост. Необратимый элемент x целостного кольца A называется неприводимым, если его нельзя представить в виде произведения двух необратимых элементов A.**

   Покажите, что в целостном кольце ненулевой простой элемент неприводим. Покажите, что обратное, вообще говоря, неверно. Покажите, что в факториальных кольцах неприводимые элементы просты.

   Пусть A – целостно и $p \neq 0$ прост. Тогда если $p = ab$, то без потери общности положим $a \in (p)$. Тогда $a = pc$ и $p = pcb$. Перенесем все в одну сторону $p(1 - cb) = 1$. Так как кольцо целостно и p не нуль, то $1 = cb$ и b обратим. А значит p неприводимо. Покажем на примере, что обратное не верно.

   Возьмём $\mathbb{Z}[i\sqrt{5}]$ оно целостно, так как подкольцо поля. Покажем, что 2 в нем неприводим. Норма $x = a + i\sqrt{5}b$ равна $a^2 + 5b^2$, если $xy = 2$, то будет верно, что $|x|^2|y|^2 = 4$, то есть произведение двух целых чисел равно 4. Что бы они не были обратимыми, нужно чтобы оба числа равнялись 2. Но $a^2 + 5b^2 = 2$ не имеет целых решение, так как b не может быть не нулём, а 2 не квадрат. А значит 2 неприводим. С другой стороны $(1+i\sqrt{5})(1-i\sqrt{5}) = 6 \in (2)$, но ни одно множимое там не лежит, так 2 их не делит, а значит 2 не прост.

   Пусть теперь x не прост, тогда мы найдём $a, b \notin (x)$, но $ab \in (x)$. Заметим, что они оба не нули и оба необратимы, в противном случае если a обратим, то $ab \in (x) \Rightarrow b = a^{-1}ab \in (x)$, что не верно. Тогда в каком-нибудь разложении на неприводимы в a и b неприводимых будет не меньше 1, иначе они обратимы, тогда по факториальности кольца в x неприводимых не меньше 2, но тогда x не неприводим, так как в факториальном кольце в разложении неприводимых всегда только одно неприводимое.

3. **Пусть A – ненулевое кольцо. Следующие утверждения равносильны:**

   (a) A **– поле,**

   (b) **в** A **нет идеалов, кроме** (0) **и** (1)**,**

   (c) **любой гомоморфизм из A в ненулевое кольцо инъективен**

   (a)⇒(b): Ненулевые элементы поля необратимы, а значит если идеал содержит что-то помимо нуля, то он всё поле.

   (b)⇒(c): Пусть в кольце A только 2 идеала, и $f : A \to B$ ядро f - идеал в a, так как единица переходит в 1, то ядро не всё кольцо, а идеал не равный кольцу – только (0), а значит f инъективен.

(c)⇒(b): Пусть $a \in A \setminus \{0\}$, $\pi : A \longrightarrow A/(a)$ - нетнъективный гомоморфизм колец, а значит кообласть нулевое кольцо, а тогда $(a) = A$, а значит a обратим. Это верно для любого ненулевого элемента, а значит A - поле.

4. **Элемент $0 \neq x \in A$ называется нильпотентом, если $x^n = 0$ для некоторого n. Докажите, что множество всех нильпотентов в A является идеалом. Он называется нильрадикалом кольца A и обозначается $\mathfrak{N}(A)$. Покажите, что в фактор-кольце $A/\mathfrak{N}(A)$ нет нильпотентов.**

   Пусть $x, y \in A$ нильпотенты и $a \in A$ в коммутативном кольце. Тогда $x^n = 0 \Rightarrow (ax)^n = 0$ и $x^n = 0 = y^m \Rightarrow (x+y)^{n+m} = 0$, а значит нильрадикал идеал. Пусть $[a] \in A/\mathfrak{N}(A)$ такой, что $[a]^n = 0$, тогда мы $a^n \in \mathfrak{A}$, а значит $(a^n)^m = 0$ и a – нильпотент, а тогда $a \in \mathfrak{N}$ и $[a] = [0]$. Тогда в фактор кольце нет делителей нуля.

5. **Докажите, что нильрадикал кольца A совпадает с пересечением всех простых идеалов A.**

   Пусть a нильпотент, тогда $a^n = 0 \in \mathfrak{p}$, но так как идеал прост, то значит $a \in \mathfrak{p}$ для любого простого идеала $\mathfrak{p}$. Теперь пусть a не нильпотент. Пусть S множество всех идеалов, что не содержат никакую степень a, это множество замкнуто относительно объединений цепей и не пусто, так как содержит (0). Тогда любая цепь имеет верхнюю грань, а значит по лемме Цорна есть максимальный элемент $\mathfrak{p}$. Пусть $x, y \notin \mathfrak{p}$. Тогда $(x) + \mathfrak{p}$ и $(y) + \mathfrak{p}$ строго больше $\mathfrak{p}$, а значит не лежат в S, тогда в них есть некоторые степени a, тогда они же есть в их произведении $(xy) + \mathfrak{p}$, а значит и этот идеал строго больше $\mathfrak{p}$, а тогда $xy \notin \mathfrak{p}$. Значит $\mathfrak{p}$ прост и не содержит a. Тогда не нильпотенты не лежат в пресечении всех простых идеалов.

6. **Радикалом Джекобсона $\mathfrak{R}(A)$ кольца A называется пересечение всех максимальных идеалов в A. Докажите, что $x \in \mathfrak{R}(A)$ эквивалентно тому, что $1 - xy$ является обратимым элементов для всех $y \in A$.**

   Пусть $x \in \mathfrak{R}(A)$ и $1 - xy$ не единица, тогда $1 - xy \in \mathfrak{m}$ в некотором максимальном идеале и $xy \in \mathfrak{m}$, но в таком случае $1 \in \mathfrak{m}$, что противоречие. В обратную сторону, если $x \notin \mathfrak{m}$ не лежит в некотором максимальном идеале, то $(x, \mathfrak{m}) = (1)$, а значит $xy + u = 1$ и $u = 1 - xy$ не единица.

7. **Кольцо A называется конечно порожденным, если существует сюръективный гомоморфизм колец $\mathbb{Z}[x_1, \dots, x_n] \twoheadrightarrow A$. Верно ли, что если A – нётерово, то всякое подкольцо A конечно порождено?**

   То, что конечно порожденные идеалы и кольца имеют схожее название – совпадение так как они порождаются по разному. Например $\mathbb{Q}$ – поле, а значит нётерово, но при этом не конечно порождено, так как из конечного набора дробей нельзя получить дробь со взаимопростым знаменателем.

8. **Радикалом $r(\mathfrak{a})$ идеала $\mathfrak{a} \subseteq A$ назовем множество**

   $$r(\mathfrak{a}) = \{x \in A | x^n \in \mathfrak{a}\}$$

   где в определении n зависит от x.

   (a) **Покажите, что $r(\mathfrak{a})$ – идеал в A, и $\mathfrak{a} \subseteq r(\mathfrak{a})$.**
   Если $x^n \in \mathfrak{a}$, то $(ax)^n$ тоже. Если $x^n, y^m \in \mathfrak{a}$, то $(x + y)^{m+n}$ тоже, так что радикал – идеал. Очевидно, что $\mathfrak{a} \subseteq r(\mathfrak{a})$, так как мы берём $n = 1$ в определении.

   (b) **Покажите, что $r(r(\mathfrak{a})) = r(\mathfrak{a})$.**
   Из прошлого пункта мы знаем, что $r(\mathfrak{a}) \subseteq r(r(\mathfrak{a}))$. Обратно, если $x^n \in r(\mathfrak{a})$, то $(x^n)^m \in \mathfrak{a}$, а значит $x \in r(\mathfrak{a})$.

   (c) **Покажите, что $r(\mathfrak{a})$ совпадает с пересечением всех простых идеалов, содержащих $\mathfrak{a}$.**
   Возьмём $A/\mathfrak{a}$. Так как есть биективное сооветствие между идеалами содержащими $\mathfrak{a}$ и идеалами фактор кольца, то $r(\mathfrak{a})$ соответствует нильрадикал фактор-кольца. Нильрадикал, как мы видели является пересечением всех простых. Тогда $r(\mathfrak{a})$ является пересечением всех прообразов простых при канонической проекции $\pi : A \twoheadrightarrow A/\mathfrak{a}$. Но так как если идеал прост в A, то его проекция тоже проста, из-за того, что простота может быть характеризована только на языке идеалов, то есть $\mathfrak{p}$ просто согда $\mathfrak{a}, \mathfrak{b} \nsubseteq \mathfrak{p}$ имплицирует $\mathfrak{ab} \nsubseteq \mathfrak{p}$ и очевидно, что при проекции это свойство проецируется. А значит радикал – это в точности пересечение всех простых содержащих идеал.

(d) **Пусть $\mathfrak{a}, \mathfrak{b}$ –идеалы в A. Покажите, что $r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b}) = r(\mathfrak{a}\mathfrak{b})$.**

Пусть простой идеал содержит пересечение идеалов $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, тогда идеал содержит и произведение идеалов $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. Если вспомнить определение радикала через пресечения мы получим $r(\mathfrak{a}\mathfrak{b}) \subseteq r(\mathfrak{a} \cap \mathfrak{b})$. Дальше, если $x^n \in \mathfrak{a} \cap \mathfrak{b}$, то верно включение и по отдельности, а значит $r(\mathfrak{a} \cap \mathfrak{b}) \subseteq r(\mathfrak{a}) \cap r(\mathfrak{b})$. Теперь пусть $x^n \in \mathfrak{a}$ и $x^m \in \mathfrak{b}$, тогда $x^{n+m} \in \mathfrak{a}\mathfrak{b}$, а значит верно и последнее включение $r(\mathfrak{a}) \cap r(\mathfrak{b}) \subseteq r(\mathfrak{a}\mathfrak{b})$.

(e) **Пусть $\mathfrak{a}, \mathfrak{b}$ – идеалы в A. Покажите, что $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.**

Пусть $x^n \in \mathfrak{a} + \mathfrak{b}$, тогда $x^n \in r(\mathfrak{a}) + r(\mathfrak{b})$, так как идеалы включены в свои радикалы. В обратную сторону, пусть $x^n \in \mathfrak{a}$ и $y^m \in \mathfrak{b}$, тогда $(x+y)^{n+m} \in \mathfrak{a}+\mathfrak{b}$, а значит включение в обратную сторону также верно.

(f) **Покажите, что в нетеровом кольце A для идеала $\mathfrak{a}$ существует число N такое, что $r(\mathfrak{a})^N \subseteq \mathfrak{a} \subseteq r(\mathfrak{a})$.**

Включение $\mathfrak{a} \subseteq r(\mathfrak{a})$ уже было нами проверено. Теперь мы знаем, что радикал – это идеал, а в нётеровом кольце идеалы конечно порождены. Тогда пусть радикал порождается следующими элементами $(a_1, \dots, a_n)$. Тогда $a_i^{n_i} \in \mathfrak{a}$ для некоторой степени, тогда положим $m = \sum_i n_i$. Тогда нетрудно заметить, что $r(\mathfrak{a})^m = \{\prod a_i^{k_i} \mid \sum_i k_i = m\}$, а также, что каждый порождающий элемент лежит в частности в $\mathfrak{a}$, так как хотя бы одна степень k_i будет не меньше n_i. Тогда верно и второе включение.

9. **Определим кольцо гауссовых чисел (здесь $i = \sqrt{-1}$)**

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

(a) **Покажите, что оно целостно, евклидово и факториально.**

Зафиксируем на этом кольце инволюцию $z \mapsto z^*$ – комплексное сопряжение. Зафиксируем на этом кольце норму $|z| = \sqrt{zz^*}$. Она очевидно мультипликативна, строго положительна для ненулевых элементов и удовлетворяет неравенству треугольника $|a + b| \leq |a| + |b|$.

Из мультипликативности и строгой положиетельности нормы следует что в этом кольце нет делителей нуля и оно целостно. Теперь покажем, что можно делить с остатком. Во первых хоть норма и не имеет значений в целых числах, но порядок, что она индуцируют изоморфен порядку целых чисел. Дальше пусть a, b два гаусовых числа, попробуем одно поделить на другое. Посмотрим на множество $a - (b)$ найдём в нём минимальный элемент относительно нормы, такой существует, так как порядок изоморфен $\mathbb{N}$. Назовём его d, тогда мы имеем $|d| \leq |a - bk|$, для любого Гауссова k. Если $|d| \geq |b|$, то если ввести на гауссовых числах структуру Z свободного модуля с каноническим базисом и каноническим скалярным произведением, то мы заметим следующее. Хотя бы одно из чисел $d + b$, $d - b$, $d + ib$, $d - ib$ будет меньше d так как если зафиксировать $b = m + in$ и $d = k + il$, то можно посмотреть на произведения:

$$\langle d, b\rangle = km + nl, \quad \langle d, -b\rangle = -km - nl, \quad \langle d, ib\rangle = -kn + lm, \quad \langle d, b\rangle = kn - lm.$$

То как минимум одно будет положительным, в противном случае они все нулевые и мы имеем $lm = kn$ и $km = -nl$. Если $|d| = 0$, то победа, мы поделили, но это вообще говоря не так, так как $|b| > 0$ ненулевое. Поэтому пары (m, n) и (k, l) ненулевые. Если без потери общности $m = 0$, то $n \neq 0$, а значит из равенства $0 = kn$ мы заключаем, что $k = 0$, а из $0 = -nl$, что $l = 0$, чего быть не может.

Теперь пусть мы нашли одно нулевое произведение. Пусть оно третье. Тогда $kn = ml$, а значит b пропорционально d. Путь $d = b * k$ (ну или с $-b$), где $k > 1$. Тогда $|d - b| = |bk - b| = |b|(k - 1)$ и мы нашли меньший элемент в $a - (b)$, противоречие. В ином случае ни одно из произведений не нулевое. А значит мы найдем пару положительных, пусть они без потери общности $\langle d, b\rangle$ и $\langle d, ib\rangle$. Пусть $d_1, d_2 \in \mathbb{R}$ - координаты d в (b, ib), они положительны, так как этот базис ортогонален, а координаты в точности равны скалярному произведению на нужный элемент базиса, поделено на квадрат нормы этого элемента. Тогда посмотрим на пару векторов $d - b$ и $d - ib$, квадраты из норм равны

$$|d - b|^2 = |d|^2 - 2\langle d, b\rangle + |b|^2 = |d|^2 + |b|^2(1 - 2d_1)$$
$$|d - ib|^2 = |d|^2 - 2\langle d, ib\rangle + |ib|^2 = |d|^2 + |b|^2(1 - 2d_2)$$

Заметим, что так как $|d| \geq |b|$, то в частности $|d| = |b(d_1 + id_2)| = |b||d_1 + id_2|$, а значит $d_1^2 + d_2^2 \geq 1$. Тогда если оба $1 - 2d_1 \geq 0$ и $1 - 2d_2 \geq 0$, то $0 \leq d_1, d_2 \leq 1/2$

и $d_1^2 + d_2^2 \leq 1/4$, чего не может быть, а значит одна из разностей отрицательна и мы вновь найдем элемент меньший минимального, чего не может быть. Тогда наше предположение о том, что $|d| \geq |b|$ не верно и мы поделили с остатком, а тогда кольцо евклидово.

Дальше я буду использовать утверждения из 5 лекции про кольца. Наше кольцо целостно и евклидово, а значит это кольцо главных идеалов. Наше целостное кольцо главных идеалов, а значит оно факториально.

(b) **Найдите в нем все обратимые элементы.**

Из-за свойств введенной ранее нормы, её значения никогда не меньше нуля и она мультипликативна, а значит у обратного элемента норма - обратное число, но из-за ограничения на значения нормы мы получаем, что у обратимых элементов норма равна 1. Такие элементы $i, -i, 1, -1$ и они правда обратимы. Других нет.

10. **Докажите, что простое натуральное число p является простым числом Гаусса тогда и только тогда, когда уравнение $x^2 + 1 = 0$ не имеет решения по модулю p, то есть -1 не является квадратом по модулю p.**

Пусть мы нашли решение $[a] \in \mathbb{Z}/(p), 0 \leq a < p$ уравнения $x^2+1 = 0$, то есть $(a^2+1) = kp$ тогда построим разложение $kp = (a-i)(a+i)$. Очевидно, что ни $(a-i)$, ни $(a+i)$ не лежат в (p), но зато лежит их произведение, а значит p не прост. Пусть теперь p не прост, а так как кольцо факториально, то p приводим, мы найдём разложение на необратимые элементы. Так как p прост в $\mathbb{Z}$, то его разложение будет содержать ненулевую мнимую часть, более того аргументы комплексных чисел должны быть противоположны, а тогда они будут иметь вид $k(a-bi)$ и $l(a+bi)$ (мы сможем найти на прямых, где лежат наши и 0, числа ближайшие к нулю, одно очевидно будет получать из другого через сопряжение, обозначим первое за $a-bi$). $k, l, a, b \in \mathbb{Z}^*$, a также не нуль, иначе $p = -klb^2$ и один из множителей будет обратим, что нам не интересно. Перемножим их $kl(a^2+b^2) = p$ из-за простоты p в $\mathbb{Z}$, $k = 1 = l$ без потери общности. Тогда $p = a^2 + b^2$, заметим, что без потери общности $0 < a, b < p$, а значит они не делят p. Тогда их классы в $[a], [b] \in \mathbb{Z}/(p)$ обратимы и найдем $0 < c < p$, что $[c] = [a][b]^{-1}$, тогда $[b]^2([c]^2+1) = [b]^2([a]^2[b]^{-2}+1) = [a]^2+[b]^2 = 0$ И так как кольцо $\mathbb{Z}/(p)$ целостно и $[b] \neq 0$, то $[c]^2+1 = 0$, а тогда мы нашли решение c уравнения $x^2+1 = 0$ по модулю p.

11. **Докажите, что простое натуральное число является простым числом Гаусса тогда и только тогда, когда оно имеет вид $4k-1$.**

Заметим, что $2 = (1-i)(1+i)$ не прост. Дальше будем под p понимать простое натуральное число отличное от 2.

Для решения этой задачи проанализируем как квадраты устроены в $\mathbb{F}_p = \mathbb{Z}/(p)$. Зафиксируем некоторые гомоморфизмы мультипликативной группы $q : x \mapsto x^2$ и $\varphi : x \mapsto x^{(p-1)/2}$. Тогда $\mathrm{Ker}(q) = \{1, -1\}$, так как $\mathbb{F}_p$ поле и в нём $x^2 = 1$ имеет не более двух решений, то есть 1 и -1, по теореме об гомоморфизме, получаем, что в поле ровно $(p-1)/2$ квадратов. Теперь заметим, что все квадраты из $\mathbb{F}_p$ лежат в $\mathrm{Ker}(\varphi)$, так как $(x^2)^{(p-1)/2} = x^{p-1} = 1$, последнее верно по теореме Эйлера. С другой стороны уравнение $x^{(p-1)/2} = 1$ имеет не более $(p-1)/2$ решений. Но у нас уже есть $(p-1)/2$ решение, а именно квадраты, тогда мы заключаем, что $\mathrm{Ker}(\varphi)$ – множество всех квадратов. Тогда в частности мы получим, что -1 квадрат тогда и только тогда, когда $(p-1)/2$ четно, потому что возведение в эту степень квадрата даёт 1.

Теперь, при делении на 4 p можете иметь в остатке только 1 или 3. Если $p = 4k+1$, $(p-1)/2$ четно, тогда -1 – квадрат, а тогда $x^2+1 = 0$ имеет решение и p не прост в $\mathbb{Z}[i]$. Иначе $p = 4k-1$, $(p-1)/2$ не четно, -1 не квадрат и $x^2+1 = 0$ не имеет решений и p прост в $\mathbb{Z}[i]$.

12. **Опишите множество всех натуральных числа, представимых в виде суммы двух квадратов.**

Будем считать, что квадраты тоже раскладываются в сумму, где одно из слагаемых нуль. Будем дальше полагать, что в разложение оба слагаемых ненулевые.

Пусть есть число нужного вида a^2+b^2. Тогда можно вынести квадрат наибольшего общего делителя a и b. Так что все представимые числа, получаются из всех представимых в виде суммы двух взаимопростых квадратов через домножение на некоторый квадрат. Дальше мы положим $a \wedge b = 1$.

Пусть x натуральное число. Оно разложимо единственным образом на произведение простых. Тогда если это число раскладывается в сумму взаимнопростых квадратов то все его простые делители тоже раскладываются в какую-нибудь сумму.

Пусть $x = a^2 + b^2$ представилось как сумма взаимопростых квадратов, тогда пусть p прост и $kp = a = x^2 + y^2$ очевидно, что p не делит не x, ни y. Тогда аналогично 10 заданию мы получим $[x]^2 + [y]^2 = 0$ и найдем в $\mathbb{F}_p$ решение уравнения $x^2 + 1 = 0$, а тогда p разложимо в сумму квадратов.

С другой стороны если у какого-нибудь числа все его простые делители раскладываются в сумму квадратов, то и само число тоже, а именно $x = \prod p_i = \prod (a_i + b_i i)(a_i - b_i i) = \prod (a_i + b_i i) \prod (a_i - b_i i) = Z * Z^*$, а значит a тоже сумма квадратов.

Тогда описание всех подходящих нам чисел будет все квадраты и все произведения простых вида $4k + 1$, умноженные на квадраты.

13. **Определим кольцо чисел Эйзенштена (здесь $\rho = \frac{-1+\sqrt{3}i}{2}$)**

$$\mathbb{Z}[\rho] = \{a + \rho b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

Наблюдение: $\rho^2 + \rho + 1 = 0$

(a) **Покажите, что оно целостно, евклидово и факториально.**

Мы можем опять ввести индуцированную с $\mathbb{C}$ мультипликативную норму. Тогда сразу станет ясно, что кольцо целостно. Проверим, что оно евклидово.

Пусть $a, b \in \mathbb{Z}[\rho]$ и a не делит b. В множестве $a + (b)$ есть минимальный элемент по норме. Назовем его d. Покажем, что $|d| < |b|$. Пусть это не так и $|d| \geq |b|$, тогда поступим также как и для Гауссовых чисел, только применим планаметрическое рассуждение. Вектора b, $-b$, ρb, $-\rho b$, $\rho^2 b$, $-\rho^2 b$ делят плоскость на углы по 60 градусов, тогда мы найдем один вектор, до которого от d не более 30 градусов, пусть без потери общности это b, тогда

$$\begin{aligned} |b - d|^2 &= |b|^2 + |d|^2 - 2\langle b, d\rangle \\ &\leq |b|^2 + |d|^2 - 2|d||b|\cos(\pi/6) \\ &\leq |d|^2 + |b|^2(1 - \sqrt(3)) \\ &\leq |d|^2 \end{aligned}$$

Тогда мы получили противоречие о минимальности d. А значит мы можем делить с остатком. Так как кольцо целостно и евклидово, то оно факториально.

(b) **Найдите в нем все обратимые элементы.**

Обратимые элементы должны обладать нормой 1, но все такие элементы $\pm 1, \pm\rho, \pm\rho^2$ обратимы.

14. **Докажите, что простое натуральное число p является простым числом Эйзенштейна тогда и только тогда, когда уравнение $x^2 - x + 1 = 0$ не имеет решения по модулю p, то есть либо $p = 2$, либо -3 не является квадратом по модулю p.**

Пусть $a^2 - a + 1 = kp$, $k \neq 0$. Тогда $(a + \rho)(a + \rho^2) = kp$ и так как p не делит ни $a + \rho$, ни $a + \rho^2$, то p не прост.

Обратно, пусть p не простое число эйзенштейна, тогда p сепарабельно, так как кольцо факториально. Пусть $p = ab$, тогда как и в прошлый раз мы найдем u, что $a = ku$ и $p = lu^*$. Но так как p прост в $\mathbb{Z}$, то $k, l = 1$ без потери общности. Тогда запишем $u = a + \rho b,\ a, b \neq 0$. Тогда в $\mathbb{F}_p$ будет верно $[a]^2 + [b]^2 - [a][b] = 0$, если поделить на $[b]$, то мы получим $([a]/[b])^2 - [a]/[b] + [1] = 0$, а значит мы нашли решение.

Для $p = 2$ решение нет, дальше $p \neq 2$. Теперь в $\mathbb{F}_p$

$$\begin{aligned} c^2 - c + 1 &= 0 \\ (c^2 - c - 1/4) + 3/4 &= 0 \\ (4c^{-}4c + 1) &= -3 \\ (2c - 1)^2 &= -3 \end{aligned}$$

То есть решение есть $\Leftrightarrow p$ не 2 и -3 квадрат.

15. **Докажите, что простое натуральное число является простым числом Эйзенштейна тогда и только тогда, когда оно равно 2 или имеет вид $6k - 1$.**

Случай $p = 2$ мы уже рассмотрели, $p = 3$ не подходит, тогда рассмотрим $p > 3$. Введем символ Лежандра для нечетного простого p

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{если} \quad [a]_p = [0]_p \\ 1 & \text{если} \quad [a]_p = [b]_p^2 \neq [0]_p \\ -1 & \text{если} \quad \text{иначе} \end{cases}$$

Заметим, что как мы видели в упражнении 11, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\ p)$, а тогда в частности этот символ мультипликативен относительно верхнего индекса. Теперь зафиксируем a не кратное p и положим $p_1 = \frac{p-1}{2}$. Для $1 \leq i \leq p_1$ положим $[a \cdot i] = [\varepsilon_i \cdot r_i]$, где $\varepsilon = \pm 1$ и $1 \leq r_i \leq p_1$ и $\varepsilon_0 = 1, r_0 = 0$. Тогда так как умножение в мультипликативной группе на разные элементы даёт разные результаты, то $-p_1 \leq i \leq p_1$ - представители всех классов, то тогда $[a \cdot i] = [\mathrm{sgn}(i)\varepsilon_{|i|} \cdot r_{|i|}]$ все классы для $-p_m \leq i \leq p_m$. Тогда $[\prod_{i \in \{-p_1..p_1\} \setminus \{0\}} i] = [\prod_{i \in \{-p_1..p_1\} \setminus \{0\}} \mathrm{sgn}(i)\varepsilon_{|i|} r_{|i|}]$, а тогда в мы получим, что $[\prod_{i \in \{1..p_1\}} i] = [\prod_{i \in \{1..p_1\}} \varepsilon_i r_i]$. Тогда $[a^{p_1}][\prod_{i \in \{1..p_1\}} i] = [\prod_{i \in \{1..p_1\}} \varepsilon_i r_i]$, а тогда $[a^{p_1}] = [\prod_{i \in \{1..p_1\}} \varepsilon_i]$.

Теперь заметим, что для дробей мы имеем:

$$\left\lfloor \frac{2ai}{p} \right\rfloor = \left\lfloor 2\left\lfloor \frac{ai}{p} \right\rfloor + 2\left\{\frac{ai}{p}\right\} \right\rfloor = 2\left\lfloor \frac{ai}{p} \right\rfloor + \left\lfloor 2\left\{\frac{ai}{p}\right\} \right\rfloor$$

это число четно или нечетно, если наименьший отрицательный вычет меньше или больше $p/2$. Отсюда получаем:

$$\varepsilon_i = (-1)^{\left\lfloor \frac{2ai}{p} \right\rfloor}$$

и поэтому символ Лежандра можно выразить следующим образом

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \left\lfloor \frac{2ai}{p} \right\rfloor}$$

Пусть теперь a нечетно, тогда $a + p$ четно:

$$\left(\frac{2a}{p}\right) = \left(\frac{2a + 2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \left\lfloor \frac{(a+p)i}{p} \right\rfloor} = (-1)^{\sum_{i=1}^{p_1} \left\lfloor \frac{ai}{p} \right\rfloor + \sum_{i=1}^{p_1} i}$$

Откуда нетрудно получить

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \left\lfloor \frac{ai}{p} \right\rfloor + \frac{p^2-1}{8}}$$

Если взять $a = 1$, то мы получим

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

А тогда для нечетных a будет верно

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \left\lfloor \frac{ai}{p} \right\rfloor}$$

Теперь пусть q, p – два простых нечетных числа. Для $x \in \{1..p_1\}$ и $y \in \{1..q_1\}$ никогда не будет равенства $qx = py$, так как $[xq]_p \neq [0]_p$. Отсюда мы заключим, что $p_1 q_1 = S_1 + S_2$, где S_1 – число пар $qx < py$ и S_2 – число пар $py < qx$. Очевидно, что число пар $x < (p/q)y$ также равняется S_1. При заданном y можно брать $x \in \{1..\left\lfloor \frac{p}{q} y \right\rfloor$. А значит

$$S_1 = \sum_{y=1}^{q_1} \left\lfloor \frac{p}{q} y \right\rfloor$$

Аналогично получим

$$S_2 = \sum_{x=1}^{p_1} \left\lfloor \frac{q}{p} x \right\rfloor$$

Тогда

$$\left(\frac{p}{q}\right) = (-1)^{S_1}, \quad \left(\frac{q}{p}\right) = (-1)^{S_2}$$

И

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S_1+S_2} = (-1)^{p_1 q_1}$$

Отсюда заключаем, что

$$\left(\frac{p}{q}\right) = (-1)^{p_1 q_1}\left(\frac{q}{p}\right)$$

Эти наблюдения были взяты из книги Виноградова "Основы теории чисел"

Теперь

$$\left(\frac{3}{p}\right) = (-1)^{p_1}\left(\frac{p}{3}\right)$$

А для -3 будет

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)(-1)^{p_1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = (-1)^{\sum_{i\in\{1..(3-1)/2\}}\left\lfloor\frac{pi}{3}\right\rfloor} = (-1)^{\left\lfloor\frac{p}{3}\right\rfloor}$$

Если $p = 6k + 1$, то

$$\left\lfloor\frac{6k}{3} + \frac{1}{3}\right\rfloor = 2k \text{ - четно}$$

Если $p = 6k + 5$, то

$$\left\lfloor\frac{6k}{3} + \frac{5}{3}\right\rfloor = 2k + 1 \text{ - нечетно}$$

Других представлений у простых больших 3 очевидно нет. Тогда мы утверждение задачи очевидно доказано.