ДОМАШНИЙ ЭКЗАМЕН

Вам предлагается множество задач различной сложности, сгруппированных по темам. Для получения зачёта нужно набрать B баллов, где:

$B = 13$, если сдать (прислать на электронную почту) работу до 23 мая, конкретно до 12:00 по Московскому времени;

$B = 17$, если сдать работу до 27 мая, 12:00 по Московскому времени;

$B = 20$, если сдать работу до 1 июня, 12:00 по Московскому времени.

Если за задачу даётся 0 баллов, то это означает, что я разобрал её на лекции (либо то, что она была в курсе ОКТЧ). Впрочем, иногда обратное неверно: некоторые задачи я на лекциях разобрал кратко, и тогда их доведение до подробного решения по-прежнему награждается.

Ближе к концу списка упражнений есть несколько сложных задач, позволяющих быстро набрать необходимое для зачёта количество баллов.

1. ПРИМЕР КОЛЬЦА БЕЗ ОТА. Проведите анализ кольца $\mathbf{Z}[\sqrt{-5}]$ целых чисел, пополненных корнем из (-5), лежащим в верхней полуплоскости (то есть, минимального кольца, содержащего $\sqrt{-5}$ и все целые числа).

   (a) (2 балла) Докажите, что это кольцо состоит из всех комплексных чисел, представимых в форме $a + b\sqrt{-5}$ и только их (где $a, b \in \mathbf{Z}$);

   (b) (1 балл) покажите, что функция $N : \mathbf{Z}[\sqrt{-5}] \to \mathbf{N}$, заданная формулой $N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$, переводит произведение в произведение. (Она называется *нормой* кольца.)

   (c) (1 балл) найдите все обратимые элементы в нашем кольце, и докажите, что числа $3, 7, (4 \pm \sqrt{-5}), (1 \pm 2\sqrt{-5})$ являются простыми;

   (d) (2 балла) На основании выше перечисленного выпишите явное противоречие Основной Теореме Арифметики в $\mathbf{Z}[\sqrt{-5}]$.

2. ДЕЛИМОСТЬ В КОЛЬЦАХ $\mathbf{Z}$ и $\mathbf{Z}[\mathbf{i}]$ и других. Ниже мы будем под $< n, K, m >$ понимать наибольший общий делитель пары элементов кольца K; если кольцо в обозначении не указано, то обычно ясно, о чём идёт речь. Для обычных целых чисел, лежащих во всех наших кольцах, неуказание кольца означает, что $K = \mathbf{Z}$.

(a) (2 балла) При каких условиях $< an + bm, cn + dm >=< n, m >$ для всех $n, m \in \mathbf{Z}$?

(b) (1 балл) Докажите, что если m, n — два взаимно простых целых числа разной чётности, то числа $m^2 - n^2$ и $2mn$ тоже взаимно простые. Также взаимно простыми будут числа $m^2 - n^2$ и $m^2 + n^2$.

(c) (5 баллов) При каких условиях $< f(n, m), g(n, m) >=< n, m >$ для всех $n, m \in \mathbf{Z}$, где f и g — два многочлена от двух переменных с целыми коэффициентами (мне ответ неизвестен; возможно, он очень сложный; кажется, я его где-то встречал в форме нерешённой задачи)?

(d) (1 балл) Докажите, что если обычное целое число n делится на целое число m в кольце Гауссовых или Эйзенштейновых чисел, то n делится на m и в обычном смысле. Докажите, что

$$< a, \mathbf{Z}, b >=< a, \mathbf{Z}[\mathbf{i}], b >=< a, \mathbf{Z}[\omega], b >$$

для двух обычных целых чисел a, b (т.е. не меняется при пересчёте его же, но в кольце Гауссовых либо Эйзенштейновых чисел).

(e) (0 баллов) Найдите обратимые элементы в кольце $\mathbf{Z}[i]$. Какую группу они образуют (по умножению)? Докажите, что любой обратимый элемент в кольце Гауссовых чисел является кубом некоторого Гауссова числа.

(f) (2 балла) Найдите обратимые элементы в кольце $\mathbf{Z}[\omega]$. Какую группу они образуют (по умножению)? Опишите обратимые элементы, которые являются квадратами в кольце $\mathbf{Z}[\omega]$. Тот же вопрос про кубы.

(g) (2 балла) Разделите в кольце Гауссовых чисел элемент $(5 + 4i)$ на $(1 - 2i)$ с остатком. Сколькими способами можно это осуществить? Решите ещё примеры: 13 на $(5 - i)$, $(2 + i)$ на $(2 - i)$.

(h) (2 балл) Рассмотрим кольцо $\mathbf{Z}[\sqrt{-3}]$ целых чисел, пополненных корнем из (-3), лежащим в верхней полуплоскости (то есть, минимальное кольцо, содержащее $\sqrt{-3}$ и все целые числа). Покажите, что в нём число 2, а также числа $(1 \pm \sqrt{-3})$ простые, и что $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Докажите, что кольцо $\mathbf{Z}[\sqrt{-3}]$ содержится в кольце $\mathbf{Z}[\omega]$ чисел Эйзенштейна. Почему приведённое выше равенство не противоречит ОТА в кольце Эйзенштейна?

(i) (0 баллов) Разлагая сумму квадратов в кольце Гауссовых чисел на множители, получите полное решение диофантова уравнения $y^2 = x^3 - 1$.

(j) (5 баллов) Конечно или бесконечно множество “гауссовых простых близнецов”, то есть Гауссовых простых, отличающихся на $\pm 1 \pm i$? (Ответ мне неизвестен!!! Вполне возможно, что это — “полный гроб” наподобие задачи о простых близнецах!)

(k) (1 балл) Сколько различных (с точностью до умножения на обратимые) простых делителей $a + bi$ в кольце Гауссовых чисел у данного простого числа $p \in \mathbf{Z}$? Разберите все случаи.

(l) (4 балла) Напишите и докажите общую формулу для количества различных представлений данного целого числа n в виде суммы двух квадратов. (Различными считаются представления, не получающиеся друг из друга путём смены знаков и порядка следования слагаемых.)

(m) (6 баллов, Эрдёш) На основе полученной формулы выведите нижнюю оценку на максимальное количество равных расстояний среди данных n точек на плоскости, пользуясь регулярной прямоугольной решёткой.

3. ПОСТРОЕНИЯ ЦИРКУЛЕМ И ЛИНЕЙКОЙ.

(a) (2 балла) Постройте правильный пятиугольник с помощью циркуля и линейки.

(b) (0 баллов) Постройте правильный 15-угольник с помощью циркуля и линейки.

(c) (3 балла) Вам дан единичный отрезок. Требуется построить с помощью циркуля и линейки отрезок длины x, удовлетворяющей уравнению

$$ax^3 + bx^2 + cx + d = 0,$$

где числа a, b, c, d — целые. Докажите, что это возможно в том и только том случае, когда это уравнение имеет хотя бы один рациональный корень.

(d) (0 баллов) На основании предыдущей задачи докажите, что правильный семиугольник не может быть построен с помощью циркуля и линейки.

(e) (3 балла) Докажите, что трисекция угла невозможна.

4. ЦЕПНЫЕ ДРОБИ

(a) (Взято у А.С. Штерна, 2 балла) Пускай a — положительное целое число. Разложите положительный корень уравнения

$$x^2 = a(x + 1)$$

в цепную дробь двумя разными способами.

(b) (2 балла) Разберитесь с алгоритмом Делоне-Арнольда построения цепной дроби ("алгоритм вытягивания носов"). Покажите, что площади всех построенных параллелограммов (которые заключают внутри себя луч с тангенсом угла наклона, равным разлагаемому числу) равны 1.

(c) (4 балла) Обозначим цепную дробь за $[a_0, a_1, \ldots]$. Тогда в неё, в принципе, можно подставлять любые вещественные числа. Пусть $a_0, a_1, \ldots, a_n, \ldots \in \mathbf{R}_+$. Докажите, что цепная дробь $[a_0, a_1, \ldots]$ определена (последовательность подходящих дробей сходится) тогда и только тогда, когда расходится ряд $\sum_{i=1}^{+\infty} a_i$.

(d) (2 балла) Докажите, что любое приближение первого рода является промежуточной дробью (в терминологии с лекции).

(e) (2 балла) Пускай число α, которое раскладывается в цепную дробь, не является полуцелым и целым. Тогда понятие подходящей дроби тождественно понятию приближения второго рода (в терминологии с лекции).

(f) (2 балла) Докажите, что для любой подходящей дроби $\dfrac{p_n}{q_n}$, вычисленной по цепной дроби для иррационального числа α, выполнено

$$\frac{1}{q_n(q_n + q_{n+1})} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

(g) (3 балла) Докажите, что если

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q},$$

то дробь $\dfrac{p}{q}$ является налучшим приближением второго рода для раскладываемого в цепную дробь числа α.

5. УРАВНЕНИЕ ПЕЛЛЯ

(a) (2 балла) Пользуясь последним пунктом предыдущего круга задач, докажите, что любое решение любого уравнения Пелля $x^2 - my^2 = \pm 1$ присутствует среди подходящих дробей цепной дроби для $\sqrt{m}$.

(b) (1 балл) Охарактеризуйте всевозможные комбинации количеств чёрных и белых шаров в урне, чтобы при случайном выуживании двух шаров в выборке без возвращения вероятность выудить два белых шара равнялась в точности 0.5.

(c) (3 балла) Решите уравнение $x^2 - 61y^2 = 1$ в целых числах.

(d) (0 баллов) Найдите какую-нибудь Пифагорову тройку (x, y, z) (то есть такую, что $x^2 + y^2 = z^2$ и $xyz \neq 0$) с соседними числами x, y, кроме стандартной $(3, 4, 5)$. Попробуйте придумать общее правило, и докажите его.

(e) (2 балла) Пускай m — обычное положительное целое число, свободное от квадратов (на самом деле, вроде бы, достаточно считать, что m не является полным квадратом). Введём на плоскости $\mathbf{R}^2$ новое умножение по формуле

$$(a, b) \times (c, d) = (ac + mbd, bc + ad).$$

Покажите, что это умножение задаёт на плоскости структуру кольца (алгебры над полем действительных чисел), но деление не всегда определено. На какие точки можно всегда делить? Покажите, что точка (a, b) обратима тогда и только тогда, когда отображение

$$L_{(a,b)} : \mathbf{R}^2 \to \mathbf{R}^2, \quad L_{(a,b)}[(c, d)] = (ac + mbd, bc + ad)$$

является взаимно-однозначным (линейным изоморфизмом $\mathbf{R}^2$).

(f) (2 балла) Рассмотрим отображение $\Psi : \mathbf{R}^2 \to \mathbf{R}$, действующее по следующей формуле:

$$\Psi[(a, b)] = a + b\sqrt{m},$$

где число $m \in \mathbf{Z}$ не является полным квадратом. Докажите, что оно является гомоморфизмом колец. Найдите его ядро. Покажите, что ограничение этого отображения на $\mathbf{Q} \times \mathbf{Q}$ является взаимно однозначным. Более того, оно является изоморфизмом полей (покажите, что $\mathbf{Q} \times \mathbf{Q}$ со введённым в предыдущем пункте умножением, а также подмножество-образ $\mathbf{Q} \times \mathbf{Q}$ в $\mathbf{R}$, являются полями).

(g) (1 балл) Охарактеризуйте множество всех решений уравнения Пелля $x^2 - my^2 = \pm 1$ в том случае, когда существует решение этого уравнения вида $x^2 - my^2 = -1$.

(h) (2 балла) Покажите, что все параллелограммы со сторонами, параллельными асимптотам семейства гипербол

$$x^2 - my^2 = \pm K,$$

и вписанные в любую пару гипербол семейства с данным K, имеют одинаковую площадь. При каком K площадь равна 4?

6. ВОКРУГ ТЕОРЕМЫ ФЕРМА

(a) (3 балла) Докажите, что если для целых положительных x, y, z, n выполнено равенство $x^n + y^n = z^n$, то с необходимостью должно быть верно, что $|x|, |y|, |z| > n$ (теоремой Ферма не пользоваться!).

(b) (3 балла) Разложите число p на простые в кольце $Z[\sqrt[p]{1}]$. (В дальнейшем обозначим $\sqrt[p]{1}$ с наименьшим поожительным аргументом за ζ).

(c) (2 балла) Используя ζ, разложите $a^p + b^p$ на линейные множители. Докажите полученное равенство.

(d) (2 балла) В кольце $Z[\zeta]$ элемент $(1 - \zeta)$ — простой.

(e) (1 балл) При $p = 3$ элемент ζ называется ω, а элемент $(1 - \zeta)$ называется λ. Покажите, что любой элемент кольца $Z[\omega]$ имеет остаток 1, 0 или -1 по модулю λ.

(f) (2 балла) Докажите, что для любого элемента a кольца Эйзенштейна существует в точности $N(a)$ классов остатков по модулю a, где $N(a)$ — норма этого кольца, то есть

$$N(a) = N(x + y\omega) = x^2 - xy + y^2.$$

(g) (8 баллов) Придумайте норму для кольца $Z[\sqrt[5]{1}]$, и доказать евклидовость последнего (относительно придуманной нормы).

(h) (5 баллов) Опишите все вещественные обратимые элементы кольца $Z[\sqrt[5]{1}]$, пользуясь результатами а-ля уравнение Пелля.

(i) (3 балла) Найдите группу обратимых элементов кольца $Z[\sqrt[5]{1}]$.

(j) (5 баллов) Решите уравнение Ферма $x^5 + y^5 = z^5$.

7. ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

(a) (4 балла) Рассмотрим соотношение на стороны a, b, c треугольника, при котором треугольник с вершинами в основаниях биссектрис является равнобедренным. Считая, что равными окажутся стороны, сходящиеся на стороне c большого треугольника, сведите это соотношение к следующему:

$$\frac{a(c-a)}{(b+c)^2} = \frac{b(c-b)}{(a+c)^2}.$$

Затем, предполагая исходный треугольник **не равнобедренным**, “упростите” это соотношение (в смысле снижения степени

многочлена). Конкретно, выведите следующие его три эквивалентные формы:

$$c^3 + c^2(a+b) = c(a^2+ab+b^2) + (a^3+a^2b+ab^2+b^3);$$

$$\frac{a}{(b+c)} + \frac{b}{(a+c)} = \frac{c}{(a+b)};$$

$$(a+b+c)(a^2+b^2-c^2) + abc = 0.$$

(b) (2 балла) В дальнейшем мы рассматриваем кубику, заданную первым из трёх уравнений (отказываясь от требования, чтобы a, b, c были сторонами какого-либо треугольника). Покажите, что полученная кубика неразложима, то есть многочлен, её задающий, не раскладывается на множители.

(c) (2 балла) Покажите вдобавок к этому, что наша кубика *неособа*, то есть на её проективизации нет ни одной точки, в которой каждое направление является касательным (или что то же самое, в которой вырождаются все три первых частных производных определяющего её многочлена).

(d) (2 балла) Покажите, что точка $(1, -1, 0)$ лежит на нашей кубике и является точкой перегиба, то есть касательное направление в ней имеет третий порядок сближения. (Тем самым мы установили, что наша кубика является *эллиптической кривой*, и найденную целочисленную точку перегиба удобно считать нулём группы.)

(e) (3 балла) Выбирая систему координат так, чтобы точка $(1, -1, 0)$ совпала в новом базисе с точкой $(0, 1, 0)$, а касательное направление совпало бы с бесконечно удалённой прямой, найдите Веерштрассову форму нашей эллиптической кривой, то есть найдите такие A, B, что в новой системе координат наша кривая выглядит как

$$y^2 = x^3 + Ax + B.$$

(f) (6 баллов) Докажите, что на всей нашей кривой (на самом деле утверждение верно для любой эллиптической кривой!) множество точек A, B, E таких, что (в обозначениях последней лекции) обе девятки точек

$$[0, A, B, E, R, \bar{R}, Q, \bar{Q}, S]; \;\; [0, A, B, E, R, \bar{R}, Q, \bar{Q}, T]$$

попарно различны, составляет “открытое множество” (то есть дополнение к нему может быть записано в виде объединения нулей конечного числа алгебраических уравнений). Пользуясь этим достижением, завершите доказательство ассоциативности, проведённое на лекции.

(g) (8 баллов) Найдите все целые решения уравнения $y^2 = x^3 + 1$.

(h) (5 баллов) Опишите группу рациональных точек эллиптической кривой $y^2 = x^3 + 1$.

8. РАЗНЫЕ ЗАДАЧИ.

(a) (0 баллов) Пускай $p = 2^r + 1$ — простое число (такие числа называются простыми числами Ферма). Докажите, что тогда r само также является степенью двойки.

(b) (0 баллов) Пускай простое (натуральное) число p имеет вид $p = qr + 1$. Тогда число a является q-й степенью по модулю p в том и только том случае, когда по модулю p верно $a^r = 1$.

(c) (2 балла) Рассмотрим уравнение $x^a + y^a = z^b$, где a и b взаимно простые. Покажите, что у такого уравнения всегда есть бесконечное множество решений, и выведите формулу, дающую целое семейство его решений.