Краткое содержание первых занятий.

1. Диофантовы уравнения.

Напоминание школьного материала: НОД, НОК, деление с остатком, алгоритм Евклида, сравнения.

Решение в целых числах уравнения

$$ax + by = c; \tag{1}$$

сведение к вопросу об уравнении $ax + by = 1$.

Теорема 1.1. *Решение (x_0, y_0) уравнения*

$$ax + by = 1 \tag{2}$$

существует тогда и только тогда, когда числа a и b взаимно просты. В этом случае все решения перечисляются так:

$$\begin{cases} x = x_0 - bm \\ y = y_0 + am \end{cases} \tag{3}$$

где m — любое целое число.

Можно попытаться решать уравнение (1) подбором, выразив, скажем, y через x

$$y = \frac{c - ax}{b} \tag{4}$$

и подставляя затем вместо x последовательно целые значения 0, 1, 2, ..., дожидаясь, пока числитель (4) окажется кратным b, так что дробь сократится и значение y тогда окажется также целым. На первый взгляд неясно, почему есть уверенность, что это вообще когда-то произойдет, но мы сейчас докажем, что успех гарантирован даже не когда-то, а не позднее значения $x = b - 1$. Для этого рассмотрим значения числителя (4) при первых b последовательных значениях x, начиная с $x = 0$:

$$c, c - a, c - 2a, c - 3a, \ldots, c - (b-1)a. \tag{5}$$

Для того, чтобы доказать, что среди этих b чисел есть число, делящееся на b, достаточно убедиться в том, что все эти числа дают разные остатки при делении на b. Поскольку существует всего b возможных остатков от деления любого числа на b (а именно, 0, 1, 2, ..., $b - 1$), из этого будет следовать, что остаток 0 среди них тоже есть.

Тот факт, что все остатки будут разные, проще всего доказать, предположив противное, т.е. что в интервале от 0 до $b-1$ существуют два разных значения x_1 и x_2 такие, что при делении их с остатком на b получается один и тот же остаток r ($0 \le r < b$), т.е.

$$\begin{array}{c} c - ax_1 = bs_1 + r \quad \text{и} \\ c - ax_2 = bs_2 + r \end{array} \tag{6}$$

Вычтем второе уравнение из первого, получим

$$a(x_2 - x_1) = b(s_1 - s_2), \tag{7}$$

откуда следует, что левая часть этого равенства делится на b. Поскольку мы предположили, что числа a и b взаимно просты, их этого следует, что на b должна делиться[1] разность $x_2 - x_1$, что невозможно, поскольку оба эти числа заключены между 0 и $b-1$, так что их разность по модулю точно меньше b.

Полученное противоречие доказывает, что все остатки разные, и, следовательно, среди них есть и нулевой, что и дает искомое решение (x_0, y_0) уравнения (1).

Формулу для перечисления всех решений (6) также нетрудно получить подобным рассуждением: пусть (x, y) — другое решение уравнения (1), отличное от (x_0, y_0), то есть

$$\begin{array}{c} ax_0 + by_0 = c \quad \text{и} \\ ax + by = c \end{array} \tag{8}$$

Тогда, вычитая первое равенство из второго, получаем $ax_0 + by_0 - ax - by = 0$, откуда получаем, что

$$a(x - x_0) = b(by_0 - y). \tag{9}$$

Теперь снова используем рассуждение, уже применявшееся нами к равенству (7): поскольку левая часть должна делится на b, а числа a и b взаимно просты, их этого следует, что на b должна делиться разность $x - x_0$. Следовательно, $x - x_0$ есть некоторая целая кратность b, то есть $x - x_0 = bm$ при некотором целом m. Получаем первое равенство $x = x_0 + bm$ из (6); второе равенство

[1] В этом месте мы, конечно, основываемся на очевидном для всех младшеклассников утверждении, что любое целое число однозначно раскладывается в произведение простых сомножителей (с точностью до порядка сомножителей). На самом деле это утверждение, конечно, требует доказательства — оно называется **Основная теорема арифметики.** Мы докажем эту теорему чуть позже, основываясь как раз на Теореме 1.1 — для этого нам, конечно, придется сначала дать другое доказательство Теоремы 1.1, не использующее Основную теорему арифметики.

легко получить из (9), подставив туда полученное выражение для x.

Без доказательства: алгоритм нахождения частного решения (x_0, y_0) с помощью разложения в цепную дробь.

Задачи для размышления:

1) Задача Дирака про трех рыбаков.

2*) Обосновать алгоритм нахождения частного решения x_0, y_0.

Напоминание: сравнения.

Китайская теорема об остатках. Если числа m и n взаимно просты, то для любых остатков a и b существует такое целое число z, что

$$\begin{cases} z \equiv a \mod m \\ z \equiv b \mod n \end{cases} \tag{10}$$

Доказательство очень простое: (10) означает, что

$$\begin{cases} z = xm + a \\ z = yn + b \end{cases} \tag{11}$$

при некоторых целых x и y. Это система двух уравнений с тремя неизвестными x, y и z. Исключая z, получаем уравнение $mx - ny = b - a$, которое по теореме (1.1) имеет решение. Ясно, что решение z не единственно: добавление к z любой кратности mn также является решением.

2. Арифметика остатков (кольца вычетов).

Напоминание: сравнения. Определение множества $\mathbb{Z}_n$ и операций сложения и умножения в нем. Вычитание. Примеры.

Теорема 2.1. *Ненулевой остаток $a \in \mathbb{Z}_n$ обратим тогда и только тогда, когда числа a и n взаимно просты.*

Обозначения: множество обратимых остатков в $\mathbb{Z}_n$ будем обозначать $\mathbb{Z}_n^*$; число элементов в $\mathbb{Z}_n^*$ будем обозначать $\varphi(n)$ — функция Эйлера.

Определение: делители нуля, нильпотентные, идемпотентные элементы в $\mathbb{Z}_n$.

Как вычислять $\varphi(n)$?

(1) Если $n = p$ — простое число, то, очевидно, $\varphi(p) = p - 1$: все натуральные числа, меньшие p, с ним взаимно просты.

(2) Если $n = p^m$ — степень простого числа, то, очевидно, $\varphi(p^m) = p^m - p^{m-1}$: натуральные числа, меньшие p, не взаимно просты с ним, если они делятся на p, и до и p^m имеется ровно p^{m-1} число, делящееся на p (это p, $2p$, $3p$, $\ldots$, $p^m - p$).
(3) **Теорема мультиплпикативности для функции Эйлера:** Если числа m и n не имеют общих делителей, то

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Теорему мультипликативности мы докажем чуть позже.

Задачи для размышления: в каких $\mathbb{Z}_n$ встречаются делители нуля, нильпотенты, идемпотенты, как их узнавать и перечислять?

Ответ про делители нуля: это в точности остатки, не взаимно простые с n.

3. Основные алгебраические структуры: группа, кольцо, поле.

Определения: бинарная операция, группа, кольцо, поле. Изоморфизм. Примеры.

В этом курсе нам встретятся только коммутативные группы, а все кольца будут коммутативными, ассоциативными и с единицей.

Напоминание: декартово произведение множеств.

Задача для размышления: вот несколько групп, состоящих из четырех элементов. Какие из них попарно изоморфны, а какие нет? 1) $\mathbb{Z}_4$ с операцией "+"; 2) комплексные числа ± 1 и $\pm i$ с операцией умножения; 3) обратимые остатки по модулю 10: $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ с операцией умножения; 4) обратимые остатки по модулю 12: $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ с операцией умножения; 5) булевы 2-векторы $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ с операцией сложения (покомпонентного).

Определение: порядок элемента группы. Примеры.

Два важных свойства этого понятия: 1) если в в последовательности степеней $\varepsilon, a, a^2, a^3, \ldots, a^m, \ldots$ есть повторы, то первое повторение всегда имеет вид $\varepsilon = a^n$ при некотором n, так что все предыдущие степени $\varepsilon, a, a^2, a^3, \ldots, a^{n-1}$ все различны. 2) если $a^N = \varepsilon$, то порядок элемента a является делителем числа N.

Теорема 3.1. *В конечной группе порядок любого элемента является делителем порядка группы.*

Мы докажем эту теорему только для случая коммутативной группы, поскольку в нашем курсе некоммутативных групп нам не встретится. Доказательство в общем случае можно прочитать в любом учебнике алгебры.

Пусть группа G состоит из N элементов: $G = \{g_1, g_2, \ldots, g_N\}$ и пусть $a \in G$. Рассмотрим произведения ag_1, ag_2, $\ldots$, ag_N. Очевидно, они все различны; действительно, если $ag_i = ag_j$, то, домножая это равенство слева на a^{-1}, получаем $a^{-1}(ag)_i = a^{-1}(ag_j)$, откуда по ассоциативности получаем $(a^{-1}a)g_i = (a^{-1}a)g_j$, то есть $1g_i = 1g_j$, откуда $1g_i = 1g_j$. Следовательно, элементы ag_1, ag_2, $\ldots$, ag_N это просто перестановка элементов g_1, g_2, $\ldots$, g_N, так что их произведения совпадают:

$$(ag_1)(ag_2)\ldots(ag_N) = g_1g_2\ldots g_N.$$

Переставляя сомножители, получаем:

$$a^N(g_1g_2\ldots g_N) = g_1g_2\ldots g_N.$$

Произведение $b = g_1g_2\ldots g_N$ это некоторый элемент группы, у него есть обратный b^{-1}. Тогда, домножая равенство $a^Nb = b$ на этот обратный, получаем $a^N = 1$, что и требовалось.

Частный случай этой теоремы для группы обратимых элементов кольца $\mathbb{Z}_n$ называется *теоремой Эйлера*: если целые числа a и n не имеют общих делителей, то $a^{\varphi(n)} \equiv 1 \mod n$. Если число n простое, то $\varphi(n) = n - 1$; в этом случае это утверждение называется *Малой теоремой Ферма*: если целые числа a не делится на простое число p, то $a^{p-1} \equiv 1 \mod p$.

Задача для размышления: При возведении в степени целого числа, не делящегося на 2 и 5, его последние две цифры будут периодически повторяться. Найти наибольший возможный период. Другими словами, найти наибольший возможный порядок элемента в $\mathbb{Z}^*_{100}$.

4. Китайская теорема об остатках. Явные формулы. Вычисление функции Эйлера.

Напоминание: порядки элементов, теоремы Эйлера и Ферма (малая).

Задача для размышления: если p — простое число, то $(p-1)! \equiv -1 \pmod p$ (теорема Вильсона).

Определение прямого произведения колец.

Напоминание: изоморфизм колец.

Примеры: $\mathbb{Z}_2 \times \mathbb{Z}_2$ не изоморфно $\mathbb{Z}_4$, потому что в $\mathbb{Z}_2 \times \mathbb{Z}_2$ единица (т.е. пара $(1,1)$) имеет по сложению порядок 2, а в $\mathbb{Z}_4$ единица имеет по сложению порядок 4. Другой пример: $\mathbb{Z}_2 \times \mathbb{Z}_3$ изоморфно $\mathbb{Z}_6$. Для построения изоморфизма достаточно убедиться в том, что все элементы $\mathbb{Z}_2 \times \mathbb{Z}_3$ являются кратностями единицы (т.е. пары

$(1,1)$), и сложение и умножение в $\mathbb{Z}_2 \times \mathbb{Z}_3$ определяется сложением и умножением этих кратностей по модулю 6.

Те же самые аргументы, примененные к произвольным m и n без общих делителей, дают следующую теорему.

Теорема 4.1. Китайская теорема об остатках (слабая форма). *Если m и n взаимно просты, то кольцо $\mathbb{Z}_{mn}$ изоморфно прямому произведению $\mathbb{Z}_m \times \mathbb{Z}_n$, причем изоморфизм задается отображением $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, сопоставляющим остатку $a \in \mathbb{Z}_{mn}$ пару $(a \pmod m, a \pmod n) \in \mathbb{Z}_m \times \mathbb{Z}_n$.*

Сильная форма китайской теоремы об остатках дает формулу обратного изоморфизма $\mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$. Необходимым ингредиентами для этого являются идемпотентные остатки e и $1-e$ в $\mathbb{Z}_{mn}$, такие что $e \equiv 1 \pmod m$ и $e \equiv 0 \pmod n$. (Тогда, соответственно, $1-e \equiv 0 \pmod m$ и $1-e \equiv 0 \pmod n$.) Для того, чтобы найти e, достаточно найти какое-нибудь решение (x_0, y_0) уравнения $mx + ny = 1$, и тогда $e = ny_0$, $1 - e = mx_0$.

Теорема 4.2. Китайская теорема об остатках (сильная форма). *В условиях предыдущей теоремы обратный изоморфизм $\mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$ задается формулой $(a, b) \mapsto ae + b(1-e)$.*

Как описать обратимые элементы прямого произведения колец $A \times B$? Очевидный ответ: пара $(a, b) \in A \times B$ обратима тогда и только тогда, когда обратимы элементы $a \in A$ $b \in B$. Другими словами, $(A \times B)^* = A^* \times B^*$. Из этого и китайской теоремы об остатках следует мультипликативность функции Эйлера, т.е. если m и n взаимно просты, то $\varphi(mn) = \varphi(m)\varphi(n)$.

Остальные формулы, необходимые для вычисления значений функции Эйлера: если число p простое, то $\varphi(p^n) = p^n - p^{n-1}$.

5. Кольцо многочленов.

Определение кольца многочленов $A[t]$ с коэффициентами в кольце A. Примеры.

Значение многочлена $P(t) \in A[t]$ на элементе $\alpha \in A$: $P(\alpha) \in A$. Получается отображение кольца многочленов $A[t]$ в множество функций из A в A, которое мы обозначим $\mathcal{F}(A, A)$, т.е. отображение $v : A[t] \to \mathcal{F}(A, A)$.

Хорошо известный со школы пример: $A = \mathbb{R}$. В этом случае отображение v инъективно, т.е. разным многочленам соответствуют разные функции действительного переменного (почему?). С другой стороны, отображение v в этом случае точно не сюръективно:

мы знаем много функций, которые не выражаются многочленами (показательные, логарифмические, тригонометрические и т.д.).

Если же A конечное кольцо, скажем, $|A| = q$, то кольцо многочленов, очевидно, бесконечно, а вот множество функций $\mathcal{F}(A, A)$, очевидно, конечно и состоит из q^q элементов (почему?). Поэтому отображение v точно не может быть инъективным, т.е. различные многочлены могут задавать одну и ту же функцию; тогда, очевидно, их разность будет задавать нулевую функцию.

Очень легко придумать многочлен степени q, который точно задает нулевую функцию: $N(t) = \prod_{\alpha \in A}(t - \alpha)$.

Задача для размышления:
1) Существуют ли многочлены меньшей степени для $A = \mathbb{Z}_n$, задающие нулевую функцию? (Ответ разный для простого и составного n.)
2) Найти все коэффициенты многочлена $N(t)$ для $A = \mathbb{Z}_p$, p — простое число.
3) Сюръективно ли отображение v для $A = \mathbb{Z}_n$? Другими словами, любая ли функция задается многочленом?

Одним из главных инструментов при работе с многочленами является деление с остатком. Пусть $P(t)$ и $Q(t)$ два многочлена из $A[t]$, и $\deg P > 0$. По определению, деление многочлена $Q(t)$ на многочлен $P(t)$ есть представление

$$Q(t) = P(t)S(t) + R(t), \text{ где } \deg R < \deg P. \tag{12}$$

При этом многочлен R называется остатком от деления Q на P, а многочлен S называется неполным частным. Вопрос о возможности и единственности деления с остатком дается следующим утверждением.

Предложение 5.1. *1) Если деление с остатком возможно и старший коэффициент многочлена P не является делителем нуля, то оно единственно.*
2) Если старший коэффициент многочлена P обратим, то деление с остатком возможно (и, следовательно, единственно).

Первое общеизвестное приложение это теорема Безу.

Теорема 5.1. Теорема Безу. *Остаток от деления многочлена $Q(t)$ на $t - \alpha$ равен $Q(\alpha)$ (т.е. значению многочлена Q в точке α). В частности, если α является корнем, то $Q(t)$ нацело делится на $t - a$.*

Следствие 5.1. *Если в кольце нет делителей нуля, то число корней любого многочлена не превосходит его степени.*

Для кольца с делителями нуля это следствие уже не верно; мы приводили много примеров для колей $\mathbb{Z}_n$ с составным n.

Многочлен положительной степени называется неприводимым, если его нельзя представить в виде произведения многочленов меньшей степени. Очевидно, что любой многочлен первой степени неприводим. Нетрудно убедиться, что любой многочлен представить в виде произведения неприводимых.

Важное наблюдение состоит в том, что если кольцо многочленов над полем по своим свойствам очень похоже на кольцо целых чисел. В частности, в кольце многочленов, как и в кольце целых чисел, верна теорема о единственности разложения на простые множители, только для многочленов термин "простые"надо заменить на "неприводимые".