МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ. СЕМИНАРЫ

НЕСТЕРЕНКО
ЮРИЙ ВАЛЕНТИНОВИЧ

МЕХМАТ МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

БЛАГОДАРИМ ЗА ПОДГОТОВКУ КОНСПЕКТА
СТУДЕНТКУ ФАКУЛЬТЕТА ВМК МГУ
НЕДОЛИВКО ЮЛИЮ НИКОЛАЕВНУ

Содержание

Семинар 1

Свойства целых чисел

Вспомним сначала некоторые факты.

Предположим, у нас есть два числа $a, b \in \mathbb{Z}$. Число b *делит*[1] число a, если $\exists$ число c такое, что $a = b \cdot c$, $b \neq 0$ (обозначается $b \mid a$).

Не все числа делятся друг на друга. Например, $2 \nmid 3$.

Теорема 1.1. *Если $b > 0$, то для любого $a \in \mathbb{Z}$ существует единственная пара чисел $q, r \in \mathbb{Z}$ таких, что*

$$a = b \cdot q + r, \quad 0 \leq r < b.$$

Замечание 1.1. Число r из теоремы 1.1 называется *остатком*, а q – *неполным частным.*

Предположим, что у нас есть целые числа $a_1, a_2, \ldots, a_m$.

Определение 1.1. Число d называется *общим делителем* a_i, если

$$d \neq 0, \quad d \mid a_i, \quad i = 1, \ldots, m.$$

Самый большой из общих делителей a_i называется их *наибольшим общим делителем.*[2]

Обозначается НОД как

$$\text{НОД}(a_1, \ldots, a_m) = (a_1, \ldots, a_m).$$

Для двух целых чисел a, b из теоремы 1.1

$$(a, b) = (b, r).$$

Алгоритм Евклида

Пусть числа $a \geq b > 0$. Обозначим $r_0 = a$, $r_1 = b$.
Разделим a на b с остатком. По теореме 1.1,

$$a = r_0 = r_1 \cdot q_1 + r_2, \quad 0 \leq r_2 < r_1.$$

Теперь разделим r_1 на r_2 с остатком. Получим, что

$$b = r_1 = r_2 \cdot q_2 + r_3, \quad 0 \leq r_3 < r_2.$$

Продолжая делить с остатком, получим наконец, что

$$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1}.$$

[1] Иногда в такой ситуации говорят, что a *делится* на b (обозначается $a \vdots b$).
[2] Чтобы НОД существовал, надо предполагать какое-нибудь из a_i отличным от нуля.

Заметим, что r_i – последовательность неотрицательных убывающих чисел. Такая последовательность конечна. Значит, цепочка вычислений будет конечна, и на каком-то шаге мы будем делить нацело, то есть

$$r_{n-1} = r_n \cdot q_n.$$

Это число $r_n = (a, b)$.

Замечание 1.2. Если чисел несколько, то вычисление НОД происходит последовательно:

$$(a_1, \ldots, a_n) = ((a_1, \ldots, a_{m-1}), a_m)\,.$$

Определение 1.2. Если $(a, b) = 1$, то a и b *взаимно просты.*

Аксиома индукции

Предположим, есть утверждения

$$A_1,\ A_2,\ \ldots,\ A_n,\ \ldots, \quad n \in \mathbb{Z}. \tag{1}$$

Если

1. A_1 – верно;
2. Для любого $n \geq 1$, если A_n верно $\Rightarrow$ A_{n+1} верно;

то все утверждения (1) верны.

Задачи

Задача 1.1. *Доказать, что*

$$10^n + 18n - 1 \vdots 27$$

при любом $n \geq 1$.

Решение Воспользуемся аксиомой индукции. Обозначим

$$a_n = 10^n + 18n - 1, \quad n \geq 1, \quad A_n :\ a_n \vdots 27.$$

Проверим утверждение A_1:

$$a_1 = 10 + 18 - 1 = 27 \vdots 27.$$

Допустим теперь, что A_n – верно, то есть $a_n \vdots 27$.

Распишем

$$a_{n+1} = 10^{n+1} + 18(n+1) - 1,$$

Найдем разность

$$a_{n+1} - 10a_n = 10^{n+1} + 18(n+1) - 1 - 10(10^n + 18n - 1) =$$

$$= 18n + 18 - 1 - 180n + 10 = -162n + 27 \vdots 27.$$

Получили, что

$$a_{n+1} - 10a_n \vdots 27.$$

Так как по нашему предположению $a_n \vdots 27$, получаем, что $a_{n+1} \vdots 27$.

Задача решена.

Задача 1.2. *Рассмотрим последовательность*

$$a_n = 2^{5n+3} + 5^n 3^{n+2}.$$

Доказать, что верно утверждение

$$A_n = a_n \vdots 17, \quad n \geq 1.$$

Решение Проверим сначала A_1. При $n = 1$

$$a_1 = 2^{5+3} + 5 \cdot 3^3 = 256 + 135 = 391 = 17 \cdot 23 \vdots 17$$

Перейдем к шагу индукции. Распишем

$$a_{n+1} = 2^{5n+8} + 5^{n+1} 3^{n+3}.$$

Найдем разность

$$a_{n+1} - 2^5 \cdot a_n =$$

$$= 5^{n+1} 3^{n+3} - 2^5 \cdot 5^n \cdot 3^{n+2} = 5^n \cdot 3^{n+2} (5 \cdot 3 - 32) = 5^n \cdot 3^{n+2} \cdot (-17) \vdots 17.$$

То есть

$$a_{n+1} - 2^5 \cdot a_n \vdots 17,$$

и, так как по индуктивному преположению a_n делится на 17, получим, что $a_{n+1} \vdots 17$.

Задача решена.

Задача 1.3. *Обозначим*

$$a_n = 2^{3^n} + 1.$$

Показать, что справедливо утверждение

$$A_n : 2^{3^n} + 1 \vdots 3^{n+1}, \quad \forall\, n \geq 1.$$

Решение Для $n = 1$ получим

$$a_1 = 2^3 + 1 = 9 \vdots 9 = 3^{1+1}.$$

Таким образом, A_1 верно.

Шаг индукции будем доказывать немного по-другому. Запишем

$$a_n - 1 = 2^{3^n}, \quad (a_n - 1)^3 = 2^{3^{n+1}}.$$

Тогда

$$a_{n+1} = (a_n - 1)^3 + 1.$$

Рассмотрим разность

$$a_{n+1} - a_n^3 = a_n^3 - 3a_n^2 + 3a_n - 1 + 1 - a_n^3 = 3a_n(-a_n + 1) \vdots 3^{n+2}.$$

Так как

$$a_n^3 \vdots \left(3^{n+1}\right)^3 = 3^{3n+3},$$

то $a_n^3 \vdots 3^{n+2}$. Значит, $a_{n+1} \vdots 3^{n+2}$. Задача решена.

Числа Фибоначчи

Определение 1.3. *Числами Фибоначчи* называют последовательность следующую последовательность целых чисел:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+1} = F_n + F_{n-1}, \quad n \geq 1.$$

Например,

$$F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5, \quad F_6 = 8, \ldots$$

Задача

Задача 1.4. *Показать, что*

$$2 \mid F_n \iff 3 \mid n.$$

Решение Будем доказывать задачу по индукции. Возьмем следующее индуктивное предположение:

$$A_n : 2 \mid F_m \iff 3 \mid m, \quad \forall\, 0 \leq m \leq n.$$

Вручную можно проверить, что A_1, A_2, A_3 – верны.

Предположим теперь, что A_n верно при $n \geq 3$.

$$F_{n+1} = F_n + F_{n-1} = F_{n-1} + F_{n-2} + F_{n-1} = 2F_{n-1} + F_{n-2}.$$

Из этого следует, что

$$2 \mid F_{n+1} \iff 2 \mid F_{n-2} \iff 3 \mid n-2 \iff 3 \mid n+1.$$

Задача решена.

Формула бинома

Запишем

$$(1+x)^0 = 1,$$
$$(1+x)^1 = 1+x,$$
$$(1+x)^2 = 1+2x+x^2,$$
$$(1+x)^3 = 1+3x+3x^2+x^3,$$

и так далее. Для произвольного n обозначим коэффициенты

$$(1+x)^n = C_n^0 + C_n^1 x + C_n^2 x^2 + \ldots + C_n^{n-1}x^{n-1} + C_n^n x^n.$$

Наша задача – вычислить эти коэффициенты. Заметим, что

$$C_n^0 = 1, \quad C_n^n = 1.$$

Выразим коэффициенты для $n+1$ через коэффициенты для n. Запишем

$$(x+1)^{n+1} = (1+x)(1+x)^n = C_n^0 + C_n^1 x + \ldots + C_n^k x^k + \ldots + C_n^{n-1}x^{n-1} + C_n^n x^n +$$
$$+ C_n^0 x + C_n^1 x^2 + \ldots + C_n^{k-1}x^k + \ldots + C_n^{n-1}x^n + C_n^n x^{n+1}.$$

Получается, что

$$C_{n+1}^k = C_n^k + C_n^{k-1}, \quad 1 \le k \le n.$$

Теорема 1.2. *Биномиальные коэффициенты вычисляются по формуле* [3]

$$C_n^k = \frac{n!}{k!(n-k)!}, \quad 0 \le k \le n. \tag{2}$$

Доказательство
Для $k = 0$, n

$$C_n^k = 1,$$

что совпадает с полученными выше коэффицентами.

Вычислим теперь коэффицент для $k \ge 1$

$$C_{n+1}^k = C_n^k + C_n^{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} =$$
$$= \frac{n!}{k!(n-k+1)!}(n-k+1+k) = \frac{(n+1)!}{k!(n+1-k)!}.$$

Таким образом, используя аксиому индукции, можно доказать формулу (2).

[3] Факториал вычисляется по формуле

$$n! = 1 \cdot 2 \cdot \ldots \cdot n, \quad 0! = 1.$$

Семинар 2

Задачи

Задача 2.1. *Доказать, что для* $\forall\ m \geq 1$ *соседние числа Фибоначчи взаимно просты, т.е.*

$$(F_m, F_{m+1}) = 1$$

Решение Обозначим это утверждение через A_n.
A_1 верно, так как

$$F_1 = 1, \quad F_2 = 2 \ \Rightarrow\ (F_1, F_2) = 1.$$

Перейдем к шагу индукции. Допустим, что A_m – верно. Нужно рассмотреть (F_{m+1}, F_{m+2}).

Вспомним сначала некоторые **свойства НОД**.
1. $d \,|\, bc, \quad (d, c) = 1 \ \Rightarrow\ d \,|\, b.$
2. Если $a = bs + c$, то

$$(a, b) = (b, c).$$

3.

$$(bs + c, b) = (c, b). \tag{3}$$

4. Если $(a, c) = 1$, то

$$(a, bc) = (a, b). \tag{4}$$

Итак, используя эти свойства, можем записать

$$(F_{m+1}, F_{m+2}) = (F_{m+1}, F_{m+1} + F_m) = (F_{m+1}, F_m) = 1.$$

Задача решена.

Задача 2.2. *Показать, что*

$$F_{m+n} = F_{n-1} \cdot F_m + F_n \cdot F_{m+1}, \quad \forall\, m \geq 0,\ n \geq 1. \tag{5}$$

Решение Обозначим через A_n утверждение, что (5) верно при всех $\leq n$.
Для $n = 1$ получим

$$F_{m+1} = 0 \cdot F_m + F_{m+1}.$$

Перейдем к шагу индукции. Предположим, что A_n верно. По определению,

$$F_{n+1+m} = F_{n+m} + F_{n-1+m} = F_{n-1} \cdot F_m + F_n \cdot F_{m+1} + F_{n-2+m} F_{n-1} F_{m+1} =$$

$$= F_n \cdot F_m + F_{n+1} \cdot F_{m+1}.$$

Итак, мы доказали для индекса $n + 1$, а для всех меньших индексов верно по индуктивному предположению.
Задача решена.

Задача 2.3. *Показать, что*

$$(F_n, F_m) = F_{(n,m)}, \quad n \text{ или } m > 0. \tag{6}$$

Решение Так как это свойство симметричное, будем считать, что $n \geq m$. Если $n = m$,

$$F_n = (F_n, F_m) = F_{(n,m)}.$$

Поэтому будем считать, что $n > m$.

Обозначим через A_k индуктивное предположение, что (6) верно при любых n, m таких, что $n + m \leq k$.

Для $k = 1$ проверяется подстановкой ($n = 0, m = 1$ или $n = 1, m = 0$).

Покажем теперь, что $A_k \iff A_{k+1}$. Предположим, что у нас есть индесы u, v такие, что $u + v = k + 1$. Будем считать, что $u > v$. Вычислим (F_u, F_v). Для этого воспользуемся свойством задачи 2.2 относительно индексов $u - v$ и v:

$$F_u = F_{u-1-v}F_v + F_{u-v}F_{v+1}.$$

Воспользовавшись свойствами (3), (4), получим, что

$$(F_u, F_v) = (F_{u-v}F_{v+1}, F_V) = (F_{u-v}, F_v) = F_{(u-v,v)}.$$

Последний переход следует из индуктивного предположения A_k. Воспользовавшись свойством (3), можем записать

$$(F_u, F_v) = F_{(u-v,v)} = F_{(u,v)}.$$

Задача решена.

Задача 2.4. *Показать, что*

$$F_n \,|\, F_m \iff n \,|\, m.$$

Решение Это свойство можно переписать в виде

$$F_n = (F_n, F_m) = F_{(n,m)} \iff n = (n, m) \iff n \,|\, m.$$

Задача решена.

Простые и составные числа

Определение 2.1. Число n называется *составным*, если

$$n = a \cdot b, \quad a < n, \quad b < n,$$

и *простым*, если такого представления не существует.

Множество простых чисел бесконечно.

Будем обозначать простые числа буквой p. Каждое число n может быть разложено следующим образом:

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \quad p_1 < p_2 < \dots < p_k. \tag{7}$$

Обозначим

$$\nu_{p_i}(n) = \alpha_i.$$

Задачи

Задача 2.5. *Доказать, что множество простых чисел вида $4k-1$ бесконечно.*

Решение Предположим обратное. Пусть $p_1, \dots, p_r$ – все простые числа вида $4k-1$. Построим число вида

$$Q = 4p_1 \dots p_r - 1$$

и покажем, что существует простое $q \mid Q$, имеющее вид $4k-1$.

Обозначим все простые делители числа Q из разложения (7) как

$$q_1, \dots, q_s.$$

Очевидно, они все нечетны. Предположим, что все [4]

$$q_i = 4l_i + 1.$$

В таком случае произведение, например, двух таких чисел выглядит как

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4c + 1.$$

Значит, число Q должно иметь вид

$$Q = 4L + 1.$$

Получили противоречие. Это значит, что существует $q \mid Q$ такое, то $q = 4l - 1$.

При этом $q \neq p_1, \dots, p_r$. Получили противоречие с исходных утверждением. Значит, множество простых чисел вида $4k-1$ бесконечно.

Задача решена.

Задача 2.6. *Пусть a, b – натуральные, $(a,b) = 1$. Показать, что тогда*

$$b \mid C_b^a, \quad b > a.$$

Решение Запишем

$$C_b^a = \frac{b!}{a!(b-a)!} = \frac{b}{a}\frac{(b-1)!}{(a-1)!(b-a)!} = \frac{b}{c}C_{b-1}^{a-1},$$

или

$$aC_b^a = bC_{b-1}^{a-1}.$$

Значит,

$$b \mid aC_b^a.$$

По условию $(a,b) = 1$. Значит, по свойствам НОД,

$$b \mid C_b^a.$$

В частности, если $b = p$ (т.е. простое), то

$$p \mid C_p^k, \quad 1 \leq k \leq p-1.$$

Задача решена.

[4] Все нечетные числа имеют вид $4k+1$ или $4k-1$.

Задача 2.7. *(малая теорема Ферма) Если p – простое, то при любом целом n*

$$p \mid n^p - n.$$

Доказательство Рассмотрим $p = 2$. В этом случае

$$n^2 - n = n(n-1) \vdots 2.$$

При $p \geq 3$ воспользуемся индукцией. Обозначим

$$a_n = n^p - n,$$

а исходное утверждение за A_n.

При $n = 1$ получим

$$a_1 = 1^p - 1 = 0 \vdots p.$$

Перейдем к шагу индукции. Предположим, что A_n справедливо. Распишем

$$a_{n+1} = (n+1)^p - (n+1).$$

Рассмотрим разность

$$a_{n+1} - a_n = (n+1)^p - n^p - 1 = C_p^0 + C_p^1 + \ldots + C_p^{p-1} n^{p-1} + C_p^p n^p - n^p - 1 =$$

$$= C_p^1 + \ldots + C_p^{p-1} n^{p-1}.$$

Так как все оставшиеся коэффициенты делятся на p,

$$p \vdots a_{n+1} - a_n$$

а так как $p \mid a_n$, то

$$p \mid a_{n+1}.$$

Утверждение доказано для $n \geq 1$. Для отрицательных чисел

$$(-n)^p - (-n) = -(n^p - n).$$

Теорема доказана.

Задача 2.8. *Найти все числа n такие, что C_n^k, $0 \leq k \leq n$ нечетны.*

Решение Будем доказывать индукцией по n следующее утверждение:
Все числа C_n^k, $0 \leq k \leq n$ нечетны $\iff$ $n = 2^t - 1$.
$\Rightarrow C_n^1 = n$ – нечетно.
Рассмотрим

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Вычислим, с какой кратностью в $n!$ входит 2.

$$\nu_2(n!) = \nu_2(1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot n) =$$

$$= \nu_2(2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2m) = \nu_2(2^m m!) = m + \nu_2(m!),$$

где $n = 2m + 1, \quad m = [n/2]$.

Аналогично, обозначив $r = [k/2]$ и $s = [(n-k)/2]$, получим

$$\nu_2(k!) = r + \nu_2(r!), \quad \nu_2((n-k)!) = s + \nu_2(s!).$$

Значит,

$$\nu_2(C_n^k) = m - r - s + \nu_2\left(\frac{m!}{r!s!}\right). \tag{8}$$

В случае, когда $k = 2r$, получим

$$r = \frac{k}{2}, \quad s = m - \frac{k}{2}, \quad r + s = m.$$

Если $k = 2r + 1$,

$$s = \left[\frac{2m + 1 - 2r - 1}{2}\right] = m - r, r + s = m.$$

Тогда, с учетом (8),

$$\nu_2(C_n^k) = \nu_2(C_m^r).$$

По индуктивному предположению, C_n^k – нечетны, значит, левая часть равна 0. Значит,

$$m = 2^l - 1, \quad n = 2(2^l - 1) + 1 = 2^{l+1} - 1, \quad t = l + 1.$$

$\Leftarrow$ Предполагаем, что $n = 2^t - 1 = 2m + 1$. Тогда $m = 2^{t-1} - 1$.

Отсюда следует, что биномиальные коэффициенты в правой части (8) нечетные. Так как это равенство вводилось в предположении, что биномиальные коэффициенты нечетные, автоматически все выполняется.

Задача решена.

Семинар 3

Задачи

Задача 3.1. *Пусть a, b, c – нечетные числа. Показать, что тогда*

$$\left(\frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}\right) = (a, b, c). \tag{9}$$

Решение Будем доказывать, что множества общих делителей чисел, стоящих справа и слева, будут одинаковы.

Предположим, что $d \,|\, a, b, c$. Тогда

$$d \,|\, 2\frac{a+b}{2} = a + b.$$

Так как d – нечетно, то $(d, 2) = 1$ и по свойствам делителей

$$d \,|\, \frac{a+b}{2}.$$

Аналогично доказывается, что

$$d \,|\, \frac{a+c}{2}, \quad d \,|\, \frac{b+c}{2}.$$

Значит, d – общий делитель чисел слева в (9).

Теперь предположим, то

$$d \,|\, \frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}.$$

Рассмотрим комбинацию

$$d \,|\, \frac{a+b}{2} + \frac{a+c}{2} - \frac{b+c}{2} = a.$$

Аналогично получим, что

$$d \,|\, \frac{a+b}{2} + \frac{b+c}{2} - \frac{a+c}{2} = b, \quad d \,|\, c.$$

Итак, получили, что множества делителей чисел в левой и правой частях (9) совпадают. Значит, сопадают и их максимумы, то есть НОДы.

Задача решена.

Задача 3.2. *Даны числа*

$$a = \underbrace{11\ldots1}_{n}, \quad b = \underbrace{11\ldots1}_{m}.$$

Найти (a, b).

Решение Будем считать, что $n \geq m$. Запишем

$$10^{n-m}b = \underbrace{11\ldots1}_{m}\overbrace{0\ldots0}^{n-m}.$$

Вычислим

$$a - 10^{n-m}b = \underbrace{11\ldots1}_{n-m}.$$

По свойству НОД можем записать

$$(a - 10^{n-m}b, b) = (a, b) = \left(\underbrace{11\ldots1}_{n-m}, \underbrace{11\ldots1}_{m}\right). \tag{10}$$

Это дает нам возможность применить индукцию. Покажем, что

$$\left(\underbrace{11\ldots1}_{n}, \underbrace{11\ldots1}_{m}\right) = \underbrace{11\ldots1}_{(n,m)}. \tag{11}$$

Сформулируем утверждение A_k:

(11) имеет место для любых n, m таких, что $n + m \leq k$.

Покажем, что $A_k \iff A_{k+1}$. Предположим, у нас есть числа $u, v \geq 1$, $u > v$, $u + v = k + 1$ (а $(u - v) + v = u < k + 1$. По (10),

$$\left(\underbrace{11\ldots1}_{u}, \underbrace{11\ldots1}_{v}\right) = \left(\underbrace{11\ldots1}_{u-v}, \underbrace{11\ldots1}_{v}\right) = \underbrace{11\ldots1}_{(u-v,v)} = \underbrace{11\ldots1}_{(u,v)}.$$

Задача решена.

Решение уравнений

Рассмотрим уравнения вида

$$ax + by = c,$$

где a, b, c – целые, а x, y – целые неизвестные.

Теорема 3.1. *Уравнение $ax + by = c$ разрешимо $\iff$ когда $(a, b) \mid c$.*

Примеры

Пример 3.1. *Найти все числа, которые удовлетворяют уравнению*

$$17x + 27y = 1.$$

Составим таблицу

	27	17
x	0	1
y	1	0

Последовательно вычитая столбцы, получим

	27	17	10	7	3	1	0
x	0	1	-1	2	-3	8	-27
y	1	0	1	-1	2	-5	17

Возьмем значения x и y из предпоследнего и последнего стоблцов. Запишем

$$\begin{cases} x = 8 - 27t \\ y = -5 + 17t \end{cases}, \quad t \in \mathbb{Z},$$

что и будет решением исходного уравнения.
Если бы у нас было уравнение

$$17x - 27y = 1,$$

могли бы его записать как

$$17x + 27(-y) = 1.$$

Тогда множество его решений это

$$\begin{cases} x = 8 - 27t \\ y = 5 - 17t \end{cases}, \quad t \in \mathbb{Z}.$$

Пример 3.2. *Найти все решения уравнения*

$$144x + 233y = 8.$$

Как и в предыдущем примере, строим таблицу

	233	144
x	0	1
y	1	0

и, вычитая столбцы, получим таблицу следующего вида

	233	144	89	55	34	21	13	8	...	0
x	0	1	-1	2	-3	5	-8	13	...	-233
y	1	0	1	-1	2	-3	5	-8	...	144

Получаем, что

$$\begin{cases} x = 13 - 233t \\ y = -8 + 144t \end{cases}, \quad t \in \mathbb{Z}.$$

Алгоритм решения уравнений

Дано уравнение

$$a_1x_1 + \ldots + a_mx_m = b, \quad a_j \in \mathbb{Z}, \quad b \in \mathbb{Z}.$$

1. Составить таблицу

$$A = \begin{pmatrix} a_1 & a_2 & \ldots & a_m \\ 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & 1 \end{pmatrix} \tag{12}$$

2. В любом столбце изменить знаки всех элементов.
3. Можно любой столбец умножить на целое число и вычесть из другого.

В итоге исходная таблица должна быть приведена к виду

$$C = \begin{pmatrix} 0 & \ldots & 0 & d & 0 & \ldots & 0 \\ c_{11} & \ldots & & c_{1k} & & \ldots & c_{1m} \\ c_{21} & \ldots & & c_{2k} & & \ldots & c_{2m} \\ \vdots & \ddots & & \vdots & & \ddots & \vdots \\ c_{m1} & \ldots & & c_{mk} & & \ldots & c_{mm} \end{pmatrix} \tag{13}$$

4. Если оказалось, что $d \nmid b$, решений нет.
5. Если $d \mid b$, уравнение разрешимо. Обозначим

$$C_j = \begin{pmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{mj} \end{pmatrix}, X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}. \tag{14}$$

Тогда решение уравнения имеет вид

$$X = t_1C_1 + \ldots + \frac{b}{d}C_k + \ldots + t_mC_m, \quad t_j \in \mathbb{Z}. \tag{15}$$

Задача

Задача 3.3. *Решить уравнение*

$$3x + 5y + 7z = 1.$$

Решение Пишем исходную таблицу:

$$\left(\begin{array}{ccc} 3 & 5 & 7 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc} 3 & -1 & 1 \\ \hline 1 & -2 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc} 0 & 0 & 1 \\ \hline 7 & -4 & -2 \\ 0 & 1 & 0 \\ -3 & 1 & 1 \end{array}\right).$$

Значит, решения этого уравнения имеет вид

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 7 \\ 0 \\ -3 \end{pmatrix} t_1 + \begin{pmatrix} -4 \\ 1 \\ 1 \end{pmatrix} t_2 + \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}, \quad t_1, t_2 \in \mathbb{Z}.$$

Задача решена.

Семинар 4

Обоснование работы алгоритма

Напишем какую-нибудь промежуточную преобразованную матрицу из алгоритма решения уравнений (ссылка):

$$B = \begin{pmatrix} v_1 & \dots & v_m \\ u_{11} & \dots & u_{1m} \\ \vdots & \ddots & \vdots \\ u_{m1} & \dots & u_{mm} \end{pmatrix}.$$

Разобьем доказательство работы алгоритма на части.

1. Для всех матриц B выполняется

$$(v_1, \dots, v_m) = (a_1, \dots, a_m) = d, \tag{16}$$

Последнее равенство получается из того, что на последнем шаге

$$(0, \dots, 0, d, 0, \dots, 0) = d,$$

то есть

$$d = (a_1, \dots, a_m).$$

Убедимся, что это действительно так.

Воспользуемся индукцией. В случае, когда $B = B_1 = A$, где A – матрица (12), утверждение (16) очевидно.

Предположим, что для $B = B_n$ утверждение выполняется. Обозначим

$$U_i = \begin{pmatrix} u_{1i} \\ \vdots \\ u_{mi} \end{pmatrix}.$$

На очередном шаге алгоритма происходят преобразования

$$U_i - qU_j, \quad (v_1, \dots, v_i - qv_j, \dots, v_m) = (v_1, \dots, v_m).$$

Последнее равенство следует из свойств НОД. Таким образом, при переходе к матрице B_{n+1} НОД (16) не изменяется.

2. Если b не делится на d, то решений нет.

Предположим обратное. Пусть существуют целые $z_1, \dots, z_m$ такие, что

$$a_1 z_1 + \dots + a_m z_m = b.$$

Из пункта (16)

$$d \,|\, a_1, \quad d \,|\, a_2, \quad \dots, \quad d \,|\, a_m,$$

а значит,

$$d \,|\, a_1 z_1 + \dots + a_m z_m \;\Rightarrow\; d \,|\, b.$$

Получили противоречие.

Обозначим через $L(X)$ линейную комбинацию

$$L(X) = a_1x_1 + \ldots + a_mx_m.$$

3. В любой промежуточной матрице B

$$L(U_1) = v_1, \quad \ldots, \quad L(U_m) = v_m. \tag{17}$$

Обозначим столбцы матрицы A (12) как $E_1, \ldots, E_m$. Для них верно

$$L(E_1) = a_1, \ldots, L(E_m) = a_m.$$

Предположим теперь, что (17) верно для матрицы B_n. Покажем, что из этого следует это же утверждение для B_{n+1}.

Если меняются знаки у столбца матрицы B, свойство (17) сохраняется. Теперь, если от столбца отнимается другой столбец, умноженный на число, то

$$U_i \ \rightarrow \ U_i - qU_j.$$

Вычислим

$$L(U_i - qU_j) = L(U_i) - qL(U_j) = v_i - qv_j,$$

то есть свойство (17) для B_{n+1} выполняется.

4. Если $d \,|\, b$, то вектор X (15) будет решением исходного уравнения.

Запишем

$$L(X) = t_1L(C_1) + \ldots + \frac{b}{d}L(C_k) + \ldots + t_mL(C_m) =$$

$$= \frac{b}{d}L(C_k) = \frac{b}{d}d = b.$$

Здесь C_i – вектор-столбцы из (14).

5. Пусть B – промежуточная матрица и

$$S = \begin{pmatrix} s_1 \\ \vdots \\ s_m \end{pmatrix}$$

– произвольный вектор с целыми координатами.

Тогда существуют целые числа $t_1, \ldots, t_m$ такие, что

$$S = t_1U_1 + \ldots + t_mU_m. \tag{18}$$

Для матрицы A достаточно взять $t_i = s_i$. Тогда

$$s_1E_1 + \ldots + s_mE_m = S.$$

Перейдем к шагу индукции. Предположим, что для $B = B_n$ утверждение (18) верно. Посмотрим, что произойдет при преобразовании столбца

$$U_i \ \to \ U_i - qU_j.$$

Для следующей линейной комбинации верно

$$t_1U_1 + \ldots + t_i(U_i - qU_j) + \ldots + (t_j + qt_i)U_j + \ldots + t_mU_m = S.$$

Осталось показать, что любое решение уравнения представимо в таком виде. Пусть X – решение. Согласно пункту 5,

$$X = t_1C_1 + \ldots + t_mC_m.$$

Подставив X в исходное уравнение, получим

$$b = L(X) = t_1L(C_1) + \ldots + t_mL(C_m) = t_kL(C_k) = t_k \cdot d.$$

Значит, $t_k = b/d$.

Таким образом, любое решение представимо в виде (15).

Семинар 5

Задачи

Задача 5.1. *Предположим, есть число вида*

$$\frac{m}{n} = \frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{p-1},$$

где p – простое, $(m, n) = 1$. Показать, что тогда $p \mid m$.

Решение Для доказательства будем складывать слагаемые в другом порядке:

$$\frac{1}{k} + \frac{1}{p-k} = \frac{p-k+k}{k(p-k)} = \frac{p}{k(p-k)},$$

где $1 \leq k \leq (p-1)/2$. Тогда дробь можно записать в виде

$$\frac{m}{n} = p\left(\frac{1}{1\cdot(p-1)} + \frac{1}{2(p-2)} + \ldots + \frac{1}{\frac{p-1}{2}\frac{p+1}{2}}\right) = p\cdot\frac{A}{B}, \quad p \nmid B.$$

$$mB = pAn, \;\; \Rightarrow \;\; p \mid Bm, \;\; (p, B) = 1, \quad \Longleftrightarrow \;\; p \mid m.$$

Задача решена.

Задача 5.2. *Даны числа $p, p+10, p+14$ – простые. Найти p.*

Решение Заметим, что

$$(p+10) - p = 10 \not\vdots 3,$$

$$(p+14) - p = 14 \not\vdots 3,$$

$$(p+14) - (p+10) = 4 \not\vdots 3.$$

При этом данные числа имеют разные остатки[5] от деления на 3. Значит, при любом значении p какое-то из чисел $p, p+10, p+14$ делится на 3.

Так как эти числа простые, единственный вариант – это $3 \mid p$, $3 = p$. Проверим оставшиеся числа:

$$3 + 10 = 13, \quad 3 + 14 = 17$$

– тоже простые.

Задача решена.

Целые части

Пусть x – действительное число.

Определение 5.1. Наибольшее целое $m \leq x$ называется *целой частью* x и обозначается $[x]$.

Если $m = [x]$, то $m \leq x < m + 1$.

Примеры:

$$[2,5] = 2, \quad [-2,5] = -3.$$

[5] Какое-то из них имеет остаток от деления 0, какое-то – 1 и какое-то – 2, но мы не знаем, в каком порядке.

Задача

Задача 5.3. *Показать, что если a – натуральное число, то*

$$\left[\frac{x}{a}\right] = \left[\frac{[x]}{a}\right].$$

Решение Обозначим $q = [x/a]$. Тогда

$$q \le \frac{x}{a} < q + 1.$$

Умножая на a, получим, что

$$aq \le x < a(q+1),$$

$$aq \le [x] \le x < a(q+1).$$

Разделив на a, получим, что

$$q \le \frac{[x]}{a} < q + 1.$$

Это и означает, что $q = [[x]/a]$.

Задача решена.

Кратности

Вспомним, что такое кратность.

Определение 5.2. Если p – простое, а A – натуральное, то $\nu_p(A)$ – *кратность*, с которой p входит в разложение A. Если $p \nmid A$, то $\nu_p(A) = 0$.

Вспомним также некоторые свойства кратностей:

$$\nu_p(AB) = \nu_p(A) + \nu_p(B);$$

$$A \mid B \iff \forall \text{ простого } p \ \nu_p(A) \le \nu + p(B);$$

$$\forall \text{ простого } p \ \nu_p(A) = 0 \iff A = 1.$$

Рассмотрим несколько задач на следующую формулу. Пусть $n \ge 1$, p – простое. Тогда

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

Ранее показали, что C_n^k – целые числа. Докажем это теперь другим путем.

Задача 5.4. *Показать, что C_n^k – целые числа.*

Для биномиальных коэффицентов справедливо

$$C_n^k = \frac{n!}{k!(n-k)!}, \quad 1 \le k < n.$$

Посчитаем

$$\nu_p(C_n^k) = \nu_p(n!) - \nu_p(k!) - \nu_p((n-k)!) = \sum_{l \ge 1} \left(\left[\frac{n}{p^l} \right] - \left[\frac{k}{p^l} \right] - \left[\frac{n-k}{p^l} \right] \right). \tag{19}$$

Обозначим

$$x = k/p^l, \quad y = (n-k)/p^l, \quad x + y = n/p^l.$$

Для них

$$[x] \le x, \quad [y] \le y, \quad [x] + [y] \le x + y, \quad [x] + [y] \le [x + y].$$

Значит, каждое слагаемое в сумме (19) будем неотрицательно. Это и означает, что биномиальные коэффициенты являются целыми числами.

Задача решена.

Задача 5.5. *Найти, на сколько нулей заканчивается десятичное представление числа* 1000!.

Решение Можно представить

$$1000! = 2^\alpha \cdot 3^\beta \cdot 5^\gamma \dots$$

Если $\alpha \ge \gamma$, то

$$2^\alpha \cdot 5^\gamma = 10^\gamma \cdot 2^{\alpha - \gamma}.$$

Вычислим кратность

$$\nu_5(1000!) = \left[\frac{1000}{5} \right] + \left[\frac{1000}{25} \right] + \left[\frac{1000}{25} \right] + \left[\frac{1000}{625} \right] = 200 + 40 + 8 + 1 = 249.$$

Так как $\gamma = 249 \ge \alpha$, то получаем, что 249 нулей.

Задача решена.

Задача 5.6. *Пусть n – натуральное, p – простое. Показать, что тогда*

$$\nu_p(n!) = \frac{n - s}{p - 1}, \tag{20}$$

где s – сумма цифр в p-ичной записи n.

Решение Вспомним, что такое p-ичное представление числа n:

$$n = a_0 + a_1 p + \ldots + a_r p^r, \quad 0 \le a_i < p.$$

Тогда

$$s = s(n) = a_0 + a_1 + \ldots + a_s.$$

Если $m = [n/p]$, то

$$\nu_p(n!) = m + \nu_p(m!). \tag{21}$$

Разделив n на p, можем записать

$$\frac{n}{p} = \frac{a_0}{p} + a_1 + \ldots + a_r p^{r-1}.$$

Тогда

$$m = a_1 + a_2 p + \ldots + a_r p^{r-1}.$$

Тогда $s = s(m) + a_0$. С другой стороны, $n - a_0 = pm$. Докажем (20) индукцией по n. При $n < p$

$$\nu_p(n!) = 0.$$

С другой стороны,

$$\frac{n - a_0}{p-1} = \frac{0}{p-1} = 0.$$

Предположим теперь, что формула (20) верна для всех чисел, меньших p.

Тогда для n формулу (21) можно записать в виде

$$\nu_p(n!) = m + \frac{m - s(m)}{p-1} =$$

$$= \frac{mp}{p-1} - \frac{s(m)}{p-1} = \frac{n - a_0}{p-1} - \frac{s(m)}{p-1} = \frac{n - s(m)}{p-1}.$$

Задача решена.

Задача 5.7. *Показать, что*

$$A = \frac{(6n)!n!}{(3n)!(2n)!(2n)!} \in \mathbb{Z}, \quad n \geq 1.$$

Решение Рассмотрим

$$\nu_p(A) = \nu_p((6n)!) + \nu_p(n!) - \nu_p((3n)!) - 2\nu_p((2n)!) =$$

$$= \sum_{l \geq 1} \left(\left[\frac{6n}{p^l} \right] + \left[\frac{n}{p^l} \right] - \left[\frac{3n}{p^l} \right] - 2 \left[\frac{2n}{p^l} \right] \right). \tag{22}$$

Покажем, что каждое слагаемое суммы (22) ≥ 0, а значит, каждое простое число входит в разложение A с неотрицательной степенью. Из этого будет следовать, что A – целое.

Для этого покажем, что

$$f(x) = [6x] + [x] - [3x] - 2[2x] \geq 0, \quad \forall x \in \mathbb{R}. \tag{23}$$

Сначала докажем, что

$$f(x+1) = f(x).$$

Заметим, что для целых a

$$[x+a] = [x] + a, \tag{24}$$

так как если $q = [x]$, то

$$q \le x \le q+1,$$

$$q + a \le x + a < q + a + 1 \;\Rightarrow [x+a] = q + a = [x] + a.$$

Значит,

$$f(x+1) = [6x+6] + [x+1] - [3x+3] - 2[2x+2] =$$

$$= [6x] + 6 + [x] + 1 - [3x] - 3 - 2[2x] - 4 = f(x).$$

Таким образом, нам достаточно показать свойство (23) на отрезке от 0 до 1. Рассмотрим возможные варианты. Так как $0 \le x \le 1$, то $[x] = 0$.

При $0 \le x < 1/6$

$$0 \le 6x < 1 \;\Rightarrow [6x] = 0,\ [3x] = 0,\ [2x] = 0, \quad f(x) = 0.$$

При $1/6 \le x < 1/3$

$$1 \le 6x < 2 \;\Rightarrow [6x] = 1,\ [3x] = 0,\ [2x] = 0, \quad f(x) = 1.$$

При $1/3 \le x < 1/2$

$$2 \le 6x < 3 \;\Rightarrow [6x] = 2,\ [3x] = 1,\ [2x] = 0, \quad f(x) = 1.$$

При $1/2 \le x < 2/3$

$$[6x] = 3,\ [3x] = 1,\ [2x] = 1, \quad f(x) = 0.$$

При $2/3 \le x < 5/6$

$$[6x] = 4,\ [3x] = 2,\ [2x] = 1, \quad f(x) = 0.$$

При $5/6 \le x < 1$

$$[6x] = 5,\ [3x] = 2,\ [2x] = 1, \quad f(x) = 1.$$

Так, получили, что

$$\forall\, x \;\; f(x) \ge 0,$$

а значит, $A \in \mathbb{Z}$.

Семинар 6

Простые числа

Обозначим $\pi(x)$ количество простых чисел p, $p \leq x$. Например, $\pi(10) = 4$.

Задачи

Задача 6.1. *Показать, что*

$$\pi(N) \leq \frac{N+5}{3}. \tag{25}$$

Решение Рассмотрим простые числа $1 \leq p \leq N$, 1 в их число не входит. Можем записать

$$\pi(N) \leq N - 1.$$

Заметим, что количество чисел на отрезке от 1 д N, делящихся на q, равно $[N/q]$. Действительно, на q делятся числа $q, \quad 2q, \quad 3q, \quad \ldots, \quad mq$, где mq – самое большое из таких чисел, то есть

$$mq \leq N < (m+1)q.$$

Значит, $m = [N/q]$.

Пусть $q = 2$. Вычтем количество всех четных чисел, кроме самой двойки:

$$\pi(N) \leq N - 1 - \left(\left[\frac{N}{2}\right]\right).$$

То же самое для $q = 2$. Так как числа, которые делятся на $2 \cdot 3$, в этом случае выбрасываются два раза, надо их прибавить:

$$\pi(N) \leq N - 1 - \left(\left[\frac{N}{2}\right]\right) - \left(\left[\frac{N}{3}\right]\right) + \left[\frac{N}{6}\right] =$$

$$= N - \left[\frac{N}{2}\right] - \left[\frac{N}{3}\right] + \left[\frac{N}{6}\right] + 1. \tag{26}$$

Рассмотрим

$$f(N) = \frac{2N}{3} - \left[\frac{N}{2}\right] - \left[\frac{N}{3}\right] + \left[\frac{N}{6}\right].$$

Вспомним свойство (24). Для любого целого a

$$[x + a] = [x] + a.$$

Вычислим

$$f(N+6) = \frac{2N+12}{3} - \left(\left[\frac{N}{2}\right] + 3\right) - \left(\left[\frac{N}{3}\right] + 2\right) + \left[\frac{N}{6}\right] + 1 = f(N).$$

Так как значения $f(N)$ повторяются, достаточно рассмотреть функцию на отрезке от 0 до 5.

$$f(0) = 0;$$

$$f(1) = \frac{2}{3};$$
$$f(2) = \frac{4}{3} - 1 = \frac{1}{3};$$
$$f(3) = 2 - 1 - 1 = 0;$$
$$f(4) = \frac{8}{3} - 2 - 1 = -\frac{1}{3};$$
$$f(5) = \frac{10}{3} - 2 - 1 = \frac{1}{3}.$$

Значит,

$$f(N) = \frac{2N}{3} - \left[\frac{N}{2}\right] - \left[\frac{N}{3}\right] + \left[\frac{N}{6}\right] \le \frac{2}{3}.$$

Вернемся к (26). Учитывая оценку для $f(N)$, получим, что

$$\pi(N) \le f(N) + \frac{N}{3} + 1 \le \frac{N+5}{3}.$$

Оценка для $\pi(N)$ доказана. [6]

Задача 6.2. *Показать, что*

$$\prod_{p \le x} p < 4^x, \quad x > 2. \tag{27}$$

Сформулируем индукционное утверждение A_n:

неравенство (27) справедливо при всех целых $x < n$.

База индукции ($n = 2$), очевидно, выполняется. Перейдем к шагу индукции.

Предположим, утверждение A_n верно при $n \ge 4$. Рассмотрим утверждение (27) при $x = n$ (т.е. проверим A_{n+1}). Возможно два случая.

1. Если $n = 2m$, то $2m - 1 < n$,

$$\prod_{p \le 2m} p = \prod_{p \le 2m-1} < 4^{2m-1} < 4^{2m}.$$

2. Если $n = 2m - 1$, тогда

$$\prod_{p \le 2m-1} = \prod_{p \le m} p \prod_{m < p \le 2m-1} p.$$

[6] П.Л. Чебышев доказал, что для $\pi(N)$ выполняется

$$a\frac{N}{\ln N} < \pi(N) < b\frac{N}{\ln N},$$

а также что, если предел

$$\frac{\pi(N)}{N/\ln N} \to l, \quad N \to \infty$$

существует, то $l = 1$.

В 1896 г. Адамар и Валле-Пуссен доказали, что данный предел существует.

Рассмотрим

$$C_{2m-1}^{m} = \frac{(2m-1)!}{m!(m-1)!}.$$

Это целое число. В знаменателе факториалы, в которых нет простых чисел из промежутка $m < p \leq 2m-1$. Значит, после сокращения получим, что

$$\prod_{m<p\leq 2m-1} p \leq C_{2m-1}^{m}.$$

Заметим еще, что

$$C_{2m-1}^{m} \leq 4^{m-1}.$$

Убедимся в справедливости этой оценки. При $m = 1$ утверждение верно. Распишем

$$C_{2m-1}^{m} = \frac{(2m-1)!}{m!(m-1)!} =$$

$$= \frac{(2m-1)(2m-2)}{m(m-1)} \frac{(2m-1)!}{m!(m-1)!} < 4C_{2m-3}^{m-1} = 4 \cdot 4^{m-2} = 4^{m-1}.$$

Тогда

$$\prod_{p\leq 2m-1} < 4^{m} \cdot C_{2m-1}^{m} \leq 4^{m} \cdot 4^{m} \cdot 4^{m-1} = 4^{2m-1}.$$

Теперь,

$$\prod_{p\leq x} p = \prod_{p\leq [x]} p < 4^{x} < 4^{x}.$$

Неравенство (27) доказано.

Задача решена.

Задача 6.3. *Пусть n – натуральное число. Показать, что тогда*[7]

$$K = [1, 2, 3, \ldots, 2n+1] > 4^{n}. \tag{28}$$

Решение Рассмотрим рациональную функцию, то есть функцию

$$R_n(x) = \frac{n!}{x(x+1)\ldots(x+n)}.$$

Убедимся, что ее можно представить в виде

$$R_n(x) = \frac{a_0}{x} + \frac{a_1}{x+1} + \ldots + \frac{a_n}{x+n}. \tag{29}$$

При $n = 1$ получим

$$R_n(x) = \frac{1}{x(x+1)} = \frac{(x+1)-x}{x(x+1)} = \frac{1}{x} - \frac{1}{x+1}.$$

[7] Символом

$$[a_1, \ldots, a_n]$$

обозначается *наименьшее общее кратное.*

При $n = 2$

$$R_n(x) = \frac{2}{x(x+1)(x+2)} = \frac{(x+2)-x}{x(x+1)(x+2)} =$$

$$= \frac{1}{x(x+1)} - \frac{1}{(x+1)(x+2)} = \frac{1}{x} - \frac{1}{x+1} - \left(\frac{1}{x+1} - \frac{1}{x+2}\right) = \frac{1}{x} - \frac{2}{x+1} + \frac{1}{x+2}.$$

Далее можно доказать по индукции. Кроме того, можно показать, что

$$a_k = \frac{(-1)^k C_n^k}{x+k}.$$

Убедимся в представлении (29). Рассмотрим[8]

$$R_n(x) = \frac{(n-1)!((x+n)-x)}{x(x+1)\dots(x+n)} = \underbrace{\frac{(n-1)!}{x(x+1)\dots(x+n-1)}}_{=R_{n-1}(x)} - R_{n-1}(x+1) =$$

$$= \frac{b_0}{x} + \frac{b_1}{x+1} + \dots + \frac{b_{n-1}}{x+n-1} - \frac{b_0}{x+1} + \frac{b_1}{x+2} + \dots + \frac{b_{n-1}}{x+n-1}.$$

Осталось только сгруппировать дроби. Получим, что

$$b_1 - b_0 = a_1,$$

$$b_2 - b_1 = a_2$$

и так далее.

Перепишем

$$R_n(n+1) = \frac{n!}{(n+1)(n+2)\dots(2n+1)} = \frac{n!n!}{(2n+1)!}.$$

Вернемся к (28).

$$K \cdot R_n(n+1) = K \cdot \left(\frac{a_0}{n+1} + \frac{a_1}{n+2} + \dots + \frac{a_n}{2n+1}\right) \in \mathbb{Z},$$

так как K – наименьшее общее кратное чисел $1, \dots, 2n+1$. Кроме того,

$$K \cdot R_n(n+1) \leq 1.$$

Тогда

$$K \leq \frac{(2n+1)!}{n!n!} > 4^n. \tag{30}$$

Последний переход докажем по индукции. При $n = 1$

$$\frac{6}{1 \cdot 1} = 6 > 4^1.$$

Предположим, что (30) верно при некотором n. Запишем при $n+1$:

$$\frac{(2n+3)!}{(n+1)!(n+1)!} = \frac{(2n+3)(2n+2)}{(n+1)(n+1)} \frac{(2n+1)!}{n!n!} \leq 4 \cdot 4^n = 4^{n+1}.$$

Задача решена.

[8]Здесь мы обозначили коэффициенты $R_n(x)$ как a_i, а коэффициенты $R_{n-1}(x)$ в аналогичном разложении как b_i.

Задача 6.4. *Пусть n, k – натуральные и такие, что*

$$2^n > (n+1)^k. \tag{31}$$

Докажите, что на отрезке от 1 до 2^n имеется $\geq k$ простых чисел.

Решение Предположим, что

$$p_1, \quad p_2, \quad \ldots, \quad p_r \tag{32}$$

– все простые числа на отрезке от 1 до 2^n. Возьмем a – целое, $1 \leq a \leq 2^n$. Тогда в разложение

$$a = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$$

входят только простые числа (32). Будем считать $k_i = 0$, если число p_i в разложение числа a не входит.

Так как $2 \leq p_l$, справедливо

$$2^{k_l} \leq p_l^{k_l} \leq a \leq 2^n \;\Rightarrow 0 \leq k_l \leq n.$$

Для каждого k_l есть $(n+1)$ возможных значений.

Каждому a ставится в соответствие набор $(k_1, \ldots, k_r)$, где $0 \leq k_l \leq n$. Тогда

$$2^n \leq \underbrace{(n+1)\ldots(n+1)}_{r} = (n+1)^r.$$

В силу (31) получаем, что

$$(n+1)^k < (n+1)^r.$$

Значит, $r > k$.

Задача решена.

Семинар 7

Задачи

Задача 7.1. *Пусть N – натуральное число. Доказать, что на отрезке от 1 до N имеется не более $\frac{3}{4}N$ чисел, делящихся на квадрат простого числа.*[9]

Решение Предположим обратное. Допустим, что

$$p_1, \quad p_2, \quad \ldots, \quad p_m \tag{33}$$

– это все простые числа. Построим все числа, которые не делятся на квадрат простого числа. Они будут иметь вид

$$p_1^{k_1} \ldots p_r^{k_r}, \quad 0 \le k \le 1.$$

Таким чисел получается $\underbrace{2 \cdot \ldots \cdot 2}_{m} = 2^m$ штук.

Мы покажем, что на отрезке от 1 до N лежит $> \frac{1}{4}N$ чисел, не делящихся на квадрат простого. Вспомним, что на отрезке от 1 до N имеется $\le \left[\frac{N}{4}\right]$ чисел, делящихся на 4, $\le \left[\frac{N}{9}\right]$ чисел, делящихся на 9, и так далее.

Обозначим T – количество чисел на отрезке от 0 до N, делящихся на квадрат простого числа. Тогда

$$T \le \left[\frac{N}{4}\right] + \left[\frac{N}{9}\right] + \left[\frac{N}{25}\right] + \ldots + \left[\frac{N}{p^2}\right],$$

где p – самое большое простое такое, что $p^2 \le N$. Тогда

$$T \le \frac{N}{4} + \frac{N}{9} + \frac{N}{25} + \ldots + \frac{N}{p^2} \le N \cdot \sum_{k=2}^{p} \frac{1}{k^2}.$$

В последнем переходе сумма берется по всем k, не только простым. Далее, [10]

$$N \cdot \sum_{k=2}^{p} \frac{1}{k^2} < N \left(\frac{1}{4} + \sum_{k=3}^{p} \frac{1}{(k-1)k} \right). \tag{34}$$

Так как

$$\frac{1}{(k-1)k} = \frac{1}{k-1} - \frac{1}{k},$$

то

$$\left(\frac{1}{3} - \frac{1}{2}\right) + \left(\frac{1}{4} - \frac{1}{3}\right) + \left(\frac{1}{5} - \frac{1}{4}\right) + \ldots + \left(\frac{1}{p-1} - \frac{1}{p}\right) = \frac{1}{2} - \frac{1}{p} < \frac{1}{2}.$$

[9] Из этой задачи также следует, что $\exists$ бесконечного много простых чисел.

[10] Здесь выносим случай $k = 2$ за сумма, так как иначе на следующем шаге оцениваем

$$\frac{1}{2^2} < \frac{1}{1 \cdot 2} = 1 - \frac{1}{2}$$

и это слишком грубая оценка для нашего решения.

Подставляя в (34), получим, что

$$T < N\left(\frac{1}{4}+\frac{1}{2}\right) = \frac{3}{4}N.$$

Задача решена.

Задача 7.2. *Показать, что*

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} > \ln x, \quad x \ge 2.$$

Решение Рассмотрим[11]

$$\left(1-\frac{1}{p}\right)^{-1} = 1+\frac{1}{p^2}+\frac{1}{p^3}+\ldots > \sum_{p^k\le x}\frac{1}{p^k}.$$

Тогда[12]

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} \le \sum_{p_j^{k_j}\le x}\frac{1}{p_1^{k_1}\ldots p_m^{k_m}} \ge$$

$$\ge \sum_{p_1^{k_1}\ldots p_m^{k_m}\le x}\frac{1}{p_1^{k_1}\ldots p_m^{k_m}} = \sum_{n\le x}\frac{1}{n}. \tag{35}$$

Воспользуемся неравенством из курса математического анализа:

$$\left(1+\frac{1}{m}\right)^m \le e = 2,7\ldots$$

Преобразовав, получим

$$m\ln\left(1+\frac{1}{m}\right) \le 1,$$

$$\ln(m+1)-\ln m \le \frac{1}{m}, \quad m \le [x]$$

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{[x]} \ge (\ln 2-\ln 1)+(\ln 3-\ln 2)+\ldots+(\ln([x]+1)-\ln[x]).$$

Тогда в (35) получаем, что

$$\sum_{n\le x}\frac{1}{x} > \ln x.$$

Задача решена.

Вспомним, что $\nu_p(m)$ – кратность, с которой p входит в разложение m на простые множители. [13]

[11] Первое равенство следует из формулы для суммы бесконечной геометрической прогрессии.

[12] Последний переход следует из того, что каждое целое число единственным способом раскладывается в произведение простых.

[13] Обсуждали следующие свойства кратности:

$$\nu_p(ab) = \nu_p(a)+\nu_p(b);$$

Задача 7.3. *Пусть $b, a_1, \ldots, a_m$ – натуральные и*

$$(b, a_i) = 1, \quad i = 1, \ldots, m. \tag{36}$$

Показать, что тогда $(b, a_1 \ldots a_m) = 1$.

Решение Для двух чисел a, b

$$\nu_p((a, b)) = \min(\nu_p(a), \nu_p(b));$$

$$\nu_p([a, b]) = \max(\nu_p(a), \nu_p(b));$$

Условие (36) означает, что $\forall\, p$

$$\nu_p((b, a_i)) = 0 = \min(\nu_p(a), \nu_p(b)), \quad i = 1, \ldots, m.$$

1. Предположим, что $\nu_p(b) = 0$. Тогда

$$\nu_p(b, a_1 \ldots a_m)) = \min(\nu_p(b), \nu_p(a_1 \ldots a_m)) = 0.$$

2. Если $\nu_p(b) \geq 1$, то

$$\nu_p(a_i) = 0, \quad i = 1, \ldots, m$$

и

$$\nu_p(a_1 \ldots a_m) = \nu_p(a_1) + \ldots + nu_p(a_m).$$

Значит, числа b и $a_1 \ldots a_m$ взаимно просты.
Задача решена.

$a \mid b$, *если* $\forall\, p\ \nu_p(a) \leq \nu_p(b)$;

$\forall\, p\ \nu_p(a) = \nu_p(b) \iff a = b$;

$\forall\, p\ \nu_p(a) \geq 0 \Rightarrow\ a \in \mathbb{Z}$.

Семинар 8

Мультипликативные функции

Обозначим через $\theta(n)$ *мультипликативную функцию*, то есть функцию, для которой

$$\theta(n): \ \mathbb{N} \to \mathbb{C},$$
$$\theta(a \cdot b) = \theta(a)\theta(b).$$

Пример 8.1. *Для* $s \in \mathbb{R}$

$$\theta(n) = n^s$$

будет мультипликативной функцией.

В частности, при $s = 0$ *получим функцию*

$$\theta(n) \equiv 1.$$

Вспомним некоторые **свойства** $\theta(n)$.

1. Пусть θ_1, θ_2 – мультипликативные функции. Тогда

$$\theta_1 \cdot \theta_2(n) = \theta_1(n) \cdot \theta_2(n)$$

тоже будет являться мультипликативной функцией.

2. Если $\theta(n) \neq 0$, то $\theta(1) = 1$.

3. Если $\theta(n)$ – мультипликативная функция, то

$$f(n) = \sum_{d \,|\, n} \theta(d) \tag{37}$$

– мультипликативная функция и для любого $n \in \mathbb{N}$ ее можно представить в виде

$$f(n) = \prod_{p \,|\, n} \left(2 + \theta(p) + \ldots + \theta\left(p^{\nu_p(n)}\right)\right). \tag{38}$$

4. Если $\theta(n)$ – мультипликативная функция и $u = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, то

$$\theta(n) = \theta\left(p_1^{\alpha_1}\right) \ldots \theta\left(p_r^{\alpha_r}\right).$$

Последнее свойство позволяет нам задать $\theta(n)$ только на степенях простых чисел и тем самым определить ее для всех целых чисел.

Функция Мёбиуса и формула обращения

Функция Мёбиуса определяется следующим образом:

$$\mu(1) = 1, \ \mu(p^\alpha) = \begin{cases} -1, & \alpha = 1, \\ 0, & \alpha \geq 2. \end{cases}$$

Тогда

$$\mu(n) = \begin{cases} 0, & \text{если } \exists p: \ p^2 \,|\, n, \\ (-1)^r, & \text{если } n = p_1 \ldots p_r, \ \ p_i \neq p_j. 1, \quad \text{если } n = 1. \end{cases}$$

Пример 8.2. *Функция*

$$\frac{\mu(n)}{n^s}$$

– *мультипликативная.*

Воспользовавшись свойством (37), построим мультипликативную функцию

$$\sum_{d\,|\,n}\frac{\mu(n)}{n^s}.$$

Применив свойство (38), получим, что ее можно представить в виде

$$\sum_{d\,|\,n}\frac{\mu(n)}{n^s}=\prod_{p\,|\,n}\left(1-\frac{1}{p^s}\right). \tag{39}$$

При $s=0$ получим

$$\sum_{d\,|\,n}\mu(n)=\begin{cases}1, & \text{если } n=1,\\ 0, & \text{если } \geq 2.\end{cases}$$

Вспомним еще **формулу обращения**. Если

$$f(n)=\sum_{d\,|\,n}\theta(d),$$

то

$$\theta(n)=\sum_{d\,|\,n}\mu(d)f\left(\frac{n}{d}\right). \tag{40}$$

Задача 8.1. *Докажите, что при случайном выборе целого числа n на отрезке $1\leq n\leq x$ и достаточно большом x с вероятностью $6/\pi^2$ получится число n, не делящееся на квадрат простого числа.*

Решение Для каждого натурального j будем обозначать b_j наибольшее натуральное число с условием[14]

$$b_j^2\,|\,j.$$

При этом

$$d^2\,|\,j \iff d\,|\,b_j.$$

Фуксируем некоторое $d\leq\sqrt{x}$. Рассмотрим

$$\sum_{j=1,d\,|\,b_j}^{[x]}1=\sum_{j=1,d^2\,|\,j}1=\left[\frac{x}{d^2}\right].$$

Последнее равенство следует из того, что в пределах $1\leq j\leq x$ есть ровно

$$\left[\frac{x}{q}\right]$$

[14]Например, при $j=12$ $b_{12}=2$.

чисел, делящихся на q. [15]

Рассмотрим теперь

$$\sum_{d\le\sqrt{x}} \mu(d)\left[\frac{x}{d^2}\right] = \sum_{d\le\sqrt{x}} \mu(d) \sum_{\substack{1\le j\le x \\ d\,|\,b_j}} 1 =$$

$$= \sum_{\substack{(j,d) \\ 1\le j\le x \\ d\,|\,b_j}} \mu(d) = \sum_{j=1}^{[x]} \sum_{d\,|\,b_j} \mu(d).$$

Здесь смогли выбросить условие $d \le \sqrt{x}$, так как

$$d\,|\,b_j \iff d^2\,|\,j \le x \Rightarrow d \le \sqrt{x}.$$

Теперь рассмотри внутреннюю сумму.

$$\sum_{d\,|\,b_j} \nu(d) = 0$$

при $b_j \ge 2$. Значит,

$$\sum_{d\le\sqrt{x}} \mu(d)\left[\frac{x}{d^2}\right] = \sum_{j=1}^{[x]} \sum_{d\,|\,b_j} \mu(d) = \sum_{\substack{1\le j\le [x] \\ b_j=1}} 1.$$

Это количество чисел n на отрезке от 1 до x, не делящихся на квадрат простого.

Запишем это количество чисел n как

$$\sum_{d\le\sqrt{x}} \mu(d)\left[\frac{x}{d^2}\right] = \sum_{\substack{1\le j\le [x] \\ b_j=1}} \mu^2(j)$$

и обозначим через $T(x)$.

Итак, наша задача – показать, что

$$\frac{T(x)}{x} \to \frac{6}{\pi^2}.$$

Можем записать

$$T(x) = \sum_{d\le\sqrt{x}} \frac{x\mu(d)}{d^2} + O(\sqrt{x}) = x \sum_{d\le\sqrt{x}} \frac{\mu(d)}{d^2} + O(\sqrt{x})$$

[15] И еще здесь воспользовались свойством, что для натурального a верно

$$\left[\frac{x}{a}\right] = \left[\frac{[x]}{a}\right].$$

где $O(\sqrt{x})$ – ошибка, которая возникает при отбрасывании в сумме-представлении для $T(x)$ целой части.

Тогда

$$\frac{T(x)}{x} = \sum_{d \le \sqrt{x}} \frac{\nu(x)}{d^2} + O(x^{-1/2}),$$

$$\lim_{x\to\infty} \frac{T(x)}{x} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}.$$

Наша задача – доказать, что

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} \tag{41}$$

Заметим, что, так как $\mu(d) \le 1$,

$$\left|\frac{\mu(d)}{d^2}\right| \le \frac{1}{d^2}.$$

Из курса матанализа известно, что

$$\sum_{d=1}^{\infty} \frac{1}{d^2} = \frac{\pi^2}{6}. \tag{42}$$

Умножим ряд (41) на ряд (42). Получим

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \sum_{k=1}^{\infty} \frac{1}{k^2} = \sum_{n=1}^{\infty} \sum_{d\cdot k=n}^{\infty} \frac{\mu(d)}{d^2}\frac{1}{k^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{d\,|\,n} \mu(d).$$

Заметим, что по свойству $\mu(n)$

$$\sum_{d\,|\,n} \mu(d) = 0, \quad \text{если } n \ge 2.$$

Значит,

$$\sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{d\,|\,n} \mu(d) = 1.$$

Получили, что

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}\frac{\pi^2}{6} = 1,$$

то есть

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}.$$

Задача решена.

Число и сумма делителей

Рассмотрим

$$\tau(n) = \sum_{d \,|\, n} 1$$

– *число делителей* числа n.

Так как $\theta(n) = 1$ – мультипликативна, по свойству (37) получим, что $\tau(n)$ – тоже мультипликативна.

Теперь, представим

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}.$$

Тогда

$$\tau(n) = \tau\left(p_1^{\alpha_1}\right) \dots \tau\left(p_r^{\alpha_r}\right).$$

Воспользовавшись свойством (38), получим

$$\tau(p^\alpha) = \underbrace{1 + \ldots + 1}_{\alpha+1} = \alpha + 1.$$

Тогда

$$\tau(n) = (\alpha_1 + 1) \dots (\alpha_r + 1).$$

Рассмотрим теперь функцию

$$\sigma(n) = \sum_{d \,|\, n} d$$

– *сумма делителей* числа n.

Сумму делителей также можно представить в виде (37), где $\theta(n) = n$. Тогда $\sigma(n)$ – мультипликативная,

$$\sigma(n) = \sigma\left(p_1^{\alpha_1}\right) \dots \sigma\left(p_r^{\alpha_r}\right)$$

и по свойству (38),

$$\sigma(p^\alpha) = 1 + p + p^2 + \ldots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}. \tag{43}$$

Таким образом,

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \dots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

Задача 8.2. *Докажите, что $\tau(n)$ есть число решений*

$$x \cdot y = n$$

в натуральных числах x, y.

Решение Заметим, что

$$(x, y) \iff x, x \,|\, n.$$

Количество таких x и есть $\tau(n)$.

Задача решена.

Задача 8.3. *Показать, что*

$$\tau(n) \leq 2\sqrt{x}.$$

Решение Сопоставим решению

$$(x, y) \ \to \min(x, y).$$

Допустим, $x \leq y$. Тогда

$$x^2 \leq xy = n \ \Rightarrow \ x \leq \sqrt{n}.$$

Аналогично, если $y < x$,

$$y^2 < xy = n \ \Rightarrow \ y < \sqrt{n}.$$

Получили требуемую оценку.

Задача решена.

Совершенные числа

У любого числа $n > 1$ есть делители 1 и n.

Определение 8.1. Число n называется *совершенным*, если его сумма его делителей

$$\sigma(n) = 2n.$$

Пример 8.3. *У числа* $n = 6$

$$\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6.$$

У числа 28

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56.$$

Проверим, что число вида

$$n = 2^s \left(2^{s+1} - 1\right),$$

где $2^{s+1} - 1$ – простое, будет совершенным.

С учетом формулы (43),

$$\sigma(n) = \sigma(2^s)\sigma(2^{s+1} - 1) = \left(2^{s+1} - 1\right)\left(2^{s+1} - 1 + 1\right) = 2^{s+1}\left(2^{s+1} - 1\right) = 2n.$$

Остановимся подробнее, в каких случаях $2^{s+1} - 1$ – простое число. В случае, когда $s + 1 = v \cdot u$,

$$2^{u \cdot v} - 1 = (2^u - 1)\left(1 + 2^u + \cdot + 2^{(v-1)u}\right).$$

Когда $s + 1 = p$ – простое, числа

$$2^{s+1} - 1 = M_p$$

называют *числами Мерсенна*. Числа M_p могут быть как простыми, так и составными. Нет общих формул, позволяющих вывести закономерность.

Задача 8.4. *Показать, что каждое четное совершенное число имеет вид*

$$2^s(2^{s+1}-1),$$

где $2^{s+1}-1$ *– простое.*

Решение Пусть n – четное совершенное число. Тогда

$$n = 2^s \cdot V,$$

где V – нечетное число, $s \geq 1$. Так как n – совершенное, $\sigma(n) = 2n$.

$$\sigma(n) = \sigma(2^s V) = \sigma(2^s)\sigma(V) = (2^{s+1}-1)\sigma(V).$$

Тогда

$$(2^{s+1}-1)\sigma(V) = 2n = 2^{s+1}V. \tag{44}$$

Заметим, что

$$(2^{s+1}-1, 2^s) = 1.$$

Отсюда получаем, что

$$\sigma(V) = 2^{s+1}W,$$

где W – какое-то число.Подставив это представление в (44), получим

$$V = (2^{s+1}-1)W.$$

Заметим, что

$$2^{s+1}W \geq 1 + V + W,$$

так как V точно имеет делители 1, v и W. Значит,

$$W(2^{s+1}-1) \geq 1 + V = 1 + (2^{s+1}-1)W.$$

Получили противоречие. Значит, $W = 1$.[16] Итак,

$$\sigma(V) = 2^{s+1}, \quad V = 2^{s+1}-1.$$

Отсюда получается, что

$$\sigma(V) = (2^{s+1}-1) + 1 = V + 1.$$

Так как сумма делителей числа V состоит из самого этого числа и 1, V – простое.
Задача решена.

Проблема: существуют ли нечетные совершенные числа?

[16]Тогда в левой части суммы мы учитываем его дважды при подсчете делителей числа V.

Функция Эйлера

Пусть $n \geq 2$ – целое число.

Определение 8.2. Количество чисел m, $1 \leq m \leq n$, взаимно простых с n, называется *функцией Эйлера* и обозначается $\varphi(n)$.

Пример 8.4. *$n = p$ – простое. Тогда*

$$\underbrace{1, 2, 3, \ldots, n-1}_{p-1}, n = p$$

– все числа $< n$ взаимно просты с ним. Тогда

$$\varphi(n) = p - 1.$$

Пример 8.5. *$n = p$. Вспомним, что количество чисел от 1 до x, делящихся на некоторое p, равно $[x/p]$. В нашем случае на p делятся*

$$\left[\frac{p^\alpha}{p}\right] = p^\alpha - 1.$$

Тогда

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Пример 8.6. *$\phi(6) = 2$, так как из чисел*

$$1, \not{2}, \not{3}, \not{4}, 5, \not{6}$$

нам подходят только 1 и 5.

Заметим, что $\varphi(2) = 1$, $\varphi(3) = 2$ и можно представить

$$\varphi(6) = \varphi(2)\varphi(3).$$

Докажем, что функция $\varphi(n)$ мультипликативна, опираясь на следующую задачу.

Задача 8.5. *Показать, что*[17]

$$\sum_{d \,|\, n} \varphi(n) = n.$$

Решение Пусть d – натуральное число. Обозначим

$$A_d = \{k \,|\, 2 \leq k \leq n,\ (k, n) = d\}.$$

Из этого определения следует, что $d \,|\, k$ и $d \,|\, n$, то есть можно записать

$$k = d \cdot k_1, \quad n = d \cdot n_1.$$

[17]Утверждение задачи 5 похоже на формулу (37). Покажем сначала справедливость утверждения задачи, потом применим формулу обращения и уже оттуда покажем, что $\varphi(n)$ – мультипликативна.

1. Если $d \nmid n$, то $A_d = \emptyset$.
2. Предположим теперь, что $d_1 \mid n$ и $d_2 \mid n$, $d_1 \neq d_2$. Если

$$k \in A_{d_1} \cap A_{d_2},$$

то

$$(k, n) = d_1, \quad (k, n) = d_2.$$

Получили противоречие. Значит,

$$A_{d_1} \cap A_{d_2} = \emptyset.$$

Если $d \mid n$,

$$d \in A_d.$$

3. Для каждого k, $1 \leq k \leq n$, $\exists d$, $k \in A_d$. Для этого достаточно положить

$$d = (k, n).$$

Теперь, можем записать

$$[1, n] = \cup_{d=1}^{n} A_d.$$

Так как эти множества не пересекаются, можем записать

$$[1, n] = \sum_{d \mid n} | A_d | = n. \tag{45}$$

Если $k \in A_d$, то $k = d \cdot k_1$ и

$$1 \leq dk_1 \leq n = dn_1.$$

Значит, $1 \leq k_1 \leq n_1$. При этом $(k_1 d, n_1 d) = d$, то

$$(k_1, n_1) = 1.$$

Тогда количество чисел k_1 равно $\varphi(n_1)$. Заметим, что

$$\varphi(n_1) = \varphi(n/d).$$

$$| A_d | = \varphi(n/d).$$

При подстановке в (45) получаем

$$\sum_{d \mid n} \varphi(n/d) = n.$$

Заметим, что если d – делитель n, то n/d – тоже делитель n. Отсюда получаем

$$\sum_{d \mid n} \varphi(d) = n. \tag{46}$$

Применим теперь к (46) формулу обращения (40), положив $\theta(n) = \varphi(n)$, $f(n) = n$.

$$\varphi(n) = \sum_{d\,|\,n} \mu(d)\frac{n}{d} = n\sum_{d\,|\,n}\frac{\mu(d)}{d}.$$

Воспользовавшись (39), получим

$$\varphi(n) = n\prod_{p\,|\,n}\left(1-\frac{1}{p}\right). \tag{47}$$

Формула (47) – общая формула для вычисления функции Эйлера.

Так как

$$\sum_{d\,|\,n}\frac{\mu(d)}{d}$$

– мультипликативна, получаем, что $\varphi(n)$ тоже мультипликативная, как произведение двух мультипликативных функций.[18]

Задача решена.

Например,

$$\varphi(6) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 6\frac{1}{2}\frac{2}{3} = 2.$$

Рассмотрим $n = 100 = 2^2 5^2$.

$$\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100\frac{1}{2}\frac{4}{5} = 40.$$

Можно вычислить другим путем.

$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (4-2)(25-5) = 2\cdot 20 = 40.$$

Вспомним теперь две теоремы.

Теорема 8.1. *(Эйлера) Для любого целого числа a, $(a,n) = 1$, разность*

$$a^{\varphi(n)} - 1$$

делится на n.

Если $n = p$ – простое, то $\varphi(n) = p - 1$.

Теорема 8.2. *(Ферма) Если p – простое число, то для любого a, не делящегося на p, разность*

$$a^p - 1$$

делится на p.

Задача 8.6. *Найти последнюю цифру в десятичной записи числа*

$$x = 7^{7^{7^7}}.$$

[18] В лекционном курсе приводится другое доказательство.

Решение Нам нужно понять, какой остаток имеет это число при делении на 10. Найдем

$$\varphi(10) = (2-1)(5-1) = 4.$$

По теореме Эйлера, $7^4 - 1$ делится на 10.

Заметим, что

$$7^{4k} - 1 = (7^4 - 1)(1 + 7^4 + \ldots + 7^{4(k-1)})$$

делится на 10.

Теперь, обозначим $l = 7^7$. Рассмотрим

$$7^l + 1 = 7^l + 1^l = (7+1) \cdot A = 8A,$$

где A – вторая часть разложения. Тогда

$$7^{7^7} + 1 = 8A.$$

Значит, число

$$7^{7^{7^7}+1} = 7x$$

имеет остаток 1 при делении на 10. Число

$$7(x-3) = 7x - 21 \vdots 10,$$

так как оба числа в разности имеют остаток 1 при делении на 10. Значит, $x - 3$ делится на 10. Тогда последняя цифра x равна 3.

Второй способ решения (с помощью сравнений)

Нам надо понять, с чем сравнимо $x = 7^{7^{7^7}}$ по $\mod 10$.

По малой теореме Ферма,

$$7^4 \equiv 1 \pmod{10}.$$

Тогда

$$7^{4k} \equiv 1 \pmod{10}.$$

$$7^{7^7} = (8-1)^{7^7} \equiv -1 \pmod 4 \equiv 3 \pmod 4.$$

Тогда

$$7^{7^7} = 3 + 4k.$$

Получаем, что

$$x = 7^{3+4k} = 7^3 \cdot 7^{4k} \equiv 7^3 \pmod{10} = 7 \cdot 49 \pmod{10} \equiv$$

$$\equiv -7 \pmod{10} \equiv 3 \pmod{10}.$$

Задача решена.

Семинар 9

Задачи

Задача 9.1. *(На применение малой т. Ферма) Доказать, что*

$$A = 2222^{5555} + 5555^{2222}$$

делится на 7.

Решение Заметим, что

$$2222 + 5555 = 7777 \equiv 0 \pmod 7.$$

Тогда

$$A \equiv 2222^{5555} + (-2222)^{5555} = 2222^{2222}\left(2222^{3333} + 1\right).$$

Обозначим

$$2222^{3333} + 1 = B.$$

Так как

$$2222 = 7 \cdot 317 + 3 \equiv 3 \pmod 7,$$

получим, что

$$B \equiv 3^{3333} + 1 \pmod 7.$$

По малой т. Ферма,

$$3^6 \equiv 1 \pmod 7.$$

Так как $3333 = 6 \cdot 555 + 3$,

$$3^{3333} = (3^6)^{555} \cdot 3^3 \equiv 3^3 = 27 \pmod 7.$$

Тогда

$$B \equiv 27 + 1 = 28 \equiv 0 \pmod 7.$$

Задача решена.

Полиномиальные сравнения

Пусть даны $x_1, \ldots, x_n$, p – простое. Рассмотрим многочлен

$$f(x_1, \ldots, x_n) = f = \sum_{(x_1,\ldots,x_n)} a_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n}, \quad a_{k_1,\ldots,k_n} \in \mathbb{Z}.$$

Определение 9.1. Два многочлена f и g

$$f \equiv g \pmod p,$$

если их разность после приведения подобных имеет коэффицентами целые числа, делящиеся на p.

Пример 9.1.

$$(x_1 + x_2)^p - x_1^p - x_2^p = \sum_{k=1}^{p-1} C_p^k x_1^k x_2^{n-k} \equiv 0 \pmod{p}, \tag{48}$$

так как для $1 \le k \le p-1$ $p \,|\, C_p^k$. *Получаетмся, что*

$$(x_1 + x_2)^p \equiv x_1^p + x_2^p \pmod{p}.$$

Задача 9.2. *Докажите, что*

$$f^p(x_1, \ldots, x_n) \equiv f(x_1^p, \ldots, x_n^p) \pmod{p}.$$

Определение 9.2. *Длиной* многчлена f будет называться количество его коэффицентов, не делящихся на p.

Определение 9.3. Обозначим

$$\|f\|$$

минимальное число m такое, что найдется многочлен $g = g(x_1, \ldots, x_n)$ такой, что

$$f \equiv g \pmod{p}$$

и длина g равна m.

Решение Доказательство задачи будем проводить по индукции.

1. $\|f\| = 0$. Значит, все коэффициенты f делятся на p.

Тогда коэффициенты $f(x_1^p, \ldots, x_n^p)$ будут делиться на p, так как останутся без изменений. Коэффициенты $f^p(x_1, \ldots, x_n)$ будут делиться на p, так как при возведении в степень каждый новый коэффицент будет представлять собой сумму слагаемых (старых коэффицентов), каждое из которых делится на p.

Значит, у разности

$$f^p(x_1, \ldots, x_n) - f(x_1^p, \ldots, x_n^p)$$

все коэффициенты будут делиться на p.

Рассмотрим еще один случай.

2. $\|f\| = 1$.В этом случае

$$f(x_1, \ldots, x_n) = a x_1^{k_1} \ldots x_n^{k_n} + p h(x_1, \ldots, x_n), \quad p \nmid a.$$

Тогда $f^p(x_1, \ldots, x_n)$ будет представимо в виде

$$f^p(x_1, \ldots, x_n) = a^p x_1^{pk_1} \ldots x_n^{pk_n} + p \cdot v(x_1, \ldots, x_n).$$

Теперь воспользуемся малой т. Ферма.

$$a^p - a = a(a^{p-1} - 1) \equiv 0 \pmod{p}. \tag{49}$$

Теперь,

$$f(x_1^p, \ldots, x_n^p) = a x_1^{pk_1 pk_n} + p h(x_1^p, \ldots, x_n^p),$$

причем $ax_1^{pk_1}{}_n^{pk_n} = g(x_1, \ldots, x_n)$ из обозначения $\|f\|$. Учитывая (49), получим

$$f^p(x_1, \ldots, x_n) - f(x_1^p, \ldots, x_n^p) \equiv 0 \pmod{p}.$$

Значит,

$$f^p(x_1, \ldots, x_n) \equiv f(x_1^p, \ldots, x_n^p) \pmod{p}.$$

3. Общий случай (шаг индукции). Предположим, $\|f\| = n$ и для любого многочлена g, $\|g\| < n$ утверждение верно. Тогда f можно представить в виде

$$f = g + h, \quad \|g\| < n, \quad \|h\| < n.$$

Воспользовавшись формулой бинома, получим, что

$$f^p = (g+h)^p = g^p + h^p + sum_{k=1}^{p-1} C_p^k g^k h^{p-k}.$$

Так как для h и g по индуктивному предположению утверждение верно, можем записать

$$\begin{gathered} f^p = g(x_1^p, \ldots, g_n^p) + (g^p(x_1, \ldots, x_n) - g(x_1^p, \ldots, x_n^p)) + h(x_1^p, \ldots, g_n^p) + \\ + (h^p(x_1, \ldots, x_n) - h(x_1^p, \ldots, x_n^p)) + sum_{k=1}^{p-1} C_p^k g^k h^{p-k} = \\ = f(x_1^p, \ldots, x_n^p) + pw(x_1, \ldots, x_n). \end{gathered}$$

Получим, что

$$f^p(x_1, \ldots, x_n) - f(x_1^p, \ldots, x_n^p) = pw(x_1, \ldots, x_n) \equiv 0 \pmod{p}.$$

Задача решена.

Задача 9.3. *Доказать следующую теорему:*

Теорема 9.1. *(Вильсона) Если p – простое, то*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Решение Рассмотрим многочлен

$$x(x-1)\ldots(x-p+1).$$

Числа

$$0, 1, 2, \ldots, p-1 \tag{50}$$

будут корнями этого многочлена. У многочлена

$$x^p - x$$

по малой т. Ферма числа (50) также будут корнями. Рассмотрим

$$F(x) = x(x-1)\ldots(x-p+1) - (x^p - x).$$

Заметим, что $\deg F \leq p-1$ и все коэффициенты $F(x)$ делятся на p.

Свободный член $F(x)$ имеет вид

$$(-1)^{p-1}(p-1)! + 1 = (p-1)! + 1 \vdots p,$$

так как p – простое и, значит, нечетное.

Теорема доказана.

Задача 9.4. *Пусть p – нечетное простое и a – целое, неделящееся на p, причем $p \mid a^2+1$. Показать, что тогда*

$$p \equiv 1 \pmod 4,$$

то есть $p = 1 + 4k$.

Решение По малой т. Ферма,

$$0 \equiv 1 - a^{p-1} \pmod p.$$

Преобразуем

$$1 - a^{p-1} = 1 - (a^2)^{\frac{p-1}{2}}.$$

По условию,

$$a^2 \equiv -1 \pmod p.$$

Тогда

$$1 - (a^2)^{\frac{p-1}{2}} \equiv 1 - (-1)^{\frac{p-1}{2}}.$$

$$|\, 1 - 1^{\frac{p-1}{2}} \,| \le 2.$$

С ограничениями на p это возможно только в том случае, когда

$$1 = (-1)^{\frac{p-1}{2}}.$$

Тогда

$$\frac{p-1}{2} = 2k, \;\; \Rightarrow \;\; p = 4k+1.$$

Задача решена.

Следствие Все простые нечетные делители числа a^2+1 имеют вид $4k+1$.

Задача 9.5. *В прогрессии $1 + 4x$, $k \ge 1$, лежит бесконечное количество простых чисел.*

Решение Предположим, что множество таких простых конечно и, значит, ограничено сверху некоторым числом n:

$$_1 < p_2 < p_3 < \ldots < p_r < n.$$

Тогда

$$N = (n!)^2 + 1 \equiv 1 \pmod{p_j}, \;\; 1 \le j \le r.$$

Существует простое $q \mid N$. Так как N нечетно, то q – нечетно. По доказанному ранее, $q = 1 + 4k$. Так как $q \ne p_1, \ldots, p_r$, получем противоречие.

Задача решена.

Замечание Справедливо более общее утверждение (теорема Дерихле). Последовательность вида

$$ak + b, \;\; (a,b) = 0, \;\; k = 0, 1, 2, \ldots$$

содержит бесконечное множество простых чисел.

Проблема До сих пор не доказано, что последовательность

$$k^2 + 1$$

содержит бесконечное множество простых.

Решение линейных полиномиальных сравнений

Будем рассматривать линейные многочлены.[19]

$$ax \equiv c \pmod{m}, \quad m \geq 2, \quad a, c \in \mathbb{Z}. \tag{51}$$

Требуется найти все целые x, удовлетворяющие сравнению (51). Все такие сравнения имеют вид

$$ax - c = my.$$

Поэтому задача сводится к решению уравнений вида

$$zx - my = c,$$

которые мы решать уже умеем.

Задача 9.6. *Решить сравнение*

$$23x \equiv -13 \pmod{73}.$$

Решение Решим с помощью алгоритма (см. семинар 4), составив таблицу

73	23	4	-1	0
0	1	-3	19	73

Получим, что

$$x = 19 + 73t.$$

Тогда

$$23 \cdot 19 \equiv -1 \pmod{73}.$$

Домножим на 13. Так как

$$19 \cdot 13 = 247 \equiv 28 \pmod{73},$$

получим, что

$$23 \cdot 17 \equiv -13 \pmod{73},$$

то есть

$$x = 28 + 73 \cdot k,$$

или

$$x \equiv 28 \pmod{73}.$$

Задача решена.

Задача 9.7. *Решить сравнение*

$$141x + 45 \equiv 0 \pmod{183}.$$

[19] Про линейные многочлены много рассказывалось на лекции. Некоторыми фактами из лекционного материала мы будем пользоваться.

Решение Вспомним один факт. Сравнение

$$ax \equiv c \pmod{m} \tag{52}$$

разрешимо тогда и только тогда, когда $d = (a, m) \mid c$, то есть

$$\begin{cases} a = d \cdot a_1, \\ c = d \cdot c_1, \\ m = d \cdot m_1. \end{cases}$$

Разделим все сравнение (52) на d, получим сравнение

$$a_1 x \equiv c_1 \pmod{m_1}$$

с меньшими коэффицентами.

Вернемся к задаче 9.7. В нашем случае можно записать

$$47x \equiv -15 \pmod{61},$$

Найдем решение с помощью таблицы:

61	47	14	5	-1	0
0	1	-1	4	-13	-61

Тогда

$$47 \cdot (-13) \equiv -1 \pmod{61},$$

и так как

$$(-13) \cdot 15 \equiv -12 \pmod{61},$$

домножим на 15, получим

$$47 \cdot (-12) \equiv -15 \pmod{61}.$$

Итак,

$$x \equiv -12 \pmod{61}.$$

Получаем три серии решений

$$x \equiv -12 \pmod{183},$$

$$x \equiv 49 \pmod{183},$$

$$x \equiv 110 \pmod{183}.$$

Задача решена.

Задача 9.8. *Решить сравнение*

$$91x + 26 \equiv 0 \pmod{133}.$$

Решение Вычислим

$$(91, 133) = (91, 42) = (7, 42) = 7.$$

Так как $7 \nmid 26$, сравнение неразрешимо.

Системы линейных сравнений

Теорема 9.2. *(Китайская теорема об остатках) Система*

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \dots \\ x \equiv a_n \pmod{m_n}. \end{cases} \tag{53}$$

разрешима, если $(m_i, m_j) = 1$ *при любых* i, j.

Алгоритм

1. Положим

$$M = m_1 \cdot \ldots \cdot m_n, \quad M_i = \frac{M}{m_i}.$$

2. Обозначим b_i решение сравнения

$$M_i t \equiv a_i \pmod{m_i}, \quad i = 1, \ldots, n.$$

3. Обозначим

$$x_0 = M_1 b_1 + \ldots + M_n b_n.$$

Все решения системы (53) имеют вид

$$x \equiv x_0 \pmod{M}.$$

Задача 9.9. *Решить систему*

$$\begin{cases} x \equiv 1 \pmod{8}, \\ x \equiv 2 \pmod{13}. \end{cases}$$

Решение Воспользуемся алгоритмом.

$$M = 8 \cdot 13 = 104, \quad M_1 = 13, \quad M_2 = 8.$$

Первое сравнение:

$$13t \equiv 1 \pmod{8},$$
$$-3t \equiv 1 \pmod{8},$$
$$-9t \equiv 3 \pmod{8},$$
$$t \equiv -3 \pmod{8},$$

так как $-9 \equiv -1 \pmod{8}$. Таким образом, $b_1 = -3$.

Второе сравнение:

$$8t \equiv 2 \pmod{13},$$
$$4t \equiv 1 \pmod{13},$$

$$12t \equiv 3 \pmod{13},$$
$$t \equiv -3 \pmod{13},$$

то $b_2 = -3$.

Теперь,

$$x_0 = 13 \cdot (-3) + 8 \cdot (-3) = -39 - 24 = -63.$$

Окончательно получим, что

$$x \equiv -63 \pmod{104} \equiv 41 \pmod{104}.$$

Задача решена.

Задача 9.10. *Решить систему*

$$\begin{cases} x \equiv 1 \pmod{5}, \\ x \equiv 2 \pmod{6}, \\ x \equiv 3 \pmod{7}. \end{cases}$$

Решение Действуем согласно алгоритму.

$$M = 5 \cdot 6 \cdot 7 = 210, \quad M_1 = 42, \quad M_2 = 35, \quad M_3 = 30.$$

Первое сравнение:

$$42t \equiv 1 \pmod{5},$$
$$2t \equiv 1 \pmod{5},$$

и умножая на 3, получим

$$t \equiv 3 \pmod{5},$$

то $b_1 = 3$. Второе сравнение:

$$35t \equiv 2 \pmod{6},$$
$$-t \equiv 2 \pmod{6},$$
$$t \equiv -2 \pmod{6},$$

то $b_2 = -2$. Третье сравнение:

$$30t \equiv 3 \pmod{7},$$
$$2t \equiv 3 \pmod{7},$$

и умножая на 4, получим

$$t \equiv 12 \equiv -2 \pmod{7},$$

тогда $b_3 = -2$. Теперь,

$$x_0 = 42 \cdot 3 + 35 \cdot (-2) + 30 \cdot (-2) = -4.$$

Окончательно получим, что

$$x \equiv -4 \pmod{210}.$$

Полиномиальные сравнения

Задачи

Задача 9.11. *Решить сравнение*

$$x^3 + 8x + 12 \equiv 0 \pmod{21}.$$

Решение Обозначим

$$f(x) = x^3 + 8x + 12, \quad m = 21 = 3 \cdot 7.$$

Рассмотрим систему сравнений

$$\begin{cases} f(x) \equiv 0 \pmod{3}, \\ f(x) \equiv 0 \pmod{7}. \end{cases} \tag{54}$$

По китайской теореме об остатках решения этой системы сможем «склеить» в решение исходного сравнения.

1. Рассмотрим сравнение

$$x^3 + 8x + 12 \equiv 0 \pmod{3},$$

$$x^3 - x \equiv 0 \pmod{3},$$

$$x(x-1)(x+1) \equiv 0 \pmod{3}.$$

Любое целое удовлетворяют этому сравнению. То есть, исходная система эквивалента сравнению

$$x^3 + 8x + 12 \equiv 0 \pmod{7},$$

$$x^3 + x - 2 \equiv 0 \pmod{7},$$

$$(x-1)(x^2 + x + 2) \equiv 0 \pmod{7}.$$

Первое решение имеет вид

$$x_1 \equiv 1 \pmod{7}.$$

2. Решим теперь

$$x^2 + x + 3 \equiv 0 \pmod{7}.$$

Быстрых алгоритмов для решения подобных сравнений нет. Перебором получим, что все значения (перебираем по остаткам от деления) не удовлетворяют сравнению. Итак, второе сравнение решения не имеет.

Объединяя решения системы (54), получим

$$x_1 \equiv 1 \pmod{21},$$

$$x_2 \equiv 8 \pmod{21},$$

$$x_3 \equiv 15 \pmod{21}.$$

Задача решена.

Задача 9.12. *Решить сравнение*

$$x^{100} + x^{50} + x^5 + 4 \equiv 0 \pmod 5. \tag{55}$$

Решение Общих решений подобных сравнений нет. Можно, как в прошлой задаче, пребирать остатки от деления, но будет неудобно возводить их в 100-ю степень. Можем понизить степень, воспользовавшись малой т. Ферма. По малой т. Ферма,

$$x^5 \equiv x \pmod 5, \ \ \forall\, x,$$

или

$$x^4 \equiv 1 \pmod 4,$$

так как $x \not\equiv 5 \pmod 5$. Понизим степени.

$$x^{100} = (x^5)^{20} \equiv x^{20} = (x^5)^4 \equiv x^4 \equiv 1 \pmod 5.$$

$$x^{50} = (x^5)^{10} \equiv x^{10} = (x^5)^2 \equiv x^2 \pmod 5.$$

$$x^5 \equiv x \pmod 5.$$

Так, можем переписать сравнение (55) в виде

$$1 + x^2 + x + 4 \equiv 0 \pmod 5,$$

$$x^2 + x \equiv 0 \pmod 5,$$

$$x(x+1) \equiv 0 \pmod 5,$$

Получим два решения

$$x_1 \equiv 0 \pmod 5,$$

$$x_2 \equiv -1 \pmod 5.$$

Заметим, что x_1 не является решением исходного сравнения (55).

Задача решена.

Подъем решений

Поговорим о решениях сравнений вида

$$f(x) \equiv 0 \pmod{p^\alpha}.$$

Сначала решается сравнение

$$f(x) \equiv 0 \pmod p.$$

Находим решение $x = x_0 \pmod p$.

Замет многократно применяется прием, позволяющий находит решения для степени p^{k+1}, зная решения для p^k.

Делается это следующим образом. Предположим, x_k – решение сравнения

$$f(x) \equiv 0 \pmod{p^k}.$$

Будем искать решения вида

$$x_{k+1} = x_k + p^k \cdot t$$

такие, что бы

$$f(x_{k+1}) \equiv 0 \pmod{p^{k+1}},$$
$$f(x_k + p^k t) \equiv 0 \pmod{p^{k+1}},$$

и, воспользовавшись формулой Тейлора, получим, что

$$f(x_k) + f'_k(x_k)p^k t \equiv 0 \pmod{p^{k+1}},$$

$$\frac{f(x_k)}{p^k} + f'_k(x_k)t \equiv 0 \pmod{p}. \tag{56}$$

Задачи

Задача 9.13. *Решить сравнение*

$$x^4 + x^2 + 6x + 1 \equiv 0 \pmod{27}.$$

Решение Заметим, что $27 = 3^3$.

1. Решим сравнение

$$x^4 + x^2 + 6x + 1 \equiv 0 \pmod{3}.$$

$$x^4 = x^3 \cdot x = x^2,$$

так как $x^3 \equiv x$.

$$2x^2 + 1 \equiv 0 \pmod{3}.$$

Перебором получим, что

$$x \equiv \pm 1 \pmod{3}.$$

2. Запишем решение предыдущего шага как

$$x = 1 + 3t.$$

Обозначим

$$f(x) = x^4 + x^2 + 6x + 1.$$

Вычислим

$$f(1) = 9 \equiv 0 \pmod{3},$$
$$f'(x) = 4x^3 + 2x + 6.$$

Воспользовавшись (56), получим

$$\frac{f(1)}{3} + f'(1)t = \frac{9}{3} + 12t = 3 + 12t \equiv 0 \pmod{3}.$$

Это сравнение верно при любом t. Итого получаем три решения:

$$x_1 \equiv 1 \pmod{9},$$

$$x_2 \equiv 4 \pmod 9,$$
$$x_3 \equiv 7 \pmod 9 \equiv -2 \pmod 9.$$

3. Возьмем решение предыдущего шага

$$x \equiv 1 \pmod 9.$$

Воспользовавшись (56), получим

$$\frac{f(1)}{9} + f'(1)t = \frac{9}{9} + 12t = 1 + 12t \equiv 0 \pmod 3.$$

Это сравнение не имеет решений, так как $3 \nmid 1$.

Теперь работаем с решением

$$x \equiv 4 \pmod 9.$$

Воспользовавшись (56), получим

$$\frac{f(4)}{9} + f'(4)t = \frac{297}{9} + 270t = 33 + 12t \equiv 0 \pmod 3.$$

Этому сравнению удовлетворяют любые t. Значит, решением будет

$$x \equiv 4 \pmod 9,$$

то есть три решения

$$x \equiv 4 \pmod{27},$$
$$x \equiv 13 \pmod{27},$$
$$x \equiv 22 \pmod{27}.$$

И, наконец, рассмотрим решение

$$x \equiv -2 \pmod 9.$$

$$x = -2 + 9t.$$
$$f(-2) = 9, \quad f'(-2) = -30.$$
$$\frac{f(-2)}{9} + f'(-2)t = \frac{9}{9} - 30t = 1 - 30t \equiv 0 \pmod 3.$$

Это сравнение решений не имеет.

Решения для случая из пункта 1.

$$x = -13$$

найдем на следующем занятии.

Семинар 10

Задачи

(Продолжение задачи 9.13) В прошлый раз решали сравнение

$$x^4 + x^2 + 6x + 1 \equiv 0 \pmod{27}.$$

Нашли, что для

$$x \equiv 1 \pmod{3}$$

сравнение имеет три решения:

$$x \equiv 4 \pmod{27},$$

$$x \equiv 13 \pmod{27},$$

$$x \equiv 22 \pmod{27}.$$

Рассмотрим теперь второй случай,

$$x \equiv -1 \pmod{3}.$$

Во-первых, преобразуем это решение до $\mod 9$.

$$x = -1 + 3t, \quad t = 0, 1, 2.$$

Найдем , какие из этих решений удовлетворяют сравнению

$$f(-1 + 3t) \equiv 0 \pmod{9}.$$

$$\frac{f(-1)}{3} + f'(-1)t = \frac{-3}{3} + 0t =\equiv 0 \pmod{3}.$$

Получили противоречие, а значит, в этом случае сравнение решений не имеет.

Задача решена.

Задача 10.1. *Решить сравнение*

$$f(x) = x^3 + 4x + 1 \equiv 0 \pmod{225}.$$

Решение Заметим, что $225 = 15^2 = 3^2 \cdot 5^2$.

1. Рассмотрим сравнение

$$x^3 + 4x + 1 \equiv 0 \pmod{9}. \tag{57}$$

Сначала решим

$$x^3 + 4x + 1 \equiv 0 \pmod{3}.$$

Можем упростить

$$x^3 + x + 1 \equiv 0 \pmod{3}.$$

Решением будет

$$x \equiv 1 \pmod 3.$$

Теперь нужно «поднять» это решение до $\pmod 9$.

$$x = 1 + 3t, \quad t = 0, 1, 2.$$

$$\frac{f(1)}{3} + f'(1)t = 2 + 7t \equiv 0 \pmod 3,$$

$$2 + t \equiv 0 \pmod 3,$$

$$t = -2 \pmod 3 \equiv 1 \pmod 3.$$

Итак, решением сравнения (57) будет

$$x \equiv 4 \pmod 9.$$

2. Теперь рассмотрим сравнение

$$x^3 + 4x + 1 \equiv 0 \pmod{25}. \tag{58}$$

Сначала решим

$$x^3 + 4x + 1 \equiv 0 \pmod 5.$$

$$x^3 - x + 1 \equiv 0 \pmod 5.$$

Перебираем остатки от деления на 5. $x = 0, 1, 2, -1$ нам не подходят. Единственное решение данного сравнения

$$x \equiv -2 \pmod 5.$$

Запишем

$$x = -2 + 5t, \quad 0 \le t < 5.$$

Должно быть выполнено

$$f(-2 + 5t) \equiv 0 \pmod{25},$$

или, по-другому,

$$\frac{f(-2)}{5} + f'(-2)t \equiv 0 \pmod 5.$$

$$f(-2) = -15, \quad f'(-2) = 16.$$

$$\frac{-15}{5} + 16t \equiv 0 \pmod 5,$$

$$-3 + 16t \equiv 0 \pmod 5,$$

$$-3 + t \equiv 0 \pmod 5,$$

$$t \equiv 3 \pmod 5.$$

При $t = 3$ получаем, что

$$x \equiv 13 \pmod{25}.$$

3. Итак, получаем для сравнений по соответствующим модулям

$$\begin{cases} x \equiv 4 \pmod 9, \\ x \equiv 13 \pmod{25}. \end{cases}$$

Можем записать в виде

$$\begin{cases} x \equiv 13 \pmod 9, \\ x \equiv 13 \pmod{25}. \end{cases}$$

То есть,

$$9 \,|\, x = 13, \quad 25 \,|\, x = 13.$$

Это значит, что

$$225 \,|\, x - 13,$$

то есть

$$x \equiv 13 \pmod{225}.$$

Задача решена.

Квадратичные сравнения

Пусть $p > 2$ – модуль. Будем рассмотривать сравнения вида

$$ax^2 + bx + c \equiv 0 \pmod p, \quad p \nmid a. \tag{59}$$

Домножив на a и учтя, что

$$b \equiv 2t \pmod p$$

всегда разрешимо, запишем

$$a^2x^2 + bax + ac = a^2x^2 + 2tax + ac = (ax + t)^2 - t^2 + ac = 0 \pmod p.$$

Обозначим $d = t^2 - ac.$ и $y = ax + t$. Тогда решение сравнения (59) будет удовлетворять упрощенному сравнению

$$y^2 \equiv d \pmod p. \tag{60}$$

И наоборот, зная y, x, найденное из сравнения

$$y \equiv ax + t \pmod p,$$

будет решением (59).

Символ Лежандра

Определение 10.1. *Символом Лежандра* $\left(\frac{a}{p}\right)$ называется функция двух переменных: простого $p > 2$, целого a

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ если } x^2 \equiv a \pmod p, \ p \nmid a \text{ разрешимо}, \\ -1, \text{ если сравнение не имеет решений}, 0, \text{ если } p \mid a. \end{cases} \tag{61}$$

Определение 10.2. Для первой строки (61) a называется *квадратичным вычетом*, а для второй строки – *квадратичным невычетом*.

Свойства символа Лежандра

Пусть p – простое нечетное, a, b – целые числа, $p \nmid a, b$.

1. Если $a \equiv b \pmod p$, то
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

2.
$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

3.
$$\left(\frac{1}{p}\right) = 1,$$
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, \text{ если } p \equiv 1 \pmod 4, \\ -1, \text{ если } p \equiv 3 \pmod 4. \end{cases}$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, \text{ если } p \equiv \pm 1 \pmod 8, \\ -1, \text{ если } p \equiv \pm 3 \pmod 8. \end{cases}$$

4. (Квадратичный закон взаимности) Пусть p, q – различные простые нечетные числа, то
$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$
то есть
$$\left(\frac{p}{q}\right) = -\left(\frac{1}{p}\right), \text{ если } p \equiv q \equiv 3 \pmod 4,$$
$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ иначе.}$$

5.
$$\left(\frac{a}{q}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Задачи

Задача 10.2. *Найти*

$$\left(\frac{111}{541}\right).$$

Решение

$$\left(\frac{111}{541}\right) = \left(\frac{3}{541}\right)\cdot\left(\frac{37}{541}\right) = \left(\frac{541}{3}\right)\left(\frac{541}{37}\right) = \left(\frac{1}{3}\right)\left(\frac{23}{37}\right),$$

так как

$$541 \equiv 1 \pmod 3, \quad 541 = 14\cdot 37 + 23.$$

Далее,

$$\left(\frac{1}{3}\right)\left(\frac{23}{37}\right) = \left(\frac{23}{37}\right) = \left(\frac{37}{23}\right) = \left(\frac{14}{23}\right) = \left(\frac{2\cdot 7}{23}\right) =$$
$$= \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = \left(\frac{7}{23}\right) = -\left(\frac{2\cdot 23}{7}\right) = -\left(\frac{2}{7}\right) = -1,$$

и последний переход следует из свойства 3.

Задача решена.

Задача 10.3. *Найти*

$$\left(\frac{529}{601}\right).$$

$$\left(\frac{529}{601}\right) = \left(\frac{23^2}{601}\right) = \left(\frac{23}{601}\right)^2 = 1.$$

Задача решена.

Задача 10.4. *Понять, разрешимо ли сравнение*

$$x^2 \equiv 68 \pmod{113}.$$

Решение Запишем символ Лежандра

$$\left(\frac{68}{113}\right) = \left(\frac{4\cdot 17}{113}\right) = \left(\frac{4}{113}\right)\left(\frac{17}{113}\right) = \left(\frac{2}{113}\right)^2\left(\frac{17}{113}\right) = \left(\frac{17}{113}\right) = \left(\frac{113}{17}\right).$$

Так как

$$113 = 6\cdot 17 + 11,$$

$$\left(\frac{113}{17}\right) = \left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Сравнение не разрешимо.

Задача решена.

Задача 10.5. *Решить сравнение*

$$5x^2 + 11x - 91 \equiv 0 \pmod{379}. \tag{62}$$

Решение Умножив обе части сравнения на 5, получим

$$25x^2 + \underbrace{55}_{5\cdot 11} x - 455 \equiv 0 \pmod{379}.$$

Найдем t, для которого

$$11 \equiv 2t \pmod{379}.$$
$$t \equiv 195 \pmod{379}.$$

Тогда (62) представимо в виде

$$25x^2 + 2 \cdot 195 \cdot 5x - 455 \equiv 0 \pmod{379},$$
$$(5x + 195)^2 - 195^2 - 455 \equiv 0 \pmod{379},$$
$$(5x + 195)^2 - 195^2 - 455 \equiv 0 \pmod{379},$$
$$\underbrace{(5x + 195)^2}_{=y} - 38480 \equiv 0 \pmod{379},$$
$$y \equiv 38480 \pmod{379}.$$

Найдем, разрешимо ли это сравнение. Для этого найдем

$$\left(\frac{38480}{379}\right) = \left(\frac{201}{379}\right) = \left(\frac{3}{379}\right)\left(\frac{67}{379}\right) = (-1)\cdot\left(\frac{379}{3}\right)\cdot(-1)\cdot\left(\frac{379}{67}\right) =$$
$$= \left(\frac{1}{3}\right)\left(\frac{44}{67}\right) = \left(\frac{4}{67}\right)\left(\frac{11}{67}\right) = -\left(\frac{67}{11}\right) = -\left(\frac{1}{11}\right) = -1.$$

Значит, у сравнения (62) решений нет.

Задача решена.

Задача 10.6. *Найти все простые p, при которых разрешимо сравнение*

$$x^2 + 3 \equiv 0 \pmod{p}. \tag{63}$$

Решение При $p = 2$ сравнение (62) разрешимо, а при $p = 3$ – неразрешимо.

Будем рассматривать теперь $p > 3$. Перепишем сравнение в виде

$$x^2 \equiv -3 \pmod{p}.$$

Распишем

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\frac{p-1}{2}} = \left(\frac{p}{3}\right).$$

Найдем, при каких p выполняется

$$\left(\frac{p}{3}\right) = 1.$$

По определению символа Лежандра, это верно при

$$p \equiv 1 \pmod{3},$$

то есть

$$p = 1 + 3k, \quad k \geq 1.$$

Задача решена.

Задача 10.7. *Доказать, что простых* $p \equiv 1 \pmod 6$ *имеется бесконечно много.*

Решение Предположим обратное. Тогда

$$p_1 < p_2 < \ldots < p_r$$

– все простые вида $6k+1$. Положим

$$A = 6p_1 \ldots p_r, \quad N = A^2 + 3.$$

Заметим, что $p_j \nmid N$, $2 \nmid N$, $3 \nmid N$ и

$$N \equiv 3 \pmod{p_j}.$$

Так как $N > 3$ и нечетное, у него есть простой делитель

$$q \mid N, \quad q \neq p_1, \ldots, p_r, \quad q \neq 3,$$

то q – нечетно.

Из задачи 10.6 получается, что $q = 1 + 3k$. При этом $2 \mid q - 1$. Значит,

$$q = 1 + 6m,$$

откуда получаем противоречие с предположением о конечном количестве чисел такого вида.

Задача решена.

Задача 10.8. *Найти все простые числа* p*, которые делят значение* $x^2 - 2$ *при целых* x*, то есть при которых сравнение*

$$x^2 - 2 \equiv 0 \pmod p$$

разрешимо.

Решение Заметим, что сравнение разрешимо, если

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv 1 \pmod 8 \text{ или } p \equiv -1 \pmod 8.$$

Кроме того, $p = 2$ удовлетворяет условию.

Задача решена.

Задача 10.9. *Докажите бесконечность множества простых в прогрессии* $8m-1$.

Решение Допустим, что множество простых вида $8m-1$ конечно. Обозначим их

$$p_1 < \ldots < p_r.$$

Положим

$$A = p_1 \cdot \ldots \cdot p_1, \quad N = A^2 - 2.$$

Заметим, что N нечетно (так как A нечетно) и

$$N \equiv -2 \pmod{p_j}, \quad j = 1, \ldots, r. \tag{64}$$

Так как

$$A = 2l + 1 \;\Rightarrow\; A^2 = (2l+1)^2 = 4l(l+1) + 1,$$

и среди чисел l и $l+1$ одно четное, то

$$A \equiv 1 \pmod 8, \quad N \equiv -1 \pmod 8. \tag{65}$$

Воспользуемся результатом предыдущей задачи. Все простые делители чисал N имеют вид $p \equiv 1 \pmod 8$ или $p \equiv -1 \pmod 8$.

Предположим, что все простые делители N сравнимы с 1 по модулю 8. Тогда, так как

$$a \equiv 1 \pmod 8, \quad b \equiv 1 \pmod 8 \;\Rightarrow\; ab \equiv 1 \pmod 8,$$

для N должно выполняться

$$N \equiv 1 \pmod 8.$$

Получаем противоречие с (65). Значит, существует $q \mid N$ – простое,

$$q \equiv -1 \pmod 8.$$

С учетом (64) получаем противоречие.

Задача решена.

Задача 10.10. *Найдите все простые числа p, делящие значения многочлена*

$$x^2 + x - 1$$

в целых точках.

Решение Значение $p = 2$ условию не удовлетворяет.

Рассмотрим $p > 2$. Выясним, для каких p

$$x^2 + x - 1 \equiv 0 \pmod p$$

разрешимо. Выделим полный квадрат:

$$4x^2 + 4x - 4 \equiv 0 \pmod p,$$
$$(2x+1)^2 - 5 \equiv 0 \pmod p,$$
$$y^2 \equiv 5 \pmod p.$$

Найдем, при каких p

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1,$$

то есть

$$z^2 \equiv p \pmod 5.$$

Отсюда

$$p \equiv \pm 1 \pmod 5.$$

Задача решена.

Заметим, что так как p нечетное, $p \pm 1$ делится на 2 и верно

$$p \equiv \pm 1 \pmod{10}. \tag{66}$$

Задача 10.11. *Показать, что существует бесконечное количество простых чисел вида* $10m-1$.

Решение Предположим обратно. Обозначим все такие числа

$$p_1 < \ldots < p_r.$$

Рассмотрим два возможных случая.

1. Предположим сначала, что r нечетно. Так как

$$p_j \equiv -1 \pmod{10},$$

для числа

$$A = p_1 \cdot \ldots p_r \equiv (-1)^r \pmod{10} \equiv -1 \pmod{10}.$$

Тогда число

$$N = A^2 + A - 1 \equiv -1 \pmod{10}.$$

Так как

$$p_j \mid A, \quad N \equiv -1 \pmod{p_j},$$

то $p_j \nmid N$.

Теперь, как и в задаче 8, если все простые делители N сравнимы с 1 по модулю 10, то и

$$N \equiv 1 \pmod{10}.$$

Получаем противоречие. С учетом (65) получается, что существует простой делитель $q \mid N$, $q = 10m-1$.

Так как

$$q \neq p_j, \quad q \mid N, \quad N \equiv -1 \pmod{p_j},$$

получаем противоречие с изначальным предположением.

2. Предположим теперь, что r – четно. Обозначим

$$A = -p_1 \cdot \ldots \cdot p_r \equiv -(-1)^r \pmod{10} \equiv -1 \pmod{10}.$$

Дальнейшие рассуждения повторяют рассуждения шага 1.

Символ Якоби

Пусть P, a – целые, P – нечетно, $(P,a)=1$. Если

$$P = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s},$$

то символ Якоби по определению полагается

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \ldots \left(\frac{a}{p_s}\right)^{\alpha_s}.$$

Для символа Якоби справедливы свойства 1-4 символа Лежандра (свойство 5 не выполняется).

Вообще говоря, символ Якоби не имеет отношения к разрешимости сравнений.

Рассмотрим **пример**. Возьмем $P = 15$, $a = 2$. Тогда

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

Но, если сравнение

$$x^2 \equiv 2 \pmod{15}$$

разрешимо, то разрешимо и сравнение

$$x^2 \equiv 2 \pmod{3}.$$

Это неверно, так как символ Лежандра

$$\left(\frac{2}{3}\right) = -1.$$

Тем не менее, символ Якоби позволяет вычислять символ Лежандра.

Пример 10.1.

$$\left(\frac{201}{379}\right) = \left(\frac{379}{201}\right) = \left(\frac{178}{201}\right) = \left(\frac{-23}{201}\right) = \left(\frac{23}{201}\right) =$$
$$= \left(\frac{201}{23}\right) = \left(\frac{-6}{23}\right) = -\left(\frac{6}{23}\right) = -\left(\frac{2}{23}\right)\left(\frac{3}{23}\right) =$$
$$= -\left(\frac{3}{23}\right) = \left(\frac{23}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Первообразные корни

Возьмем $m \geq 2$ и целое a, $(a, m) = 1$. По т. Эйлера,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Определение 10.3. Наименьшее натуральное число d с условием

$$a^d \equiv 1 \pmod{m}$$

называется *порядком* a.

Определение 10.4. Число g – *первообразный корень*, если порядок q равен $\varphi(m)$.

Вспомним, что класс вычетов по модулю m

$$\mathbb{Z}/_m\mathbb{Z}$$

образует кольцо. Можно проверить, что классы чисел, взаимно простых с m (т.н. приведенные классы вычетов), образуют подмножество в этом кольце и мультипликативную группу, обозначаемую

$$G = (\mathbb{Z}/_m\mathbb{Z})^*$$

Можно найти $\varphi(m)$ классов вычетов, взаимно простых с m. Вопрос о том, когда существуют первообразные корни, связан с вопросом о том, когда такие группы являются циклическими.

Теорема 10.1. *Для простых чисел $m = p$ существуют первообразные корни. Количество их равно $\varphi(p-1)$*

Теорема 10.2. *Пусть a не делится на p и для кждого простого q, делящего $p-1$, выполняется условие*

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}.$$

Тогда a – первообразный корень.

Пример 10.2. *Возьмем $p = 23$. Тогда*

$$p - 1 = 22 = 2 \cdot 11.$$

Проверим для $a = 2$ условие

$$a^{11} \not\equiv 1 \pmod{23}.$$

$$2^{11} = 2(2^5)^2 \equiv 2 \cdot 9^2 \pmod{23} - 2 \cdot 81 = 162 \equiv 1 \pmod{23}.$$

Условие теоремы 10.2 не выполняется.
Для $a = 3$ получим

$$3^{11} = 2^2 \cdot 27^3 \equiv 9 \cdot 4^3 \pmod{23} = 9(-5) = -45 \equiv 1 \pmod{23}.$$

Для $a = 4$

$$4^{11} = (2^{11})^2 \equiv 1 \pmod{23}.$$

Для $a = 5$

$$5^{11} = 5 \cdot 25^5 \equiv 5 \cdot 2^5 \pmod{23} = 5 \cdot 32 \equiv 5 \cdot 9 \pmod{23} =$$

$$45 \equiv -1 \pmod{23},$$

$$5^2 = 25 \equiv 2 \pmod{23}.$$

Таким образом, $a = 5$ – первообразный корень по $\mod(23)$.

Семинар 11

Индексы

Определение 11.1. Пусть p – простое, g – первообразный корень по модулю p. Для

$$\forall\, a, \quad p \nmid a,$$

сравнение

$$g^x \equiv a \pmod{p}$$

имеет единственное решение на $0 < x \leq p-1$. Такое число x называется *индексом* числа a и обозначается

$$x = \mathsf{ind} a.$$

Свойства индексов похожи на свойства логарифмов. Так,

$$\mathsf{ind} ab \equiv \mathsf{ind} a + \mathsf{ind} b \pmod{p-1}. \tag{67}$$

Задачи

Задача 11.1. *Найти x, для которого*

$$3^x \equiv 2 \pmod{17}.$$

Решение Домножим это сравнение на 9. Получим

$$3^{x+2} \equiv 2 \cdot 9 = 18 \equiv 1 \pmod{17}.$$

Можно проверить, что 3 – первообразный корень по mod (17) (аналогичные задачи решали на прошлом семинаре).

Единственный случай, когда такое сравнение верно, это

$$3^0 \equiv 1 \pmod{p}.$$

Значит,

$$x + 2 \equiv 0 \pmod{18},$$
$$x \equiv 16 \pmod{18}.$$

Задача решена.

Задача 11.2. *Решить сравнение*

$$x^{119} \equiv 2 \pmod{19}.$$

Решение Найдем такую степень, при возведении в которую данное сравнение в левой части получим x. Для этого решим сравнение

$$119t \equiv 1 \pmod{18}.$$

Получим, что при $t = 5$

$$119 \cdot 5 \equiv 1 \pmod{18}.$$

Вольспозуемся тем, что

$$x^{18} \equiv 1 \pmod{19},$$

и получим

$$x \equiv 2^5 \pmod{19} \equiv -6 \pmod{19}.$$

Задача решена.

Цепные дроби

Предположим, что у нас есть последовательность целых чисел[20]

$$a_0, a_1, \ldots, a_n \in \mathbb{Z}, \quad a_j \geq 1, \quad j = 1, 2, \ldots.$$

Построим дробь

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \ldots 6 \frac{1}{a_n}}} = \frac{p_n}{q_n}. \tag{68}$$

Цепную дробь (68) принято обозначать

$$[a_0; a_1 \ldots, a_n].$$

Если исходная последовательность бесконечна, то последовательность (68) сходится к некоторому иррациональному числу.

Вспомним некоторые свойства цепных дробей.

Свойства

1.

$$p_{-1} = 1, p_0 = q_1,$$

$$q_{-1} = 0, q_0 = 1,$$

$$\begin{cases} p_{k+1} = a_{k+1}p_k + p_{k-1}, \\ q_{k+1} = a_{k+1}q_k + q_{k-1}, \end{cases} \quad k \geq 0$$

$$\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k].$$

2.

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}, \quad k \geq 0. \tag{69}$$

3. Если последовательность a_i бесконечна, то

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \ldots,$$

$$\frac{p_1}{q_1} > \frac{p_3}{q_3} > \ldots$$

[20]Возможно, бесконечная.

Алгоритм разложения в цепную дробь

Надо разложить в последовательность (68) число α. Обозначим

$$\alpha_0 = \alpha, \quad a_0 = [\alpha_0],$$

то есть целую часть от α. Тогда

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \quad k \geq 1.$$

Конечные цепные дроби

Решим уравнение

$$ax - by = 1.$$

Можем разложить

$$\frac{a}{b} = [a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

Обозначим

$$a = p_n, \quad b = q_n.$$

Тогда, согласно (69),

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}.$$

В случае, когда k нечетно, достаточно положить

$$x = q_{k-1}, \quad y = p_{k-1},$$

а в случае, когда k четно,

$$x = -q_{k-1}, \quad y = -p_{k-1}. \tag{70}$$

Задачи

Задача 11.3. *Разложить*

$$\alpha = -\frac{77}{92}.$$

Решение Согласно алгоритму, положим

$$\alpha_0 = -\frac{77}{92}, \quad [\alpha_0] = a_0 = -1.$$

Тогда

$$\alpha_1 = \frac{1}{-\frac{77}{92} + 1} = \frac{92}{-77 + 92} = \frac{92}{15}, \quad a_1 = 6;$$

$$\alpha_2 = \frac{1}{\frac{92}{15} - 6} = \frac{15}{2}, \quad a_2 = 7;$$

$$\alpha_3 = \frac{1}{\frac{15}{2} - 7} = 2, \quad a_3 = 2.$$

Получаем, что

$$-\frac{77}{92} = [-1; 6, 2, 3].$$

Решим теперь уравнение

$$-77x - 22y = 1. \tag{71}$$

Здесь

$$a = -77, \quad b = 92.$$

Составим табличку

n	-1	0	1	2	3
a		-1	6	7	9
p	1	-1	-5	$\underline{-36}$	-77
q	0	1	6	$\underline{43}$	92

Тогда, по описанному выше алгоритму (70),

$$x = 43, \quad y = -36$$

являются решениями уравнения (71).

Задача решена.

Задача 11.4. *Решить уравнение*

$$30x - 17y = 1. \tag{72}$$

Решение Положим

$$\alpha = \frac{30}{17},$$

$$\alpha_0 = \frac{30}{17}, \quad [\alpha_0] = a_0 = 1.$$

Вычислим

$$\alpha_1 = \frac{1}{\frac{30}{17} + 1} = \frac{17}{13}, \quad a_1 = 1;$$

$$\alpha_2 = \frac{1}{\frac{17}{13} - 1} = \frac{13}{4}, \quad a_2 = 3;$$

$$\alpha_3 = \frac{1}{\frac{13}{4} - 3} = 4, \quad alpha_3 = 4.$$

Получаем

$$\frac{30}{17} = [1; 1, 3, 4].$$

Составим, как и в прошлой задаче, таблицу

n	-1	0	1	2	3
a		1	1	3	4
p	1	1	2	$\underline{7}$	30
q	0	1	1	$\underline{4}$	17

Так, частное решение уравнения (72) будет иметь вид

$$x = 4, \quad y = 7.$$

Общее решение имеет вид

$$\begin{cases} x = 4 + 17t, \\ y = 7 + 30t \end{cases} \qquad t \in \mathbb{Z}.$$

Задача решена.

Задача 11.5. *Показать, что*

$$\frac{1}{q_k(q_{k+1} + q_k)} \leq \left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k q_{k+1}}, \quad k \geq 0.$$

Решение Вычислим

$$\alpha - \frac{p_k}{q_k} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k+1}} - \frac{p_k}{q_k} = \frac{p_{k-1} q_k - p_k q_{k-1}}{q_k(\alpha_{k+1} q_k + q_{k-1})} = \frac{(-1)^k}{q_k(\alpha_{k+1} q_k + q_{k-1})}.$$

Так,

$$\left| \alpha - \frac{p_k}{q_k} \right| = \frac{1}{q_k(\alpha_{k+1} q_k + q_{k-1})}, k \geq 0.$$

Воспользуемся тем, что $\alpha_{k+1} \geq a_{k+1}$. Тогда

$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k(a_{k+1} q_k + q_{k-1})} = \frac{1}{q_k q_{k+1}}.$$

Здесь воспользовались свойством 1.

Теперь, так как $\alpha_{k+1} \leq a_{k+1} + 1$,

$$\left| \alpha - \frac{p_k}{q_k} \right| \geq \frac{1}{q_k((a_{k+1} + 1) q_k + q_{k-1})} = \frac{q_k(q_{k+1} + q_k)}{.}$$

Задача решена.

Задача 11.6. *Разложить*

$$\alpha = 2 + \sqrt{5}.$$

Решение Аналогично предыдущим примерам, положим

$$\alpha_0 = 2 + \sqrt{5}, \quad a_0 = 4.$$

Тогда

$$\alpha_1 = \frac{1}{2 + \sqrt{5} - 4} = \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2 = \alpha_0.$$

Значит,

$$\alpha = [4; 4, 4, 4, \ldots] = [4; \overline{4}] = [\overline{4}].$$

Задача решена.

Задача 11.7. *Разложить*

$$\alpha = \sqrt{23}.$$

Решение Положим

$$\alpha_0 = \sqrt{23}, \quad a_0 = 4.$$

$$\alpha_1 = \frac{1}{\sqrt{23}-4} = \frac{\sqrt{23}+4}{7}, \quad a_1 = 1.$$

$$\alpha_2 = \frac{1}{\frac{\sqrt{23}+4}{7}-1} = \frac{7}{\sqrt{23}-3} = \frac{7(\sqrt{23}+3)}{14} = \frac{\sqrt{23}+3}{2}, \quad a_2 = 3.$$

$$\alpha_3 = \frac{1}{\frac{\sqrt{23}+3}{2}-3} = \frac{2}{\sqrt{23}-3} = \frac{2(\sqrt{23}+3)}{14} = \frac{\sqrt{23}+3}{7}, \quad a_3 = 1.$$

$$\alpha_4 = \frac{1}{\frac{\sqrt{23}+3}{7}-1} = \frac{7}{\sqrt{23}-4} = \frac{7(\sqrt{23}+4}{7} = \sqrt{23}+4, \quad a_4 = 8.$$

$$\alpha_5 = \frac{1}{\sqrt{23}+4-8} = \frac{\sqrt{23}+4}{7} = \alpha_1.$$

Таким образом,

$$\sqrt{23} = [4; \overline{1,3,1,8}].$$

Задача решена.

Теорема 11.1. *(Эйлера – Лагранжа) Цепная дробь числа α будет периодической $\iff$ α – квадратичная иррациональность.*[21]

Задача 11.8. *Доказать, что*

$$[\underbrace{2;2,\ldots,2}_{n}] = \frac{(1+\sqrt{2})^{n+1}-(1-\sqrt{2})^{n+1}}{(1+\sqrt{2})^{n}-(1-\sqrt{2})^{2}}, \quad n \geq 1. \tag{73}$$

Решение При $n = 1$ в правой части (73) получим

$$\frac{1+2\sqrt{2}+2-1+2\sqrt{2}-2}{2\sqrt{2}} = \frac{4\sqrt{2}}{2\sqrt{2}} = 2.$$

Для $n = 2$

$$\frac{1+3\sqrt{2}+32+2\sqrt{2}-1+3\sqrt{2}-32+2\sqrt{2}}{4\sqrt{2}} = \frac{10\sqrt{2}}{4\sqrt{2}} = \frac{5}{2} = 2+\frac{1}{2}.$$

[21] Разложение более сложных иррациональностей в цепные дроби представляют собой сложную задачу. Так, например,

$$e = [2;1,2,1,1,4,1,1,6,1,\ldots],$$

и некоторая закономерность наблюдается, а у числа π найти какую-либо закономерность в разложении затруднительно.

Обозначим теперь

$$u_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}, \quad u_0 = 0, \quad u_1 = 1. \tag{74}$$

Попробуем найти реккурентное уравнение, которому удовлетворяет (74).

Найдем число, которое является корнем для обеих скобок в правой части (74). Оба случая можно описать уравнением

$$(x-1)^2 = 2,$$

то есть

$$x^2 = 2x + 1.$$

Для них можем записать

$$x_i^2 = 2x_i + 1,$$
$$x_i^{n+1} = 2x_i^n + x_i^{n-1}.$$

Получается, что последовательности x_1^n, x_2^n удовлетворяют реккурентному соотношению. Можем записать в виде

$$V_{n+1} = 2V_n + V_{n-1}.$$

Раз они удовлетворяют соотношению, удовлетворяет и их разности и для u_n можем записать

$$u_{n+1} = 2u_n + u_{n-1}.$$

В частности,

$$u_2 = 2, \quad u_3 = 5, \ldots$$

При этом

$$\alpha_{n+1} = \frac{u_{n+1}}{u_n}.$$

Значит,

$$\alpha_{n+1} = 2 + \frac{\alpha_n}{.}$$

Это можем переписать в виде

$$\alpha_n = \frac{1}{\alpha_{n+1} - 2}.$$

$$\alpha_{n+1} = 1 + \frac{1}{\alpha_n} = 2 + \frac{1}{2 + alpha_{n-1}} = 2 + \frac{1}{2 + \frac{1}{2+\ldots+\underbrace{\frac{1}{\alpha_2}}_{=2}}} = \underbrace{[2; 2, \ldots, 2]}_{n}.$$

Задача решена.

Задача 11.9. *Число α задано*

$$\alpha = [2; 1, 1, 3].$$

Чему равно α?

Решение Рассмотрим сначала число

$$\beta = [\overline{1,1,3}] = [1;\overline{1,3,1}].$$

Тогда

$$\alpha = 2 + \frac{1}{\beta}. \tag{75}$$

Можем записать

$$\beta = [1,1,3,\beta],$$

то есть

$$\beta = 1 + \frac{1}{1 + \frac{1}{3+\frac{1}{\beta}}}.$$

Заполним таблицу

n	-1	0	1	2	3
a		1	1	3	β
p	1	1	2	7	$7\beta+2$
q	0	1	1	4	$4\beta+1$

Тогда

$$\beta = \frac{7\beta+2}{4\beta+1}.$$

Решим это уравнение.

$$4\beta^2 + \beta = 7\beta + 2$$

$$4\beta^2 - 6\beta - 2 = 0$$

$$2\beta^2 - 3\beta - 1 = 0$$

$$\beta_{1,2} = \frac{3 \pm \sqrt{9+8}}{4} = \frac{3 \pm \sqrt{17}}{4}.$$

Так как $\beta > 0$, получаем, что

$$\beta = \frac{3+\sqrt{17}}{4}.$$

Вернемся к α. Из (75) получаем, что

$$\alpha = 2 + \frac{4}{\sqrt{17}+3} = 2 + \frac{4(\sqrt{17}+3)}{8} = 2 + \frac{\sqrt{17}+3}{2} = \frac{\sqrt{17}+7}{2}.$$

Задача решена.

Задача 11.10. *Пусть α – квадратичная ираациональность, раскладываемая в чисто периодическую дробь, а $\beta = -\frac{1}{\alpha'}$, где α' – второй корень уравнения для α. Доказать, что написанный в обратном порядке период числа α является периодом числа β.*

Решение По определению,

$$\alpha = \alpha_0 = [\overline{a_0, a_1, \ldots, a_n}], \quad \alpha_{m+1} = \alpha.$$

Можно записать

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

в виде

$$\alpha_{k+1} = u_{k+1} + v_{k+1}\alpha, \quad u_{k+1}, v_{k+1} \in \mathbb{Q}.$$

Заметим, что если α' – второй корень уравнения для α, то

$$(\alpha + \beta)' = \alpha' + \beta', \quad (\alpha\beta)' = \alpha'\beta', \tag{76}$$

$$\alpha_{m+1} = \alpha_0.$$

Положим

$$\beta_k = -\frac{1}{\alpha'_{m+1-k}}, \quad k = 0, 1, \ldots, m.$$

Запишем выражение для α_k в виде

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}.$$

Тогда

$$\alpha'_k = a_k + \frac{1}{\alpha'_{k+1}}.$$

$$-\frac{1}{\alpha'_{k+1}} = a_k - \alpha'_k = a_k + \frac{1}{(-1/\alpha'_k)}.$$

Тогда

$$\beta_{m-k} = a_k + \frac{1}{\beta_{m+1-k}}.$$

Начнем раскладывать β в цепную дробь. Получим

$$\beta_0 = a_m + \frac{1}{\beta_1} = a_m + \frac{1}{a_{m-1} + 1/\beta_2} = \ldots = a_m + \frac{1}{a_{m-1} + \frac{1}{a_{m-2} + \ldots + \frac{1}{a_1 + \frac{1}{\beta_m}}}} =$$

$$= a_m + \frac{1}{a_{m-1} + \frac{1}{a_{m-2} + \ldots + \frac{1}{a_1 + \frac{1}{a_0 + \beta_{m+1}}}}}.$$

Вспомним, что

$$\beta_{m+1} = -\frac{1}{\alpha'} = \beta.$$

Значит,

$$\beta = [a_m; \ldots a_1, a_0, \beta].$$

Получается, что

$$\beta = [\overline{a_m, \ldots, a_0}].$$

Задача решена.

Задача 11.11. *Пусть $d > 1$ и не делится на квадрат простого числа. Справедливо представление*

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_k, 2a_0}], \quad a_0 = [\sqrt{d}],$$

$(a_1, \ldots, a_k)$ *– симметрична.*[22]

Решение Обозначим

$$\gamma = \sqrt{d} + [\sqrt{d}] > 1.$$

Тогда

$$\gamma' = -\sqrt{d} + [\sqrt{d}], \quad -1 < \gamma' < 0.$$

Так как $\sqrt{d}$ – периодическая,

$$\sqrt{d} = [a_0, a_1, \ldots, a_m].$$

Нам понадобится следующая теорема.

Теорема 11.2. *Разложение числа α в цепную дробь будет чисто периодическим $\iff$ α – квадратическая иррациональность, $\alpha > 1$, $-1 < \alpha' < 0$.*

Так как условия теоремы для γ выполняются, получим, что и

$$\gamma = [\overline{2a_0, a_1, \ldots, a_m}].$$

В соответствии с задачей 8,

$$-\frac{1}{\gamma'} = [a_m, a_{m-1}, \ldots, a_1, 2a_0].$$

Это значит, что

$$a_m = 2a_0, \quad a_{m-1} = a_1, \ldots a_1 = a_{m-1}.$$

Тогда

$$\sqrt{d} = [a_0; a_1, \ldots, a_{m-1}, 2a_0],$$

так как

$$\gamma = [2a_0, a_1, \ldots, a_{m-1}, 2a_0, a_1, \ldots] = \sqrt{d} + a_0.$$

Задача решена.

[22]Например,

$$\sqrt{23} = [4; 1, 3, 1, 8].$$

Алгоритм решения уравнения

Рассмотрим уравнение Пелля

$$x^2 - dy^2 = 1,$$

где d – целое, $d > 1$ и $p^2 \nmid d$.

1. Разложить

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_l, 2a_0}],$$

набор $(a_1, \ldots, a_k)$ симметричен.

2. Найти p_k, q_k.

3. Определим самое маленькое решение

$$x_1 + y_1\sqrt{d} = \begin{cases} p_k + q_k\sqrt{d}, \text{ если } k \text{ – нечетно}, \\ (p_k + q_k\sqrt{d})^2, \text{ если } k \text{ – четно}. \end{cases}$$

Все решения (x_m, y_m) уравнения Пелля имеют вид

$$x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m, \quad m = 1, 2, \ldots, \quad x_m, y_m > 0.$$

Пример 11.1. *Рассмотрим уравнение*

$$x^2 - dy^2 = 1, \quad d = 29.$$

Разложим

$$\sqrt{29} = [5; \underbrace{2, 1, 1, 2}_{k=4}, 10].$$

Найдем

$$\frac{p_0}{q_0} = \frac{5}{1}, \quad \frac{p_1}{q_1} = \frac{11}{2}, \quad \frac{p_2}{q_2} = \frac{16}{3}, \quad \frac{p_3}{q_3} = \frac{27}{5}, \quad \frac{p_4}{q_4} = \frac{70}{13}.$$

Тогда

$$x_1 + y_1\sqrt{d} = \left(70 + 13\sqrt{29}\right)^2 = 9801 + 1820\sqrt{29}.$$

Получается, самое маленькое решение данного уравнение

$$x_1 = 9801, \quad y_1 = 1820.$$

Также можно посчитать, например

$$x_2 = 192119201, \quad y_2 2 = 35675640.$$

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ