Тема 3. Элементы алгебраической и аналитической теории чисел

Теоретический материал

§1. Цепные дроби.

Конечной цепной дробью называется выражение

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}}, \quad (1)$$

где a_0 - целое число, a_i, $i > 0$, – натуральные числа, $a_k > 1$. Будем записывать цепную дробь (1) в виде $[a_0 : a_1 : \ldots : a_k]$.

Каждое рациональное число $\frac{p}{q}$ можно представить единственным образом в виде конечной цепной $\frac{p}{q} = [a_0 : a_1 : \ldots : a_k]$, при этом a_i - неполные частные алгоритма Евклида нахождения наибольшего общего делителя чисел p и q, то есть

$$p = a_0 q + r_1,$$

$$q = a_1 r_1 + r_2,$$

$$r_1 = a_2 r_2 + r_3,$$

$$\ldots$$

$$r_{k-2} = a_{k-1} r_{k-1} + r_k,$$

$$r_{k-1} = a_k r_k.$$

Для заданной конечной цепной дроби $[a_0 : a_1 : \ldots : a_k]$ цепная дробь $[a_0 : a_1 : \ldots : a_n]$ $(0 \le n \le k)$ называется n-й *подходящей цепной дробью*.

Бесконечной цепной дробью называется выражение

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k + \ddots}}}}, \quad (2)$$

где a_0 - целое число, a_i, $i > 0$, – натуральные числа. Будем записывать цепную дробь (2) в виде $[a_0 : a_1 : \ldots : a_k : \ldots]$.

Для заданной бесконечной цепной дроби $[a_0 : a_1 : \ldots : a_k : \ldots]$ цепная дробь $\frac{p_n}{q_n} = [a_0 : a_1 : \ldots : a_n]$ $(n \ge 1)$ называется n-й *подходящей цепной дробью*. Цепная дробь (2) называется сходящейся, если существует конечный предел $\lim_{n \to \infty} \frac{p_n}{q_n}$. Любая бесконечная цепная дробь сходится. Для любого действительного числа α существует единственное разложение в цепную дробь (2): $\alpha = [a_0 : a_1 : \ldots : a_k : \ldots]$.

Приведем алгоритм поиска разложения действительного числа α в цепную дробь.

Если α рациональное, то, применяя алгоритм Евклида, построим разложение числа α в конечную цепную дробь. Пусть число α иррациональное. Пусть $a_0 = [\alpha]$, $\alpha = a_0 + \frac{1}{\alpha_1}$, число α_1 является положительным иррациональным, большим 1. Далее $a_1 = [\alpha_1]$, $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, $\alpha_2 > 1$ – иррациональное число, и так далее, получим $\alpha = [a_0 : a_1 : \dots : a_k : \dots]$.

Рациональное число $\frac{a}{b}$ называется *наилучшим приближением* к действительному числу α, если не существует ни одной рациональной дроби $\frac{x}{y}$, $y \le b$, которая была бы ближе к числу α, чем $\frac{a}{b}$. Известно, что при $n \ge 1$ любая подходящая дробь $\frac{p_n}{q_n}$ к действительному числу α является наилучшим приближением.

Бесконечная цепная дробь $[a_0 : a_1 : \dots : a_k : \dots]$ называется *периодической*, если последовательность чисел $a_0, a_1, \dots, a_k, \dots$ является периодической, т.е. существует числа k и s_0 такие, что $a_s = a_{s+k}$ для любых $s \ge s_0$. Если $s_0 = 0$, то цепная дробь называется *чисто периодической*. Иррациональное число α называется квадратической иррациональностью, если α является корнем некоторого квадратного уравнения $ax^2 + bx + c = 0$ с целыми коэффициентами.

Известно, что все квадратические иррациональности (и только они) разлагаются в периодическую цепную дробь.

§2. Алгебраические и трансцендентные числа.

Комплексное число α называется *алгебраическим*, если существует ненулевой многочлен $f(x) \in Q[x]$ с рациональными коэффициентами такой, что $f(\alpha) = 0$. Если $f(x)$ - многочлен наименьшей степени среди всех таких многочленов, для которых $f(\alpha) = 0$, то $f(x)$ называется *минимальным многочленом* алгебраического числа α, а степень n минимального многочлена $f(x)$ называется *степенью* алгебраического числа α. Для каждого алгебраического числа α существует единственный минимальный многочлен $f(x) \in Q[x]$ со старшим коэффициентом, равным 1. Например, степень любого рационального числа равна 1, степень числа $\sqrt{2}$ равна 2, а $f(x) = x^2 - 2$ является минимальным многочленом для $\sqrt{2}$.

Многочлен $f(x) \in Q[x]$ называется *неприводимым* над Q, если не существует многочленов $g(x)$, $h(x) \in Q[x]$, степени, меньшей чем степень $f(x)$, таких, что $f(x) = g(x)h(x)$.

Достаточное условие неприводимости многочлена над полем Q даёт следующий признак Эйзенштейна: пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ - многочлен с целыми коэффициентами положительной степени n и существует простое число p, такое, что числа $a_{n-1}, a_{n-2}, \dots, a_1$ делятся на p, число a_n не делится на p, число a_0 делится на p, но не делится на p^2, тогда многочлен $f(x)$ неприводим над полем Q.

Для любого алгебраического числа α минимальный многочлен $f(x)$ является неприводимым над Q.

Если α - корень неприводимого над Q многочлена $f(x)$ степени n, то α - алгебраическое число степени n.

Сумма $\alpha+\beta$, разность $\alpha-\beta$, произведение $\alpha\beta$, частное α/β $(\beta \neq 0)$ алгебраических чисел α, β являются алгебраическими числами.

Комплексное число α называется *трансцендентным,* если оно не является алгебраическим.

Известно, что числа π, e являются трансцендентными. Лиувилль доказал следующее достаточное условие трансцендентности числа.

Теорема Лиувилля. Пусть α - действительное число такое, что для любого натурального n и любого действительного $c>0$ существует хотя бы одна рациональная дробь $\frac{a}{b} \neq \alpha$ такая, что $\left|\alpha-\frac{a}{b}\right|<\frac{c}{b^n}$, то α - трансцендентное число.

§3. Приложения цепных дробей к решению диофантовых уравнений.

Линейное уравнение. Решение линейного уравнения $ax+by=c$, где $(a,b)|c$, задается формулой:

$x=(-1)^{k-1}q_{k-1}p_k c/a+q_k t,$

$y=(-1)^k p_{k-1}q_k c/b-p_k t,\ t\in Z,$

где $\frac{a}{b}=[a_0:a_1:\ldots:a_k]=\frac{p_k}{q_k}$, $[a_0:a_1:\ldots:a_{k-1}]=\frac{p_{k-1}}{q_{k-1}}$.

Уравнение Пелля. Пусть d - натуральное число, не являющееся точным квадратом. Уравнение $x^2-dy^2=1$ в натуральных числах называется уравнением Пелля. Для нахождения решений уравнения Пелля нужно разложить число $\sqrt{d}$ в цепную дробь: $\sqrt{d}=[a_0:(a_1:a_2:\ldots:a_s)]$. Все решения уравнения Пелля находятся по формулам:

$x_n=\frac{1}{2}\left(\left(x_0+y_0\sqrt{d}\right)^n+\left(x_0-y_0\sqrt{d}\right)^n\right),$

$y_n=\frac{1}{2\sqrt{d}}\left(\left(x_0+y_0\sqrt{d}\right)^n-\left(x_0-y_0\sqrt{d}\right)^n\right),$

где $x_0=p_{k-1}$, $y_0=q_{k-1}$, $\frac{p_{k-1}}{q_{k-1}}$ - подходящая дробь для $\sqrt{d}$, k – четное число, такое a_k является концом периода наименьшей четной длины с началом в a_1.

Задачи

1. Разложить число $17/24$ в конечную цепную дробь.

►Применяем алгоритм Евклида:

$24 = 1 \cdot 17 + 7, 17 = 2 \cdot 7 + 3, 7 = 2 \cdot 3 + 1, 3 = 3 \cdot 1$. Поэтому $\frac{17}{24} = [0:1:2:2:3]$.◄

2. Разложить в цепную дробь число $\sqrt{5}$.

►Имеем $a_0 = [\sqrt{5}] = 2$, $\alpha_1 = \frac{1}{\sqrt{5}-2} = \sqrt{5} + 2$, $a_1 = [\sqrt{5} + 2] = 4$, $\alpha_2 = \frac{1}{\sqrt{5}-2} = \alpha_1$. Поэтому $[\sqrt{5}] = [2:(4)]$.◄

3. Найти решение уравнения $17x + 24y = 1$.

►Имеем $\frac{17}{24} = [0:1:2:2:3]$, $k = 4, p_4 = 17, q_4 = 24, p_3 = 5, q_3 = 7$,

$x = (-1)^{k-1} q_{k-1} p_k c/a + q_k t = -7 + 24t$,

$y = (-1)^k p_{k-1} q_k c/b - p_k t = 5 - 17t$. ◄

4. Решить уравнение Пелля $x^2 - 5y^2 = 1$.

►Имеем $[\sqrt{5}] = [2:(4)]$, тогда $k = 2, \frac{p_1}{q_1} = [2:4] = \frac{9}{4}$. Поэтому $x_0 = 9, y_0 = 4$,

$x_n = \frac{1}{2}\left(\left(9 + 4\sqrt{5}\right)^n + \left(9 - 4\sqrt{5}\right)^n\right)$,

$y_n = \frac{1}{2\sqrt{5}}\left(\left(9 + 4\sqrt{5}\right)^n - \left(9 - 4\sqrt{5}\right)^n\right)$.◄

5. Доказать, что существуют трансцендентные числа.

►Докажем, что число $\alpha = \sum_{m=1}^{\infty} \frac{1}{10^{m!}}$ является трансцендентным. Воспользуемся теоремой Лиувилля. Возьмем произвольные натуральное n и действительное $c > 0$. Выберем натуральное k так, чтобы $10^{k!} \geq \frac{2}{c}$, $k \geq n$. Положим $a = 10^{k!} \sum_{m=1}^{k} \frac{1}{10^{m!}}$, $b = 10^{k!}$. Тогда имеем

$\left|\alpha - \frac{a}{b}\right| = \sum_{m=k+1}^{\infty} \frac{1}{10^{m!}} < \frac{1}{10^{(k+1)!}}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) = \frac{2}{10^{k!}} \cdot \frac{1}{10^{k!k}} \leq c \cdot \frac{1}{b^n}$.◄

6. Найдите минимальный многочлен для элементов $a = \sqrt[3]{5}$, $a = \sqrt{2} + \sqrt{3}$.

►1) $x^3 - 5$. Допустим, степень минимального многочлена равна 2, тогда $\sqrt[3]{5} = \alpha + \beta\sqrt{d}$, где $\alpha, \beta \in Q, d \in N, \sqrt{d} \notin N$. Имеем $5 = \alpha^3 + 3\alpha\beta^2 d + 3\alpha^2\beta\sqrt{d} + \beta^3 d\sqrt{d}$. Отсюда $3\alpha^2\beta + \beta^3 d = 0$. Следовательно, $\beta = 0$. Но тогда $\sqrt[3]{5} \in Q$. Противоречие.

2) $a^2 = 5 + 2\sqrt{6}$,

$$x^4 - 10x^2 + 1 = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}).$$

Если предположить, что $f(x)$ - минимальный многочлен для a, то $f(x) \mid x^4 - 10x^2 + 1$. Из множителей $x \pm \sqrt{2} \pm \sqrt{3}$ нельзя составить многочлен с рациональными коэффициентами степени, меньше четвертой. Поэтому $f(x) = x^4 - 10x^2 + 1$.◄

7. Докажите, что многочлен $f(x) = x^{2010} + x^{2009} + ... + x + 1$ является неприводимым над Q.

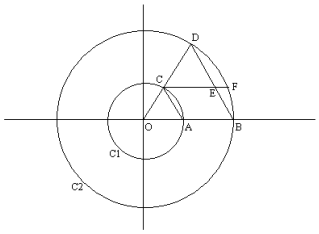
► Достаточно показать, что многочлен $g(x) = f(x+1)$ неприводим над Q. Имеем

$g(x) = \dfrac{(x+1)^{2011} - 1}{x} = x^{2010} + C_{2011}^1 x^{2009} + ... + C_{2011}^{2009} x + C_{2011}^{2010}$. Так как 2011 - простое число, то C_{2011}^k делится на 2011 для любого $k = \overline{1, 2010}$. При этом C_{2011}^{2010} не делится на 2011^2. Согласно признаку Эйзенштейна многочлен $g(x)$, а значит и многочлен $f(x)$, неприводим над Q. ◄

8. Пусть n - натуральное число, α - действительное положительное число. Докажите, что если числа α^n и $(\alpha + 1)^n$ рациональные, то число α также рациональное.

► Число α является алгебраическим и степень числа α не превосходит n. Обозначим $\alpha^n = p$, $(\alpha + 1)^n = q$. Рассмотрим многочлены $g_1(x) = x^n - p$, $g_2(x) = (x+1)^n - q$. Пусть $f(x)$ - минимальный многочлен числа α, тогда $g_1(x) \vdots f(x)$, $g_2(x) \vdots f(x)$.

Докажем, что не существует числа $\lambda \in C$, $\lambda \neq \alpha$, такого, что $g_1(\lambda) = g_2(\lambda) = 0$. Допустим, такое число λ существует. Тогда $g_1(\lambda) = 0$, $h_2(\lambda + 1) = 0$, где $h_2(x) = x^n - q$. Очевидно, $q > p, q > 1$. Рассмотрим комплексную плоскость и окружности $C_1 : |z| = \sqrt[n]{p}$, $C_2 : |z| = \sqrt[n]{q}$. Расстояние между этими окружностями равно 1, т.к. $\sqrt[n]{q} - \sqrt[n]{p} = \alpha + 1 - \alpha = 1$.



Имеем $OA = \sqrt[n]{p}, AB = 1$, пусть точке C соответствует число λ, точке F соответствует число $\lambda + 1$. Продлим OC до пересечения с окружностью C_2 в точке D, пусть CF пересекает BD в точке E. Треугольники OAC и OBD подобны, следовательно, $AC \| BD$. Кроме того, $CF \| AB$. Следовательно, $ACEB$ - параллелограмм. Значит, $CE = AB = 1$. Но тогда $CF > CE = 1$, что невозможно.

Так как $g_1(x) \vdots f(x)$, $g_2(x) \vdots f(x)$ и многочлены g_1, g_2 не могут иметь общих корней, отличных от α, то $f(x) = (x - \alpha)^k$, где $k \in N$. Поскольку $f(x) \in Q[x]$, то $\alpha \in Q$. ◄

9. Доказать, что для любых натуральных взаимно простых m, n $(m \geq 3)$ обобщённое уравнение Ферма $x^{m/n} + y^{m/n} = z^{m/n}$ не имеет решений в натуральных числах x, y, z.

►1) **Случай $m = 1$.** Уравнение имеет вид $\sqrt[n]{\frac{x}{y}} + 1 = \sqrt[n]{\frac{z}{y}}$. В силу задачи 8 числа $\sqrt[n]{\frac{x}{y}}$ и $\sqrt[n]{\frac{z}{y}}$ рациональные. Поэтому $x = ta^n$, $y = tb^n$, $z = t(a+b)^n$, где t, a, b – натуральные, $(a, b) = 1$.

2) **Случай произвольного $m \geq 3$.**

Предположим, существует решение (x, y, z). Тогда $x^m = ta^n$, $y_1 = tb^n$, $z_1 = t(a+b)^n$, где $(a, b) = 1$. Отсюда следует, что $t = q^m$. Тогда числа $x_1 = \frac{x}{q}$, $y_1 = \frac{y}{q}$, $z_1 = \frac{z}{q}$ натуральные и $x_1 = a^{n/m}$, $y_1 = b^{n/m}$, $z_1 = (a+b)^{n/m}$. Отсюда $a = p^m$, $b = q^m$, $a + b = r^m$. Поэтому $p^m + q^m = r^m$, что противоречит большой теореме Ферма. ◄

Задачи для самостоятельного решения

1. Пусть n - натуральное число, α - комплексное число, такие, что числа α^n и $(\alpha + 1)^n$ рациональные. Можно ли утверждать, что число α также рациональное?

2. Докажите, что многочлен $f(x) = x^7 - 14$ является неприводимым над Q.

3. Найдите минимальный многочлен для элемента $a = \sqrt[3]{1 - \sqrt{2}}$.

4. Найти (с обоснованием) 3 решения уравнения Пелля $x^2 - 7y^2 = 1$ с наименьшими по модулю значениями y.

5. Найти пять членов разложения в цепную дробь чисел π, e.

6. Решить в натуральных числах уравнение $x^{2/n} + y^{2/n} = z^{2/n}$.