Алгебраические и целые алгебраические числа. 15 июля

Первое действие

Определение: Комплексное число α называется **алгебраическим**, если оно является корнем многочлена с целыми коэффициентами; **целым алгебраическим**, если оно является корнем унитарного многочлена с целыми коэффициентами; **трансцендентным**, если оно не является алгебраическим. Числа e и π трансцендентны, но доказать это очень непросто.

1.1 Опишите наименьшее числовое поле, содержащее π.

1.2 Докажите, что число, являющееся одновременно рациональным и целым алгебраическим, является целым.

1.3 Докажите счетность множества алгебраических чисел и выведите отсюда бесконечность множества трансцендентных чисел.

1.4 а) **Теорема Лиувилля** Будем называть комплексное число α хорошо приближаемым, если оно не является рациональным и для любых натуральных N, n найдется такое рациональное $\frac{p}{q}$, что $|\alpha - \frac{p}{q}| < \frac{1}{Nq^n}$. Докажите, что все хорошо приближаемые числа являются трансцендентными.

б) Постройте пример хорошо приближаемого числа.

1.5 а) Пусть $p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ - многочлен с целыми коэффициентами. Докажите, что у многочлена $\prod\limits_{1 \le i < j \le n} (x - \alpha_i \alpha_j)$ все коэффициенты также целые.

б) Докажите, что сумма, разность и произведение целых алгебраических чисел также является целым алгебраическим.

в) Докажите, что алгебраические числа образуют поле.

г) Докажите, что все корни многочлена с алгебраическими коэффициентами являются алгебраическими числами, а корни всех унитарных многочленов с целыми алгебраическими коэффициентами являются целыми алгебраическими числами.

Второе действие

Определение: Будем говорить, что целые алгебраические числа α, β сравнимы по модулю натурального числа n и писать $\alpha \equiv \beta \pmod{n}$, если число $\frac{\alpha-\beta}{n}$ является целым алгебраическим.

2.1 Докажите следующие свойства таких сравнений по модулю.

1) $\alpha \equiv \beta \pmod{n}$ и $\beta \equiv \gamma \pmod{n} \Rightarrow \alpha \equiv \gamma \pmod{n}$.

2) $\alpha \equiv \beta \pmod{n} \Rightarrow p(\alpha) \equiv p(\beta) \pmod{n}$ для любого многочлена $p(x)$ с целыми алгебраическими коэффициентами.

3) Если α и β - целые числа, то сравнимость по модулю n в определенном выше смысле эквивалентна обычной сравнимости по модулю n.

2.2 Пусть $\zeta = \cos(\frac{2\pi}{8}) + i\sin(\frac{2\pi}{8})$.

а) Покажите, что ζ является целым алгебраическим числом.

б) Докажите, что для любого нечетного простого p выполнена цепочка сравнений (по модулю p) и равенств $\zeta^p + \zeta^{-p} \equiv (\zeta + \zeta^{-1})^p = 2^{\frac{p-1}{2}}(\zeta + \zeta^{-1}) \equiv (\frac{2}{p})(\zeta + \zeta^{-1})$.

в) Докажите, что $(\frac{2}{p}) = 1$, если $p \equiv \pm 1 \pmod{8}$, и $(\frac{2}{p}) = -1$, если $p \equiv \pm 3 \pmod{8}$.

2.3 Рассмотрим последовательность $\{a_n\}$, заданную начальными условиями $a_0 = 3, a_1 = 0, a_2 = 2$ и соотношениями $a_n = a_{n-2} + a_{n-3}$.

а) Пусть α, β, γ - корни многочлена $x^3 - x - 1$. Докажите, что $a_n = \alpha^n + \beta^n + \gamma^n$.

б) Докажите, что a_p делится на p для любого простого p, используя сравнимость целых алгебраических чисел по модулю p.

в) Докажите тот же результат с помощью комбинаторной интерпретациии: a_n есть количество способов разрезать клетчатое кольцо из n клеток на доминошки и триминошки.

Квадратичный закон взаимности Для различных нечетных простых p и q выполнено $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

2.4 Пусть $\zeta = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p})$. Для $1 \leq a \leq p-1$ обозначим $g_a = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{ak}$. Числа g_a называются **квадратичными суммами Гаусса.**

а) Докажите, что числа g_a являются целыми алгебраическими.

б) Докажите, что $g_a = (\frac{a}{p})g_1$.

в) Докажите, что $g_1^2 = (-1)^{\frac{p-1}{2}}p$. (*Подсказка:* рассмотрите выражение $\sum_{a=1}^{p-1} g_a g_{-a}$ и докажите, что оно одновременно равно и $(\frac{-1}{p})(p-1)g_1^2$, и $p(p-1)$)

г) Докажите цепочку сравнений (по модулю q) и равенств

$$\left(\frac{q}{p}\right) g_1 = g_q \equiv g_1^q = ((-1)^{\frac{p-1}{2}}p)^{\frac{q-1}{2}} g_1 \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) g_1.$$

д) Выведите квадратичный закон взаимности.