Листок №3

Кац Лев

30 октября 2020 г.

A3 ♢ 1

Пусть $g \in \mathbb{Q}[x]$. Тогда нам подходят:

1. $g \cdot (1+x^2) + (1+x)$
2. $g \cdot (1+x^4) + (1+x^3)$
3. $g \cdot (1+x^8) + (1+x^5)$

A3 ♢ 3

1.

Рассмотрим $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ – мультипликативную подгруппу. Это конечная, а значит циклическая подгруппа (ζ – порождающий). Построим функцию $[x=n]$ – индикатор того, что $i = n$:

$$[x=n] = 1 - (x-n)^{\operatorname{ord}\zeta},$$

он равен 1, если $x - n$ и 0 иначе. Тогда:

$$f(x) = \sum_{q \in \mathbb{F}} f(q)\,[x=q]\,,$$

это многочлен.

2.

Пусть $f,\ g \in \mathbb{F}$ такие, что $\forall x \in \mathbb{F}\; f(x) = g(x)$. Рассмотрим многочлен $f - g$. Он равен нулю в каждой точке, то есть у него $|\mathbb{F}|$ корней. У нас степень многочленов (в 1) не превосходит $\operatorname{ord}\zeta = |\mathbb{F}| - 1$, а тогда $f - g = 0$.

A3 ♢ 4

От противного: пусть их конечный набор $f_1, \ldots, f_n$. Рассмотрим многочлен $g \equiv \prod_{k=1}^{n} f_k + 1$. Он дает остаток 1 при делении на f_k – любой неприводимый многочлен. Однако g можно разложить в произведение неприводимых многочленов, противоречие.

А3 ♢ 5

Перечислим их (для $2 \le \deg f \le 3$ достаточно подбирать те, у которых просто нет корней. Иначе нужно проверять делимость на неприводимые меньшей степени).

а)

Понятно, что свободный коэффициент при степени больше 1 будет равен 1, а количество членов нечетным.

- x, $x+1$;
- x^2+x+1;
- x^3+x^2+1, x^3+x+1;
- x^4+x^3+1, $\cancel{x^4+x^2+1=(x^2+x+1)^2}$, x^2+x+1, $x^4+x^3+x^2+x+1$;
- $\cancel{x^5+x^4+1=(x^2+x+1)(x^3+x+1)}$, x^5+x^3+1, x^5+x^2+1, $\cancel{x^5+x+1=(x^2+x+1)(x^3+x^2+1)}$, $x^5+x^4+x^3+x^2+1$, $x^5+x^4+x^3+x+1$, $x^5+x^4+x^2+x+1$, $x^5+x^3+x^2+x+1$.

б)

- x^2+1, $2x^2+2$
- x^2+x+2, $2x^2+2x+1$
- x^2+2x+2, $2x^2+x+1$

г)

Можем просто возвести элементы в квадрат:

- $\{0,1\}$
- $\{0,1,4\}$
- $\{0,1,4,7\}$
- $\{0,1,4,9\}$

Лемма (я буду ее использовать в задачах):

$f \in \mathbb{Z}[x]$ имеет корень $p/q: \ \gcd(p,q)=1 \iff$ старший коэффициент делится на q, свободный – на p

Доказательство

$$\begin{aligned}
0 &= a_0\left(\frac{p}{q}\right)^n + \ldots + a_{n-1}\left(\frac{p}{q}\right)^1 + a_n \Big/ \cdot q^n \\
-a_0 &= q\left(a_1 p^n + \ldots + a_n q^{n-1}\right) \\
-a_n q^n &= p\left(a_0 p^{n-1} + \ldots + a_{n-1} q^{n-1}\right)
\end{aligned}$$

A3 $\diamondsuit$ 6

Будем использовать теорему о том, что для произвольного поля $\mathbb{K}$ $\mathbb{K}[x]/(f)$ – поле $\iff f$ – неприводим в $\mathbb{K}$.

а)

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

б)

f является неприводимым. Иначе разложение выше на неприводимые было бы не единственным в $\mathbb{R}[x]$.
Найдем обратный. Заметим, что $x^4+1=(x+1)(x^3-x^2+x-1)+2$, то есть $[0]_f=[x+1]_f\cdot\left[x^3-x^2+x-1\right]_f+[2]_f$. А тогда:

$$[1]_f=[x+1]_f\cdot\left(\left[x^3-x^2+x-1\right]_f\cdot[0.5]_f\right)$$

в)

f является неприводимым, поскольку у него нет рациональных корней. Заметим, что $x^3+x+1=(x+1)(x^2-x+2)-1$ – ура, сразу нашли обратный.

A3 $\diamondsuit$ 7

а)

Наш многочлен может быть представлен в виде произведения многочленов со степенями 2 и 2, либо 3 и 1 (невозможно, так как нет рациональных корней). Попробуем первый случай.

$$\begin{aligned}
(a_0x^2+a_1x+a_2)(x^2+b_1x+b_2) = a_0x^4+(a_0b_1+a_1)x^3+(a_0+1+a_1b_1)x^2+ \\
+(b_1a_2+a_1b_2)x+a_2b_2= \\
=x^4-8x^3+12x^2-6x+2,
\end{aligned}$$

получаем 5 уравнений, у которых нет рациональных решений, потому неприводим.

б)

A3 ◊ 9

а)

Пусть b обратим:

$$\nu(a) \le \nu(ab) \le \nu(abb^{-1}) = \nu(a) \Longrightarrow \nu(a) = \nu(ab)$$

Пусть b не обратим. Тогда $\exists\ p, r \in A : a = p(ab) + r,\ \nu(r) < \nu(ab)$. Тогда $a(1 - pb) = r$, тогда $\nu(a) \le \nu(a(1 - pb)) = \nu(r) < \nu(ab) = \nu(a)$, противоречие.

б)

Рассмотрим $\{ax + by : \ x, y \in A\}$. В нем есть элемент $M \ne 0$ с наименьшей нормой (потому что это целые числа). Очевидно, он делится на любой общий делитель, при этом $\exists\, p, r \in A : a = pM + r,\ \nu(r) < M$. Если $r \ne 0$, то он будет одновременно лежать в множестве и противоречить выбору M, поэтому он 0. Аналогично M делится на b. Почему наибольшая норма? Пусть есть общий делитель с большей нормой. Тогда M делится на него и значит имеет норму не меньше, противоречие.

в)

Очевидно, на каждом шаге норма уменьшается, а потому шагов может быть только конечное число. Также из второго свойства понятно, почему в конце $r_{n+1} = 0$ (в противном случае можно будет построить следующий элемент с меньшей нормой). Почему r_n – наибольший общий делитель? Заметим, что $\gcd(r_k, r_{k+1}) = \gcd(r_{k+1}, r_{k+2})$, поскольку обе пары имеют одинаковый набор общих делителей (по построению). Также заметим, что $\gcd(r_n, 0) = r_n = \gcd(a, b)$.

A3 ◊ 10

В качестве нормы возьмем целую часть от квадрата модуля комплексного числа, т.е $\nu(a) = \lfloor x\overline{x} \rfloor$. Для такой нормы очевидно выполнено первое свойство (в обоих пунктах):

$$\nu(ab) \ge \lfloor a\overline{a} \rfloor \cdot \lfloor b\overline{b} \rfloor \ge \lfloor a\overline{a} \rfloor = \nu(a)$$

Докажем второе свойство методом относительно долгого вглядывания в Рис 1. Конечно же, конкретные числа там подписаны только для наглядности, а важно там то, что a оказывается в одном из квадратов или треугольников (или на стороне, что неважно).

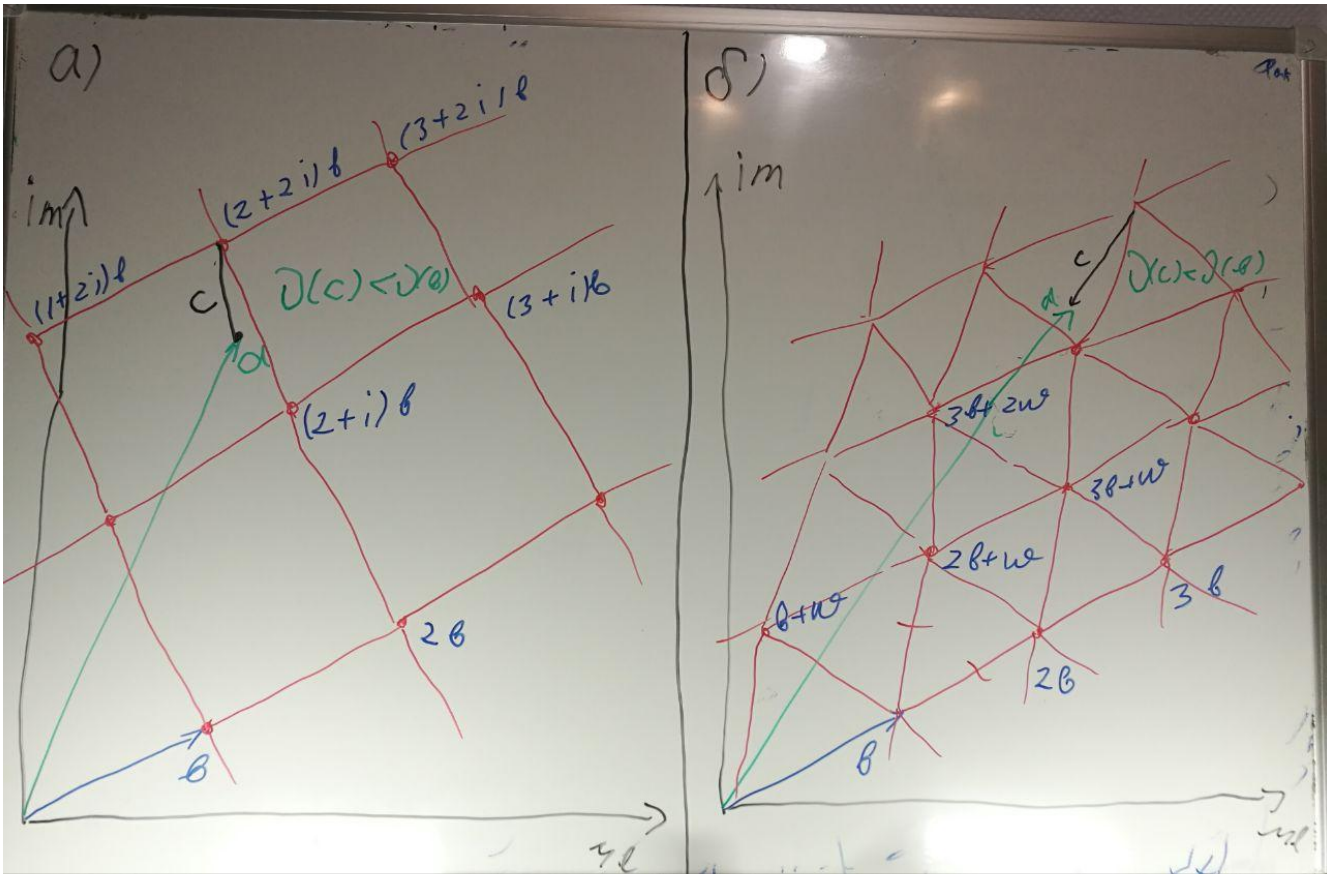

Рис. 1 : А3 ◊ 10, доказательство свойства 2

А3 ◊ 11

Возьмем элемент $M \in I \backslash \{0\}$ с наименьшей нормой. Заметим, что $\forall b \in I \backslash \{0\} b = qM + r$, где $r = 0$, так как иначе в I будет элемент с нормой $\nu(M)$. Заметим также, что кратные M элементы содержатся в I, а тогда идеал главный.

А3 ◊ 12

$x, y \in \mathbb{Q}[x, y]$. Идеал, порожденный ими не может быть порожден одним элементом, тогда не является кольцом главных идеалов.
Аналогично $x, 3 \in \mathbb{Z}[x]$.

А3 ◊ 14

а)

$$\begin{aligned}
z &= (1+i)^5/(1-i)^3, \\
|z| &= \sqrt{2}^5/\sqrt{2}^3 = 2, \\
\operatorname{Arg} z &= \frac{5\pi}{4} - \frac{3\pi}{4} + 2\pi k = \frac{\pi}{2} + 2\pi k, \\
\operatorname{Im}(z) &= 2, \\
\operatorname{Re}(z) &= 0.
\end{aligned}$$

б)

$$\begin{aligned}
z &= \left((\sqrt{3}+i)/(1-i)\right)^{30}, \\
|z| &= (2/\sqrt{2})^{30} = 2^{15}, \\
\operatorname{Arg} z &= \frac{\pi}{6}\cdot 30 + 2\pi k = \pi + 2\pi k \\
\operatorname{Im}(z) &= 0, \\
\operatorname{Re}(z) &= -2^{15}.
\end{aligned}$$

в)

$$\begin{aligned}
z &= a + ib, \\
|z| &= \sqrt{a^2+b^2}, \\
\operatorname{Arg} z &= \arcsin\left(b/\sqrt{a^2+b^2}\right), a \geq 0 \,\mathrm{else}\, \pi - \arcsin\left(b/\sqrt{a^2+b^2}\right), \\
\operatorname{Im}(z) &= b, \\
\operatorname{Re}(z) &= a.
\end{aligned}$$

A3 ♢ 15

$$\begin{aligned}
\sin 5\varphi = \operatorname{Im}\left((\cos\varphi + i\sin\varphi)^5\right) = \operatorname{Im}\big(\cos^5\varphi + i\sin^5\varphi + 5i\cos^4\varphi\sin\varphi + \\
+5\sin^4\varphi\cos\varphi - 10\sin^2\varphi\cos^3\varphi - 10i\sin^3\varphi\cos^2\varphi\big) = \\
= \sin^5\varphi + 5\cos^4\varphi\sin\varphi - 10\sin^3\varphi\cos^2\varphi = \\
= 16\sin^5\varphi - 20\sin^3\varphi + 5\sin\varphi
\end{aligned}$$

Подставим $\varphi = \frac{4\pi}{5}$ и обозначая за x:

$$0 = x(16x^4 - 20x^2 + 5)$$

Сделав замену $y = (4x^2 - 2.5)^2$ находим решение:

$$x = 0,\ x = \pm\frac{1}{2}\sqrt{\frac{5}{2} \pm \frac{\sqrt{5}}{2}}$$

В нашем случае $1 > \sin\varphi > 0$, потому:

$$\sin\frac{4\pi}{5} = \frac{1}{2}\sqrt{\frac{5}{2} - \frac{\sqrt{5}}{2}}$$

Заметим, что $\cos\frac{2\pi}{5} = \sin\frac{\pi}{10}$. Просто в лоб подставить кажется сложным, поэтому попробуем выразить из $\sin\frac{\pi}{5}$, используя соотношение для косинуса двойного угла и тот факт, что $\sin\frac{\pi}{5} = \sin\frac{4\pi}{5}$:

$$\cos\frac{2\pi}{5} = 1 - 2\sin^2\frac{\pi}{5} = 1 - \left(\frac{5}{2} - \frac{\sqrt{5}}{2}\right) = \frac{\sqrt{5}-1}{2}$$

A3 ♢ 16

Это циклическая группа, порожденная ζ.

$$\sum_{i=0}^{n-1}(\zeta^i)^s = \frac{\zeta^{ns}-1}{\zeta-1} = 0$$
$$\prod_{i=0}^{n-1}(\zeta^i)^s = \zeta^{s\sum_{i=1}^{n-1}} = \zeta^{1/2(n-1)ns} = 1$$

A3 ♢ 17

Заметим, что:

$$(1+i)^n = \sqrt{2}^n\left(\cos\left(\frac{\pi n}{4}\right) + i\sin\left(\frac{\pi n}{4}\right)\right) = \sum_{k=0}^{n}\binom{n}{k}i^k$$

Также заметим свойство биномиальных коэффициентов:

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + ... = \binom{n}{1} + \binom{n}{3} + ... = 2^{n-1}$$

Тогда:

$$\frac{\mathrm{Re}\left((1+i)^n\right) + 2^{n-1}}{2} = \frac{\sqrt{2}^n\cos\left(\frac{\pi n}{4}\right) + 2^{n-1}}{2} = \binom{n}{0} + \binom{n}{4} + \binom{n}{8} + ...$$
$$\frac{\mathrm{Im}\left((1+i)^n\right) + 2^{n-1}}{2} = \frac{\sqrt{2}^n\sin\left(\frac{\pi n}{4}\right) + 2^{n-1}}{2} = \binom{n}{1} + \binom{n}{5} + \binom{n}{9} + ...$$

Это немного контринтуитивно для меня, но как и ожидалось, числа получаются целыми положительными для любых n.