Токмаков Александр, ФКН, группа БПМИ165

Домашнее задание 4

№1

$$2^{2017} + 3^{2017} \mod 10$$

Посмотрим, какие остатки от деления на 10 дают степени 2 и 3:

$$2^1 \mod 10 = 2 \qquad 3^1 \mod 10 = 3$$
$$2^2 \mod 10 = 4 \qquad 3^2 \mod 10 = 9$$
$$2^3 \mod 10 = 8 \qquad 3^3 \mod 10 = 7$$
$$2^4 \mod 10 = 6 \qquad 3^4 \mod 10 = 1$$
$$2^5 \mod 10 = 2$$

Таким образом, $2^{(5^n)} \equiv 2^{(5^{n-1})} \equiv ... \equiv 2 \mod 10$ и $3^{4k} \equiv \left(3^4\right)^k \equiv 1^k \equiv 1 \mod 10$.

$$2^{2017} + 3^{2017} \equiv 2^{625 \cdot 3 + 142} + 3^{4 \cdot 504 + 1} \equiv \left(2^{(5^4)}\right)^3 \cdot 2^{142} + 3^{4 \cdot 504} \cdot 3 \equiv 2^3 \cdot 2^{142} + 1 \cdot 3 \equiv$$
$$\equiv 2^{145} + 3 \equiv 2^{(5^3)+20} + 3 \equiv 2^{21} + 3 \equiv \left(2^5\right)^4 \cdot 2 + 3 \equiv 2^5 + 3 \equiv 2 + 3 \equiv 5 \mod 10$$

Последняя цифра этого числа 5.

№2

Разложить $p(x) = x^4 + 4$ над $\mathbb{Q}$

Найдём комплексные корни многочлена $p(x)$:

$$x^4 + 4 = 0 \quad \Leftrightarrow \quad x^4 = -4 = 4\left(\cos(\pi) + i\sin(\pi)\right)$$
$$x \in M = \left\{ \sqrt[4]{4\left(\cos\pi\right) + i\sin(\pi))} \right\} = \left\{ \sqrt{2}\left(\cos\left(\frac{\pi}{4} + \frac{\pi n}{2}\right) + i\sin\left(\frac{\pi}{4} + \frac{\pi n}{2}\right)\right) \ \mid n \in \{0, 1, 2, 3\} \right\}$$

Многочлен раскладывается над $\mathbb{C}$:

$$p(x) = \prod_{x_n \in M} (x - x_n)$$

Теперь, если перемножить скобки с сопряжёнными корнями, должно получиться разложение над $\mathbb{Q}$ (вообще-то, над $\mathbb{R}$, но здесь коэффициенты окажутся рациональными):

$$n = 0 \text{ и } n = 3: \quad \left(x - \sqrt{2}\left(\cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)\right)\right) \cdot \left(x - \sqrt{2}\left(\cos\left(\frac{\pi}{4} + \frac{3\pi}{2}\right) + i\sin\left(\frac{\pi}{4} + \frac{3\pi}{2}\right)\right)\right) =$$
$$= \left(x - \sqrt{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)\right) \cdot \left(x - \sqrt{2}\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\right) = (x - (1+i)) \cdot (x - (1-i)) = x^2 - 2x + 2$$
$$n = 1 \text{ и } n = 2: \quad \left(x - \sqrt{2}\left(\cos\left(\frac{\pi}{4} + \frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{4} + \frac{\pi}{2}\right)\right)\right) \cdot \left(x - \sqrt{2}\left(\cos\left(\frac{\pi}{4} + \pi\right) + i\sin\left(\frac{\pi}{4} + \pi\right)\right)\right) =$$
$$= \left(x - \sqrt{2}\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)\right) \cdot \left(x - \sqrt{2}\left(-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\right) = (x - (-1+i)) \cdot (x - (-1-i)) = x^2 + 2x + 2$$

Действительно, получилось разложение $p(x)$ на неприводимые многочлены над $\mathbb{Q}$:

$$p(x) = (x^2 - 2x + 2)(x^2 + 2x + 2)$$

Эти многочлены неприводимы, потому что могут раскладываться только на линейные множители, а корни у них комплексные.

№3

$$\forall a \in F \quad a \cdot 0 = 0$$

Воспользуемся следующими аксиомами поля:

1 Коммутативность сложения:	$\forall a, b \in F \quad a + b = b + a$
2 Существование нейтрального по сложению:	$\exists 0 \in F \mid \forall a \in F \quad a + 0 = a$
3 Существование обратного по сложению:	$\forall a \in F \quad \exists(-a) \in F \mid a + (-a) = 0$
4 Существование нейтрального по умножению:	$\exists e \in F \mid \forall a \in F \quad a \cdot e = a$
5 Дистрибутивность сложения относительно умножения:	$\forall a, b, c \in F \quad \cdot a(b + c) = ab + ac$
6 Ассоциативность сложения:	$\forall a, b, c \in F \quad (a + b) + c = a + (b + c)$

Легко видеть, что (цифры возле знака = соответствуют аксиомам из списка выше):

$$0 =_3 a + (-a) =_4 a \cdot e + (-a) =_2 a \cdot (e + 0) + (-a) =_1 a \cdot (0 + e) + (-a) =_5 (a \cdot 0 + a \cdot e) + (-a) =_6$$
$$=_6 a \cdot 0 + (a \cdot e + (-a)) =_4 a \cdot 0 + (a + (-a)) =_3 a \cdot 0 + 0 =_2 a \cdot 0$$

№4

Заметим, что если многочлен второй степени не имеет корней, то он неприводим. Действительно, если многочлен второй степени приводим, то он раскладывается на линейные множители $p(x) = (x-a)(a-b)$, и тогда a и b - его корни. Также заметим, что если многочлен $p(x)$ неприводим, то многочлен $a \cdot p(x), a \neq 0$ тоже неприводим, поэтому можно рассматривать только многочлены со старшим коэффициентом 1 (остальные неприводимые получатся домножением на все ненулевые элементы поля). Переберём такие многочлены степени 2 из $\mathbb{Z}_3[x]$ (их $1 \cdot 3 \cdot 3 = 9$ штук) и попробуем найти их корни:

$$\begin{aligned}
p(x) &= x^2 + 0x + 0, \quad p(0) = 0^2 + 0 \cdot 0 + 0 = 0 \\
p(x) &= x^2 + 0x + 2, \quad p(1) = 1^2 + 0 \cdot 1 + 2 = 0 \\
p(x) &= x^2 + 1x + 0, \quad p(0) = 0^2 + 1 \cdot 0 + 0 = 0 \\
p(x) &= x^2 + 1x + 1, \quad p(1) = 1^2 + 1 \cdot 1 + 1 = 0 \\
p(x) &= x^2 + 2x + 0, \quad p(0) = 0^2 + 2 \cdot 0 + 0 = 0 \\
p(x) &= x^2 + 2x + 1, \quad p(2) = 2^2 + 2 \cdot 2 + 1 = 0
\end{aligned}$$

У шести многочленов нашлись корни, значит осталось 3 неприводимых. Покажем, что у них нет корней:

$$\begin{aligned}
p(x) &= x^2 + 0x + 1, \quad p(0) = 0^2 + 0 \cdot 0 + 1 = 1, \quad p(1) = 1^2 + 0 \cdot 1 + 1 = 2, \quad p(2) = 2^2 + 0 \cdot 2 + 1 = 2 \\
p(x) &= x^2 + 1x + 2, \quad p(0) = 0^2 + 1 \cdot 0 + 2 = 2, \quad p(1) = 1^2 + 1 \cdot 1 + 2 = 1, \quad p(2) = 2^2 + 1 \cdot 2 + 2 = 2 \\
p(x) &= x^2 + 2x + 2, \quad p(0) = 0^2 + 2 \cdot 0 + 2 = 2, \quad p(1) = 1^2 + 2 \cdot 1 + 2 = 2, \quad p(2) = 2^2 + 2 \cdot 2 + 2 = 1
\end{aligned}$$

Таким образом, в $\mathbb{Z}_3[x]$ есть ровно 6 неприводимых многочленов степени 2:

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2, \quad 2x^2 + 2, \quad 2x^2 + 2x + 1, \quad 2x^2 + x + 1$$

№5

$$\nexists x, y \in \mathbb{Z} \mid 15x^2 - 7y^2 = 9$$

Пусть решения существуют. Попробуем их найти:

$$15x^2 = 9 + 7y^2, \quad x, y \in \mathbb{Z} \quad \Rightarrow \quad x^2 = \tfrac{9+7y^2}{15} \in \mathbb{Z} \quad \Rightarrow \quad 9 + 7y^2 = 15a, \quad a \in \mathbb{Z}$$
$$9 + 7y^2 = 15a, \quad x, y \in \mathbb{Z} \quad \Rightarrow \quad y^2 = \tfrac{15a-9}{7} = 2a + 1 + \tfrac{a-2}{7} \in \mathbb{Z} \quad \Rightarrow \quad a - 2 = 7b, \quad b \in \mathbb{Z} \quad \Rightarrow \quad a = 7b + 2, \quad b \in \mathbb{Z}$$
$$\Rightarrow \quad y^2 = \tfrac{15(7b+2)-9}{7} = 15b + 3, \quad b \in \mathbb{Z} \quad \Rightarrow \quad y^2 \equiv 3 \mod 15$$

Но такого не бывает:

$$y \equiv 0 \mod 15 \quad \Rightarrow \quad y^2 \equiv 0 \mod 15$$
$$y \equiv 1 \mod 15 \quad \Rightarrow \quad y^2 \equiv 1 \mod 15$$

$$
\begin{aligned}
y \equiv 2 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 4 \mod 15 \\
y \equiv 3 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 9 \mod 15 \\
y \equiv 4 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 1 \mod 15 \\
y \equiv 5 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 10 \mod 15 \\
y \equiv 6 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 6 \mod 15 \\
y \equiv 7 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 4 \mod 15 \\
y \equiv 8 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 4 \mod 15 \\
y \equiv 9 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 6 \mod 15 \\
y \equiv 10 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 10 \mod 15 \\
y \equiv 11 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 1 \mod 15 \\
y \equiv 12 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 9 \mod 15 \\
y \equiv 13 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 4 \mod 15 \\
y \equiv 14 \mod 15 \quad &\Rightarrow \quad y^2 \equiv 1 \mod 15
\end{aligned}
$$

Значит, у уравнения $15x^2 - 7y^2 = 9$ нет решений в целых числах.