Дополнительные задачи про вычеты.

A5$\frac{1}{2}\diamond$1. Покажите, что в разложении числа $n \in \mathbb{N}$ на простые множители в $\mathbb{Z}[i]$ вместе с каждым невещественным множителем z содержится (в той же степени, что и z) и сопряжённый к нему множитель $\overline{z}$.

A5$\frac{1}{2}\diamond$2. Как соотносятся друг с другом следующие свойства простого числа $p\in\mathbb{N}$:

а) p перестаёт быть простым в $\mathbb{Z}[i]$; **б)** -1 является квадратом в $\mathbb{Z}/p\mathbb{Z}$;

в) p является суммой двух квадратов натуральных чисел; **г)** $p \not\equiv -1 (\mathrm{mod}\, 4)$.

A5$\frac{1}{2}\diamond$3 (разложение в сумму двух квадратов). Докажите, что $n \in \mathbb{N}$ тогда и только тогда не является ни квадратом, ни суммой двух квадратов, когда его разложение на простые множители (в $\mathbb{Z}$) содержит нечётную степень простого числа, сравнимого с 3 по модулю 4.

A5$\frac{1}{2}\diamond$4 (символ Лежандра – Якоби). Для простого $p \in \mathbb{N}$ и любого $n\in\mathbb{Z}$ положим

$$\left(\frac{n}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 0\,, \text{ если } n \equiv 0 (\mathrm{mod}\, p)\,, \\ 1\,, \text{ если } n (\mathrm{mod}\, p) \text{ ненулевой квадрат в } \mathbb{F}_p\,, \\ -1\,, \text{ если } n (\mathrm{mod}\, p) \text{ не квадрат в } \mathbb{F}_p\,. \end{cases}$$

а) Является ли $\left(\frac{n}{p}\right)$ при фиксированном p мультипликативным характером числа n?

б) Найдите $\left(\frac{-1}{p}\right)$ и $\left(\frac{2}{p}\right)$. **в)** Вычислите $\sum\limits_{n=1}^{p-1}\left(\frac{n}{p}\right)$. **г)** Сравните $\left(\frac{m}{p}\right)$ и знак $\prod\limits_{j=1}^{\frac{p-1}{2}} \frac{\sin\left(\frac{2\pi m}{p}\cdot j\right)}{\sin\left(\frac{2\pi}{p}\cdot j\right)}$.

д) Сравните $\left(\frac{m}{p}\right)$ и знак перестановки чисел поля $\mathbb{F}_p$, задаваемой умножением их на m.

A5$\frac{1}{2}\diamond$5 (квадратичный закон взаимности). Разложив все отношения синусов из зад. A6$\frac{2}{3}\diamond$4 г) по формулам из зад. A4 $\diamond$ 4, докажите соотношение

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad \text{для любых простых } p, q \in \mathbb{N}\,.$$

A5$\frac{1}{2}\diamond$6. Найдите $\left(\frac{43}{109}\right)$.

Первообразные корни в кольце вычетов. Пусть a — обратимый элемент кольца $\mathbb{Z}/(n)$. Назовём *порядком* вычета a наименьшее натуральное число k такое, что $a^k = 1$. Элемент a называется *первообразным корнем по модулю* n, если все прочие обратимые вычеты являются его степенями.

A5$\frac{1}{2}\diamond$7. Пусть порядки $k_1, k_2, \ldots, k_n$ вычетов $a_1, a_2, \ldots, a_n$ попарно взаимно просты. Чему равен порядок вычета $a = a_1 a_2 \cdots a_n$?

A5$\frac{1}{2}\diamond$8. Пусть вычеты порядков k и ℓ существуют. Существует ли вычет порядка $\mathrm{нок}(k, \ell)$?

A5$\frac{1}{2}\diamond$9. Докажите, что для существования первообразного корня необходимо и достаточно существование обратимого вычета порядка $\varphi(n)$. По любому ли простому модулю существует первообразный корень?

A5$\frac{1}{2}\diamond$10*. Пусть ϱ — первообразный корень по простому модулю $p > 2$. Докажите, что существует $\vartheta \in \mathbb{N}$, такое что $(\varrho + p\vartheta)^{p-1} \equiv 1 (\mathrm{mod}\, p)$, но $(\varrho + p\vartheta)^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$. Является ли класс $\varrho + p\vartheta$ первообразным корнем $(\mathrm{mod}\, p^k)$ для всех $k\in\mathbb{N}$?

A5$\frac{1}{2}\diamond$11*. Докажите существование первообразного корня $(\mathrm{mod}\, 2p^k)$ $\forall\, k\in\mathbb{N}$ и простого p.

A5$\frac{1}{2}\diamond$12. Существует ли первообразный корень по модулю 21?