Кольца и поля вычетов.

A5◇1. Составьте таблицы умножения для колец **а)** $\mathbb{Z}/(4)$ **б)** $\mathbb{Z}/(5)$ **в)** $\mathbb{Z}/(6)$ **г)** $\mathbb{Z}/(7)$ **д)** $\mathbb{Z}/(8)$ **е)** $\mathbb{Z}/(9)$ **ж)** $\mathbb{Z}/(10)$ **з)** $\mathbb{Z}/(11)$ **и)** $\mathbb{Z}/(13)$. В каждом из этих колец найдите: все обратимые элементы, все делители нуля, все нильпотенты, все квадраты и все кубы. Для обратимых элементов постройте таблицу обратных.

A5◇2. Равносильны ли друг другу следующие свойства числа $a \in \mathbb{Z}/(n)$:
а) a обратим; **б)** отображение умножения на a: $\mathbb{Z}/n\mathbb{Z} \xrightarrow{x \mapsto ax} \mathbb{Z}/n\mathbb{Z}$ взаимно однозначно; **в)** $ax = 0 \Rightarrow x = 0$; **г)** $ax = ay \Rightarrow x = y$; **д)** $\forall y\ \exists x\ :\ ax = y$; **е)** $\text{НОД}(a, n) = 1$.

A5◇3. Делится ли **а)** $2222^{5555} + 5555^{2222}$ на 7? **б)** $2^{70} + 3^{70}$ на 13?

A5◇4. Найдите остаток от деления $2007^{2008^{2009}}$ на 11.

A5◇5. Верно ли, что: **а)** $a^2 + b^2 \vdots 7 \Rightarrow a \vdots 7$ и $b \vdots 7$? **б*)** $a^3 + b^3 + c^3 \vdots 7 \Rightarrow abc \vdots 7$? **в*)** $a^2 + b^2 + c^2 + d^2 + e^2 \vdots 9 \Rightarrow abcde \vdots 9$?

A5◇6. Имеет ли уравнение $x^2 + y^2 + z^2 = 2xyz$ ненулевые решения в целых числах?

A5◇7 (позиционные признаки делимости). Вычислите остатки всех степеней десятки от деления на 2, 5, 4, 3, 9, 11, 7, 13 и скажите, как, проделав как можно более простые манипуляции над цифрами десятичной записи данного натурального числа, узнать его остаток от деления на 2, 5, 4, 3, 9, 11, 7, 13.

A5◇8 (функция Эйлера). Обозначим через $\varphi(n)$ число обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$.
а) Покажите, что $\varphi(n)$ является *мультипликативным характером*[1]
б) Покажите, что для $n = p_1^{k_1} \cdots p_n^{k_n}$ (где все p_i просты и различны)
$$\varphi(m) = \varphi\left(p_1^{k_1}\right) \varphi\left(p_2^{k_2}\right) \cdots \varphi\left(p_n^{k_n}\right) = m \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right).$$
в) Найдите все m такие, что $\varphi(m) = 10$.
г) (теорема Эйлера) Вычислите $a^{\varphi(m)}$ для произвольного обратимого $a \in \mathbb{Z}/n\mathbb{Z}$.

A5◇9 (поле $\mathbb{F}_p$). Обозначим через $\mathbb{F}_p$ кольцо вычетов $\mathbb{Z}/(p)$ по простому модулю $p \in \mathbb{N}$.
а) Покажите, что $\mathbb{F}_p$ — поле.
б) Решите в $\mathbb{F}_p$ уравнение $x^2 = 1$.
в) Вычислите произведение всех ненулевых элементов поля $\mathbb{F}_p$.
г) (теорема Вильсона) Равносильна ли простота натурального $p \geqslant 2$ тому, что $(p-1)!+1$ делится на p?
д) Является ли мультипликативная группа ненулевых элементов $\mathbb{F}_p$ циклической?
е) (малая теорема Ферма) Какие значения принимают многочлены $x^p - x$, x^{p-1} и $x^{\frac{p-1}{2}}$ на $\mathbb{F}_p$ и на квадратах из $\mathbb{F}_p$?
ж) Сколько в $\mathbb{F}_p$ ненулевых квадратов?
з) Всегда ли в $\mathbb{F}_p$ разрешимо уравнение $x^2 + y^2 = -1$?
и*) (лемма Гаусса) Выпишем $\mathbb{F}_p$ в виде: $-(p-1)/2$, ..., -1, 0, 1, ..., $(p-1)/2$. Докажите, что $a \in \mathbb{F}_p$ тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» от умножения на a, чётно.

A5◇10*. При каких p в $\mathbb{F}_p$ разрешимы уравнения[2] **а)** $x^2 = -1$ **б)** $x^2 = 2$

A5◇11*. При каких p существует ненулевой гомоморфизм $\mathbb{Z}[\sqrt{-1}] \longrightarrow \mathbb{F}_p$? Всегда ли такой гомоморфизм сюръективен и каково его ядро?

---

[1] функция $\mathbb{Z} \xrightarrow{f} \mathbb{C}$ называется *мультипликативным характером*, если $f(mn) = f(m)f(n)$ для любых взаимно простых m и n

[2] ОТВЕТЫ: а) $p = 2$ и $p \equiv 1 \pmod 4$; б) — когда $(p^2-1)/8$ чётно