Сравнения и вычеты.

А2-1. Докажите, что уравнение $15x^2 - 7y^2 = 9$ не имеет решений в целых числах.

А2-2. Докажите, что уравнения $x^2 + y^2 + z^2 = 2xyz$ и $5x^3 + 11y^3 + 13z^3 = 0$ не имеют целочисленных решений, кроме $x = y = z = 0$.

Кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$ состоит, по определению, из n остатков $0, 1, \dots, (n-1)$ от деления на n. Элементы кольца вычетов можно складывать и умножать — результатами этих опреаций , по определению, считаются остаток от суммы и остаток от произведения остатков-операндов.

А2-3°. Проверьте, что $\mathbb{Z}/n\mathbb{Z}$ удовлетворяет аксиомам коммутативного кольца с единицей.

А2-4. Составьте таблицы умножения для колец $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ и $\mathbb{Z}/8\mathbb{Z}$. В каждом из этих колец найдите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты.

А2-5°. Проверьте, что отображение $\mathbb{Z} \xrightarrow{\mathrm{res}_n} \mathbb{Z}/n\mathbb{Z}$, переводящее число $m \in \mathbb{Z}$ в его остаток от деления на n является *гомоморфизмом колец*, т. е. переводит суммы в суммы, а произведения – в произведения.

Редукция по модулю n — это научное название для гомоморфизма из предыдущей задачи. Применяя редукцию по модулю n к какому-либо уравнению в кольце $\mathbb{Z}$ мы получаем уравнение $\mathbb{Z}/n\mathbb{Z}$, причём из его неразрешимости в $\mathbb{Z}/n\mathbb{Z}$ вытекает, очевидно, неразрешимость исходного уравнения в $\mathbb{Z}$. Ввиду конечности кольца $\mathbb{Z}/n\mathbb{Z}$, анализ разрешимости уравнений часто резко упрощается при редукции по подходящему модулю. Имея это в виду вернитесь ещё раз к зад. А2-1 и зад. А2-2.

Алгоритм Евклида есть процедура, позволяющая быстро отыскать *НОД* пары натуральных чисел A, B (или многочленов A, B от одной переменной над полем) и состоящая в следующем. Пусть $A > B$ (соотв. $\deg A > \deg B$). Положим

$$E_1 = A\ , \quad E_2 = B\ , \quad E_\nu = \text{остаток от деления } E_{\nu-2} \text{ на } E_{\nu-1} \quad .$$

Последовательность E_ν (соотв. $\deg E_\nu$) строго монотонно убывает до тех пор, пока очередной E_ν не будет нулевым. Последний ненулевой элемент последовательности E_ν равен *НОД*(A, B).

А2-6. Докажите это и убедитесь, что *НОД* делится нацело на любой другой общий делитель.

А2-7. Пусть A, B – целые числа (соотв. многочлены). Докажите, что всегда можно подобрать такие целые числа (соотв. многочлены) a, b, что $aA + bB =$ *НОД*(A, B). Подберите такие a, b и вычислите *НОД*(A, B) для

а) $A = 1537$ и $B = 1387$,   **б)** $A = x^5 - 1$ и $B = x^4 + x^2 + 1$.

А2-8. Пусть m – произвольное, а a, b – взаимно простые числа (или элементы $k[x]$). Докажите, что

а) если m делится на a и на b, то m делится и на ab;

б) если a делит mb, то a делит m.

А2-9. Докажите, что класс $k \mod n$ тогда и тоько тогда обратим в $\mathbb{Z}/n\mathbb{Z}$, когда n и k взаимно просты в $\mathbb{Z}$.

A2-10. Пусть p – простое число.

а) Докажите, что $\mathbb{Z}/p\mathbb{Z}$ является полем.

б) Найдите все такие $x \in \mathbb{Z}/p\mathbb{Z}$, что $x^2 = 1$.

в) Чему равно произведение всех ненулевых чисел в $\mathbb{Z}/p\mathbb{Z}$?

г) Докажите *теорему Вильсона*: число p является простым тогда и только тогда, когда

$$(p-1)! + 1 \equiv 0 \pmod{p} .$$

д) Докажите *малую теорему Ферма*: для любого целого числа m, не делящегося на простое число p, имеет место сравнение

$$m^{p-1} \equiv 1 \, (\operatorname{mod} p) .$$

е) Докажите, что ровно половина ненулевых элементов $\mathbb{Z}/p\mathbb{Z}$ является квадратами;

ж) Докажите, что уравнение $x^2 + y^2 = -1$ всегда разрешимо в кольце $\mathbb{Z}/p\mathbb{Z}$.

з) Какие значения может принимать функция $y = x^{\frac{p-1}{2}}$ на ненулевых элементах $\mathbb{Z}/p\mathbb{Z}$?

и) Докажите, что ненулевой x тогда и только тогда является квадратом в $\mathbb{Z}/p\mathbb{Z}$, когда

$$x^{\frac{p-1}{2}} = 1 .$$

A2-11*. Запишем все числа $x \in \mathbb{Z}/p\mathbb{Z}$ (где p – простое) по порядку в виде

$$-\frac{p-1}{2}, \; \ldots, \; -1, \; 0, \; 1, \; \ldots, \; \frac{p-1}{2} .$$

Докажите следующие утверждения:

а) *лемма Гаусса*: число a является квадратом в $\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда, когда количество положительных x, меняющих знак при умножении на a, чётно;

б) число -1 является квадратом в $\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда, когда $p \equiv 1 \, (\operatorname{mod} 4)$ или $p = 2$.

в) число 2 является квадратом в $\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда, когда число $(p^2-1)/8$ — чётно;