2. Элементарная арифметика

2.1. Решить в целых числах уравнения:

а) $23x - 17y = 5$,

б) $35x + 21y = 14$.

2.2. Оценить количество операций, необходимых для вычисления (a,b) для целых чисел a, b алгоритмом Евклида.

2.3. Имеют ли решения в целых числах уравнения:

а) $3x^2 + 2 = y^2$,

б) $7x^2 + 2 = y^3$,

в) $15x^2 - 7y^2 = 9$?

2.4. Доказать, что хотя бы одна сторона пифагорова треугольника (прямоугольного треугольника с целыми длинами сторон) делится на 5.

2.5. Найти все пифагоровы треугольники.

2.6. Найти все целочисленные решения уравнения

$$2x^2 - 3y^2 + 5z^2 + 4xy - 6xz - 2yz = 0.$$

2.7. Найти три последние цифры числа $1997^{1000000}$. Оценить количество цифр в этом числе.

2.8. Решить сравнение $2^n \equiv n \pmod p$, где p — простое число.

2.9. Пусть

$$u_n = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \qquad (n \text{ двоек}).$$

Доказать, что последовательность u_n стабилизируется по любому модулю $m \in \mathbb{N}$.

2.10. а) Пусть $m_1, \ldots, m_k$ — попарно взаимно простые модули; $a_1, \ldots, a_n$ — произвольные целые числа. Доказать, что существует такое число $N \in \mathbb{Z}$, что $N \equiv a_i \pmod{m_i}$ для любого i, причем N определено однозначно по модулю $m_1 \ldots m_k$ (китайская теорема об остатках).

б) Найти все такие $N \in \mathbb{Z}$, что

$$N \equiv 2 \pmod 7, \quad N \equiv 3 \pmod{18}, \quad N \equiv 3 \pmod{13}.$$

в) Доказать, что если $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ (p_i — различные простые числа), то кольца Z_m и $Z_{p_1^{\alpha_1}} \oplus \cdots \oplus Z_{p_k^{\alpha_k}}$ изоморфны.

г) Верно ли, что $Z_4 \cong Z_2 \oplus Z_2$?

д) Пусть A — кольцо, $A^\times$ — группа его обратимых элементов. Доказать, что если $A = A_1 \oplus \cdots \oplus A_k$, то $A^\times = A_1^\times \times \cdots \times A_k^\times$.

е) Пусть $\varphi(m) = |Z_m^\times|$ — функция Эйлера. Доказать, что $\varphi(mn) = \varphi(m)\varphi(n)$ при $(m,n) = 1$.

ж) Для $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

$$\varphi(m) = m\Big(1 - \frac{1}{p_1}\Big) \dots \Big(1 - \frac{1}{p_k}\Big).$$

2.11. Найти все такие $m \in \mathbb{N}$, что

а) $\varphi(m) = 10$.

б) $\varphi(m) = 2^k$ для некоторого $k \in \mathbb{N}$.

2.12. Сколько делителей нуля в кольцах Z_{24}, Z_{683} ?

2.13. Доказать, что

$$\sum_{d|m} \varphi(d) = m.$$

2.14. Описать все решения уравнения $ax = b$ в кольце Z_m.

2.15. Решить уравнение $x^2 + 4x + 7 = 0$ в кольцах Z_{19}, Z_{15}, Z_{25}.

2.16. Решить уравнения

а) $x^3 = 10$ в Z_{37}.

б) $6x^3 + 27x^2 + 17x + 20 = 0$ в Z_{30}.

2.17. Сколько корней имеет уравнение $x^7 = 35$ в Z_{601} ?

2.18. Решить сравнение $x^2 - 1 \equiv 0 \pmod m$ когда

а) $m = p^k$, $p \neq 2$ — простое число,

б) $m = 2^k$,

в) m — любое натуральное число.

2.19. Пусть $f(x) \in \mathbb{Z}[x]$.

а) Доказать, что разрешимость сравнения $f(x) \equiv 0 \pmod m$ при $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ равносильна разрешимости системы сравнений $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ при $i = 1, \dots, k$.

б) Показать, что если существует решение x_0 сравнения $f(x) \equiv 0 \pmod p$ и $f'(x_0) \not\equiv 0 \pmod p$, то существует единственное решение x сравнения $f(x) \equiv 0 \pmod{p^\alpha}$, такое, что $x \equiv x_0 \pmod p$ (лемма Гензеля).

2.20. Пусть p/q есть несократимая дробь, $f(x) \in \mathbb{Z}[x]$ и $f(p/q) = 0$. Доказать, что

а) q есть делитель старшего коэффициента $f(x)$,

б) p есть делитель свободного члена $f(x)$,

в) $p - mq$ есть делитель $f(m)$, $m \in \mathbb{Z}$.

2.21. Найти рациональные корни многочленов

$$x^3 - 6x^2 + 15x - 14, \qquad 24x^4 - 42x^3 - 77x^2 + 56x + 60.$$

2.22. Доказать, что многочлен $f(x) \in \mathbb{Z}[x]$ не имеет целых корней, если $f(0)$ и $f(1)$ — нечетные числа.

2.23. а) Пусть $f(x) \in \mathbb{F}_p[x]$; тогда многочлены $f(x), f(x+1), \ldots, f(x+p-1)$ либо все равны, либо попарно различны.

б) Многочлен $x^p - x - a$ при $a \not\equiv 0 \pmod p$ неприводим над $\mathbb{F}_p$.

2.24. Доказать неприводимость над $\mathbb{Q}$ многочленов

а) $x^5 + 2x^3 + 3x^2 - 6x - 5$,

б) $x^5 - 6x^3 + 2x^2 - 4x + 5$,

в) $x^{105} - 9$,

г) $(x - a_1)\ldots(x - a_n) - 1$, где $a_1, \ldots, a_n$ — попарно различные целые числа.

2.25. Доказать, что если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$ (т. е. не может быть разложен в произведение двух многочленов меньших степеней), то он неприводим и над $\mathbb{Q}$ (лемма Гаусса).

2.26. Пусть $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}$, причем существует такое простое число p, что $p \mid a_i,\ 0 \leqslant i < n$, и $p^2 \nmid a_0$. Тогда $f(x)$ неприводим над $\mathbb{Q}$ (критерий Эйзенштейна).

2.27. Пусть $\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$ — множество обратимых вычетов по модулю простого нечетного числа p. Умножение на $a \in Z_p^{\times}$ задает перестановку этого множества. Пусть k — количество положительных представителей, перешедших в отрицательные, тогда *символ Лежандра* $\left(\frac{a}{p}\right) = (-1)^k$.