

Представимость чисел в виде суммы двух квадратов

Задача 1. Пусть p — простое вида $4k + 1$, и пусть $x = (2k)!$. Докажите, что $x^2 \equiv -1 \pmod{p}$.

Задача 2. Пусть p — простое вида $4k + 1$, и пусть x удовлетворяет сравнению $x^2 \equiv -1 \pmod{p}$. Докажите, что

- а) $(a + xb)(a - xb) \equiv a^2 + b^2 \pmod{p}$ при $a, b \in \mathbb{Z}$;
- б) среди чисел вида $m + xn$, где $m, n \in \mathbb{Z}$, $0 \leq m, n \leq [\sqrt{p}]$, найдутся два с равными остатками от деления на p ;
- в) найдётся ненулевое число вида $a + bx$, делящееся на p , где $a, b \in \mathbb{Z}$, причем $|a| < \sqrt{p}$ и $|b| < \sqrt{p}$;
- г) p представимо в виде суммы двух квадратов целых чисел.

Задача 3. Пусть p — простое число вида $4k+3$, числа a и b целые и a^2+b^2 делится на p . Докажите, что a делится на p и b делится на p .

Задача 4. Докажите, что произведение чисел, представимых в виде суммы двух квадратов целых чисел, само представимо в виде суммы двух квадратов целых чисел.

Задача 5. Сформулируйте и докажите теорему о том, как по разложению числа на простые множители узнать, представимо ли это число в виде суммы двух квадратов целых чисел.

Функция Эйлера и китайская теорема об остатках

Определение 1. Определим функцию Эйлера $\varphi(m)$ как количество обратимых элементов в \mathbb{Z}_m .

Задача 6. Докажите, что это определение согласуется с данным в задаче 15 листка 15 $\frac{1}{2}$.

Задача 7. Пусть k и l — взаимно простые натуральные числа. Сопоставим элементу $[n]_{kl}$ пару элементов $([n]_k, [n]_l)$. Докажите, что

- а) в $([0], [0])$ переходит только $[0]$;
- б) данное сопоставление является биекцией между \mathbb{Z}_{kl} и $\mathbb{Z}_k \times \mathbb{Z}_l$;
- в) пусть $\alpha \in \mathbb{Z}_{kl}$ отображается в пару (α_1, α_2) . Тогда α — обратимый элемент тогда и только тогда, когда α_1 и α_2 — обратимые элементы;
- г) $\varphi(kl) = \varphi(k)\varphi(l)$.

Задача 8. Найдите а) $\varphi(1)$, б) $\varphi(p)$, в) $\varphi(p^k)$, г) $\varphi(m)$. где p — простое, k, m — произвольные натуральные числа.

Задача 9. (*Китайская теорема об остатках*)

- а) Пусть натуральные m_1, \dots, m_k попарно взаимно просты. Докажите, что для любых целых b_1, \dots, b_k существует такое целое x , что $x \equiv b_1 \pmod{m_1}$, \dots , $x \equiv b_k \pmod{m_k}$, и это x можно единственным образом выбрать так, что $0 \leq x < m_1 \cdot m_2 \cdot \dots \cdot m_k$.
- б) Используя функцию Эйлера, явно укажите такое x .

Задача 10. Укажите все целые числа, которые удовлетворяют системе

- $$\text{a) } \begin{cases} x \equiv 3 \pmod{5}; \\ x \equiv 7 \pmod{17}. \end{cases} \qquad \text{б) } \begin{cases} x \equiv 2 \pmod{13}; \\ x \equiv 4 \pmod{19}. \end{cases}$$

Задача 11. Найдите такое целое $a > 0$, что $a/2$ — точный квадрат, $a/3$ — точный куб, $a/5$ — точная 5-я степень.

Задача 12*. Существует ли а) сколь угодно длинная; б) бесконечная арифметическая прогрессия, каждый член которой — степень натурального числа с целым показателем, большим 1?

[illegible]