

Арифметика вычетов

1. Докажите, что при любом $n \in \mathbb{N}$ число $(2^n - 1)^n - 3$ делится на $2^n - 3$.
 2. Докажите, что существует бесконечно много простых чисел, дающих при делении на 4 остаток 3, т. е. простых чисел вида $4k + 3$. То же для простых чисел вида $6n + 5$.
 3. (a, b, c) — пифагорова тройка ($a, b, c \in \mathbb{N}$, $a^2 + b^2 = c^2$). Докажите, что $abc : 60$.
 4. p , $p + 10$ и $p + 14$ — простые числа. Найдите p .
 5. p , $4p^2 + 1$, $6p^2 + 1$ — простые числа. Найдите p .
 6. Докажите, что $n^3 + 2$ не делится на 9 ни при каком целом n .
 7. Докажите, что существует бесконечно много натуральных чисел, не представимых в виде суммы
(а) двух (b) трех
квадратов целых чисел.
 8. Доказать, что нет такого числа в последовательности 11, 111, 1111, 11111, $\dots$ которое является квадратом целого числа.
 9. Докажите, что ни одно из чисел вида 10^{3n+1} нельзя представить в виде суммы двух кубов натуральных чисел.
 10. Решите сравнения:
(а) $8x \equiv 3 \pmod{13}$; (b) $7x \equiv 2 \pmod{11}$;
(с) $17x \equiv 1 \pmod{37}$; (d) $80x \equiv 17 \pmod{169}$.
- Определение.** Вычет a называется *обратимым* по модулю m , если существует вычет b (быть может, совпадающий с вычетом a) такой, что $a \cdot b \equiv 1 \pmod{m}$. В таком случае вычет b называется *обратным* к a .
11. Вычет a обратим по модулю m тогда и только тогда, когда $\text{НОД}(a, m) = 1$.
 12. Докажите, что если вычет обратим, то обратный к нему единственный.
 13. При каких условиях вычет обратен сам себе?
 14. **Теорема Вильсона.** Докажите, что для простого p выполнено сравнение $(p - 1)! \equiv -1 \pmod{p}$.