Арифметика III: Сравнения по модулю

Соглашение. Все числа в этом листке целые, а p — еще и простое.

▷ **Определение 1.** Говорят, что целые числа a и b *сравнимы по модулю* n, если $a-b \in (n)$. Обозначение: $a \equiv b \pmod{n}$.

Как было доказано в предыдущем листке, это отношение эквивалентности. Соответствующее фактормножество обозначается $\mathbb{Z}/n\mathbb{Z}$ (его элементы иногда называют *вычетами по модулю* n; их можно отождествлять с остатками от деления на n).

Задача 1. Пусть $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$. Обязательно ли
а) $a+b \equiv a'+b' \pmod{n}$; б) $ab \equiv a'b' \pmod{n}$; в) $a^k \equiv a'^k$; г) $k^a \equiv k^{a'}$;
д*) $f(a,b) \equiv f(a',b')$ для произвольного многочлена f с целыми коэффициентами?

Задача 2. Какие остатки по модулю 4 может иметь полный квадрат?

Задача 3. Имеют ли следующие уравнения решения в целых числах?
а) $12x+5=y^2$; б) $15x^2-7y^2=9$; в) $x^2+y^2=3z^2$; г) $8x^3-13y^3=17$; д) $2^x-1=5^y$.

Задача 4. Существует бесконечно много натуральных чисел, не представимых в виде суммы а) двух, б) трех квадратов.

Задача 5. а) Пусть $ax \equiv ay \pmod{n}$, $a \not\equiv 0 \pmod{n}$. Обязательно ли $x \equiv y \pmod{n}$?
б) Пусть $[a]$ — ненулевой вычет по модулю n. Всегда ли отображение умножения на a ($m_a\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $[x] \mapsto [ax]$) является биекцией?

Задача 6. Решите сравнения
а) $7x \equiv 1 \pmod{11}$; б) $7x \equiv 1 \pmod{12}$; в) $7x \equiv 5 \pmod{12}$.

Задача 7 (китайская теорема об остатках).
а*) Пусть числа n и m взаимно просты. Тогда естественное отображение $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ является биекцией.
б) Пусть числа $n_1, \ldots, n_k$ попарно взаимно просты. Тогда для любых чисел $b_1, \ldots, b_k$ найдется такое целое число x, что $x \equiv b_i \pmod{n_i}$.

Задача 8. Решите системы сравнений

а) $\begin{cases} x \equiv n-1 \pmod{n}; \\ x \equiv n \pmod{n+1}. \end{cases}$ б) $\begin{cases} x \equiv 2 \pmod{5}; \\ x \equiv 3 \pmod{7}; \\ x \equiv 4 \pmod{9}. \end{cases}$ в) $\begin{cases} x \equiv 1 \pmod{4}; \\ x \equiv 2 \pmod{7}; \\ x \equiv 3 \pmod{10}. \end{cases}$

▷ **Определение 2.** *Порядком* вычета $[a]$ по модулю l называется наименьшее натуральное число n, такое что $a^n \equiv 1 \pmod{l}$.

Задача 9. а) Любой ненулевой вычет по простому модулю имеет порядок.
б) $a^n \equiv 1$, тогда и только тогда когда n делится на порядок a.

Задача 10. Если число p простое, то $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Задача 11 (малая теорема Ферма). Если число p простое, то $a^p \equiv a \pmod{p}$.
(Следствие: если $a \not\equiv 0 \pmod{p}$, то $a^{p-1} \equiv 1 \pmod{p}$.)

Задача 12. Вычислите а) $2^{1001} \mod 11$; б) $2010^{2011} \mod 57$.

Задача 13. а) Если $p > 3$, то $p^2 \equiv 1 \pmod{24}$.
б) Если $p > 2$, то $7^p - 5^p - 2$ делится на $6p$.

Задача 14*. Вычислите $\underbrace{11\ldots1}_{p-1} \mod p$.

Задача 15. а) Если ненулевой вычет $[a]$ является полным квадратом по простому модулю p, то $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.
б*) Верно ли обратное утверждение?

Задача 16*. Вычислите $1^{2011} + 2^{2011} + \cdots + (p-1)^{2011} \mod p$.

Задача 17* (теорема Вильсона). Число p является простым тогда и только тогда, когда $(p-1)! \equiv -1 \pmod p$.

Задача 18*. а) Для каких простых p вычет $[-1]$ является полным квадратом по модулю p?
б) А вычет $[-3]$? (Указание: рассмотрите в $\mathbb{Z}/p\mathbb{Z}$ подходящее квадратное уравнение с дискриминантом -3.)

Задача 19*. Пусть $[a]$ — ненулевой вычет по простому модулю p. Рассмотрим отображение m_a из задачи 5 как перестановку множества $(\mathbb{Z}/p\mathbb{Z})^\times$ ненулевых вычетов по модулю p.
а) Какую циклическую структуру может иметь эта перестановка? (Например, может ли она представлять собой произведение независимых циклов длин 7 и 11?)
б) Найдите знак[1] этой перестановки. (Начать можно со случая, когда a является полным квадратом по модулю p.)

[1]Знак перестановки — это число -1, если перестановка нечетная, и 1, если четная.