Системы вычетов, обратные остатки, лекция

1. **(а)** Даны взаимно числа a и n. Докажие, что множество остатков чисел

$$\{0 \cdot a, 1 \cdot a, \ldots, (n-1) \cdot a\}$$

от деления на n совпадает (в некотором порядке) с множеством

$$\{0, 1, \ldots, n-1\}.$$

Верно ли это утверждение для не взаимно простых чисел a и n?

(б) Докажите, что для взаимно простых чисел m и n и любого целого числа r найдется целое x такое, что $mx \equiv r (\mathrm{mod} n)$, причем все такие x сравнимы между собой по модулю n. Если $r = 1$, то m и x называют обратными друг к другу по модулю n.

(в) Даны взаимно простые числа m и n. Докажите, что существуют целые x и y такие, что $mx + ny = 1$.

2. **(а)** Пусть p - простое число. Какие остатки обратны сами себе по модулю p?

(б) Теорема Вильсона. Докажите, что для любого простого числа p верно

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

3. Обозначим через $f(a)$ обратный остаток к a по модулю p. Докажите, что

(а) $ax \equiv bx \pmod{p}$ равносильно $a \equiv b \pmod{p}$ для x не кратных p;

(б) $ax \cdot f(bx) \equiv a \cdot f(b) \pmod{p}$ для b, x не кратных p;

(в) $af(b) \cdot cf(d) \equiv ac \cdot f(bd) \pmod{p}$ для b, d не кратных p;

(г) $af(b) \pm cf(d) \equiv (ad \pm cb) f(bd) \pmod{p}$ для b, d не кратных p.

Замечание. На самом деле, в задаче выше мы можем обозначить через $\dfrac{1}{a}$ обратный остаток к a по модулю p (это всего лишь обозначение). Тогда мы по сути доказали, что если знаменатель не кратен p, то с обратными остатками можно работать как с рациональными числами.

4. Докажите, что если простое число $p \neq 3$ является делителем числа вида $a^2 + 9$ для некоторого целого a, то p является делителем числа вида $c^2 + 1$ для некоторого целого c.

[Yandex] Филатов Андрей
[9 класс (профи + база)]

Системы вычетов, обратные остатки. Семинар.

Дедлайн сдачи и разбор задач — 26 марта

Чтобы сдавать задачи продвинутого уровня, нужно сдать все задачи базового.

Базовый уровень.

1. Для каждого ненулевого остатка по модулю **(а)** 7; **(б)** 11; **(в)** 19 найдите обратный.

2. **(а) Обратная теорема вильсона.** Докажите, что если для натурального числа n выполнено $(n-1)! \equiv -1 (\mathrm{mod} n)$, то n - простое число.

(б) Какой остаток дает 97! при делении на 101?

3. Предположим, что $p > 2$. Преобразуем сумму

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

в дробь $\dfrac{m}{n}$. Докажите, что m делится на p.

Продвинутый уровень.

4. Натуральные числа m и n таковы, что для каждого натурального k верно

$$(11k - 3, n) = (11k - 3, m).$$

Докажите, что $m = 11^s n$ или $n = 11^s m$ для некоторого $s \geqslant 0$.

5. Предположим, что $p > 3$. Преобразуем сумму

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}$$

в дробь $\dfrac{m}{n}$. Докажите, что m делится на p.