Показатели, квадратичные вычеты, лекция

Определение. Показателем числа a по простому модулю p ($\text{НОД}(a,p) = 1$) называется наименьшее натуральное d такое, что $a^d \equiv 1 \pmod p$. *Обозначение* $\text{ord}_p(a)$ происходит от английского слова *order*.

1. Пусть $\text{ord}_p(a) = d$ для простого p. Докажите, что тогда

   (а) числа $a, a^2, \ldots, a^d$ попарно не сравнимы по модулю p;

   (б) $a^{d_1} \equiv a^{d_2} \pmod p$ тогда и только тогда, когда $d_1 \equiv d_2 \pmod d$;

   (в) если для натурального k выполнено $a^k \equiv 1 \pmod p$, то k кратно d;

   (г) d является делителем $p-1$.

2. Пусть $\text{ord}_p(a) = d$ для простого p. Докажите, что тогда

   (а) если d кратно h, то показатель числа a^h по модулю p равен $\dfrac{d}{h}$;

   (б) если $\text{ord}_p(b) = k$ и $\text{НОД}(k,d) = 1$, то dk является показателем числа ab по модулю p.

3. Рассмотрим все числа вида $10^i - 10^j$ при $0 \leqslant j < i \leqslant 99$. Сколько из них делятся на 101?

Определение. Говорят, что число a является *квадратичным вычетом* по модулю m, если a взаимно просто с m и существует корень сравнения $x^2 \equiv a \pmod m$.

Далее везде p - *нечетное* простое число, a обычно не делится на p.

Определение. Вычет, не являющийся квадратичным по модулю p и не делящийся на p, называется *квадратичным невычетом* по модулю p.

4. Сколько существует квадратичных вычетов и невычетов по модулю p?

Определение. *Символом Лежандра* называется выражение, обозначаемое $(\dfrac{a}{p})$, равное 1, если a - квадратичный вычет по модулю p; -1, если a - невычет по модулю p и 0, если a кратно p.

5. **Свойства символа Лежандра:**

   (а) $(\dfrac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod p$ (критерий Эйлера);

   (б) $(\dfrac{ab}{p}) = (\dfrac{a}{p})(\dfrac{b}{p})$ (мультипликативность).

6. Докажите, что -1 является квадратичным вычетом по модулю p тогда и только тогда, когда $p = 4k+1$ для целого k.

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

Показатели, квадратичные вычеты. Семинар.

Дедлайн сдачи и разбор задач — 9 апреля

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

Базовый уровень.

1. Докажите, что показатели взаимно обратных чисел по модулю p совпадают.
2. Решите сравнение $3x^2 - 4x + 1 \equiv 0 \pmod{131}$. Без перебора!
3. Дано нечетное простое p, а также простые числа q и r. Известно, что $q^r + 1$ кратно p. Докажите, что либо $p-1$ кратно $2r$, либо $q^2 - 1$ кратно p.
4. Сколько делителей от 1 до 200 имеет число $2^{239} - 1$?

Продвинутый уровень.

5. Пусть N - произведение первых ста простых чисел. Сравнимо ли 2^N с единицей по модулю 17?
6. Докажите, что у сравнения $(x^2-2)(x^2-3)(x^2-6) \equiv 0 \pmod p$ всегда есть решение.
7. Докажите, что число p является делителем числа x^2-x+3 тогда и только тогда, когда оно является делителем числа вида $y^2 - y + 25$.