Листочек 3.

Щеголихин Егор М3298

№2.

а) $\frac{a}{b} = \frac{c \cdot a}{c \cdot b}$ $c, a, b \in \mathbb{Z}$ $(a, b) = 1$

$v_p\left(\frac{a}{b}\right) = v_p\left(\frac{c \cdot a}{c \cdot b}\right)$?

$v_p\left(\frac{c}{b}\right) = v_p(a) - v_p(b)$

$v_p\left(\frac{ca}{cb}\right) = v_p(ca) - v_p(cb)$

Докажем для a и $c \in \mathbb{Z}$, что $v_p(a \cdot c) = v_p(a) + v_p(c)$.

Это очевидно, пусть $a = p^{k_1} \cdot a'$, $(a', p) = 1$

$c = p^{k_2} \cdot c'$, $(c', p) = 1$

$v_p(a \cdot c) = v_p\left(p^{k_1+k_2} \cdot a' \cdot c'\right) = k_1 + k_2$

$v_p(a) + v_p(c) = v_p(p^{k_1} a') + v_p(p^{k_2} \cdot c') = k_1 + k_2$.

$v_p\left(\frac{ca}{cb}\right) = v_p(ca) - v_p(cb) = v_p(c) + v_p(a) - v_p(c) - v_p(b) = v_p(a) - v_p(b)$ - ЧТД.

1. $v_p(xy) = v_p(x) + v_p(y)$

$x = \frac{a}{b}$ $y = \frac{c}{d}$ $a, b, c, d \in \mathbb{Z}$

$v_p\left(\frac{ac}{bd}\right) = v_p(ac) - v_p(bd) = v_p(a) + v_p(c) -$
$v_p(b) - v_p(d) = v_p(a) - v_p(b) + v_p(c) - v_p(d) =$
$= v_p\left(\frac{a}{b}\right) + v_p\left(\frac{c}{d}\right) = v_p(x) + v_p(y)$ - ЧТД

2. $v_p(x+y) =$
$x = \frac{a}{b} \quad y = \frac{c}{d} \quad a, b, c, d \in \mathbb{Z}$
$= v_p\left(\frac{a}{b} + \frac{c}{d}\right) = v_p\left(\frac{ad + cb}{bd}\right) = v_p(ad+cb) - v_p(b)$
$- v_p(d)$ $(=)$

Покажем, что для p и $q \in \mathbb{Z}$

~~$v_p(p+q) \geq \min(v_p, v_p(q))$~~

$v_p(u, q) \geq \min(v_p(u), v_p(q))$

$u = p^{k_1} \cdot u' \quad q = p^{k_2} \cdot q'$ Б.О.С. $k_1 \geq k_2$

$v_p(u+q) = v_p(p^{k_1} u' + p^{k_2} q') = v_p(p^{k_2}(p^{k_1-k_2} u' + q')) = v_p(p^{k_2}) + v_p(p^{k_1-k_2} u' + q') \geq k_2 = \min($
$v_p(u), v_p(q))$

$(=)$ $v_p(ad+cb) - v_p(b) - v_p(d) \geq \min(v_p(a) + v_p(d), v_p(b) + v_p(c)) - v_p(b) - v_p(d)) = \min(v_p(a) - v_p(b), v_p(c) - v_p(d))$
$= \min(v_p(x), v_p(y))$ - ЧТД.

3. Докажем, что 2 нормированных ряда не эквивалентны между собой.

$$\sum_{i=k}^{\infty} a_i p^i \quad \text{и} \quad \sum_{j=m}^{\infty} b_j p^j$$

~~Доказательство~~ Предположим, что нашлось такое N, возьмём $n > N$.

$$\sum_{i=k}^{\infty} a_i p^i - \sum_{j=m}^{n} b_j p^j = \text{для удобства вычитания дополним ряды нулями слева}$$

$$= \sum_{i=0}^{n} (a_i - b_j) p^i$$

одно из двух $\sum_{i=0}^{n} (a_i - b_i) p^i = 0$ или

$\sum_{i=0}^{n} (a_i - b_i) p^i \vdots p^n$.

первое не может выполняться для всех $n > N$, ведь это бы означало, что ряды равны

Тогда $\sum_{i=0}^{n} (a - b_i) p^i \vdots p^n$ $|a_i - b_i| < p$, т.к. $a_i < p$ и $b_i < p$

Тогда по сути весь ряд является числом p-ичной системы исчисления (возможно с отр. дефрами), но тогда мы знаем в p-ичной системе исчисления число делится $n < p^n$, а значит, если оно $\neq 0$ не равно нулю, то не делится на p^n. Противоречие

Будем решать $g^x = a \pmod p$

и $g^x = a \iff g \cdot g^{-x} = 1 \pmod p$

Будем восстанавливать x по биту"

Очевидно, что g^x является кв. вычетом тогда и только тогда $x : 2$

Начнем с первого бита, узнаем чётное или нечётное x. Для этого проверим является ли а вычетом.

Возведем $g^{x \cdot \frac{p-1}{2}}$, если равно 1, то

x - чётно

иначе $\frac{x}{2}$ - нечётно

Теперь если нам нужно проверить является ли второй бит. Для этого если x чётно нам достаточно посмотреть на $\frac{x}{2}$, а если нечётно $\frac{x+1}{2}$, т.е. мы проверяем $(g^{\frac{x}{2}})$ - квадратичный вычет или $(g^{\frac{x-1}{2}})$, т.

$(g^{\frac{x}{2}})^{\frac{p-1}{2}} = (g^x)^{\frac{p-1}{2^2}}$ или $(g^{x+1})^{\frac{p-1}{2^2}}$

Если не оказалось, что кв. вычет, то нужно к x теперь прибавить 2, ведь мы угадали на

И теперь аналогично для всех последующих бит (g^{x+k}) Имеем, что на каждом

шаг мы узнаем число вида

$$(g^x)^{\frac{p-1}{2^N}} \quad (g^{k+k})^{\frac{p-1}{2^N}} = (g^x \cdot g^k)^{\frac{p-1}{2^N}} =$$

$$= (a \cdot g^k)^{\frac{p-1}{2^N}}$$

проблема посчитать ~~???~~ возведение в $\frac{p-1}{2^N}$, но нас спасает, что $p = 2^{2^k}+1$, ведь

$p-1 : 2^{2^k}$ и делится на все меньшие степени двойки

у нас всего шагов количество битов $-O(\log(n))$ и на каждом шаге мы возводим за $O(\log(n))$

т.е в итоге $O(\log^2(n))$