q-Babbage Theorem

Определение 1. **q-биномиальный коэффициент** $Q_n^k(q)$ — — многочлен от q, коэффициент при q^l которого равен количеству правильных путей из $(0,0)$ в $(k, n-k)$, площадь под которыми равна l. Если переменная («вес клетки») не указана, то используется q. Также можно брать q-бином от множества, тогда считается количество путей из этого множества.

Лемма 1. Степень вхождения $[p]$ в $[r]$ равна 1, если $p \mid r$, иначе $([p],[r]) = 1$.

Доказательство. Если $p \nmid r$, то у $[r]$ нет корня, являющегося корнем p-й степени из 1, откуда следует вторая часть утверждения. Если $r = kp$, то выполняется $[r] = [p](q^{p(k-1)} + q^{p(k-2)} + \dots) \equiv [p]k \mod [p]^2$, откуда следует первая часть. ■

Лемма 2. Степень вхождения $[p]$ в $[r]!$ равна $\lfloor \frac{r}{p} \rfloor$.

Доказательство. Все множители в $[r]!$ вида $[k]$, где $p \nmid k$, взаимно просты с $[p]$ и не влияют на степень вхождения. Также $\prod\limits_k \frac{[kp]}{[p]} \equiv \lfloor \frac{r}{p} \rfloor! \mod [p]$, т.е. степень вхождения равна количеству этих множителей. ■

Лемма 3. Q_{bp}^k делится на $[p]$ и не делится на $[p]^2$ при $p \nmid k$.

Доказательство. Заметим, что $Q_{bp}^k = \frac{[bp]!}{[k]![bp-k]!}$ и степень вхождения $[p]$ в числитель равна b, а в знаменатель — $b-1$. ■

Теорема 4. $Q_{ap}^{bp}(q) \equiv Q_a^b(q^{p^2}) \mod [p]^2$.

Доказательство. Доказываем по индукции по a. База при $a = 0$ верна.

Шаг индукции. Посмотрим на какой-то правильный путь $\mathcal{P}$ в прямоугольнике $bp \times (a-b)p$. Пусть, не умаляя общности, $a \geq 2b$, и прямая через точки $(0, bp)$ и $(bp, 0)$ пересекается с $\mathcal{P}$ в точке $(x, bp-x)$. Заметим, что q-бином от множества $\{\mathcal{P} : x = x_0\}$ равен $Q_{bp}^{x_0} q^{(bp-x_0)^2} Q_{(a-b)p}^{bp-x_0}$. Тогда по 3 этот q-бином делится на $[p]^2$ при $p \nmid x_0$, нас интересуют только пути, проходящие через какую-то (причём ровно 1) точку вида $(xp, (b-x)p)$. Для таких путей работает предположение индукции, т.е.

$$Q_{ap}^{bp}(q) \equiv \sum_{x=0}^{b} Q_{ap-bp}^{bp-xp}(q) Q_{bp}^{xp}(q) \cdot q^{(bp-xp)^2} \equiv \sum_{x=0}^{b} Q_{a-b}^{b-x}(q^{p^2}) Q_b^x(q^{p^2}) \cdot (q^{p^2})^{(b-x)^2}.$$

Заметим, что эта сумма равна $Q_a^b(q^{p^2})$ по тождеству Вандермонда. ■

Теорема 5. $Q_{ap}^{bp} \equiv C_a^b \cdot (1 + \frac{1}{2} pb(a-b)(q^p - 1)) \mod [p]^2$.