Теорема Куммера

$$\binom{m+n}{m} \quad = \quad C_{m+n}^{m}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C_{m+n}^{m} \\ &= \frac{(m+n)!}{m!n!}\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C_{m+n}^{m} \\ &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned} \binom{m+n}{m} &= C_{m+n}^{m} \\ &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots \end{aligned}$$

Теорема (Ernst Eduard Kummer [1852]). *Запишем числа m и n в позиционной системе счисления с основанием p и сложим их «в столбик»; $\alpha_p(m,n)$ равно количеству переносов из разряда в разряд при этом сложении.*

Теорема Куммера

$$\binom{m+n}{m} = \frac{(m+n)!}{m!n!}$$

$$= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots$$

Теорема Куммера

$$\binom{m+n}{m} = \frac{(m+n)!}{m!n!}$$

$$= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots\end{aligned}$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

$$\alpha_p(m,n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n)$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

$$p, 2p, 3p, \dots,$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

$$p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

Имеется $\left\lfloor \dfrac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \ldots, \left\lfloor \dfrac{k}{p} \right\rfloor p$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2: $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2: $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \frac{k}{p^3} \right\rfloor$ чисел кратных p^3: $p^3, 2p^3, 3p^3, \dots, \left\lfloor \frac{k}{p^3} \right\rfloor p^3$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \dots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2: $p^2, 2p^2, 3p^2, \dots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \frac{k}{p^3} \right\rfloor$ чисел кратных p^3: $p^3, 2p^3, 3p^3, \dots, \left\lfloor \frac{k}{p^3} \right\rfloor p^3$

$\vdots$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Имеется $\left\lfloor \dfrac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \dots, \left\lfloor \dfrac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \dfrac{k}{p^2} \right\rfloor$ чисел кратных p^2: $p^2, 2p^2, 3p^2, \dots, \left\lfloor \dfrac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \dfrac{k}{p^3} \right\rfloor$ чисел кратных p^3: $p^3, 2p^3, 3p^3, \dots, \left\lfloor \dfrac{k}{p^3} \right\rfloor p^3$

$\vdots$

$$\beta_p(k) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \dots$$

Теорема Куммера

$$\binom{m+n}{m} = \frac{(m+n)!}{m!n!}$$

$$= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

Теорема Куммера

$$\binom{m+n}{m} = \frac{(m+n)!}{m!n!}$$

$$= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots$$

$$k! = 2^{\beta_2(k)} 3^{\beta_3(k)} \dots p^{\beta_p(k)} \dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

$$\alpha_p(m,n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n)$$

Теорема Куммера

$$\binom{m+n}{m} = \frac{(m+n)!}{m!n!} = 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

$$\begin{aligned}\alpha_p(m,n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n)\\ &= \left\lfloor\frac{m+n}{p}\right\rfloor + \left\lfloor\frac{m+n}{p^2}\right\rfloor + \left\lfloor\frac{m+n}{p^3}\right\rfloor + \dots\\ &\quad - \left\lfloor\frac{m}{p}\right\rfloor - \left\lfloor\frac{m}{p^2}\right\rfloor - \left\lfloor\frac{m}{p^3}\right\rfloor - \dots\\ &\quad - \left\lfloor\frac{n}{p}\right\rfloor - \left\lfloor\frac{n}{p^2}\right\rfloor - \left\lfloor\frac{n}{p^3}\right\rfloor - \dots\end{aligned}$$

Теорема Куммера

$$
\begin{aligned}
\alpha_p(m,n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\
= \quad & \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\
& - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\
& - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots
\end{aligned}
$$

Теорема Куммера

$$\begin{aligned}
\alpha_p(m,n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\
= \quad & \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\
& - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\
& - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots \\
= \quad & \left(\left\lfloor \frac{m+n}{p} \right\rfloor - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{n}{p} \right\rfloor \right) + \left(\left\lfloor \frac{m+n}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + \\
& + \left(\left\lfloor \frac{m+n}{p^3} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + \dots
\end{aligned}$$

Теорема Куммера

$$\left\lfloor \frac{m+n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor = \begin{cases} 1, & \text{если есть перенос} \\ 0, & \text{если нет переноса} \end{cases}$$

Теорема Куммера

$$\left\lfloor \frac{m+n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor = \begin{cases} 1, & \text{если есть перенос} \\ 0, & \text{если нет переноса} \end{cases}$$

$m = \sum_{j=0}^r m_j p^j =$	m_r	$\ldots$	m_k	m_{k-1}	$\ldots$	m_0
$n = \sum_{j=0}^r n_j p^j =$	n_r	$\ldots$	n_k	n_{k-1}	$\ldots$	n_0
$m + n = \sum_{j=0}^r \ell_j p^j =$	ℓ_r	$\ldots$	ℓ_k	ℓ_{k-1}	$\ldots$	ℓ_0

$\lfloor m/p^k \rfloor =$	m_r	$\ldots$	m_k
$\lfloor n/p^k \rfloor =$	n_r	$\ldots$	n_k
$\lfloor (m+n)/p^k \rfloor =$	ℓ_r	$\ldots$	ℓ_k

Теорема Куммера

$$\begin{aligned}
\alpha_p(m,n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\
= \quad & \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\
& - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\
& - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots
\end{aligned}$$

Теорема Куммера

$$
\begin{aligned}
\alpha_p(m,n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\
= \quad & \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\
& - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\
& - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots \\
= \quad & \left(\left\lfloor \frac{m+n}{p} \right\rfloor - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{n}{p} \right\rfloor \right) + \left(\left\lfloor \frac{m+n}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + \\
& + \left(\left\lfloor \frac{m+n}{p^3} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + \dots
\end{aligned}
$$

Следствие теоремы Куммера

Следствие теоремы Куммера

Лемма. При сложении чисел a и b в двоичной системе счисления не проходит ни одного переноса из разряд в разряд в том и только том случае, когда биномиальный коэффициент $\binom{a+b}{a}$ явлется нечетным

Следствие теоремы Куммера

Лемма. При сложении чисел a и b в двоичной системе счисления не проходит ни одного переноса из разряд в разряд в том и только том случае, когда биномиальный коэффициент $\binom{a+b}{a}$ явлется нечетным, то есть существует натуральное число d такое, что

$$\binom{a+b}{a} = 2d + 1.$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \wedge b \Longrightarrow \binom{a}{c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \wedge b \Longrightarrow \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a-c$	...	0	...	0	...	1	...	0	...
$b-c$	...	0	...	1	...	0	...	0	...

$$c = a \wedge b \Longrightarrow \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн. } \&$$

$$\& \binom{(a-c)+(b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a-c$	...	0	...	0	...	1	...	0	...
$b-c$	...	0	...	1	...	0	...	0	...

$$c = a \wedge b \Longrightarrow \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн. } \&$$

$$\& \binom{(a-c)+(b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a-c$	...	0	...	0	...	1	...	0	...
$b-c$	...	0	...	1	...	0	...	0	...

$$c = a \wedge b \Longleftarrow \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн. } \&$$

$$\& \binom{(a-c)+(b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a - c$	...	0	...	0	...	1	...	0	...
$b - c$	...	0	...	1	...	0	...	0	...

$$c = a \wedge b \Longleftrightarrow \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн. } \& \binom{(a-c)+(b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a-c$	...	0	...	0	...	1	...	0	...
$b-c$	...	0	...	1	...	0	...	0	...

$$c = a \wedge b \Longleftrightarrow \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн. } \& \\ \& \binom{(a-c)+(b-c)}{a-c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	...	0	...	0	...	1	...	1	...
b	...	0	...	1	...	0	...	1	...
c	...	0	...	0	...	0	...	1	...
$a-c$	...	0	...	0	...	1	...	0	...
$b-c$	...	0	...	1	...	0	...	0	...

$$c = a \wedge b \iff \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн. } \& \binom{(a-c)+(b-c)}{a-c} \text{ нечетн.}$$

Биномиальные коэффициенты

$$(1+u)^m = \binom{m}{m} u^m + \binom{m}{m-1} u^{m-1} + \binom{m}{m-2} u^{m-2} + \\ + \dots + \binom{m}{n} u^n + \dots + \binom{m}{1} u + \binom{m}{0}$$

$$2^m = \binom{m}{0} + \dots + \binom{m}{n} + \dots + \binom{m}{m}$$

$$c = \binom{m}{n} \iff \exists upq \{(1+u)^m = pu^{n+1} + cu^n + q \,\& \\ c < u \,\&\, q < u^{n-1} \,\&\, u > 2^m\}$$