Глава 1

Основные понятия

1.1 Алгоритмы

1.2 Математическое введение

1.2.1 Математическая индукция

1.2.2 Числа, степени и логарифмы

1.2.3 Суммы и произведения

1.2.4 Целочисленные функции и элементарная теория чисел

1.2.5 Перестановки и факториалы

1.2.6 Биномиальные коэффициенты

10.

Пусть p — простое число. Покажите:

e.

$$\binom{n}{k} \equiv \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor}\binom{n \bmod p}{k \bmod p} (\text{по модулю } \ p)$$

Основная формула биномиального коэффициента:

$$\binom{n}{k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k(k-1)(k-2)\dots 1}$$

Рассмотрим $k \bmod p$ первых сомножителей в знаменателе. Все они делятся на p с остатком. Если $k \bmod p > 0$, то

$$\begin{aligned}
\prod_{i=0}^{(k \bmod p)-1} k-i &\equiv \prod_{i=1}^{k \bmod p} i && \text{(по модулю } p\text{)}\\
k &\equiv k \bmod p && \text{(по модулю } p\text{)}\\
k-1 &\equiv (k \bmod p)-1 && \text{(по модулю } p\text{)}\\
\ldots &\equiv \ldots \\
k-(k \bmod p)+2 &\equiv 2 && \text{(по модулю } p\text{)}\\
k-(k \bmod p)+1 &\equiv 1 && \text{(по модулю } p\text{)}
\end{aligned}$$

Например, для $k = 17, p = 7$:

$$\begin{aligned}
17 \bmod 7 &= 3\\
(17 \bmod 7)-1 &= 2\\
\prod_{i=0}^{2} 17-i &\equiv \prod_{i=1}^{3} i && \text{(по модулю 7)}\\
17 \cdot 16 \cdot 15 &\equiv 3 \cdot 2 \cdot 1 && \text{(по модулю 7)}\\
4080 &\equiv 6 && \text{(по модулю 7)}\\
4080 \bmod 7 &= 6
\end{aligned}$$

Эта формула также справедлива для случая, когда k делится на p без остатка. Например, для $k = 14, p = 7$:

$$\begin{aligned}
14 \bmod 7 &= 0\\
(14 \bmod 7)-1 &= -1\\
\prod_{i=0}^{-1} 14-i &\equiv \prod_{i=1}^{0} i && \text{(по модулю 7)}\\
1 &\equiv 1 && \text{(по модулю 7)}
\end{aligned}$$

Теперь рассмотрим $k \bmod p$ первых сомножителей в числителе $n(n-1)\ldots(n-(k \bmod p)+1)$. Среди них может не оказаться сомножителя кратного p. Тогда:

$$\prod_{i=0}^{(k \bmod p)-1} n-i \equiv (n \bmod p)((n \bmod p)-1)\dots((n \bmod p)-(k \bmod p)+1) \quad (\text{по модулю } p)$$

$$n \equiv n \bmod p \quad (\text{по модулю } p)$$

$$n-1 \equiv (n \bmod p)-1 \quad (\text{по модулю } p)$$

$$\dots \equiv \dots$$

$$n-(k \bmod p)+2 \equiv (n \bmod p)-(k \bmod p)+2 \quad (\text{по модулю } p)$$

$$n-(k \bmod p)+1 \equiv (n \bmod p)-(k \bmod p)+1 \quad (\text{по модулю } p)$$

Например, для $n=20, k=17, p=7$:

$$20 \bmod 7 = 6$$

$$(20 \bmod 7)-1 = 5$$

$$\prod_{i=0}^{2} 20-i \equiv 6 \cdot 5 \cdot 4 \quad (\text{по модулю } 7)$$

$$20 \cdot 19 \cdot 18 \equiv 6 \cdot 5 \cdot 4 \quad (\text{по модулю } 7)$$

$$6840 \equiv 120 \quad (\text{по модулю } 7)$$

$$6840 \bmod 7 = 1120 \bmod 7 = 1$$

Для случая $k \bmod p = 0$ произведение в числителе, также как и в знаменателе, обращается в 1. Если среди первых $k \bmod p$ сомножителей в числителе встретится число, кратное p, то

$$\prod_{i=0}^{(k \bmod p)-1} n-i \equiv 0 \quad (\text{по модулю } p)$$

Подставим получившиеся соотношения в дробь

$$\frac{\prod_{i=0}^{(k \bmod p)-1} n-i}{\prod_{i=0}^{(k \bmod p)-1} k-i} \equiv \frac{(n \bmod p)((n \bmod p)-1)\dots((n \bmod p)-(k \bmod p)+1)}{\prod_{i=1}^{k \bmod p} i} \quad (\text{по модулю } p)$$

$$\frac{\prod_{i=0}^{(k \bmod p)-1} n-i}{\prod_{i=0}^{(k \bmod p)-1} k-i} \equiv \binom{n \bmod p}{k \bmod p} \quad (\text{по модулю } p)$$

Для случая $\prod_{i=0}^{(k \bmod p)-1} n-i \equiv 0 \pmod p$ соотношения также справедливы, т.к. $\binom{0}{k} = \begin{cases} 0 \text{ при } k>0 \\ 1 \text{ при } k=0 \end{cases}$.