# Lucas Theorem

Rongen Lin

Nanjing University

March 24, 2021

# Our Goal

## Problem

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$.

?

?

## Problem I

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$, $P \in \text{Prime}$.

# Lucas Theorem

# Lucas Theorem

## Lucas Theorem

$$\binom{N}{K} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i} \bmod P,$$

where $N = \sum_{i=0}^{m} n_i P^i$, $K = \sum_{i=0}^{m} k_i P^i$, $0 \leq n_i, k_i < P$, $P \in \text{Prime}$.

# Lucas Theorem

## Lucas Theorem

$$\binom{N}{K} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i} \bmod P,$$

where $N = \sum_{i=0}^{m} n_i P^i$, $K = \sum_{i=0}^{m} k_i P^i$, $0 \le n_i, k_i < P$, $P \in \text{Prime}$.

$$\binom{122}{41} \equiv \binom{2}{1}\binom{4}{3}\binom{4}{1} \equiv 2 \pmod 5$$

$$122 = 2 \times 5^0 + 4 \times 5^1 + 4 \times 5^2$$

$$41 = 1 \times 5^0 + 3 \times 5^1 + 1 \times 5^2$$

$$\binom{122}{41} = 509210537125015289581387223531062$$

# Proof of Lucas Theorem

## Lemma I

$$(1+x)^P \equiv 1 + x^P \pmod{P}.$$

# Proof of Lucas Theorem

## Lemma I

$$(1+x)^P \equiv 1 + x^P \pmod{P}.$$

## Proof.

Since

$$\binom{P}{i} = \frac{P}{j}\binom{P-1}{j-1} \equiv 0 \pmod{P}$$

holds for $0 < i < P$, we have

$$(1+x)^P = 1 + x^P + \sum_{i=1}^{P-1} \binom{P}{i} x^i \equiv 1 + x^P \pmod{P}.$$

Similarly, $(1+x)^{P^k} \equiv 1 + x^{P^k} \pmod{P}$. □

# Proof of Lucas Theorem

## Lucas Theorem

$$\binom{N}{K} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i} \bmod P,$$

where $N = \sum_{i=0}^{m} n_i P^i$, $K = \sum_{i=0}^{m} k_i P^i$, $0 \leq n_i, k_i < P$, $P \in \text{Prime}$.

# Proof of Lucas Theorem

## Lucas Theorem

$$\binom{N}{K} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i} \bmod P,$$

where $N = \sum_{i=0}^{m} n_i P^i$, $K = \sum_{i=0}^{m} k_i P^i$, $0 \leq n_i, k_i < P$, $P \in \text{Prime}$.

## Proof.

$$(1+x)^N = (1+x)^{\sum_{i=0}^{m} n_i P^i} = \prod_{i=0}^{m} (1+x)^{n_i P^i} \equiv \prod_{i=0}^{m} (1+x^{P^i})^{n_i}.$$

Compare coefficients of both sides, then we have

$$\binom{N}{K} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i} \bmod P.$$

□

# Proof of Lucas Theorem

## Lucas Theorem

$$\binom{N}{K} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i} \bmod P,$$

where $N = \sum_{i=0}^{m} n_i P^i$, $K = \sum_{i=0}^{m} k_i P^i$, $0 \leq n_i, k_i < P$, $P \in \text{Prime}$.

## Proof.

$$(1+x)^N = (1+x)^{\sum_{i=0}^{m} n_i P^i} = \prod_{i=0}^{m} (1+x)^{n_i P^i} \equiv \prod_{i=0}^{m} (1+x^{P^i})^{n_i}.$$

Compare coefficients of both sides, then we have

$$\binom{N}{K} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i} \bmod P.$$

Really???

□

!

## Problem I

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$, $P \in \text{Prime}$.

!

## Problem I

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$, $P \in \text{Prime}$.

## Solution I.

$O(P)$ for preprocessing, and $O(\log N)$ per query.

?

?

## Problem II

Calculate

$$\binom{N}{K} \bmod P^k.$$

$0 \leq N, K \leq 10^9$, $2 \leq P^k \leq 10^6$, $P \in \text{Prime}$.

?

## Problem II

Calculate

$$\binom{N}{K} \bmod P^k.$$

$0 \leq N, K \leq 10^9$, $2 \leq P^k \leq 10^6$, $P \in \text{Prime}$.

Can solution I work? Why?

# Further Discussion

# Further Discussion

## Lemma II

Let $F(p, n) \triangleq \max\{x : p^x \mid n\}$, then

$$F(p, n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

# Further Discussion

## Lemma II

Let $F(p,n) \triangleq \max\{x : p^x \mid n\}$, then

$$F(p,n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

## Proof.

$$\begin{aligned} F(p,n!) &= \sum_{k=1}^{n} \max\{x : p^x \mid k\} \\ &= \sum_{k=1}^{n} \sum_{i=1}^{\infty} \left[p^i \mid k\right] = \sum_{i=1}^{\infty} \sum_{k=1}^{n} \left[p^i \mid k\right] = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor. \end{aligned}$$

# Further Discussion

# Further Discussion

$$\binom{N}{K} = \frac{N!}{K!(N-K)!}$$

# Further Discussion

$$\binom{N}{K} = \frac{N!}{K!(N-K)!} \qquad \mod P^k$$

# Further Discussion

$$\binom{N}{K} = \frac{N!}{K!(N-K)!} \qquad \mod P^k$$

$F(p,n) \triangleq \max\{x : p^x \mid n\}$.
Let $x = F(P, N!), y = F(P, K!), z = F(P, (N-K)!)$, then

$$\binom{N}{K} = \frac{\frac{N!}{P^x}}{\frac{K!}{P^y}\frac{(N-K)!}{P^z}} P^{x-y-z}.$$

# Further Discussion

$$\binom{N}{K} = \frac{N!}{K!(N-K)!} \mod P^k$$

$F(p,n) \triangleq \max\{x : p^x \mid n\}$.
Let $x = F(P, N!), y = F(P, K!), z = F(P, (N-K)!)$, then

$$\binom{N}{K} = \frac{\frac{N!}{P^x}}{\frac{K!}{P^y}\frac{(N-K)!}{P^z}} P^{x-y-z}.$$

Only need to calculate $\frac{n!}{P^x} \bmod P^k$, where $x = F(P, n!)$.

# Further Discussion

# Further Discussion

$$\frac{n!}{P^x} \mod P^k$$

# Further Discussion

$$\frac{n!}{P^x} \mod P^k$$

$n = 10, P = 2, k = 2$:

# Further Discussion

$$\frac{n!}{P^x} \mod P^k$$

$n = 10, P = 2, k = 2$:

$$10! = \overbrace{\boxed{1 \times 2 \times 3 \times 4}}^{P^k} \times \boxed{5 \times 6 \times 7 \times 8} \times 9 \times 10$$

# Further Discussion

$$\frac{n!}{P^x} \mod P^k$$

$n = 10, P = 2, k = 2$:

$$10! = \overbrace{\boxed{1 \times 2 \times 3 \times 4}}^{P^k} \times \boxed{5 \times 6 \times 7 \times 8} \times 9 \times 10$$
$$= 2 \times 4 \times 6 \times 8 \times 10 \times 1 \times 3 \times 5 \times 7 \times 9$$

# Further Discussion

$$\frac{n!}{P^x} \mod P^k$$

$n = 10, P = 2, k = 2$:

$$\begin{aligned} 10! &= \overbrace{\boxed{1 \times 2 \times 3 \times 4}}^{P^k} \times \boxed{5 \times 6 \times 7 \times 8} \times 9 \times 10 \\ &= 2 \times 4 \times 6 \times 8 \times 10 \times 1 \times 3 \times 5 \times 7 \times 9 \\ &= 2^5 \times (1 \times 2 \times 3 \times 4 \times 5) \times \boxed{1 \times 3} \times \boxed{5 \times 7} \times 9 \end{aligned}$$

# Further Discussion

$$\frac{n!}{P^x} \mod P^k$$

$n = 10, P = 2, k = 2$:

$$\begin{aligned} 10! &= \overbrace{\boxed{1 \times 2 \times 3 \times 4}}^{P^k} \times \boxed{5 \times 6 \times 7 \times 8} \times 9 \times 10 \\ &= 2 \times 4 \times 6 \times 8 \times 10 \times 1 \times 3 \times 5 \times 7 \times 9 \\ &= 2^5 \times (1 \times 2 \times 3 \times 4 \times 5) \times \boxed{1 \times 3} \times \boxed{5 \times 7} \times 9 \end{aligned}$$

$$\underline{n!} \equiv P^{\lfloor \frac{n}{P} \rfloor} \cdot \underline{\left(\left\lfloor \frac{n}{P} \right\rfloor\right)!} \cdot \left( \prod_{i,(i,P)=1}^{P^k} i \right)^{\left\lfloor \frac{n}{P^k} \right\rfloor} \cdot \left( \prod_{i,(i,P)=1}^{n} i \right)$$

!

# !

## Problem II

Calculate

$$\binom{N}{K} \bmod P^k.$$

$0 \le N, K \le 10^9$, $2 \le P^k \le 10^6$, $P \in \text{Prime}$.

## Solution II

$F(p, n) \triangleq \max\{x : p^x \mid n\}$.
Let $x = F(P, N!), y = F(P, K!), z = F(P, (N-K)!)$, then

$$\binom{N}{K} = \frac{\frac{N!}{P^x}}{\frac{K!}{P^y}\frac{(N-K)!}{P^z}} P^{x-y-z}.$$

Calculate $\frac{n!}{P^x} \bmod P^k$ three times, then merge them by ExGcd.

# Further Discussion II

# Further Discussion II

## Problem III

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$ (or more).

# Further Discussion II

## Problem III

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$ (or more).

## Solution III

# Further Discussion II

## Problem III

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$ (or more).

## Solution III

- Factorize $P = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$.

# Further Discussion II

## Problem III

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$ (or more).

## Solution III

- Factorize $P = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$.
- Apply Solution II to calculate $\binom{N}{K} \bmod p_i^{k_i}$ for $1 \leq i \leq m$.

# Further Discussion II

## Problem III

Calculate

$$\binom{N}{K} \bmod P.$$

$0 \leq N, K \leq 10^9$, $2 \leq P \leq 10^6$ (or more).

## Solution III

- Factorize $P = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$.
- Apply Solution II to calculate $\binom{N}{K} \bmod p_i^{k_i}$ for $1 \leq i \leq m$.
- Merge them by CRT.

Q & A