

Trường hợp 1: $r = 0$ (subtask 2)

- Trường hợp 1.1: $n < p$. Vì p là số nguyên tố lớn hơn n nên $n!$ không chia hết cho p . Suy ra giả giai thừa của n cũng không chia hết cho p . Vậy $(k, v) = (-1, -1)$.
- Trường hợp 1.2: $n \geq p$. Suy ra $n!$ chia hết cho p . Do đó ta chỉ cần thay thừa số $k \geq 2$ nhỏ nhất mà k không chia hết cho p .

Nếu $n = 2$: $\Rightarrow p = 2 \Rightarrow (k, v) = (-1, -1)$.

Nếu $n > 2$: $p = 2 \Rightarrow (k, v) = (3, 1)$.

$$p \neq 2 \Rightarrow (k, v) = (2, 1).$$

Trường hợp 2: $r > 0$ (subtask 1, 3)

- Trường hợp 2.1: $n \geq 2p$. Suy ra $n!$ luôn chứa ít nhất 2 thừa số chia hết cho $p \Rightarrow$ Giả giai thừa của n luôn chia hết cho $p \Rightarrow (k, v) = (-1, -1)$.
- Trường hợp 2.2: $p \leq n < 2p$. Suy ra $n!$ chứa đúng 1 thừa số chia hết cho $p \Rightarrow n!$ chia hết cho $p \Rightarrow$ cần thay thừa số $k = p$.

Ta có $\frac{n!}{p}$ và p nguyên tố cùng nhau nên tồn tại số nghịch đảo của $\frac{n!}{p}$ theo modun p , vì vậy:

$$\frac{n!}{p} \cdot v \equiv r \pmod{p} \Leftrightarrow \left(\frac{n!}{p}\right)^{-1} \cdot \frac{n!}{p} \cdot v \equiv \left(\frac{n!}{p}\right)^{-1} \cdot r \pmod{p} \Leftrightarrow v \equiv \left(\frac{n!}{p}\right)^{-1} \cdot r \pmod{p}$$

Vậy ta lấy $v = \left(\left(\frac{n!}{p}\right)^{-1} \cdot r\right) \% p$, khi đó $v < p = k$.

Chú ý rằng do p nguyên tố, $\frac{n!}{p}$ không chia hết cho p nên ta tính $\left(\frac{n!}{p}\right)^{-1}$ theo định lí Fermat

$$\text{nhỏ: } \left(\frac{n!}{p}\right)^{-1} \equiv \left(\frac{n!}{p}\right)^{p-2} \pmod{p}.$$

- Trường hợp 2.3: $n < p$ ($\leq 10^7$). Ta cần thử từng giá trị của k ($2 \leq k \leq n$). Với mỗi giá trị của k , ta cần tìm v sao cho:

$$\frac{n!}{k} \cdot v \equiv r \pmod{p} \Leftrightarrow v \equiv r \cdot k \cdot (n!)^{-1} \pmod{p}$$

(Do $n!$ và p nguyên tố cùng nhau). Vậy ta lấy $v = (r \cdot k \cdot (n!)^{-1}) \% p$. Giá trị v này chỉ chấp nhận nếu $v < k$. Trong trường hợp không có giá trị k nào thỏa mãn thì đưa ra câu trả lời $(k, v) = (-1, -1)$.

Độ phức tạp thời gian của thuật toán là $O(p)$.