Problem 11118
(American Mathematical Monthly, Vol.111, December 2004)

Proposed by V. Dimitrov (Bulgaria).

Let p be an odd prime, and let k be a positive integer. Prove that

$$\sum_{j=0}^{k} \binom{k(p-1)}{j(p-1)} \equiv 2 + p(1-k) \mod p^2.$$

Solution proposed by Roberto Tauraso, Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy.

Let $\omega = e^{2\pi i/(p-1)}$ then it is well known that

$$\begin{bmatrix} n \\ r \end{bmatrix}_{p-1} := \sum_{j \equiv r \mod (p-1)} \binom{n}{j} = \frac{1}{p-1} \sum_{s=0}^{p-2} \omega^{-rs} (1+\omega^s)^n.$$

In order to prove that

$$\begin{bmatrix} k(p-1) \\ 0 \end{bmatrix}_{p-1} \equiv 2 + p(1-k) \mod p^2$$

we need the following preliminary results (the proofs are given later):

(a) $\begin{bmatrix} k(p-1) \\ 0 \end{bmatrix}_{p-1} = 2 + p(1-k) \mod p^2$ for $1 \leq k \leq p$;

(b) $\sum_{r=0}^{p-2} (-1)^r \begin{bmatrix} n \\ -r \end{bmatrix}_{p-1} = \sum_{r=0}^{p-2} (-1)^r \begin{bmatrix} n \\ r \end{bmatrix}_{p-1} = 0.$

(c) $\begin{bmatrix} p(p-1) \\ r \end{bmatrix}_{p-1} = (-1)^r (p+1) \mod p^2$ for $1 \leq r \leq p-2$;

Finally, by **(a)**, the proof can be completed by induction by showing that

$$\begin{bmatrix} n + p(p-1) \\ 0 \end{bmatrix}_{p-1} \equiv \begin{bmatrix} n \\ 0 \end{bmatrix}_{p-1} \mod p^2.$$

$$\begin{aligned}
\begin{bmatrix} n+p(p-1) \\ 0 \end{bmatrix}_{p-1} &= \frac{1}{p-1}\sum_{s=0}^{p-2}(1+\omega^s)^{n+p(p-1)} \\
&= \frac{1}{p-1}\sum_{s=0}^{p-2}(1+\omega^s)^{n}\sum_{t=0}^{p(p-1)}\binom{p(p-1)}{t}\omega^{st} \\
&= \sum_{t=0}^{p(p-1)}\binom{p(p-1)}{t}\cdot\frac{1}{p-1}\sum_{s=0}^{p-2}\omega^{st}(1+\omega^s)^{n} \\
&= \sum_{t=0}^{p(p-1)}\binom{p(p-1)}{t}\cdot\begin{bmatrix} n \\ -t \end{bmatrix}_{p-1} \\
&= \sum_{r=0}^{p-2}\begin{bmatrix} p(p-1) \\ r \end{bmatrix}_{p-1}\cdot\begin{bmatrix} n \\ -r \end{bmatrix}_{p-1} \\
&\equiv \begin{bmatrix} n \\ 0 \end{bmatrix}_{p-1} + (p+1)\sum_{r=0}^{p-2}(-1)^r\begin{bmatrix} n \\ -r \end{bmatrix}_{p-1} \mod p^2 \quad \text{(by } \mathbf{(a)} \text{ and } \mathbf{(c)}\text{)} \\
&\equiv \begin{bmatrix} n \\ 0 \end{bmatrix}_{p-1} \mod p^2 \quad \text{(by } \mathbf{(b)}\text{)}.
\end{aligned}$$

Proof of **(a)**. Since $(p-1)! = -1 \mod p$ then, for any $1 \leq j \leq p$ there is an integer q such that

$$(j(p-1))! = (jp-j)\cdots(jp-(p-1))\cdot(j-1)p\cdot((j-2)p+p-1)\cdots 1 = (-1+qp)p^{j-1}.$$

Hence there are integers q_1, q_2, q_3, q such that

$$\binom{k(p-1)}{j(p-1)} = \frac{(-1+q_1p)p^{k-1}}{(-1+q_2p)p^{j-1}\cdot(-1+q_3p)p^{k-j-1}} = (-1+qp)p \equiv -p \mod p^2.$$

Therefore

$$\begin{bmatrix} k(p-1) \\ 0 \end{bmatrix}_{p-1} = 2 + \sum_{j=1}^{k-1}\binom{k(p-1)}{j(p-1)} \equiv 2 + \sum_{j=1}^{k-1}(-p) \equiv 2 + p(1-k) \mod p^2.$$

Proof of **(b)**. Since $p-1$ even then

$$\begin{aligned}
\sum_{r=0}^{p-2}(-1)^r\begin{bmatrix} n \\ r \end{bmatrix}_{p-1} &= \sum_{r=0}^{p-2}(-1)^r\sum_{q=0}^{\lfloor n/(p-1)\rfloor}\binom{n}{(p-1)q+r} \\
&= \sum_{q=0}^{\lfloor n/(p-1)\rfloor}\sum_{r=0}^{p-2}(-1)^{(p-1)q+r}\binom{n}{(p-1)q+r} = \sum_{j=0}^{n}(-1)^j\binom{n}{j} = 0.
\end{aligned}$$

Proof of **(c)**. The case $r = 0$ follows from **(a)**. Assume that $1 \leq r \leq p-2$. Since

$$\binom{p(p-1)}{pr} \equiv \binom{p-1}{r} \mod p^2 \quad \text{and} \quad \binom{p(p-1)}{j} = 0 \mod p \quad \text{if } p \not| j$$

then

$$\begin{bmatrix} p(p-1) \\ r \end{bmatrix}_{p-1} = \sum_{q=0}^{p-1}\binom{p(p-1)}{q(p-1)+r} = \binom{p(p-1)}{pr} + pa_r \equiv \binom{p-1}{r} + pa_r \mod p^2$$

where a_r is the following integer

$$a_r \equiv \sum_{q=0, q\neq r}^{p-1}\frac{p-1}{q(p-1)+r}\binom{p(p-1)-1}{q(p-1)+r-1}.$$

By Lucas' Theorem

$$a_r \equiv \sum_{q=0}^{r-1} \frac{-1}{r-q} \binom{p-2}{q} \binom{p-1}{r-1-q} + \sum_{q=r+1}^{p-1} \frac{-1}{r-q} \binom{p-2}{q-1} \binom{p-1}{p+r-1-q} \mod p$$

Since

$$\binom{p-1}{j} \equiv (-1)^j \ , \ \binom{p-2}{j} \equiv (-1)^j (j+1) \ , \ \sum_{q=1}^{p-1} \frac{1}{q} \equiv 0 \mod p$$

then

$$a_r \equiv (-1)^r \left(\sum_{q=0}^{r-1} \frac{q+1}{r-q} + \sum_{q=r+1}^{p-1} \frac{q}{r-q} \right) \equiv (-1)^r \left(\sum_{q=0}^{r-1} \frac{1}{r-q} + \sum_{q=0 q \neq r}^{p-1} \frac{q}{r-q} \right)$$

$$\equiv (-1)^r \left(\sum_{q=1}^{r} \frac{1}{q} + \sum_{q=0 q \neq r}^{p-1} \frac{q-r}{r-q} + r \sum_{q=0 q \neq r}^{p-1} \frac{1}{r-q} \right) \equiv (-1)^r \left(\sum_{q=1}^{r} \frac{1}{q} + 1 \right) \mod p$$

Therefore

$$\begin{bmatrix} p(p-1) \\ r \end{bmatrix}_{p-1} \equiv \binom{p-1}{r} + p \left((-1)^r \left(\sum_{q=1}^{r} \frac{1}{q} + 1 \right) \right)_{\bmod p} \mod p^2.$$

□