Problem 11292
(American Mathematical Monthly, Vol.114, May 2007)

Proposed by D. Callan (USA).

Show that if p is a prime and $p \geq 5$ then p^2 divides $\displaystyle\sum_{k=1}^{p^2-1}\binom{2k}{k}$.

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

Consider the following identity proved by Zhi-Wei Sun and Hao Pan in *A combinatorial identity with applications to Catalan numbers*, Discrete Mathematics, vol. 306, no. 16, pp. 1921–1940: let l and m be nonnegative integers such that $m = 0 \mod 3$

$$\sum_{k=0}^{l}(-1)^{m-k}\binom{l}{k}\binom{m-k}{l+1}\binom{2k}{k+m-2l} = \binom{l}{m/3}\binom{2m/3}{l+1}$$

Let $l = p^2-1$ and $m = 2l = 2p^2-2$ and note that $m = 2p^2-2 = 0 \mod 3$ since $p = \pm 1 \mod 3$ (p is a prime greater than 3). Therefore the previous identity becomes

$$\sum_{k=0}^{p^2-1}(-1)^k\binom{p^2-1}{k}\binom{(2p^2-2)-k}{p^2}\binom{2k}{k} = \binom{p^2-1}{(2p^2-2)/3}\binom{2(2p^2-2)/3}{p^2}.$$

We will prove that for $0 \leq k \leq p^2-1$

$$(-1)^k\binom{p^2-1}{k}\binom{(2p^2-2)-k}{p^2}\binom{2k}{k} = \binom{2k}{k} \mod p^2 \tag{1}$$

and

$$\binom{p^2-1}{(2p^2-2)/3}\binom{2(2p^2-2)/3}{p^2} = 1 \mod p^2. \tag{2}$$

then the required identity easily follows because

$$\sum_{k=1}^{p^2-1}\binom{2k}{k} = \sum_{k=0}^{p^2-1}\binom{2k}{k} - \binom{2\cdot 0}{0} = 1-1 = 0 \mod p^2.$$

First note that

$$(-1)^k\binom{p^2-1}{k} = \prod_{j=1}^{k}\frac{j-p^2}{j} \equiv \prod_{i=1}^{\lfloor k/p\rfloor}\frac{i-p}{i} \mod p^2$$

and

$$\binom{(2p^2-2)-k}{p^2} = \binom{(2p^2-2)-k}{p^2-2-k} = \prod_{j=1}^{p^2-2-k}\frac{p^2+j}{j} \equiv \prod_{i=1}^{\lfloor (p^2-2-k)/p\rfloor}\frac{p+i}{i} \mod p^2.$$

Since for $k \neq -1 \mod p$ we have that

$$\lfloor (p^2-2-k)/p\rfloor + \lfloor k/p\rfloor = p-1,$$

then

$$(-1)^k\binom{p^2-1}{k}\binom{(2p^2-2)-k}{p^2} = 1 \mod p^2$$

and (1) holds for such k.

Identity (2) is verified by taking $k = (2p^2 - 2)/3$: k is an even number and $k = -1 \mod p$ implies that $3k = -3 = 2p^2 - 2 = -2 \mod p$ which is impossible.
Now assume that $k = -1 \mod p$ that is $k = ap - 1$ with $1 \leq a \leq p$. If $a = p$ then

$$\binom{2k}{k} = \binom{2p^2-2}{p^2-1} = \frac{(2p^2-2)\cdots(p^2+1)p^2}{(p^2-1)!} = \frac{p^2}{p^2-1}\prod_{j=1}^{p^2-2}\frac{p^2+i}{i} \equiv 0 \mod p^2$$

and (1) holds.
On the other hand, if $1 \leq a < p$ then by Lucas theorem

$$\binom{2k}{k} = \binom{2ap-2}{ap-1} \equiv \binom{2a-1}{a-1}\binom{p-2}{p-1} = 0 \mod p.$$

Morevorer

$$\binom{p^2-1}{k} = \binom{p^2-1}{ap-1} \equiv \binom{p-1}{a-1}\binom{p-1}{p-1} = \frac{(p-1)\cdots(p-(a-1))}{(a-1)!} = (-1)^{a-1} = (-1)^k \mod p$$

and

$$\binom{2p^2-2-k}{p^2} \equiv \binom{1}{1}\binom{p^2-2-k}{0} = 1 \mod p.$$

hence

$$(-1)^k\binom{p^2-1}{k}\binom{2p^2-2-k}{p^2}\binom{2k}{k} = (Ap+1)Bp \equiv Bp = \binom{2k}{k} \mod p^2$$

and (1) holds also in this case. □