Megoldás. A szám utolsó két számjegye p alapú számrendszerben a szám p^2-es maradéka. Ennek meghatározásához először megmutatjuk, hogy ha p prímszám, k pedig tetszőleges nemnegatív egész, akkor

$$\binom{(k+1)p}{p} \equiv k+1 \pmod{p}.$$

Ennek belátásához szükségünk lesz a következő észrevételre: ha két p-vel nem osztható egész szám p^2-tel osztva ugyanannyi maradékot ad, a hányadosuk pedig egész szám, akkor az p^2-tel osztva 1-et ad maradékul. Vagyis, ha a p-vel nem osztható a, b, x egész számokra $ax \equiv b \pmod{p^2}$ és $a \equiv b \pmod{p^2}$, akkor $x \equiv 1 \pmod{p^2}$. Valóban, ha $a(x-1) = ax - a$ osztható p^2-tel, akkor $x-1$ is osztható p^2-tel. Ugyanígy látható, hogy ha a nem osztható p-vel, akkor $c_1 \not\equiv c_2 \pmod{p^2}$ esetén $ac_1 \not\equiv ac_2 \pmod{p^2}$.

Legyen most k tetszőleges nemnegatív egész szám. Ekkor a

$$(kp+1)(kp+2)\dots(kp+p-1)$$

szorzatot teljesen kibontva, abban „majdnem minden” tag osztható lesz p^2-tel, azaz

$$(kp+1)\dots(kp+p-1) \equiv (p-1)! + kp(p-1)!\left(\frac{1}{1}+\frac{1}{2}+\dots+\frac{1}{p-1}\right) \pmod{p^2}.$$

Mivel $(p-1)!$ nem osztható p-vel, és az $1, 2, \dots, p-1$ számok p-vel osztva mind különböző (nemnulla) maradékot adnak, azért a p-vel nem osztható

$$\frac{(p-1)!}{1}, \frac{(p-1)!}{2}, \dots, \frac{(p-1)!}{p-1}$$

számok is mind különböző maradékot adnak p-vel osztva, így $p > 2$ miatt

$$(p-1)!\left(\frac{1}{1}+\frac{1}{2}+\dots+\frac{1}{p-1}\right) \equiv 1+2+\dots+(p-1) = \frac{p(p-1)}{2} \equiv 0 \pmod{p}.$$

Ezért

$$(kp+1)(kp+2)\dots(kp+p-1) \equiv (p-1)! \pmod{p^2},$$

ahonnan az előbb látottak szerint:

$$\binom{(k+1)p}{p} = \frac{(k+1)p}{p} \cdot \frac{(kp+1)(kp+2)\dots(kp+p-1)}{(p-1)!} \equiv (k+1)\cdot 1 \pmod{p^2}.$$

A bizonyított összefüggés szerint:

$$\sum_{i=1}^{p} \binom{i\cdot p}{p} \cdot \binom{(p-i+1)p}{p} \equiv \sum_{i=1}^{p} i\cdot(p-i+1) \pmod{p^2}.$$

A kapott összeget a számtani sorozatok és a négyzetszámok összegképletének felhasználásával tovább alakítva:

$$\sum_{i=1}^{p} i\cdot(p-i+1) = (p+1)\sum_{i=1}^{p} i - \sum_{i=1}^{p} i^2 = (p+1)\frac{p(p+1)}{2} - \frac{p(p+1)(2p+1)}{6} =$$

$$= (p+1)\frac{(3p^2+3p)-(2p^2+p)}{6} = \frac{p(p+1)(p+2)}{6}.$$

A $\frac{p(p+1)(p+2)}{6}$ hányados p^2-tel való osztási maradékát keresve elegendő $\frac{(p+1)(p+2)}{6}$-nak a p-vel vett maradékát meghatározni. Mivel $p > 3$ prím, a 6-tal való osztási maradéka 1 vagy 5 lehet.

Az első esetben, amikor $p = 6k+1$,

$$\frac{(p+1)(p+2)}{6} = \frac{(6k+2)(6k+3)}{6} = 6k^2+5k+1.$$

Ezt $p = 6k+1$-gyel maradékosan osztva: $6k^2+5k+1 = k(6k+1)+4k+1$, vagyis a maradék $4k+1$.

A második esetben, amikor $p = 6k+5$,

$$\frac{(p+1)(p+2)}{6} = \frac{(6k+6)(6k+7)}{6} = 6k^2+13k+7.$$

Maradékosan osztva $p = 6k+5$-tel: $6k^2+13k+7 = (k+1)(6k+5)+2k+2$, a maradék $2k+2$.

Így $\frac{p(p+1)(p+2)}{6}$-nak a p^2-tel való osztási maradéka az első esetben $p(4k+1)$, a másodikban pedig $p(2k+2)$.

Tehát ha $p = 6k+1$ alakú, akkor a p alapú számrendszerben az utolsó két számjegy $(4k+1)$ és 0, ha pedig $p = 6k+5$ alakú, akkor az utolsó két számjegy $(2k+2)$ és 0.