

۱- نشان دهید ۲- یک بابائینه مربعی درصفت عدد اول فرد p است اگر و تنها اگر $p \equiv 1, 2 \pmod{4}$.

۲- تمام جواب‌های معادله پهنجی $9x^4 - 19x^2 + 3 \equiv 0 \pmod{59}$ را تعیین کنید.

۳- فرض کنید $q > 2$ اول باشد، اگر $p = 2^q - 1$ نیز اول باشد، ثابت کنید که معادله

$$x^2 \equiv 3 \pmod{p}$$

حل پذیر نیست.

۴- حل پذیری معادلات پهنجی $x^2 \equiv 1993 \pmod{1997}$ و $x^2 \equiv 1993 \pmod{1999}$ را

بررسی کنید. (برای هر 3 عدد 1993 ، 1997 و 1999 اول هستند).

۵- معادله $(1999/1999)$ ، $(175/213)$ و $(14/331)$ را محاسبه کنید.

۶- فرض کنید $p = 2^{2n} + 1$ که $n \geq 1$. اگر p اول باشد، نشان دهید $3^{(p-1)/2} \equiv 1 \pmod{p}$.

بر p بخش پذیر است.

۷- فرض کنید p عددی اول و q کوچکترین بابائینه مربعی مثبت درصفت p باشد.

نشان دهید q اول است.