TEN 2009. Esercizi preliminari al crivello quadratico.

1. Sia p un numero primo.
   (a) Dimostrare che $\bar{x} \in \mathbb{Z}_p^*$ è un quadrato, ossia x è un quadrato modulo p, se e solo se $x^{\frac{p-1}{2}} \equiv 1 \bmod p$ (sfruttare il fatto che $\mathbb{Z}_p^*$ è ciclico).
   (b) Sia $\bar{x} \in \mathbb{Z}_p^*$ un quadrato. Quante radici quadrate ha in $\mathbb{Z}_p^*$?

2. Sia $p = 13$.
   (a) Determinare tutti i quadrati in $\mathbb{Z}_{13}^*$.
   (b) Per ogni quadrato $\bar{a} \in \mathbb{Z}_{13}^*$, determinare le radici quadrate di $\bar{a}$ in $\mathbb{Z}_{13}^*$.
   (c) Per ogni $a \in \mathbb{Z}$ che è un quadrato modulo 13, determinare *tutte le soluzioni* $x \in \mathbb{Z}$ della congruenza $x^2 \equiv a \bmod p$.

3. Sia p un numero primo che soddisfa $p \equiv 5 \bmod 8$ e sia a un quadrato modulo p.
   (a) Dimostrare che ci sono due possibilità: $a^{\frac{p-1}{4}} \equiv 1 \bmod p$ oppure $a^{\frac{p-1}{4}} \equiv -1 \bmod p$.
   (b) Verificare che se $a^{\frac{p-1}{4}} \equiv 1 \bmod p$, allora $a^{\frac{p+3}{8}}$ è una radice quadrata di a modulo p.
   (c) Verificare che se $a^{\frac{p-1}{4}} \equiv -1 \bmod p$, allora $2a \cdot (4a)^{\frac{p-5}{8}}$ è una radice quadrata di a modulo p (usare il seguente risultato: 2 *è un quadrato modulo p se e solo se* $p \equiv \pm 1 \bmod 8$).

4. Sia n un intero e sia p un primo.
   (a) Verificare che un intero della forma $x^2 - n$ è divisibile per p se e solo se n è un quadrato modulo p.
   (a) Sia n un quadrato modulo p e siano $\bar{a}$ e $\bar{b}$ le due radici quadrate di $\bar{n}$ in $\mathbb{Z}_p^*$. Determinare tutti gli interi della forma $x^2 - n$ che sono divisibili per p.

5. Usare la congruenza $294^2 \equiv 10^2 \bmod 1349$ per determinare una fattorizzazione non banale di 1349.

6. Sia n intero dispari (dunque $n \equiv 1, 3, 5, 7 \bmod 8$) e sia $x = 2k+1,\ k \in \mathbb{Z}$, un numero dispari. Si hanno le seguenti possibilità:

$$\begin{cases} n \equiv 3, 7 \bmod 8 \Rightarrow\ x^2 - n \text{ è divisibile per 2 e per nessun'altra potenza di 2;} \\ n \equiv 5 \quad \bmod 8 \Rightarrow\ x^2 - n \text{ è divisibile per 4 e per nessun'altra potenza di 2;} \\ n \equiv 1 \quad \bmod 8 \Rightarrow\ x^2 - n \text{ è divisibile per 8 e possibilmente per altre potenze } 2^k, \text{ per } k \geq 4. \end{cases}$$