Teoria Elementare dei Numeri Appello 2 25 febbraio 2015, ore 10-12.

COGNOME ..... *NOME* .....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche.*
NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

1. *Sia $n = 1457$. Avendo a disposizione le seguenti relazioni modulo n*

$$59^2 \equiv 3^4 \cdot 7, \quad 62^2 \equiv 2 \cdot 3 \cdot 5 \cdot 31, \quad 82^2 \equiv 2^7 \cdot 7, \quad 58^2 \equiv 2 \cdot 3^2 \cdot 5^2, \quad 43^2 \equiv 2^3 \cdot 7^2,$$

determinare un fattore non banale di n (almeno impostare il procedimento...).

Moltiplicando fra loro la prima, la terza e la quinta relazione, troviamo

$$(59 \cdot 82 \cdot 43)^2 \equiv (2^5 \cdot 7^2 \cdot 3^2)^2 \mod \text{n.}$$

Dunque modulo n

$$a = 59 \cdot 82 \cdot 43 \equiv 1140, \qquad b = 999, \qquad a + b \equiv 682, \quad a - b \equiv 141,$$

da cui ricaviamo

$$\gcd(682, 1457) = 31, \qquad \gcd(141, 1457) = 47$$

fattori non banali di n.

2. *Sia dato il primo $p = 61$.*
   (a) Determinare la più piccola radice primitiva $\bar{a}$ di $\mathbf{Z}_p^*$.
   (b) Calcolare il logaritmo discreto di $\bar{x} = \overline{42}$ in base $\bar{a}$.

Sol.: Abbiamo $p = 61$, $p - 1 = 60 = 2^2 \cdot 3 \cdot 5$

$$2^{12} \equiv 9, \quad 2^{20} \equiv 47, \quad 2^{30} \equiv -1 \mod 61.$$

Dunque $\bar{2}$ è la più piccola radice primitiva in $\mathbf{Z}_{61}^*$.

Innanzitutto $\log_{\bar{2}} \bar{2} = 1$, $\log_{\bar{2}} \overline{-1} = 30$, $\log_{\bar{2}} \bar{1} = 0$. Dalle relazioni

$$-1 \equiv 60 = 2^2 \cdot 3 \cdot 5, \quad 2 \equiv 63 = 3^2 \cdot 7, \quad 3 \equiv 64 = 2^6 \mod 61,$$

troviamo le seguenti relazioni fra i rispettivi logaritmi in base $\bar{2}$:

$$\begin{cases} \log \bar{3} + \log \bar{5} = \log \overline{-1} - 2 \log \bar{2} = 28 \\ 2 \log \bar{3} + \log \bar{7} = \log \bar{2} = 1 \\ \log \bar{3} = 6 \log \bar{2} = 6. \end{cases} \mod 60$$

Dunque possiamo ricavare $\log_{\bar{2}} \overline{7} = -11$ e

$$\log_{\bar{2}} \overline{42} = \log_{\bar{2}} \overline{2} + \log_{\bar{2}} \overline{3} + \log_{\bar{2}} \overline{7} = 1 + 6 - 11 = -4 \equiv 56 \mod 60.$$

3. *Caratterizzare i primi p per cui (-1) è un quadrato modulo p.*

Sol.: Se $p = 2$, allora $-1 \equiv 1$ che è un quadrato. Sia adesso p un primo > 2 (dispari). Abbiamo che -1 è un quadrato modulo p se e solo se $(-1)^{(p-1)/2} \equiv 1 \mod \text{p.}$ Questo significa che l'ordine di (-1) in $\mathbf{Z}_p^*$, che è uguale a 2 per ogni primo $p > 2$, divide l'intero $(p-1)/2$. Dunque $(p-1)/2$ è pari, ossia $(p-1)/2 = 2k$, con k intero. In altre parole

$$p - 1 = 4k \quad \Leftrightarrow \quad p \equiv 1 \mod 4.$$

4. *Stiamo cercando di fattorizzare l'intero n usando il metodo delle curve ellittiche, con smoothness bound B fissato. Dopo 999 cicli dell'algoritmo andati a vuoto, troviamo un fattore primo p di n usando la curva ellittica E. Quale proprietà verosimilmente ha $E(\mathbf{Z}_p)$, che le precedenti 999 curve ellittiche su $\mathbf{Z}_p$ non avevano?*

Sol.: Verosimilmente la curva $E(\mathbf{Z}_p)$ ha ordine B-smooth (vedi note).

5. *Sia p un numero primo $p \equiv 1 \mod 4$ e sia E la curva su $\mathbf{Z}_p$ di equazione $Y^2 = X^3 + X$.*
   (a) Verificare che, per ogni primo p come sopra, E definisce una curva ellittica su $\mathbf{Z}_p$.
   (b) Verificare che, per ogni p come sopra, il gruppo $E(\mathbf{Z}_p)$ non è ciclico.

Sol.: (a) Il discriminante della curva E di equazione $Y^2 = X^3 + X$ è uguale a $\Delta = 4 \not\equiv 0 \mod$ p, per ogni primo $p \equiv 1 \mod 4$ (che è dispari). Dunque E definisce una curva ellittica su $\mathbf{Z}_p$, per ogni primo $p \equiv 1 \mod 4$.

(b) Determiniamo i punti di ordine 2 su $E(\mathbf{Z}_p)$: sono i punti (x, y) con ordinata $y = 0$ e ascissa data da una radice del polinomio $X^3 + X$ in $\mathbf{Z}_p$. Il polinomio $X^3 + X = X(X^2 + 1)$ si annulla in 0 per ogni p e in altri due punti, ossia nelle due radici quadrate di -1 in $\mathbf{Z}_p$, se e solo se -1 è un quadrato modulo p. Dall'esercizio 3, sappiamo che ciò si verifica se e solo se $p \equiv 1 \mod 4$. Per questi primi, la curva $E(\mathbf{Z}_p)$ ha tre punti di ordine due. Questo dice che il gruppo $E(Z_p)$ non è ciclico, perché in un gruppo ciclico ci sono esattamente $\varphi(2) = 1$ elementi di ordine 2.