Teoria Elementare dei Numeri (Schoof) 1^o compito 11 dicembre 2006, ore 17:00–19:00.

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

Risolvere gli esercizi negli spazi predisposti. Accompagnare le risposte con spiegazioni *chiare ed essenziali*. Consegnare SOLO QUESTO FOGLIO. Ogni esercizio vale 6 punti.

1. Calcolare il logaritmo discreto di $7 \in \mathbf{Z}_{59}^*$ rispetto alla radice primitiva $g = 2 \pmod{59}$. Calcolare il logaritmo discreto di $11 \in \mathbf{Z}_{61}^*$ rispetto alla radice primitiva $g = 2 \pmod{61}$.

   Ci sono tanti modi per fare questo esercizio: per tentativi, con il metodo dei canguri, con il metodo "baby steps—giant steps" ... Qua usiamo il metodo del calcolo dell'indice: cerchiamo delle relazioni moltiplicative fra i primi piccoli.

   Abbiamo che $2^6 = 64 \equiv 5 \pmod{59}$ e quindi $\log(5) = 6$. Siccome $1 \equiv 60 = 4 \cdot 3 \cdot 5 \pmod{59}$ abbiamo che $0 = 2 + \log(3) + \log(5)$ e quindi $\log(3) = -8$. Infine abbiamo che $8 \cdot 7 = 56 \equiv -3 \pmod{59}$. Siccome il logaritmo di -1 è uguale a $(59-1)/2 = 29$, concludiamo che $\log(7) + 3 = 29 + \log(3) = 29 - 8 = 21$ e quindi $\log(7) = 18$.

   Similmente, per il secondo esercizio: siccome $2^6 \equiv 3 \pmod{61}$ si ha che $\log(3) = 6$. Dal fatto che $4 \cdot 3 \cdot 5 = 60 \equiv -1 \pmod{61}$ e $\log(-1) = (61-1)/2 = 30$ segue che $2 + \log(3) + \log(5) = 30$ e quindi $\log(5) = 30 - 2 - 6 = 22$. Infine, abbiamo che $11 \cdot 6 = 66 \equiv 5 \pmod{61}$ e quindi $\log(11) + 1 + \log(3) = \log(5)$, da cui $\log(11) = 22 - 1 - 6 = 15$.

2. Sia n un numero naturale. Calcolare $(n-1)! \pmod{n}$; cioè determinare $a \in \{0, 1, 2, \ldots, n-1\}$ tale che $(n-1)! \equiv a \pmod{n}$. *Spiegare la risposta!*

   Se n è primo, allora ogni $x = 1, 2, \ldots, n-1$ è invertibile e quindi esiste un unico elemento *inverso* $y = 1, 2, \ldots, n-1$ tale che $x \cdot y \equiv 1 \pmod{n}$. Se x è diverso da 1 e $n-1$, abbiamo che $x \neq y$. Accoppiando gli elementi con i loro inversi, troviamo che $(n-1)!$ è uguale ad un prodotto di tanti fattori "1" e di 1 e $n-1$. Questo implica che $(n-1)! \equiv 1 \cdot (n-1) = n-1 \pmod{n}$. Questa congruenza è anche valida per $n = 2$.

   Se n non è primo, allora sia p il divisore primo più piccolo. Siccome $\frac{n}{p} \leq n-1$, abbiamo che $n = p \cdot \frac{n}{p}$ divide $(n-1)!$ e quindi $(n-1)! \equiv 0 \pmod{n}$. Questo argomento non è valido se per caso succede che $p = \frac{n}{p}$. In questo caso abbiamo che $n = p^2$. Se $p \geq 3$, allora sia p che $2p$ sono $\leq n-1$ e quindi $n = p^2$ divide $(n-1)!$ Anche in questo caso abbiamo quindi che $(n-1)! \equiv 0 \pmod{n}$. Invece, se $p = 2$ e quindi $n = 4$, abbiamo che $(n-1)! = 6 \equiv 2 \pmod{4}$.

3. Calcolare $\varphi(2006)$, $\varphi(2007)$.

   Abbiamo che $2006 = 2 \cdot 17 \cdot 59$ e quindi $\varphi(2006) = 1 \cdot 16 \cdot 58 = 928$. Similmente, siccome $2007 = 3^2 \cdot 223$ abbiamo che $\varphi(2007) = 2007 \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{223}) = 6 \cdot 222 = 1332$.

4. Sia E la curva di equazione $Y^2 = X^3 - 4X - 1$ su $\mathbf{Z}_7$.
   (a) Controllare che si tratta di una curva ellittica.
   (b) Determinare $\#E(\mathbf{Z}_7)$. In altre parole, contare i punti di E su $\mathbf{Z}_7$.
   (c) È ciclico il gruppo $E(\mathbf{Z}_7)$? Spiegare la risposta.

(a) Il discriminante del polinomio $X^3 - 4X - 1$ è uguale a $4 \cdot (-4)^3 + 27 \cdot (-1)^2 \equiv -4 - 1 \equiv 2 \pmod 7$ e quindi non è congruo a zero modulo 7. Ecco perché l'equazione descrive una curva ellittica.
(b) Per i valori $X = 0, 1, 2, 3, 4, 5, 6 \pmod 7$ troviamo che $X^3 - 4X - 1$ è congruo rispettivamente a $-1, 3, -1, 0, -2, -1, 2 \pmod 7$ rispettivamente. Fra questi sette numeri, solo 0 e 2 sono quadrati. Siccome $0^2 = 0$ e $(\pm 3)^2 \equiv 2 \pmod 7$, troviamo il punto $(3, 0)$ e i due punti $(6, 3)$ e $(6, -3)$. Non dimenticando il punto all'infinito, abbiamo quindi trovato *quattro* punti.
(c) Il gruppo $E(\mathbf{Z}_7)$ ha quattro elementi. I punti in $E(\mathbf{Z}_7)$ hanno quindi ordine $1, 2$ oppure 4. Siccome $(6, 3) + (6, 3)$ è uguale al punto $(3, 0)$, vediamo che $(6, 3)$ non può avere ordine 1 o 2 e quindi necessariamente ha ordine 4. Il punto $(6, 3)$ è quindi un generatore e $E(\mathbf{Z}_7)$ è un gruppo ciclico.

5. Sia $n \in \mathbf{Z}$ un numero pari.
   (a) Per $n = 8, 10, 12$ fattorizzare $n^2 + 1$.
   (b) Spiegare perché i divisori primi di $n^2 + 1$ sono sempre congrui a 1 (mod 4).

Abbiamo che $8^2 + 1 = 65 = 5 \cdot 13$ e $12^2 + 1 = 145 = 5 \cdot 29$. Il numero $10^2 + 1 = 101$ è primo.

Sia p un divisore primo di $n^2 + 1$. Abbiamo necessariamente che $p > 2$. Siccome $n^2 \equiv -1 \pmod p$, vediamo che $n^4 \equiv 1 \pmod p$ mentre $n^k \not\equiv 1 \pmod p$ per $k = 1, 2, 3$. In altre parole, l'ordine di $\overline{n} \in \mathbf{Z}_p^*$ è uguale a 4. Siccome l'ordine di ogni elemento di $\mathbf{Z}_p^*$ divide l'ordine del gruppo $\mathbf{Z}_p^*$, concludiamo che 4 divide $p - 1$, come richiesto.