Teoria Elementare dei Numeri (Schoof) 4^o compito 12 settembre 2008, ore 10:30–12:30.

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. Per $m = 66$, 67 e 68 esibire un numero naturale n tale che $\varphi(n) = m$ oppure spiegare che non esiste.

   Siccome 67 é primo, abbiamo che $\varphi(67) = 66$. Per vedere che 67 e 68 non sono valori della funzione φ, osserviamo prima che $\varphi(m)$ divide $\varphi(m)$ quando m divide n. In particolare, $\varphi(n)$ è pari quando n è divisibile per 4 o per un numero primo dispari. E quindi se $\varphi(n)$ è dispari, allora $n = 1$ oppure 2. Concludiamo che 67 non è valore della funzione φ.

   Similmente, supponiamo che $\varphi(n) = 68 = 4 \cdot 17$. Se n è divisibile per il quadrato di un numero primo p dispari, allora necessariamente $p = 17$ e $\varphi(p^2) = 16 \cdot 17$ divide $\varphi(n)$. Contraddizione. Quindi n è una potenza di 2 per un prodotto di numeri primi dispari p distinti e $\varphi(n)$ è una potenza di 2 per il prodotto dei numeri $\varphi(p) = p - 1$. Esiste quindi un divisore primo $p \equiv 1 \pmod{17}$ di n. Siccome $1 + 17k$ non è primo per $k \geq 5$, abbiamo che $p \geq 103 = 1 + 6 \cdot 17$ e quindi $\varphi(n) \geq \varphi(p) \geq 102$ contraddizione.

2. Determinare tutti gli elementi $\overline{x}$ di $\mathbf{Z}_{1001}$ che soddisfano $\overline{x}^2 = \overline{1}$.

   Abbiamo che $1001 = 7 \cdot 11 \cdot 13$. Modulo $p = 7$, 11 e 13 le uniche soluzioni dell'equazione $X^2 \equiv 1 \pmod{p}$ sono $X \equiv \pm 1 \pmod{p}$. Per il Teorema Cinese del resto ci sono quindi $2 \cdot 2 \cdot 2 = 8$ soluzioni modulo $1001 = 7 \cdot 11 \cdot 13$. Esse sono $\overline{x} = \pm\overline{1}$, $\pm\overline{155}$, $\pm\overline{274}$ e $\pm\overline{428}$.

3. Sia $p > 2$ un numero primo. Spiegare perché ogni divisore d di $2^p - 1$ soddisfa $d \equiv 1 \pmod{2p}$.

   Basta far vedere che ogni divisore *primo* q di $2^p - 1$ soddisfa la congruenza. Se q divide $2^p - 1$, allora $\overline{2}$ ha ordine p nel gruppo $\mathbf{Z}_q^*$ e quindi p divide $q - 1$. Siccome q è anche dispari, abbiamo che $q \equiv 1 \pmod{2p}$ come richiesto.

4. Sia q un numero primo e siano $a, b \in \mathbf{Z}$. Dimostrare: se $a \equiv b \pmod{q}$, allora $a^q \equiv b^q \pmod{q^2}$.

   Se $a \equiv b \pmod{q}$, allora $b = a + kq$ per un certo $k \in \mathbf{Z}$. Adesso calcoliamo $b^q = (a + kq)^q$ modulo q^2. Siccome $(kq)^i \equiv 0 \pmod{q^2}$ per $i \geq 2$ abbiamo per la formula del binomio di Newton che $b^q \equiv a^q + \binom{q}{1} a^{q-1} kq \equiv a^q \pmod{q^2}$ come richiesto.

5. Sia E la curva ellittica di equazione $Y^2 = X^3 - X$. Esibire un numero primo $p > 2$ tale che la curva $E \pmod{p}$ possieda un punto di ordine 3.

   Per $p = 11$, il punto $P = (4, 4)$ ha la proprietà che $P + P = (4, -4) = -P$. Concludiamo che P ha ordine 3.