Teoria Elementare dei Numeri 2017 Appello 2 27 febbraio 2018, ore 9:30–11:30.

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. (a) Calcolare $\varphi(2^5 \cdot 3^3 \cdot 11)$, spiegando quali proprietà di φ (la funzione φ di Eulero) sono state usate.
   (b) Dimostrare almeno due di tali prorietà.

2. Sia p un numero primo e sia a un intero. Dimostrare che a è un quadrato modulo p se e solo se $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

3. (a) Mostrare che $\bar{5}$ è una radice primitiva di $\mathbf{Z}_{23}^*$.
   (b) Calcolare il logaritmo discreto di $\overline{14}$ rispetto alla radice primitiva $\bar{5}$.
   (c) Dedurre che anche $\overline{14}$ è una radice primitiva e quanto vale il logaritmo discreto di $\bar{5}$ in base $\overline{14}$.

4. Sia E la curva di equazione $Y^2 = X^3 + 1$ su Z_5.
   (a) Verificare che si tratta di una curva ellittica.
   (b) Determinare l'ordine del punto $(2, 2)$ nel gruppo $E(Z_5)$.

5. Sia n un intero. Supponiamo che valgano le seguenti congruenze modulo n:

$$399^2 \equiv 2^5 \cdot 3 \cdot 5, \qquad 763^2 \equiv 2^6 \cdot 3, \qquad 773^2 \equiv 2^6 \cdot 3^5, \qquad 976^2 \equiv 2 \cdot 5^3.$$

   Fra quali interi possiamo cercare potenziali fattori non banali di n? (è sufficiente impostare il calcolo...)

1. Vedi Nota sulla φ di Eulero.

2. Vedi Foglio7 degli esercizi svolti.

3. Poiché $5^2 \not\equiv 1 \mod 23$ e $5^{11} \not\equiv 1 \mod 23$ vediamo che 5 è una radice primitiva modulo 23. Una volta trovata una radice primitiva g, è molto facile determinare le altre: ogni radice primitiva ha la forma g^a, con $a \in \mathbf{Z}$ coprimo con $\varphi(p-1)$. Per esempio $5^{-1} \equiv 14$ è una radice primitiva modulo 23. Sia il logaritmo discreto di 14 rispetto alla radice primitiva 5 che il logaritmo discreto di 5 rispetto alla radice primitiva 14 sono uguali a -1.

4. Si verifica che $\Delta = 27 \not\equiv 0 \mod 5$, per cui E definisce una curva ellittica su $\mathbf{Z}_5$. Inoltre $E(\mathbf{Z}_5) = \{(0,1), (0,4), (2,2), (2,3), (4,0)\} \cup \infty$, per cui $\#E(\mathbf{Z}_5) = 6$. L'ordine del punto $(2, 2)$ è un divisore di $\#E(\mathbf{Z}_5)$, diverso da 1. La somma $P + P$ è uguale al punto $(0, 4)$. Questo dimostra che nessumo fra $P, P + P$ e $P + P + P$ è uguale a zero. L'ordine di P è quindi 6.

5. Moltiplicando fra loro la seconda e la terza relazione (alternativamente prima terza e quarta, oppure prima seconda e quarta) si ottiene la relazione quadratica

$$(763 \cdot 773)^2 \equiv (2^6 \cdot 3^3)^2 \mod n.$$

Potenziali fattori non banali di n sono $\gcd(763 \cdot 773 \pm 2^6 \cdot 3^3, n)$.