Crittografia (Schoof) 2^o compito 13 luglio 2010, ore 16:00–18:00.

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

Accompagnare le risposte con spiegazioni *chiare ed essenziali.* Ogni esercizio vale 7.5 punti.

1. Determinare due radici primitive distinte g ed h di $\mathbf{Z}_{23}^*$. Calcolare il logaritmo discreto di h rispetto alla radice primitiva g e il logaritmo discreto di g rispetto alla radice primitiva h.

3. Per ogni $n \in \mathbf{Z}_{>0}$, determinare il resto della divisione di $(n-1)!$ per n.

3. Sia E la curva di equazione $Y^2 = X^3 + 1$ su $\mathbf{Z}_5$.
   (a) Verificare che si tratta di una curva ellittica.
   (b) Determinare l'ordine del punto $(2, 2)$ nel gruppo $E(\mathbf{F}_5)$.

4. Sia $n \in \mathbf{Z}_{>1}$. Sia $a \in \mathbf{Z}$ e sia d un divisore di $n-1$ tali che
   - $a^d \equiv 1 \pmod{n}$;
   - $\mathrm{mcd}(a^{d/q} - 1, n) = 1$ per ogni divisore primo q di d.

   Dimostrare che se $d > \sqrt{n}$, allora n è primo.

   (Nella dimostrazione l'ordine di un certo elemento in un certo gruppo ha un ruolo importante. Spiegare bene perché tale elemento ha proprio quell'ordine).

1. Poiché $5^2 \not\equiv 1 \pmod{23}$ e $5^{11} \not\equiv 1 \pmod{23}$ 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 $\phi(p-1)$. 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.

2. Questo è l'esercizio 3 del primo foglio. Per $n = 1, 2, 3, 4$ il resto è uguale a $0, 1, 2, 2$ rispetttivamente. Se $n > 2$ è primo, allora $(n-1)!$ è congruo modulo n al prodotto degli elementi di $\mathbf{Z}_n^*$. Ogni elemento si cancella con il suo inverso. Gli unici elementi che sono *uguali* al loro inverso sono ± 1. Il prodotto vale quindi $-1 \cdot 1 \equiv n-1 \pmod{n}$.
   Se invece $n > 4$ non è primo, sia p il divisore primo più piccolo. Allora, sia p che n/p sono fattori del prodotto $(n-1)!$. Se sono *distinti* questo implica che $(n-1)! \equiv 0 \pmod{n}$. Se sono uguali, si ha che $n = p^2$. Poiché $n > 4$, i numeri p e $2p$ sono fattori *distinti* del prodotto $(n-1)!$ e quindi anche in questo caso si ha che $(n-1)! \equiv 0 \pmod{n}$.

3. Si controlla che si tratta di una curva ellittica su $\mathbf{Z}_5$ con 6 punti che hanno le coordinate in $\mathbf{Z}_5$. L'ordine del punto $(2, 2)$ è un divisore di $\#E(\mathbf{Z}_5) = 6$. La somma $P + P$ è uguale al punto $(0, -1)$. Questo dimostra che nessumo fra P, $P + P$ e $P + P + P$ è uguale a zero. L'ordine di P è quindi 6.

4. Questo è il quarto esercizio del compito precedente.