

Esercizi

9 giugno 2011

1. si consideri il gruppo moltiplicativo $G = (\frac{\mathbb{Z}}{3^n\mathbb{Z}})^*$;
 - Si dimostri che G è ciclico e un generatore è $g[-4]_{3^n}$;
 - si determini il logaritmo discreto di $[2]_{3^n}$ in base g (il risultato sarà dato a meno del segno)
2. Valutare il simbolo di Legendre $(\frac{7411}{9283})$, osservando che 7411 e 9283 sono entrambi primi congrui a 3 modulo 4.
3. Trovare che c'è un numero finito di numeri di Carmichael del tipo $3pq$ con p, q primi.
4. data la curva ellittica R definita dall'equazione $y^2 = x^3 + 8$ in $GF(1331)$, si dica, giustificando le risposte:
 - se E ha punti di ordine 11 ($1331 = 11^3$);
 - si determini l'ordine di E ;
 - si determini l'ordine del punto $P = (1, 3)$;
 - si determini la struttura del gruppo della curva su $GF(11)$;
 - si determini la possibile struttura del gruppo abeliano E .
5. Si fattorizzi il numero $n = 2701$ con il metodo ρ , usando la funzione $f(x) = x^3 + x + 1$, $x_0 = 1$. Si consiglia di considerare $x_k - x_j$ dove $j = 2^h - 1$ se k è un intero con $h + 1$ cifre binarie. (ci si fermerà a $x_6 - x_3$). Si consideri quindi la chiave pubblica $(2701, 5)$ (improbabile) e si trovi una chiave di decifratura. Si indichi la procedura per decifrare BOI (usiamo l'alfabeto delle 26 lettere) e se si vuole si provi a farlo.
6. Sapendo che $5^x \equiv 27 \pmod{103}$ si trovi x .
7. Si consideri la curva E di equazione: $y^2 = x^3 + 3$ su $K = GF(31)$.

- Si supponga noto che la curva ha 43 punti. Dati $A = (1, 2)$ e $B = (17, 24)$. Calcolare il numero a tale che $B = aA$.
 - Si calcoli $E[31]$;
 - Si dica, giustificando la risposta se E è supersingolare.
8. Sia E la curva di equazione $y^2 = x^3 + 7$ sul campo $K = GF(41)$; si provi
- il gruppo $E(GF(41^{2h+1}))$ della curva ellittica $y^2 = x^3 + 7$ sul campo $GF(41^{2h+1})$ ha un elemento di ordine 7 comunque si scelga $h \in \mathbb{N}$;
 - Si provi che 42 divide $41^{2h+1} + 1$ per ogni h .
9. Si dimostri che una m -pla $([x_1]_n, \dots, [x_m]_n) \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ è primitiva se e solo se

$$M.C.D.(n, x_1, \dots, x_m) = 1$$

10. Data la curva ellittica E su $GF(557)$ definita dall'equazione

$$y^2 = x^3 - 10x + 21,$$

se ne determini l'ordine, sapendo che il punto $P = (2, 3)$ ha ordine 189. Cosa si può dire della struttura del gruppo abeliano $E(GF(557))$.

11. Si determini l'ordine della curva

$$y^2 = x^3 + x + 1$$

sul campo $GF(5)$.

12. Si consideri la curva ellittica E

$$x^3 + 7x + 12 = y^2$$

sul campo $GF(103)$. Si provi che il punto $(19, 0)$ ha ordine 2. Sapendo inoltre che il punto $(-1, 2)$ ha ordine 13, si determini l'ordine di E .

13. Dato il gruppo G della curva ellittica E di equazione

$$y^2 = x^3 + x + 1,$$

siano $P = (0, 1)$ e $Q = (413, 959)$ due suoi punti. Supponendo di sapere che $\langle P \rangle$ ha cardinalità 1067, e che $Q \in \langle P \rangle$, si determini il logaritmo discreto di Q in base P .

14. Si provi Che $n \in \mathbb{Z}$ è un numero primo se e solo se $(n-1)! \equiv -1 \pmod{n}$.
15. Si dia una dimostrazione diretta dele Teorema di Dirichlet nel caso $a = 1$ Sia e m numero primo, ovvero si dimostri che se q è un numero primo, esistono infiniti primi p congrui 1 modulo q
16. Provare che la congruenza $x^4 \equiv -1 \pmod{p}$ ha soluzione se e solo se $p \equiv 1 \pmod{8}$.
17. Sia m un intero divisibile per r diversi primi p_1, \dots, p_r , $p_i \neq p_j$ se $i \neq j$. Si provi che la congruenza

$$x^2 \equiv 1 \pmod{m}$$

ha 2^r soluzioni distinte tra 0 e m .

18. Si calcoli $\left(\frac{42}{47}\right)$; $\left(\frac{5}{160465489}\right)$; $\left(\frac{3083}{3911}\right)$.
19. Dato un numero primo dispari p , si provi che -3 è un resto quadratico modulo p se e solo se $p \equiv 1 \pmod{3}$.
20. Detta Sia ξ una radice q -esima primitiva dell'unità in $F_{p^{q-1}}$. Detta G la quantità

$$G = \sum_{j=0, \dots, q-1} \binom{j}{q} \xi^j,$$

si provi che vale

$$G^2 = (-1)^{\frac{q-a}{2}} q.$$

21. Sia b un intero maggiore di 1 e sia p un primo dispari che non divida b , $b-1$ o $b+1$; si consideri l'intero $n = \frac{b^{2p}-1}{b^2-1}$. Si provi che n non è un numero primo, che $2p$ divide $n-1$ e che n è uno pseudoprimo rispetto alla base b .
22. Si provi che, comunque si scelga l'intero positivo b , esistono infiniti n che risultano pseudoprimi rispetto a b .
23. Si provi che nessun intero della forma $n = 3p$ ($p > 3$) primo può essere uno pseudo primo rispetto alle basi 2, 5, 7.
24. Si provi che, per ogni numero primo fissato r , ci sono solo un numero finito di numeri di Carmichael della forma rpq (con p, q primi)

25. Si provi che tutti i caratteri mod m (m è un intero positivo), si possono costruire a partire dai caratteri $\chi_1, \chi_2, \chi_3, \chi_4$ costruiti a lezione
26. Se N denota il numero di soluzioni della congruenza $x^n \equiv a \pmod{p}$ e n divide $p - 1$, allora

$$N = 1 \text{ se } a \equiv 0 \pmod{p},$$

$$N = \sum_x^n \chi(a) \text{ altrimenti}$$

dove $\sum_x^n \chi(a)$ è la somma di tutti i $\chi(a)$ tali che $\chi^n = \chi_0$ (carattere principale)

27. Determinare una classe di interi n della forma $n = p(2p - 1)$, con p e $2p - 1$ entrambi primi, tali che n sia uno pseudoprimo forte per il 25% delle basi possibili.
28. Si fattorizzi il numero $n = 8051$ con il metodo ρ , usando la funzione $f(x) = x^2 + 1, x_0 = 1$. Si consiglia di considerare $x_k - x_j$ dove $j = 2^h - 1$ se k è un intero con $h + 1$ cifre binarie. (ci si fermerà a $x_6 - x_3$).
29. Provare che se n è pseudoprimo di Eulero rispetto alla base $b \in \mathbb{Z}_n$, allora è uno pseudoprimo rispetto alla base b^{-1} .
30. Data la curva ellittica E su $GF(7)$

$$y^2 = x^3 + 2,$$

si determinino i punti di E e si trovi il gruppo $E(GF(7))$.

31. Si determini l'ordine della curva

$$y^2 = x^3 + x + 1$$

sul campo $GF(5)$.

32. Si consideri la curva ellittica E

$$x^3 + 7x + 12 = y^2$$

sul campo $GF(103)$. Si provi che il punto $(19, 0)$ ha ordine 2. Sapendo inoltre che il punto $(-1, 2)$ ha ordine 13, si determini l'ordine di E .

33. Dato il gruppo G della curva ellittica E di equazione

$$y^2 = x^3 + x + 1,$$

siano $P = (0, 1)$ e $Q = (413, 959)$ due suoi punti. Supponendo di sapere che $\langle P \rangle$ ha cardinalità 1067, e che $Q \in \langle P \rangle$, si determini il logaritmo discreto di Q in base P .