

Esercizi di Teoria dei numeri e crittografia

19 giugno 2008

1. Si provi Che $n \in \mathbb{Z}$ è un numero primo se e solo se $(n-1)! \equiv -1 \pmod n$.
2. Si provi che $[-1]$ è un quadrato in \mathbb{Z}_p se e solo se $p \equiv 1 \pmod 4$.
3. Si dimostri il Teorema di Dirichlet per $m = 8$, $a = -3, -1, 1, 3$. (Si ricorda che il Teorema dice che se $m, a \in \mathbb{N}$ e $\text{MCD}(a, m) = 1$ allora esistono infiniti primi congrui ad a modulo m).
4. Supponendo nota la formula

$$\sum_{j=1, \dots, n} j^2 = \frac{n(n+1)(2n+1)}{6}$$

si confronti (in termini di $O(f)$) il numero di bit operazioni richieste per ottenere ciascuno dei due membri dell'uguaglianza.

5. Si dimostri che la φ di Eulero non è suriettiva su \mathbb{N} . In particolare, se p è un numero primo, esiste $n \in \mathbb{N} : \varphi(n) = p$ se e solo se $p = 2$.
6. Si provi che gli ideali primi di \mathbb{Z} coincidono con i suoi ideali massimali.
7. Si calcoli $\left(\frac{42}{47}\right)$.
8. Si dimostri che il polinomio $f(x) = x^4 + 1$ è irriducibile in $\mathbb{Z}[x]$. È riducibile in $\mathbb{Z}_p[x]$ per ogni primo p . Scrivere la fattorizzazione per $p = 3, 5, 17$.
9. Detta 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

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

10. Calcolare $2^{1000000} \bmod 77$.
11. Dato il campo finito $GF(q)$ con $q = p^m$, e sia $f(x)$ un polinomio irriducibile di grado m su \mathbb{Z}_p . Allora due elementi di $GF(q)$ possono essere divisi in $O(\log^3 q)$ bit operazioni.
12. Dire se 7411 è un residuo quadratico modulo 9283.
13. Provare che 3 non è un residuo quadratico modulo ogni primo di Mersenne maggiore di 3.
14. Si provi che nessun intero della forma $n = 3p$ ($p > 3$) primo può essere uno pseudo primo rispetto alle basi 2, 5, 7.
15. 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)
16. Trovare tutti i numeri di Carmichael della forma $3pq$.
17. Sia

$$n = (6m + 1)(12m + 1)(18m + 1)$$

Provare che se m è dispari, n è uno pseudoprimo di Eulero per la metà delle possibili basi $b \in \mathbb{Z}_n^*$;

se n è pari, per un quarto.

18. Calcolare $\left(\frac{91}{167}\right)$.
19. Provare che $\left(\frac{-2}{p}\right) = 1$ se $p \equiv 1 \text{ o } 3 \pmod{8}$;
 $\left(\frac{-2}{p}\right) = -1$ se $p \equiv 5 \text{ o } 7 \pmod{8}$.
20. 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 $x_6 - x_3$). Si consideri quindi la chiave pubblica $(8051, 5)$ (improbabile) e si trovi una chiave di decifratura. Si indichi la procedura per decifrare BOI (usiamo l'alfabeto delle 26 lettere);
21. Valutare il simbolo di Legendre $\left(\frac{3083}{3911}\right)$, osservando che 7411 e 9283 sono entrambi primi congrui a 3 modulo 4.

22.

23. Trovare che c'è un numero finito di numeri di Carmichael del tipo $5pq$ con p, q primi.

24. 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} .

25. Data la curva ellittica E su $GF(7)$

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

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

26. Si determini l'ordine della curva

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

sul campo $GF(5)$.

27. 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 .

28. 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 .