

Esercizi di Teoria dei numeri e crittografia 2009

5 giugno 2009

1. Si provi Che $n \in \mathbb{Z}$ è un numero primo se e solo se $(n-1)! \equiv -1 \pmod n$.
2. 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).
3. Provare che la congruenza $x^4 \equiv -1 \pmod p$ ha soluzione se e solo se $p \equiv 1 \pmod 8$.
4. 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 .

5. Si calcoli $\binom{42}{47}$; $\binom{5}{160465489}$; $\binom{3083}{3911}$.
6. Dato un numero primo dispari p , si provi che -3 è un resto quadratico modulo p se e solo se $p \equiv 1 \pmod 3$.
7. 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

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

8. 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 .

9. Si provi che, comunque si scelga l'intero positivo b , esistono infiniti n che risultano pseudoprimi rispetto a b .
10. Si provi che nessun intero della forma $n = 3p$ ($p > 3$) primo può essere uno pseudo primo rispetto alle basi 2, 5, 7.
11. 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)
12. 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
13. 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)

14. 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.
15. 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 $x_6 - x_3$).
16. 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} .
17. Data la curva ellittica E su $GF(7)$

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

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

18. Si determini l'ordine della curva

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

sul campo $GF(5)$.

19. 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 .

20. 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 .