CR410 AA12/13 (Crittografia 1)

Raccolta dei Testi d'Esame

ESAME DI METÀ SEMESTRE **Roma, 3 Aprile 2013.**

---

1. Dato il numero binario $n = (101010110)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)
2. Determinare una stima per il numero di operazioni bit necessarie per calcolare $[\sqrt{a}]^{b^a} \bmod b$ dove $b \leq a^a$. *
3. Trovare le soluzioni $X \in \mathbf{Z}$ della congruenza $X^3 \equiv 1 \bmod 91$?
4. Mostrare che se $f(X) = aX^2 + bX + c \in \mathbf{Z}/k\mathbf{Z}[X]$, le moltiplicazioni nell'anello quoziente $\mathbf{Z}/k\mathbf{Z}[x]/(f(X))$ si possono calcolare in $O(\log^2 k)$ operazioni bit. Vale la stessa conclusione se $\deg f > 2$?
5. Si illustri il funzionamento dell'algoritmo di Stein (algoritmo binario) per calcolare il massimo comune divisore di 72 e 90.
6. Supponiamo $a, m \in \mathbf{Z}$, e $(a, m) = 1$. Dimostrare che l'inverso moltiplicativo $a^*(\bmod m)$ è una potenza di a. Spiegare perchè se m ha al più due fattori primi allora conoscere tale potenza è computazionalmente equivalente a fattorizzare m.
7. Dopo aver enunciato il criterio di Korselt per i numeri di Carmichael lo si applichi per mostrare che $2821 = 7 \times 13 \times 31$ è un numero di Carmichael.
8. Quale la probabilit che un numero minore di 100 coprimo con 14 risulti primo?
9. Calcolare la successione di Miller Rabin di 3 modulo 49.
10. Spiegare nei dettagli il funzionamento del crittosistema RSA.

ESAME DI FINE SEMESTRE **Roma, 28 Maggio, 2013.**

---

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:
   a. Fornire un esempio di un'equazione di Weierstrass singolare.
   b. E' vero che in alcuni gruppi ciclici il logaritmo discreto è particolarmente facile da calcolare?
   c. Fornire due esempi di campi finiti $\mathbf{F}_q$ in cui tutti gli elementi di $\mathbf{F}_q^* \setminus \{1\}$ sono generatori.
   d. Fornire un esempio di un polinomio primitivo in un campo con 9 elementi.
2. Enunciare e dimostrare il Teorema di struttura dei sottocampi di $\mathbf{F}_{p^n}$. Lo si utilizzi per costruire un esempio di campo finito con esattamente 5 sottocampi.
3. Supponiamo che n, m siano interi, che $m \equiv 5 \bmod 4n$, che $n \equiv 7 \bmod 10$. Calcolare il simbolo di Jacobi $\left(\frac{n}{m}\right)$.

---

* ESERCIZIO RELATIVO AL PROGRAMMA NON SVOLTO NELL'AA 2013/2014

4. Spiegare il funzionamento di alcuni sistemi crittografici che basano la propria sicurezza sul problema del logaritmo discreto.
5. Spiegare la rilevanza del metodo Baby-Steps-Giant-Steps nella teoria delle curve ellittiche su campi finiti.
6. Sia $E : y^2 = x^3 - x$. Determinare la struttura del gruppo $E(\mathbf{F}_5)$ e calcolare $\#E(\mathbf{F}_{125})$. E' possibile determinare anche la struttura di $E(\mathbf{F}_{125})$?
7. Dimostrare che se E è una curva ellittica definita su un campo finito $\mathbf{F}_q$ con caratteristica dispari da un'equazione $y^2 = x^3 + a_2x^2 + a_4x + a_6$, allora i punti di ordine 2 hanno la forma $(\alpha, 0)$ dove $\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6 = 0$. Si forniscano esempi di curve ellittiche con 0, 1 e 3 punti di ordine 2 e si spieghi percè non è possibilie che ve ne siano 2.
8. Scrivere e dimostrare le formula per l'inverso $-P$ e per il punto $2P$ del punto $P(x, y) \in E(\mathbf{F}_q)$ dove E è una curva ellittica definita da una equazione di Weierstrass generale.

APPELLO A **Roma, 7 Giugno, 2013.**

---

1. Si descriva un algoritmo per calcolare in tempo polinomiale la parte intera di $m^{1/5}$ per ogni intero positivo m.
2. Descrivere l'algoritmo di moltiplicazione di Karatsuba. *
3. Dimostrare che se p è primo, allora $x^4 \equiv 1 \bmod p$ ammette $\gcd(p-1, 4)$ soluzioni. Determinare un velore di m tale che $X^4 \equiv 1 \bmod m$ ammette esattamente 32 soluzioni.
4. Calcolare il simbolo di Legendre $\left(\frac{97543}{21345}\right)$ utilizzando le propritetà dei simboli di Jacobi.
5. Si illustri l'algoritmo di Euclide esteso con particolare riguardo alle relazioni ricorsive per il calcolo dell'identità di Bezout. Lo si abblichi per calcolare l'identità di Bezout tra 54 e 98.
6. Si determini la probabilità che un polinomio irriducibile su $\mathbf{F}_5$ di grado 6 risulti primitivo.
7. Determinare i polinomi minimi e gli ordini degli elementi di $\mathbf{F}_{16}$.
8. Considerare una curva ellittica E definita su un campo con 2^{10} elementi. Supponiamo che $P \in E(\mathbf{F}_{2^{10}})$ abbia ordine 7 e che $Q \in E(\mathbf{F}_{2^{10}})$ abbia ordine 19. Se sappiamo che $E(\mathbf{F}_{2^{10}})$ non è ciclico, cosa possiamo dire della sua struttura?
9. Sia $E : y^2 = x^3 + x$, Dimostrare che se $p \equiv 1 \bmod 4$ allora il gruppo $E(\mathbf{F}_p)$ non è ciclico. Determinare tale gruppo nel caso in cui $p = 3$.
10. Spiegare il funzionamento di tutti i protocolli crittografici incontrati nel corso.

---

* RELATIVO AL PROGRAMMA NON SVOLTO NELL'AA 2013/2014

APPELLO B **Roma, 1 Luglio 2013.**

1. Si descrivano le complessità delle operazioni elementari tra interi.
2. Descrivere l'algoritmo dei quadrati successivi in un qualsiasi monoide moltiplicativo discutendone la complessità.
3. Dimostrare che il gruppo moltiplicativo di un campo finito è ciclico.
4. Dopo aver descritto la nozione di base forte, si dimostri che tutte le basi modulo un primo sono forti e si fornisca un esempio di un numero composto e di una sua base forte (non banale cioè diversa da -1).
5. Si descriva e si dimostri il Teorema Cinese dei resti discutendo in particolare l'analisi della complessità per determinare le soluzioni di un sistema di congruenze.
6. Si descriva il reticolo dei sottocampi di $\mathbf{F}_{2^6}$ e per ciascun sottocampo proprio, si elenchino i polinomi irriducibili e quelli primitivi.
7. Determinare i polinomi minimi e gli ordini degli elementi di $\mathbf{F}_9$.
8. Fornite un esempio di curva ellittica definita su un campo con 25 elementi per cui $E(\mathbf{F}_{25}$ non è ciclico.
9. Sia $E : y^2 = x^3 5x + 8$ e siano $P = (6, 3), Q = (9, 10) \in E(\mathbf{F}_{37})$. Calcolare $2P$ e $P + Q$.
10. Spiegare il funzionamento di tutti i protocolli crittografici incontrati nel corso.

APPELLO C **Roma, 3 Febbraio 2014.**

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:
   a. E' vero che se E è una curva ellittica definita su $\mathbf{F}_{2^n}$, allora non ha mai un equazione della forma $y^2 = x^3 + ax + b$?
   b. E' vero che se tutti i fattori primi di $n - 1$ sono più piccoli di $\log n$, allora è possibile determinare un fattore non banale di n in modo rapido? come?
   c. E' vero che se $p > 3$, il polinomio $X^2 + 2 \in \mathbf{F}_p$ è irriducibile per alcuni valori di p ma non tutti?
   d. E' vero che esistono modi per moltiplicare interi con complessità inferiore a quella quadratica?*

2 Se $n \in \mathbf{N}$, sia $\tau(n)$ il numero dei divisori di n. Supponiamo che sia nota la fattorizzazione (unica) di $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Fornire una stima per il numero di operazioni bit necessarie per calcolare $\tau(n)$. (*Suggerimento: Usare il fatto che τ è una funzione moltiplicativa e calcolare una formula per $\tau(p^\alpha)$*).

3. Siano m, n interi tali che $m \equiv 3 \bmod 4$, che $m \equiv 2 \bmod n$ e che $n \equiv 1 \bmod 8$. Si calcoli il seguente simbolo di Jacobi: $\left(\frac{(11m+n)^7}{m}\right)$.

---

* ESERCIZIO RELATIVO AL PROGRAMMA NON SVOLTO NELL'AA 2013/2014

4. Illustrare l'algoritmo dei quadrati successivi in un gruppo analizzandone la complessità. Considerare la curva ellittica $E : y^2 = x^3 - x$. Illustrare l'algoritmo appena descritto calcolando $[5](1,0)$ dove $(1,0) \in E(\mathbf{F}_7)$.
5. Si dia la definizione di pseudo primo forte in base 2 e si mostri che se $n = 2^\alpha + 1$ è pseudo primo forte in base 2, allora $2^{2^\beta} \equiv -1 \bmod n$ per qualche $\beta < \alpha$.
6. Fissare una radice primitiva di $\mathbf{F}_{2^4}$ ed utilizzarla per simulare un scambio chiavi alla Diffie–Hellmann.
7. Dopo aver definito la nozione di polinomio primitivo su un campo finito, si calcoli la probabilità che un polinomio irriducibile f di grado 8 su $\mathbf{F}_5$ risulti primitivo?.
8. Fattorizzare $f(x) = (x^{12} + 5x^2 + 1)(x^2 + x + 2)(x^{10} + x^2 + 1)$ su $\mathbf{F}_2$ e determinare il numero di elementi del campo di spezzamento di f.
9. Dopo aver verificato che si tratta di una curva ellittica, determinare (giustificando la risposta) l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_7$
$$y^2 = x^3 - x + 5.$$

APPELLO X **Roma, 13 Settembre 2013.**

---

1. Si descrivano:
   -a- L'algoritmo dei quadrati successivi;
   -b- L'algoritmo MCD–binario;
   -c- L'algoritmo di Pollard per la fattorizzazione degli interi;
   -d- L'algorimo di Pholig–Hellman per il calcolo dei logaritmi discreti;
   -e- Dopo aver descritto la nozione di algoritmo probabilistico di tipo Montecarlo, l'algoritmo di Miller–Rabin.
2. Determinare ordine e struttura di $E(\mathbf{F}_5)$ dove $E : y^2 = x^3 + 2$.
3. Dopo aver descritto quali sono i fattori irriducibili in $\mathbf{F}_p[x]$ di $x^{p^6} - x$ (p primo), nel caso in cui $p = 2$, li si elenchino tutti specificando quali tra questi sono primitivi.
4. Siano n e m interi tali che $m \equiv 3 \bmod 4$, $m \equiv 2 \bmod n$ e $n \equiv 1 \bmod 8$. Si calcoli il simbolo di Jacobi $\left(\frac{(5m+n)^7}{m}\right)$.
5. Dimostrare che se $\mathbf{F}_q$ è un campo finito di caratteristica dispari, allor esiste sempre una curva ellittica su $\mathbf{F}_q$ con gruppo dei punti razionali non ciclico.
6. Si descrivano i principali algoritmi di cifratura e decifratura.