ESAME DI METÀ SEMESTRE **5 Aprile 2002**

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

2. Mostrare che le moltiplicazioni nell'anello quoziente $\mathbf{Z}/n\mathbf{Z}[x]/(x^d)$ si possono calcolare in $O(\log^2 n^d)$ operazioni bit mentre le addizioni in $O(\log n^d)$ operazioni bit.

3. Dato il numero binario $n = (10011100101)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)

4. Calcolare il massimo comun divisore tra 240 e 180 utilizzando sia l'algoritmo euclideo che quello binario. Calcolare anche l'identità di Bezout.

5. Dimostrare che se $n = p_1 \cdots p_{20}$ è un intero privo di fattori quadratici, e $f(x) \in \mathbf{Z}/n\mathbf{Z}[x]$ ha grado 10, allora la congruenza $f(x) \equiv 0 \bmod n$ è risolvibile se e solo se lo sono le 20 congruenze $\begin{cases} f(x) \equiv 0 \bmod p_1 \\ \vdots \\ f(x) \equiv 0 \bmod p_{20}. \end{cases}$
   Dedurre che la prima congruenza $f(x) \equiv 0 \bmod n$ ha al più 10^{20} soluzioni. Sapreste dare un esempio in cui le soluzioni sono esattamente 10^{20}?

6. Illustrare l'algoritmo dei quadrati successivi in un gruppo analizzandone la complessità. Fare anche un esempio.

7. Mettere in ordine di priorità e spiegare il significato di ciascuna delle seguenti operazioni:

   $$x\sim \qquad x \wedge y \qquad x\&y \qquad x{+}{+} \qquad x\backslash y \qquad x = y \qquad x\%y \qquad x|y \qquad x \ll n$$

8. 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 $\beta < \alpha$.

9. Scrivere un programma in Pari che produca due vettori v e w. In cui v contiene i primi 100 *pseudo-primi composti* in base 2 e il secondo i primi 100 *pseudo primi di Eulero composti* in base 2.

10. Implementare RSA utilizzando il sistema Pari e creando tre funzioni distinte (una per generare le chiavi, una per cifrare e una per decifrare).

ESAME DI FINE SEMESTRE **5 Giugno 2002**

1. Quale è la probabilità che un polinomio irriducibile f di grado 8 su $\mathbf{F}_7$ risulti primitivo?

2. Spiegare il metodo di fattorizzazione $p - 1$.

3. Fissare una radice primitiva di $\mathbf{F}_{5^2}$ ed utilizzarla per simulare un scambio chiavi alla Diffie–Hellmann

4. Fattorizzare $f(x) = (x^{10} + 3x^5 + 1)(x^2 + 2)(x^2 + 1)$ su $\mathbf{F}_5$ e dopo averne fissato un campo di spezzamento $\mathbf{F}$, si scrivano tutte le radici di $f(x)$ in $\mathbf{F}$.

5. Spiegare il funzionamento del crittosistema Massey–Omura sul gruppo dei punti razionali di una curva ellittica.

6. 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 $\mathbf{F}_7$

$$y^2 = x^3 - x + 5.$$

7. Spiegare l'algoritmo di Berlekamp.

8. Spiegare il significato delle seguenti funzioni di Pari:
ispseudoprimes(n); znprimroot(n); znstar(n); znorder(x); ffinit(p, n, x).

9. Implementare in pari il crittosistema di El Gamal.

10. Dato un gruppo ciclico G, sia g un suo generatore e p un primo tale che $p^4 \| \#G$. Supponiamo che X denoti il logaritmo discreto di $\alpha \in G$. Si scriva uno pseudo codice per calcolare $X \bmod p^4$.

ESAME FINALE **5 Giugno 2002**

1. Si stimi il numero di operazioni bit necessarie a calcolare la derivata di un polinomio di grado n^2 in cui tutti i coefficienti sono minori di n.

2. Si risolva il seguente sistema di equazioni di congruenze

$$\begin{cases} x^3 \equiv 1 \bmod 7 \\ x^2 \equiv 1 \bmod 5 \end{cases}.$$

3. Quale è la probabilità che un polinomio irriducibile f di grado 8 su $\mathbf{F}_7$ risulti primitivo?

4. Si illustri la nozione di pseudo primo di eulero e si indichi la sua applicazione in crittografia.

5. Fattorizzare $f(x) = (x^{10} + 3x^5 + 1)(x^2 + 2)(x^2 + 1)$ su $\mathbf{F}_5$ e dopo aver fissato un campo di spezzamento $\mathbf{F}$ per f, si scrivano tutte le radici di $f(x)$ in $\mathbf{F}$.

6. Spiegare il funzionamento del metodo dello scambio delle chiavi Diffie–Hellman sul gruppo dei punti razionali di una curva ellittica.

7. Dopo aver verificato che si tratta di una curva ellittica, determinare l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_7$

$$y^2 = x^3 - x + 5.$$

8. Si calcoli il seguente simbolo di Jacobi: $\left(\frac{234564}{134431}\right)$.

9. Scrivere in una sola riga il codice (in PARI) per ottenere:
   a Numero di cifre binarie di x;
   b L' inverso aritmetico di $a \in (\mathbf{Z}/n\mathbf{Z})^*$;
   c Un primo con al massimo m cifre binarie.

10. Scrivere un programma in PARI per ottenere un vettore contenente i numeri minori di 10^{20} che sono pseudoprimi forti, per almeno una base random.

ESAME FINALE **9 Luglio 2002**

(1) Sia m un intero dispari. Dopo aver dimostrato che ammette soluzione, si stimi il numero di operazioni bit necessarie a risolvere il seguente sistema

$$\begin{cases} X \equiv 1 \bmod m \\ X \equiv 2 \bmod m+1 \\ X \equiv 3 \bmod m+2. \end{cases}$$

(2) Si descriva un'algoritmo per calcolare $[\sqrt{m}]$, dove $m \in \mathbf{N}$ in tempo polinomiale

(3) Si descrivano i valori di $a \in \mathbf{F}_p$ per cui $x^2+a \in \mathbf{F}_p[x]$ è irriducibile e si dimostri che non è mai primitivo.

(4) Si dimostri che se m è un intero dispari composto, allora esiste sempre un base $a \in U(\mathbf{Z}/m\mathbf{Z})$ rispetto a cui m non è pseudo primo di Eulero. Quale è l'applicazione di questa proprietà nei test di primalità?

(5) Fattorizzare $f(x) = (x^{12}+3x^4+1)(x^2+x+2)(x^{10}+x^2+1)$ su $\mathbf{F}_2$ e determinare il numero di elementi del campo di spezzamento di f.

(6) Spiegare il funzionamento del crittosistema RSA e simularne un'applicazione con un modulo RSA di esattamente tre cifre.

(7) Dopo aver verificato che si tratta di una curva ellittica, determinare l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_{11}$

$$E : y^2 = x^3 - 1.$$

Quale è l'ordine del punto $(5,5)$ in $E(\mathbf{F}_{11})$?

(8) 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: $\left(\frac{(5m+n)^3}{m}\right)$.

(9) Si scriva un programma Pari che implementi il metodo di fattorizzazione di Pollard.

(10) Scrivere un programma in pari che verifichi se un numero n di cui è nota la fattorizzazione in primi ($n = p_1 \cdots p_t$) è o meno un numero di Carmichael.

ESAME FINALE **9 Settembre 2002**

(1) Si dia una stima (in funzione del parametro t) per il numero di operazioni bit necessarie al calcolo del determinante di una matrice 3×3 a coefficienti interi in cui gli elementi della prima colonna sono in valore assoluto minori di t, quelli della seconda colonna sono in valore assoluto minori di e^t e quelli della terza sono in valore assoluto minori di t^t.

(2) Si descriva un'algoritmo per calcolare in tempo polinomiale $2^m (\bmod\ m+1)$. Si stimi anche il numero di operazioni bit necessarie.

(3) Si enunci e dimostri la formula per il numero di polinomi irriducibili di grado 8 su $\mathbf{F}_p$. Quale è la probabilità che un polinomio di grado 4 monico su $\mathbf{F}_3$ e che non ammette zeri in $\mathbf{F}_3$ risulti irriducubile su $\mathbf{F}_3$?

(4) Descrivere il test di primalità di Miller Rabin spiegandone gli aspetti probabilistici.

(5) Si descrivano gli ordini degli elementi del campo di spezzamento del polinomio $x^4 + x + 1$ su $\mathbf{F}_2$.

(6) Spiegare il funzionamento del crittosistema Massey–Omura e simularne un'applicazione in un campo con 32 elementi.

(7) Dopo aver verificato che si tratta di una curva ellittica, determinare l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_7$

$$E : y^2 = x^3 - x + 1.$$

determinando l'ordine di ciascun punto.

(8) Sia m un intero tale che $m \equiv 17 \bmod 28$. Si calcoli (se è ben definito) il seguente simbolo di Jacobi: $\left(\frac{5m+7}{m^5}\right)$.

(9) Si scriva un programma Pari che verifichi se un polinomio di grado 3 a coefficienti in $\mathbf{F}_5$ è o meno primitivo.

(10) Scrivere un programma in pari che implementi il metodo di fattorizzazione ρ di Pollard.

ESAME FINALE **19 Febbraio 2003**

1. Si stimi il numero di operazioni bit necessarie a calcolare l'integrale a di un polinomio di grado n in cui tutti i coefficienti sono minori di e^n.

2. Si risolva il seguente sistema di equazioni di congruenze

$$\begin{cases} x^2 \equiv 4 \bmod 11 \\ x^3 \equiv 2 \bmod 5 \end{cases}.$$

3. Quale è la probabilità che un polinomio irriducibile f di grado 6 su $\mathbf{F}_{11}$ risulti primitivo?

4. Si illustri la nozione di pseudo primo forte e se ne indichi l' applicazione in crittografia.

5. Fattorizzare $f(x) = (x^{14} + 3x^7 + 1)(x^2 + 2)(x^2 + 1)$ su $\mathbf{F}_7$ e dopo aver fissato un campo di spezzamento $\mathbf{F}$ per f, si scrivano tutte le radici di $f(x)$ in $\mathbf{F}$.

6. Spiegare il funzionamento del metodo dello scambio delle chiavi Diffie–Hellman e simularne un applicazione in un campo finito con 19 elementi.

7. Dopo aver verificato che si tratta di una curva ellittica, determinare l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_5$

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

8. Si calcoli il seguente simbolo di Jacobi: $\left(\frac{983932}{72637}\right)$.

9. Scrivere in una sola riga il codice (in PARI) per ottenere:
   a Numero di cifre decimali di x;
   b Il resto della divisione euclidea di a per b;
   c Un più piccolo numero primo con 100 cifre binarie.

10. Scrivere un programma in PARI per ottenere un vettore contenente i numeri minori di 10^{20} che sono pseudoprimi di Eulero, per almeno una base random.