Università Degli Studi Di

Napoli

Federico II

Elaborato di Metodi algebrici in Crittografia

Numeri primi e test di primalità

Gabriele Intoccia P62000091

Indice

Capitolo 1

Storia dei numeri primi

La prima testimonianza dei numeri primi risale tra il 20.000 a.C. e il 18.000 a.C. Si tratta dell'Osso di Ishango, ritrovato nel 1950 tra i monti dell'Africa equatoriale Centrale.

Figura 1.1: Osso di Ishango

In una delle colonne in cui è suddiviso l'osso compaiono i numeri primi 11, 13, 17 e 19.

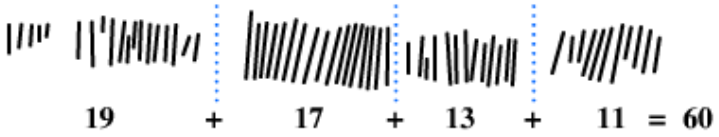

Figura 1.2: Terza colonna, dal basso verso l'alto

Storici e ricercatori, nell'interpretazione di questo reperto, escludono ovviamente che i paleolitici avessero conoscenza dei numeri primi e che quindi che si trattasse di una coincidenza.

Un'altra testimonianza dei numeri primi risale al secondo millennio a.C., periodo in cui in Mesopotamia furono trovate alcune tavolette contenenti le soluzioni di problemi aritmetici che, per essere risolti, richiedevano una buona conoscenza della fattorizzazione in primi. Allo stesso millennio appartiene anche il papiro di Rhind (trascritto intorno al 1650 a.C.), che contiene alcune espansioni in frazioni egizie dei numeri nella forma $\frac{2}{n}$ (con n numero dispari compreso fra 5 e 101).

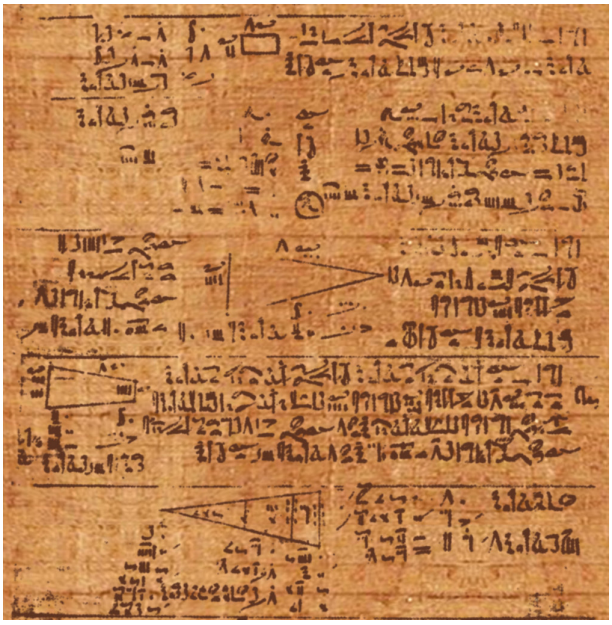

Figura 1.3: Papiro di Rhind

Tuttavia le prime testimonianze sopravvissute dello studio esplicito dei numeri primi provengono dalla matematica dell'antica Grecia; infatti la prima definizione di numero primo è quella fornita da Euclide nel VII libro degli *Elementi* (300 a.C. circa):

> *Numero primo è quello che è misurato (cioè diviso) soltanto dall'unità.*

Sempre gli *Elementi* di Euclide dimostrarono l'infinità dei numeri primi e il teorema fondamentale dell'aritmetica.
Sempre di origine greca è il Crivello di Eratostene, un antico algoritmo per trovare tutti i numeri primi fino a un dato limite, che verrà illustrato nel Capitolo successivo. L'interesse verso di i numeri primi riprese vigore nel XVII

secolo, con le dimostrazioni di nuovi e importanti risultati alcuni dei quali dovuti a Pierre de Fermat. Egli espresse molte delle sue scoperte sottoforma di congettura, quindi senza provvedere alle relative dimostrazioni, che furono invece furono trovate nel XVIII secolo dal matematico svizzero Leonhard Euler, noto in Italia come Eulero. Fermat enunciò (senza dimostrazione) anche il piccolo teorema di Fermat (successivamente dimostrato da Leibniz ed Eulero) che costituisce uno dei test di primalità.
Sempre nel XVII secolo il monaco francese Marin Mersenne pose l'attenzione sui primi della forma $2^p - 1$, con p primo, che oggi sono chiamati in suo onore, primi di Mersenne.
Invece a Christian Goldbach, è attribuita la sua omonima congettura secondo cui ogni numero pari è la somma di due numeri primi.
Sull'applicazione dei numeri primi all'analisi si ottennero importanti risultati grazie a Legendre e Gauss, i quali ipotizzarono che il numero di numeri primi minori o uguali a $x > 0$ reale, fosse asintoticamente uguale alla funzione $\frac{x}{logx}$.

Molti matematici hanno lavorato su test di primalità per numeri maggiori di quelli in cui la divisione di prova è praticamente applicabile, come ad esempio il test di Pépin per i numeri di Fermat (1877), il teorema di Proth, il test di primalità di Lucas-Lehmer e il test di primalità di Lucas generalizzato. Dal 1951 molti numeri primi dal valore elevato sono stati trovati utilizzando questi test grazie all'ausilio di computer. La ricerca di numeri primi sempre più grandi ha generato interesse anche al di fuori dei circoli matematici, attraverso la Great Internet Mersenne Prime Search e altri progetti di calcolo distribuito. L'idea che i numeri primi avessero poche applicazioni al di fuori

della matematica pura andò in frantumi negli anni '70 quando furono inventati la crittografia a chiave pubblica e il sistema crittografico RSA.
Nel Capitolo successivo verranno illustrati sia alcuni importanti risultati ottenuti e già citati, sia alcuni test di primalità.

Capitolo 2

Numeri Primi

2.1 Introduzione ai numeri primi

Una definizione rigorosa di numero primo è la seguente:

Definizione 2.1. *Un numero primo p è un intero maggiore di 1 che non ha altri divisori a parte p e 1.*

La primalità di un numero è legata all'irrudicibilità; infatti, dato A un anello unitario, possiamo definire l'irriducibilità e la primalità come segue:

Definizione 2.2. *Un elemento $a \in A$ non nullo e non invertibile si dice irriducibile se ogni volta che a si scrive come prodotto $a = bc$ con b e c in A, allora o l'elemento b oppure l'elemento c è invertibile.*

Definizione 2.3. *Un elemento $a \in A$ non nullo e non invertibile si dice primo se ogni volta che a divide un prodotto bc con b e c in A, allora divide uno dei due fattori. Ovvero*

$$a|bc \quad allora \quad a|b \quad oppure \quad a|c$$

Scopo di questo paragrafo è la caratterizzazione dei numeri primi. Il primo importante risultato, già citato nel precedente capitolo, è il Teorema Fondamentale dell'Aritmetica, esposto da Euclide. Prima di enunciarlo risulta fondamentale la seguente proposizione che lega con condizione necessaria e sufficiente i concetti di primalità e irriducibilità in $\mathbb{Z}$.

Teorema 2.1. *Un numero intero positivo $p > 1$ è irriducibile se e solo se vale la seguente proprietà:*
(P) ogni qualvolta p divide un prodotto ab, allora o p divide a oppure p divide b.

Dimostrazione. Supponiamo che p sia irriducibile e proviamo che vale la (P). Supponiamo dunque che p divida ab e che p non divida a. Poichè p non divide a, e poichè p non ha altri fattori che p e 1, si ha che p e a non hanno fattori non banali in comune, ossia $MCD(a, p) = 1$. Quindi esistono interi s e t tali che $1 = sa + tp$. Moltiplicando per b ambo i membri, si ottiene $b = sab + tpb$. Dato che $p|ab$ e $p|p$, si conclude che $p|b$.
Viceversa, supponiamo che valga la (P). Se p non fosse primo, avremmo $p = hk$ con h, k interi minori di p. D'altra parte $p|hk = p$ e quindi o $p|h$ oppure $p|k$, relazioni entrambe assurde, perchè h e k sono minori di p. □

Teorema 2.2 (Teorema Fondamentale dell'Aritmetica)**.** *Sia n un intero maggiore di 1. Allora*

$$n = p_1^{h_1} p_2^{h_2} p_3^{h_3} \cdots p_s^{h_s}$$

dove $p_1, p_2, p_3, ..., p_s$ sono numeri primi distinti e gli esponenti h_j sono positivi, per ogni $j = 1, ..., s$. Inoltre l'espressione di n, detta decomposizione in fattori primi o fattorizzazione di n, è unica a meno dell'ordine.

Dimostrazione. - **Esistenza della fattorizzazione.**
Procederemo per induzione sull'intero n da fattorizzare. Se $n = 2$ l'asserto è ovvio. Supponiamo allora di avere provato l'esistenza di una fattorizzazione per ogni intero positivo k, con $2 \leq k < n$, e dimostriamo la stessa cosa per n. Se n è primo non c'è nulla da dimostrare. Sia quindi n riducibile: siccome possiamo scrivere $n = ab$, con a e b positivi ed entrambi maggiori di 1 e quindi minori di n. Allora, per l'ipotesi induttiva, a e b sono fattorizzabili in un prodotto di primi

$$a = p_1 p_2 \dots p_r \quad b = \bar{p}_1 \bar{p}_2 \dots \bar{p}_s$$

Quindi

$$n = p_1 p_2 \dots p_r \bar{p}_1 \bar{p}_2 \dots \bar{p}_s$$

Pertanto basta raggruppare, a secondo membro della precedente uguaglianza, i numeri primi fra loro uguali per ottenere l'asserto.
- **Unicità della fattorizzazione.** Per dimostrare l'unicità della fattorizzazione per ogni intero n, procederemo per induzione sul numero m di fattori irriducibili di una qualche fattorizzazione di n. Si noti che il numero di fattori che appare nella fattorizzazione è $m = h_1 + h_2 + ... + h_s$. Se $m = 1$, significa che il numero n che ha quella come fattorizzazione è un primo p. Supponiamo che $n = p$ abbia un'altra fattorizzazione

$$n = q_1^{k_1} q_2^{k_2} q_3^{k_3} \cdots q_t^{k_t}$$

Essendo p un primo che divide il secondo membro esso dividerà uno dei fattori del secondo membro, ad esempio $p|q_1$ (per la proposizione precedente). Anche q_1 è primo, quindi non ha fattori propri, da cui $p = q_1$. Per la legge di cancellazione valida in $\mathbb{Z}$, si ottiene

$$1 = q_1^{k_1-1} q_2^{k_2} \dots q_t^{k_t}$$

Questa relazione implica che tutti gli esponenti al secondo membro sono nulli, altrimenti avremmo un prodotto di interi maggiori di 1 il cui prodotto dà 1. Dunque il secondo membro si riduce a q_1 e quindi $p = q_1$ è l'unica fattorizzazione di n. Abbiamo così provato la base dell'induzione. Supponiamo ora che l'unicità della fattorizzazione sia stata dimostrata per ogni intero che abbia una fattorizzazione in $m-1$ fattori irriducibili. Sia n un intero che ha una fattorizzazione in m fattori irriducibili. Siano allora

$$n = p_1^{h_1} p_2^{h_2} \dots p_s^{h_s} = q_1^{k_1} q_2^{k_2} \dots q_t^{k_t}$$

due fattorizzazioni di n in fattori irriducibili la cui fattorizzazione di sinistra ha m fattori irriducibili, cioè $h_1 + h_2 + ... + h_s = m$. Ora, p_1 è un primo che divide il secondo membro, quindi dividerà ad esempio q_1 (grazie ancora la proposizione precedente). Come prima, risulta $p_1 = q_1$, e quindi, per la legge di cancellazione, si ha

$$p_1^{h_1} p_2^{h_2} \dots p_s^{h_s} = q_1^{k_1} q_2^{k_2} \dots q_t^{k_t}$$

dove al primo membro il numero di fattori irriducibili è $m-1$. Per l'ipotesi induttiva vale in questo caso l'unicità della fattorizzazione e dunque i q_j coincidono con i p_i a meno dell'ordine. E' allora chiaro che anche la fattorizzazione di n è unica. □

Un altro importante risultato di Euclide è quello sull'infinità dei numeri primi.

Teorema 2.3. *Esistono infiniti numeri primi.*

Dimostrazione. Supponiamo che l'insieme dei numeri primi sia finito, costituito ad esempio dai numeri $p_1 < p_2 < ... < p_n$. Consideriamo il numero $N = p_1 \dots p_n + 1$. Questo numero non è primo perchè maggiore di p_n che, per ipotesi, è il numero primo più grande. Allora N ha la decomposizione in fattori primi

$$N = p_1^{h_1} \dots p_s^{h_s}$$

con almeno uno dei numeri $h_1, ..., h_n$ positivo. Supponiamo sia $h_i > 0$. Allora $p_i|N$. Inoltre $p_i|(N-1) = p_1 \dots p_n$. Quindi $p_i|1 = N - (N-1)$, il che è assurdo, dato che $p_i > 1$. □

Del teorema precedente esistono in realtà molte dimostrazioni, una di queste è basata su un teorema di Eulero.

Teorema 2.4. *La serie dei reciproci dei numeri primi diverge. Ossia se* $\{p_1, ..., p_n, ...\}$ *è la successione, eventualmente finita, di tutti i numeri primi in ordine crescente, si ha*

$$\sum_{n=1}^{\infty} \frac{1}{p_s} = \infty$$

La dimostrazionee di questo teorema è basata sulla funzione zeta di Riemann.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Segnaliamo ancora un altro famoso risultato ottenuto da Dirichlet, da cui pure segue l'infinità dell'insieme dei numeri primi:

Teorema 2.5. *Siano n, k interi positivi primi tra loro. Vi sono infiniti numeri primi p tali che $p \equiv k (\mathrm{mod}\, n)$.*

Nessuna dimostrazione consente di stabilire quanti sono i numeri primi minori di un fissato numero. In particolare se, per ogni numero reale $x > 0$, indichiamo con $\pi(x)$ il numero di primi p tali che $p \leq x$, non esiste una formula per il calcolo di tale funzione in termini di funzioni elementari ma, come vedremo nel successivo paragrafo, essa si può approssimare con una funzione elementare.

2.2 Teorema dei numeri primi

Il teorema dei numeri primi descrive la distribuzione asintotica dei numeri primi tra gli interi positivi. Formalizza l'idea intuitiva che i numeri primi diventano meno comuni man mano che crescono quantificando con precisione la velocità con cui ciò si verifica.
Introduciamo $\pi(x)$ con $x \geq 1$ funzione di conteggio primi, ovvero la funzione che conta il numero di numeri primi minori o uguali a un numero reale x. Un primo risultato importante, congetturato da Gauss e da Legendre, è che $\pi(x)$ fosse asintoticamente uguale alla funzione $x/(log(x))$, ossia che valesse la relazione di limite

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{log(x)}} = 1$$

nel senso che il limite del quoziente delle due funzioni $\pi(x)$ e $x/log(x)$ all'aumentare di x è 1. Questa congettura in letteratura è nota come legge

asintotica della distribuzione dei numeri primi. Un'affermazione equivalente è

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1$$

dove $\mathrm{li}(x)$ è la funzione integrale logaritmica.

Un passo importante verso tale congettura fu fatto nel 1851 da Chebishev, che provò il seguente teorema:

Teorema 2.6. *Esistono due numeri A e B, con $0 < A \leq 1$ e $1 \leq B \leq 2$, tali che, per ogni $n \in N$ sufficientemente grande, valga la relazione*

$$A\frac{n}{log(n)} \leq \pi(x) \leq B\frac{n}{log(n)}$$

La congettura di Legendre e Gauss fu provata solo alla fine del XIX secolo da Hadamard e de la Vallèe Poussin con metodi analitici (utilizzando le proprietà della funzione zeta di Riemann). Tale teorema è noto come il Teorema dei Numeri Primi.

Osserviamo che al teorema dei numeri primi si può dare una interpretazione probabilistica: dato un intero positivo n, la probabilità che un intero positivo p scelto a caso tra 2 e n sia primo, è $\pi(n)/n$ che per n molto grande è dello stesso ordine di grandezza di $1/log(n)$.

2.2.1 Sperimentazione

Interesse di questa sezione è quella di sperimentare i risultati ottenuti dal Teorema dei numeri primi. Innanzitutto si è implementato su Matlab un codice per la funzione di conteggio di primi. Esso ha come input (n_1, n_2), estre-

mi dell'intervallo degli interi dove vogliamo "contare" i primi, x intervallo generico, e come output la funzione di conteggio di primi.

```
function [C]=CountPrimes(n1,n2,x)
Counter = 0;
z=length(x);
y = isprime(x);
C=zeros(1,z);
for i = n1:n2
   if y(i) == true
      Counter = Counter + 1;
   elseif y(i)== false
       Counter=Counter;
   end
   C(i)=C(i)+Counter;
end
fprintf('pi(x) = %d\n', Counter)
plot(x,C,'-')
end
```

Figura 2.1: Algoritmo per la funzione conteggio di primi

per $n_1 = 1$ e $n_2 = 60$ otteniamo il seguente plot della funzione

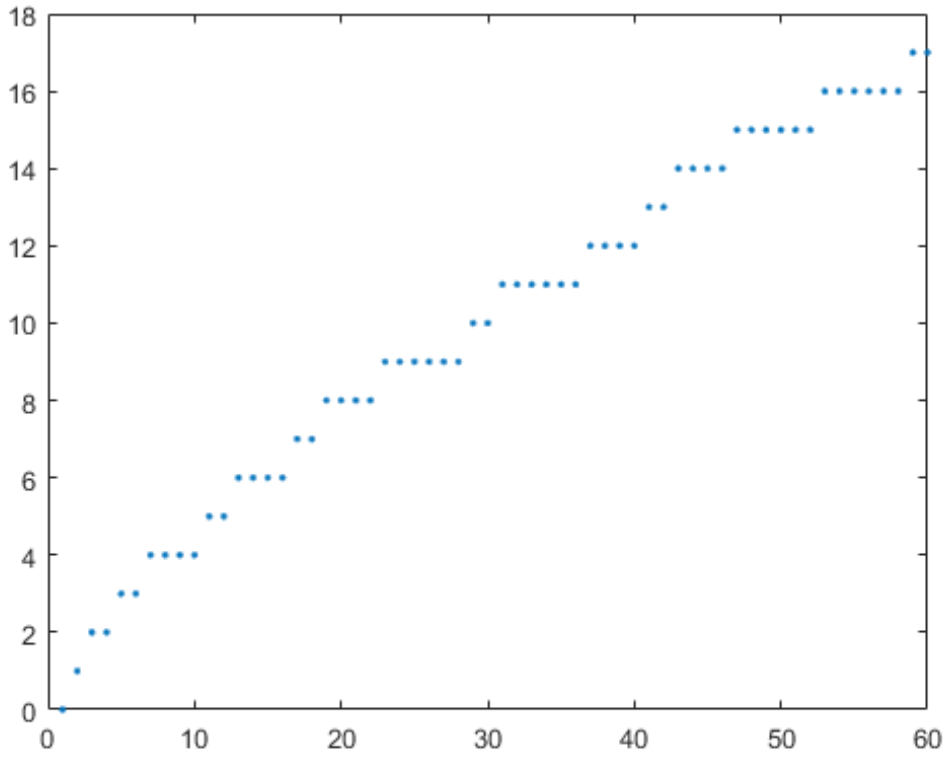

Figura 2.2: Funzione conteggio di primi per $n = 60$

Vogliamo ora confrontare la funzione $\pi(x)$ con l'approssimazione $x/log(x)$ e li(x). Si è dunque utilizzata la funcion `logint(x)` che ci restituisce il logaritmo integrale. Per $n = 10^4$ riportiamo il seguente plot:

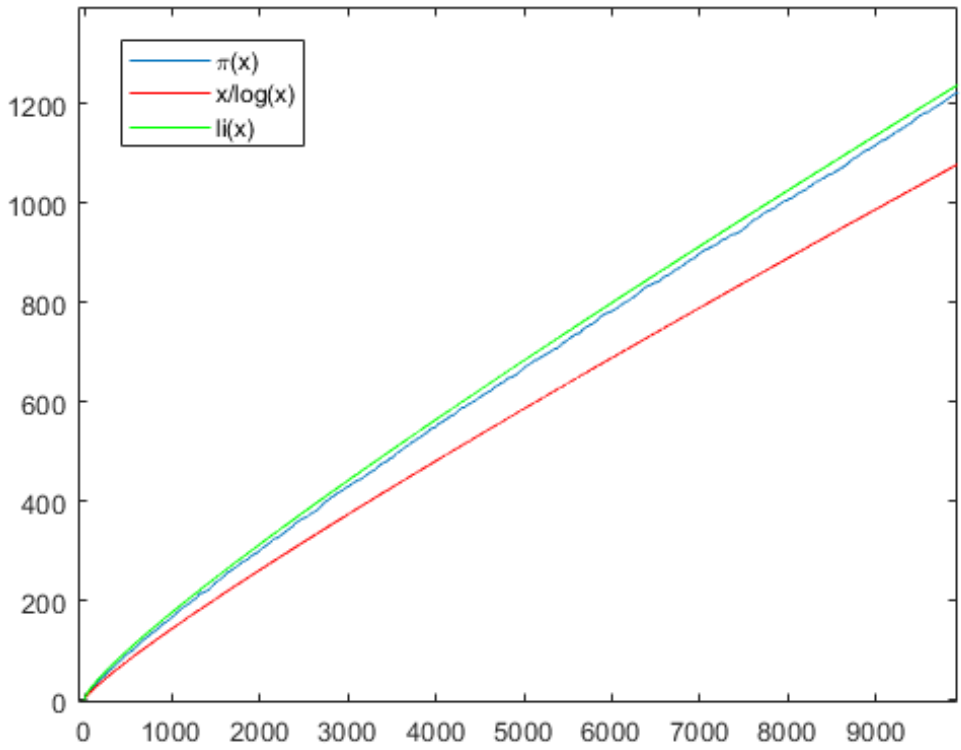

Figura 2.3: Comparazione tra le funzioni $pi(x)$, $x/logx$ e $li(x)$

Si può notare che l'approssimazione di $\pi(x)$ con $li(x)$ risulta essere di gran lunga migliore di quella con $x/logx$.

E' quindi necessario fare alcune considerazioni sull'errore. Dalla Figura 2.3 si può notare intutivamente che l'errore assoluto che si commette approssimando $\pi(x)$ è molto più piccolo quando lo si approssima con $li(x)$ piuttosto che con $x/logx$. Infatti è importante a tal riguardo menzionare due risultati: il primo è dovuto a de la Vallée-Poussin che dimostrò che l'errore che si

commette approssimando $\pi(x)$ è

$$\pi(x) - \mathrm{li}(x) = O\left(x\mathrm{e}^{-a\sqrt{\ln x}}\right) = O\left(\frac{x}{(\ln x)^m}\right)$$

Il secondo risultato, molto recente, è dovuto a Trudgian che ha dimostrato che l'errore assoluto che si commette approssimando $\pi(x)$ è:

$$\left|\pi(x) - \mathrm{li}(x)\right| \leq 0.2795 \frac{x}{(\log x)^{3/4}} \exp\left(-\sqrt{\frac{\log x}{6.455}}\right)$$

per $x \geq 229$.

```
n1=1;
n2=10^3;
x=n1:n2;
[Pi]=CountPrimes(n1,n2,x);
f=@(t) t./log(t);
y=f(x);
hold on
plot(x,y,'red')

Li = logint(x);
plot(x,Li, 'green')

legend('\pi(x)', 'x/log(x)', 'li(x)')
figure;
w=1:10^3;
w1=length(w);
for i=1:w1
    err=i.*exp(-2.*sqrt(log(i)));
end
err;
plot(w,err)
```

Figura 2.4: Main per il confronto della funzione $\pi(x)$

2.3 Il crivello di Eratostene

Il crivello di Eratostene è un antico algoritmo per trovare tutti i numeri primi fino a un dato limite e si basa sul seguente procedimento:

1. si scrivono tutti i numeri naturali a partire da 2 fino a n in un elenco detto setaccio;

2. si cancellano (setacciano) tutti i multipli del primo numero del setaccio (escluso esso stesso);

3. si seleziona il primo numero non cancellato maggiore di 2 e si ripete l'operazione con i numeri che seguono, proseguendo fino a che non si applica l'operazione all'ultimo numero non cancellato.

Gli algoritmi volti a riconoscere se un dato numero è primo o meno, si dicono *test di primalità*. Il crivello di Eratostene, per il teorema dei numeri primi, è un algoritmo di complessità esponenziale e dunque poco efficiente se si applica a numeri grandi. In generale trovare un algoritmo di fattorizzazione che abbia tempo polinomiale non è semplice. Proprio sulla difficoltà di decomporre un numero in fattori primi si basa la attuale sicurezza di alcuni sistemi crittografici, che permettono la trasmissione di dati segreti tra due soggetti senza che ad essi possano accedere terzi incomodi.
Riportiamo di seguito l'algoritmo implementato per il crivello di Eratostene

```
1   function [E]=Eratostene(n)
2   a=1:n;
3   a(1)=0;
4   for i=1:n
5   v = 2:i/2;
6   c = v(mod(i,v)==0);
7       if c
8           a(i)=0;
9       end
10  end
11  E=nonzeros(a);
12  end
```

Figura 2.5: Algoritmo del Crivello di Eratostene.

dove n è l'estremo superiore dell'intervallo in cui vogliamo trovare i numeri primi. Tale algoritmo per valori grandi di n inizia a dare problemi. Ad esempio per $n = 10^5$ il tempo computazionale inizia a diventare lungo perchè, come è stato già spiegato, esso è un algoritmo di complessità esponenziale.

```
>> Eratostene

ans =

  Columns 1 through 21

     2     3     5     7    11    13    17    19    23    29    31    37    41    43    47    53    59    61    67    71    73

  Columns 22 through 25

    79    83    89    97

>>
```

Figura 2.6: Risultato dell'algoritmo di Eratostene per $n = 100$

2.4 Il piccolo teorema di Fermat e il teorema di Wilson

In questa sezione enunceremo due teoremi che fungono da base per due test di primalità, ovvero il test di Lucas (il cui algoritmo verrà implementato per i numeri di Mersenne) e il test di Wilson.

Teorema 2.7 (Il piccolo teorema di Fermat)**.** *Sia a un intero e p un numero primo. Allora*

$$a^p \equiv a (\mathrm{mod}\, p)$$

e, se a non è divisibile per p, si ha

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Teorema 2.8 (Wilson)**.** *Se p è un numero primo, allora*

$$(p-1)! \equiv -1 (\mathrm{mod}\, p)$$

Vale anche il reciproco di questo teorema, quindi

Proposizione 2.1. *Se $(n-1)! \equiv -1 (\mathrm{mod}\, n)$, allora n è primo.*

Pertanto il teorema di Wilson, insieme al suo inverso, ci offre una caratterizzazione dei numeri primi:

n è primo se e solo se $(n-1)! + 1$ è divisibile per n

2.5 Primi di Mersenne e test di Lucas

Definizione 2.4. *Un numero di Mersenne è un numero della forma*

$$M_p = 2^p - 1$$

con p primo.

Se M_p è esso stesso un numero primo, allora prende il nome di primo di Mersenne. Infatti non tutti i primi p sono tali che M_p sia primo. Ad esempio se $p = 11$ si ha che $M_{11} = 211 - 1 = 2047 = 23 \cdot 89$.
Grazie al piccolo Teorema di Fermat, possiamo enunciare il test di primalità di Lucas, che ci permette di stabilire la non primalità di un numero di Mersenne.

Teorema 2.9 (Test di Lucas)**.** *Il numero $M_p = 2^p - 1$, con p primo maggiore di 2, è un numero primo se e solo se M_p divide S_p, dove S_k è definito per ricorrenza nel modo seguente:*

$$S_2 = 4 \qquad S_k = S_{k-1}^2 - 2.$$

Di seguito riportiamo il codice implementato per la ricerca dei numeri di Mersenne attraverso il quale possiamo calcolare i numeri di Marsenne con p numero primo:

```
1  function [Mp]=Mersenne(p)
2  a=primes(p);
3  Mp=2.^a-1;
4  end
```

Figura 2.7: Algoritmo per generare i numeri di Marsenne

Per esempio per $p = 11$ otteniamo:

```
Mp =

     3     7    31   127  2047
```

Ora passiamo ad illustrare l'algoritmo di Lucas per determinare la primalità di un numero di Mersenne:

```
function[X]=Lucas(n)
for p=3:n
a=primes(p);
prm=a(length(a));
if p~=prm
   continue
else
Mp=(2^p)-1;
k=p-1;
S=4;
for i=1:k-1
    S=mod(S^2-2,Mp);
end
  if S==0
       X = sprintf('Mp = %d è primo.',Mp);
       disp(X)
  else
       X = sprintf('Mp = %d non è primo. ',Mp);
       disp(X)
  end
end
end
```

Figura 2.8: Algoritmo per il test di Lucas

dove n è l'estremo superiore dell'intervallo dove vogliamo testare la primalità di un numero di Mersenne.

Prendendo come esempio $n = 30$ si ottiene il seguente risultato in accordo con la teoria:

```
Mp = 7 è primo.
Mp = 31 è primo.
Mp = 127 è primo.
Mp = 2047 non è primo.
Mp = 8191 è primo.
Mp = 131071 è primo.
Mp = 524287 è primo.
Mp = 8388607 non è primo.
Mp = 536870911 non è primo.
```

C'è da osservare che il test di Lucas è abbastanza efficiente dal punto di vista computazionale; infatti occorre effettuare $p-1$ quadrati modulo M_p e ciascuno dei quali richiede $\mathcal{O}(\log^2 M_p) = \mathcal{O}(p^2)$ operazioni bit.

Capitolo 3

Numeri pseudoprimi

Definizione 3.1. *Siano a, $n \in N$. Se n è dispari ma vale $a^{n-1} \equiv_n 1$, si dice che n è pseudoprimo di Fermat in base a. Un numero che sia pseudoprimo di Fermat per ogni base a e tale che* $\mathrm{MCD}(a, n) = 1$ *è detto numero di Carmichael.*

Su questa defizione si basa il test di primalità di Fermat: esso permette di affermare con certezza che se un intero n non verifica l'equazione $a^{n-1} \equiv_n 1$, allora n non è primo.
Se invece $2n - 1 \equiv 1(\mathrm{mod}\, n)$ possiamo dire che n è primo? La risposta è negativa. Infatti il più piccolo pseudoprimo di Fermat in base 2 è $n = 341$, poiché n non è primo, infatti $n = 341 = 11\dot{3}1$ ma $2340 \equiv_3 411$. Invece $n = 91 = 7 \cdot 13$ non è pseudoprimo in base 2, poiché $2906 \equiv_9 11$ ma lo è in base 3 perché $390 \equiv_9 11$

Teorema 3.1. *Le basi per cui n è pseudoprimo di Fermat formano un sottogruppo di $\mathcal{U}_n$*

3.1 Numeri di Carmichael

Enunciamo la seguente ipotesi, che chiameremo ipotesi H:

> se n non è primo, esiste un a, con $1 < a < n$, relativamente primo con n, tale che n non è uno pseudoprimo in base a.

Questa ipotesi è verificata quando effettuiamo il seguente test probabilistico $\mathcal{T}_m$ in maniera ricorsiva:

1. scegliamo a caso un intero a_m tale che $1 < a_m < n$ con a_m diverso da $a_1, ..., a_{m-1}$ e calcoliamo il MCD(a_m, n);
2. se MCD$(a_m, n) > 1$ allora n non è primo e abbiamo finito;
3. se MCD$(a_m, n) = 1$ e n non è pseudoprimo in base a_m allora n non è primo e abbiamo finito;
4. altimenti n è pseudoprimo in base a_m e sottoponiamo n al test $\mathcal{T}_{m+1}$.

La probabilità che n non sia primo e sia uno pseudoprimo in base a_m è minore di $1/2$. Quindi, la probabilità che n non sia primo ma passi i test $\mathcal{T}_1, ..., \mathcal{T}_m$ è minore di $1/2^m$. Quindi purchè il precedente test probabilistico abbia validità occorre far valere l'ipotesi H. Purtroppo essa non è mai fondata a causa dell'esistenza dei numeri di Carmichael.

Definizione 3.2 (Numero di Carmichael)**.** *Se n è un numero dispari, non primo, che sia pseudoprimo in base a per ogni a tale che $1 < a < n$ e* MCD$(a, n) = 1$*, allora n si dice un numero di Carmichael.*

La seguente proposizione contiene un'informazione saliente sui numeri di Carmichael.

Proposizione 3.1. *Sia $n > 1$ un numero dispari non primo.*

1. *Se n è divisibile per un quadrato maggiore di 1, allora n non è un numero di Carmichael.*

2. *Se n non è divisivile per un quadrato maggiore di 1, allora n è di Carmichael se e solo se $p-1$ divide $n-1$ per ogni fattore primo p di n.*

Proposizione 3.2. *Un numero di Carmichael è prodotto di almeno tre numeri primi distinti.*

Dimostrazione. Per la parte 1) della precedente proposizione sappiamo che un numero di Carmichael è prodotto di primi distinti. Supponiamo per assurdo che $n = pq$ sia numero di Carmichael prodotto di soli due primi distinti con $p < q$. Per la parte 2) della precedente proposizione sappiamo che $n - 1 \equiv 0 (\mathrm{mod}\, q - 1)$. Ma

$$n - 1 = p(q - 1 + 1) - 1 = p(q - 1) + p - 1 \equiv p - 1 (\mathrm{mod}\, q - 1)$$

e d'altra parte p-1 non è equivalente a 0 modulo $q-1$, perchè $0 < p-1 < q-1$. Si ha così l'assurdo. □

3.2 Pseudoprimi di Eulero

Prima di definire gli pseudoprimi di Eulero, enunciamo la seguente Proposizione:

Proposizione 3.3. *Sia p un primo dispari (cioè diverso da 2)*

1. *la funzione $\rho : x \in \mathcal{U}_p \longrightarrow x^2 \in \mathcal{U}_p^2$ è un endomorfismo del gruppo $\mathcal{U}_p$ e ha nucleo $\mathrm{Ker}(\rho) = \{\pm 1\}$ e la sua immagine ha indice 2.*

2. *gli elementi di $\mathcal{U}_p^2$ sono gli interi per cui $x^2 = a \bmod p$ ha soluzione non nulla; essi si dicono residui quadratici modulo p, RQ_p e sono esattamente $\frac{p-1}{2}$*

Dimostrazione. Essendo $\mathbb{Z}_p$ un campo (perchè p primo) per il teorema di Ruffini il polinomio X^2 ha al più due radici, per cui $\ker(\rho) = \{\pm 1\}$. Dal teorema degli omomorfismi $\mathcal{U}_p^2 = \mathrm{Im}(\rho)$ ha ordine $\frac{p-1}{2}$ e dunque indice 2 in $\mathcal{U}_p$. □

Definizione 3.3. *Sia p primo. Si definisce simbolo di Legendre la funzione*

$$a \in \mathbb{Z} \longrightarrow \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è rediduo quadratico } \bmod p \\ 0 & \text{se } a = 0 \\ -1 & \text{altrimenti} \end{cases} \tag{3.1}$$

Inoltre, per ogni $a, b \in \mathbb{Z}$ valgono le seguenti proprietà

1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
2. $\left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

Teorema 3.2 (Criterio di Eulero)**.** *Sia p un primo dispari, allora*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\bmod p)$$

Il Criterio di Eulero si può usare come test di primalità, per verificare se un numero dispari n non è primo. Infatti:

se esiste a tale che $\left(\frac{a}{p}\right) \neq a^{\frac{n-1}{2}} (\mathrm{mod}\, n)$ allora n non è primo.

Definizione 3.4 (Pseudoprimo di Eulero)**.** *Sia dato un numero intero b. Un numero intero positivo dispari n, non primo e tale che* $\mathrm{MCD}(n, b) = 1$*, si dice uno pseudoprimo di Eulero in base b se*

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) (\mathrm{mod}\, n)$$

Lemma 3.1. *Se n è uno pseudoprimo di Eulero in base b, allora n è anche uno pseudoprimo in base b.*

Proposizione 3.4. *Sia n numero intero positivo dispari non primo. I numeri positivi $b < n$ primi con n tali n sia uno pseudoprimo di Eulero in base b, sono non più della metà di tutti i numeri positivi $b < n$ tali che* $\mathrm{MCD}(b, n) = 1$*.*

Proposizione 3.5. *Sia $n > 1$ un numero dispari non primo. Se n è pseudoprimo di Eulero nelle basi b_1 e b_2 tali che* $\mathrm{MCD}(b_1, n) = \mathrm{MCD}(b_2, n) = 1$*, allora n è pseudoprimo nelle basi $b_1 b_2$ e $b_1 b_{-1}^2$, dove b_2^{-1} è inverso di b_2 modulo n.*

Proposizione 3.6. *Sia $n > 1$ un numero dispari che non sia un quadrato perfetto. Allora vi è un intero positivo $b < n$, primo con n, tale che* $\left(\frac{b}{n}\right) = -1$

Proposizione 3.7. *Sia $n > 1$ un numero dispari non primo. Esiste un numero intero positivo $b < n$ primo con n e tale che n non è uno pseudoprimo di Eulero in base b.*

Sulle queste considerazioni si basa il test probabilistico di primalità di Solovay–Strassen.

Teorema 3.3 (Test di primalità di Solovay–Strassen)**.** *Fissiamo un intero dispari $n > 1$. Il test $\mathcal{T}_1$ consiste nei seguenti passi:*

1. *scegliamo a caso un intero b_1 con $1 < b_1 < n$ e calcoliamo il* $\mathrm{MCD}(b_1, n)$*;*
2. *se* $\mathrm{MCD}(b_1, n) > 1$ *allora n non è primo e abbiamo finito;*
3. *se* $\mathrm{MCD}(b_1, n) = 1$ *e n non è pseudoprimo di Eulero in base b_1;*
4. *altrimenti n è pseudoprimo in base b_1 e sottoponiamo n al test $\mathcal{T}_2$.*

Definiamo poi il test $\mathcal{T}_m$ ricorsivamente nel modo seguente:

1. *scegliamo a caso un intero b_m con $1 < b_m < n$ con b_m diverso da $b_1, ..., b_m$ e calcoliamo il* $\mathrm{MCD}(b_m, n)$*;*
2. *se* $\mathrm{MCD}(b_m, n) > 1$ *allora n non è primo e abbiamo finito;*
3. *se* $\mathrm{MCD}(b_m, n) = 1$ *e n non è pseudoprimo di Eulero in base b_m;*
4. *altrimenti n è pseudoprimo in base b_m e sottoponiamo n al test $\mathcal{T}_{m+1}$.*

3.3 Pseudoprimi forti e il test di probabilistico di primalità di Miller–Rabin

Definizione 3.5. *Sia n un numero intero positivo dispari non primo e $b < n$ un numero intero positivo tale che* $\mathrm{MCD}(b, n) = 1$. *Scriviamo $n = 2^s t + 1$, con t dispari. Il numero n si dice uno pseudoprimo forte in base b se vale una delle seguenti due condizioni:*

$$b^t \equiv 1 (\mathrm{mod}\, n)$$

oppure esiste un numero intero non negativo $r < s$ tale che

$$b^{2^r t} \equiv -1 (\mathrm{mod}\, n)$$

Il numero $n = 25$ è un pseudoprimo forte per la base $b = 7$. Infatti $7^2 = 49 = -1 (\mathrm{mod}\, 25)$ e dunque $7^{12} = 7^{\frac{n-1}{2}} \equiv 1 (\mathrm{mod}\, 5)$

Proposizione 3.8. *Sia n un numero intero positivo dispari e $b < n$ un numero intero positivo tale che* $\mathrm{MCD}(b, n) = 1$. *Se n è uno pseudoprimo forte in base b allora n è uno pseudoprimo di Eulero in base b.*

da queste considerazioni possiamo enunciare il teorema del test probabilistico di primalità di Miller–Rabin.

Teorema 3.4 (Test probabilistico di primalità di Miller–Rabin)**.** *Fissiamo un intero dispari $n > 1$. Scriviamo $n = 2^s t + 1$ con t dispari. Il test $\mathcal{T}_1$ consiste nei seguenti passi:*

1. *scegliamo a caso un intero b_1 con $1 < b_1 < n$ e calcoliamo il* $\mathrm{MCD}(b_1, n)$*;*

2. *se* $\mathrm{MCD}(b_1, n) > 1$ *allora* n *non è primo e abbiamo finito;*

3. *se* $\mathrm{MCD}(b_1, n) = 1$ *calcoliamo* b_1^t *modulo* n*. Se* $b_1^t \equiv \pm 1 (\mathrm{mod}\, n)$ *,* n *è primo o è uno pseudoprimo forte in base* b_1*;*

4. *altrimenti calcoliamo* b_1^{2t} *modulo* n*. Se* $b_1^{2t} \equiv -1 (\mathrm{mod}\, n)$ *,* n *è primo o è uno pseudoprimo forte in base* b_1*;*

5. *altrimenti procediamo allo stesso modo. Se tutte le potenze successive* $b_1^{2^r t}$ *per* $r = 1, ..., s-1$ *non sono mai congrue a -1 modulo* n *allora* n *non è un primo. Altrimeni* n *è uno pseudoprimo forte in base* b_1

Definiamo poi il test $\mathcal{T}_m$ *ricorsivamente nel modo seguente:*

1. *scegliamo a caso un intero* b_m *con* $1 < b_m < n$ *con* b_m *diverso da* $b_1, ..., b_m$ *e calcoliamo il* $\mathrm{MCD}(b_m, n)$*;*

2. *se* $\mathrm{MCD}(b_m, n) > 1$ *allora* n *non è primo e abbiamo finito;*

3. *se* $\mathrm{MCD}(b_m, n) = 1$ *si calcola* b_m^t *modulo* n *e si procede come dal passo 3) di* $\mathcal{T}_1$ *in poi.*

```
function [X]=MillerRabin(a,s,m)
if b>1
    X = sprintf('%n non è primo.',n);
    disp(X)
end
if b==1
    t=mod(a^m,n);
    if t==mod(1,n) || t==mod(-1,n)
        X = sprintf('%d è primo o pseudoprimo forte.',n);
        disp(X)
    else
        t1=mod(a^(2*m),n);
        if t1==mod(-1,n)
            X = sprintf('%d è primo o pseudoprimo forte.',n);
            disp(X)
        else
            for r=3:s-1
                tr=mod(a^(2^r),n);
                if tr==mod(-1,n)
                    X = sprintf('%d è primo o pseudoprimo forte.',n);
                    disp(X)
                else
                    X = sprintf('%d non è primo.',n);
                    disp(X)
                end
            end
        end
    end
end
```

Figura 3.1: Algoritmo per il test di Miller-Rabin, basato sul teorema precedentemente esposto.

Dove $s \in \mathbb{N}$, $m \in \mathbb{N}$ dispari, e a numero scelto a caso in $\mathbb{N}$.

Bibliografia

[1] Bach, Eric; Shallit, Jeffrey (1996). Algorithmic Number Theory. MIT Press.

[2] Welleda Maria Baldoni, Ciro Ciliberto, Giulia Maria Piacentini Cattaneo. *Aritmetica, crittografia e codici*. Springer Milano

[3] Welleda Maria Baldoni, Ciro Ciliberto, Giulia Maria Piacentini Cattaneo. *Aritmetica, crittografia e codici*. Springer Milano

[4] Dardano Samo Ulderico. *Appunti del corso in Metodi algebrici per la Crittografia.* 2023

[5] S. Leonesi, C. Toffalori. *Numeri e Crittografia*. Springer.