Alcune proprietà dei numeri primi, II

Alessandro Languasco & Alessandro Zaccagnini

In questo secondo articolo della serie incominciata con [5] riprendiamo la descrizione di alcune proprietà elementari dei numeri primi. Cominciamo con il secondo punto dell'elenco esposto nel §4 dell'articolo già citato.

1 Come riconoscere i numeri primi e come scomporre in fattori primi

Vogliamo subito precisare che il problema di dimostrare la primalità di un intero è cosa diversa da quella di ricercarne gli eventuali fattori. Infatti esistono dei risultati che garantiscono la primalità di un numero mediante opportune condizioni equivalenti; il fatto che tali condizioni risultino non verificate consente quindi di concludere che tale numero è composto senza doverne esibire un divisore. Per essere utili in pratica tali condizioni devono però coinvolgere oggetti matematici "semplici" e richiedere per la loro verifica un quantità di calcoli limitata.

Cominciamo la nostra presentazione esaminando una condizione necessaria e sufficiente per la primalità che utilizza solamente delle congruenze: il famoso Teorema di Wilson di cui diamo una dimostrazione nel §3.1 di [4].

Teorema 1.1 (Wilson) *L'intero $n \geq 2$ è primo se e solo se $(n-1)! \equiv -1 \bmod n$.*

Per esempio, $(10-1)! = 362880 \equiv 0 \not\equiv -1 \bmod 10$, e quindi 10 non è un numero primo, mentre $(13-1)! = 479001600 \equiv -1 \bmod 13$ e quindi 13 è un numero primo. Chiaramente l'enunciato del Teorema di Wilson 1.1 non richiede alcuna conoscenza sui fattori di n ma si basa solamente sulla verifica di una opportuna congruenza che coinvolge n. Sfortunatamente in questo caso la quantità di calcoli da effettuare per verificare la congruenza è proporzionale a n stesso e quindi il Teorema di Wilson non può essere utilizzato in pratica per verificare la primalità di un intero "grande" perché richiederebbe un'attesa troppo lunga prima di ottenere una risposta.

Esistono però altri risultati che, sebbene non costituiscano una condizione equivalente alla primalità di un intero, possono essere verificati con un numero

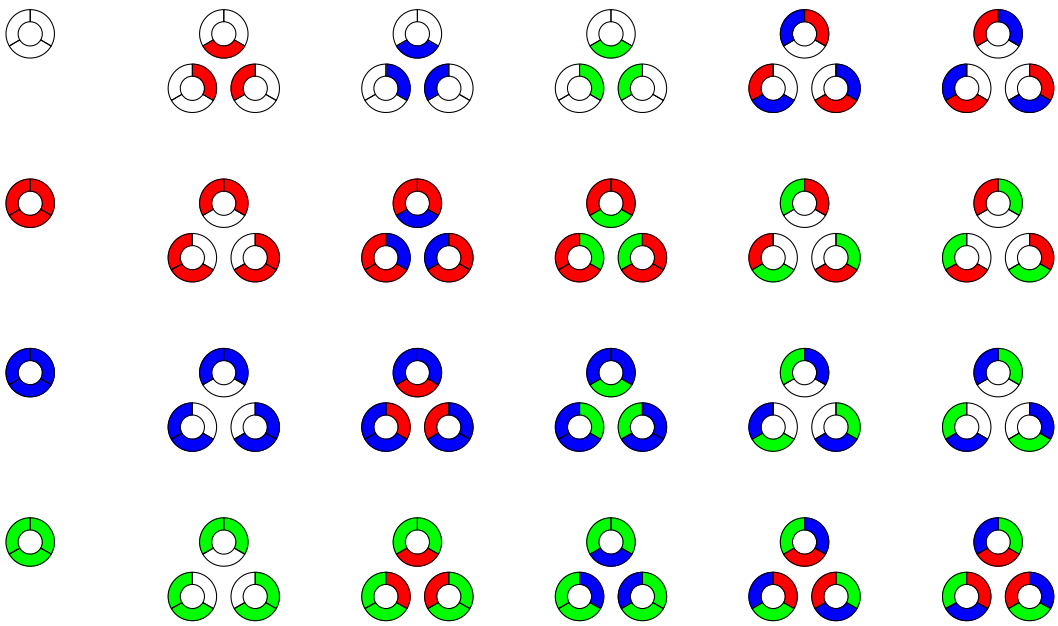

Figura 1: Dimostrazione del Piccolo Teorema di Fermat: le 64 collane con 3 perline di 4 colori; quelle policrome sono raggruppate in classi di collane equivalenti per rotazione.

di calcoli estremamente più contenuto; un esempio famoso è il Piccolo Teorema di Fermat. Data la sua enorme importanza, diamo una dimostrazione del Piccolo Teorema di Fermat diversa dalle due che abbiamo incluso in [4], e di natura combinatoria. Questa dimostrazione ci pare particolarmente interessante perché non fa uso di concetti complicati (neppure delle congruenze che pure non sono particolarmente complesse) ma sfrutta solo il conteggio di opportuni oggetti, e quindi non richiede alcuna nozione preliminare, ma solo del buon senso comune. Questa, come altre dimostrazioni elementari di teoremi importanti, si trova in Mortola [6].

Teorema 1.2 (Piccolo Teorema di Fermat) *Sia a un intero qualsiasi, e p un numero primo. Allora $a^p \equiv a \bmod p$.*

Dim. Consideriamo tutte le *collane* con p perline, ciascuna delle quali può avere uno qualsiasi fra a colori diversi. Vi sono evidentemente a^p collane possibili, a delle quali sono monocromatiche. Suddividiamo le rimanenti $a^p - a$ collane (policrome, cioè con perline di almeno due colori diversi) in classi di equivalenza, come segue: due collane sono equivalenti se una si ottiene dall'altra mediante un'opportuna rotazione del piano. Evidentemente ogni classe non può contenere più di p collane fra loro equivalenti, ma, poiché p è primo, per il Lemma 1.3 ogni classe ne deve contenere esattamente p. Dunque, p divide $a^p - a$. □

La Figura 1 illustra la dimostrazione nel caso $p = 3$, $a = 4$.

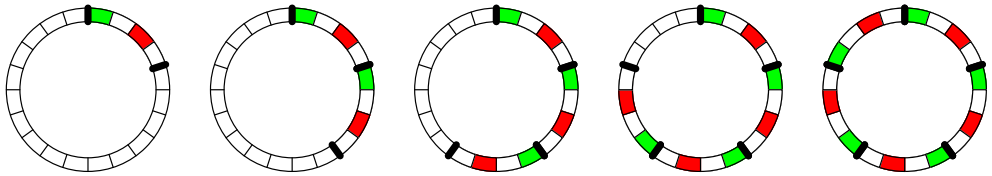

Figura 2: La dimostrazione del Lemma 1.3. La collana è invariante per una rotazione in senso orario di 4 perline, e quindi, scelte in modo arbitrario 4 perline consecutive, a sinistra, sappiamo che le 4 perline immediatamente adiacenti, sempre in verso orario, devono essere colorate allo stesso modo. Per lo stesso motivo, anche le successive 4 hanno la stessa colorazione, e cosí via: il numero totale di perline deve essere un multiplo di 4, e quindi non è primo.

Lemma 1.3 *Se p è un numero primo, nessuna collana policroma con p perline è equivalente ad una propria rotazione non banale.*

Dim. Supponiamo che la collana data sia equivalente alla propria rotazione in senso orario di r perline, con $r > 1$ (altrimenti la collana sarebbe monocromatica) ed $r < p$ (altrimenti la rotazione sarebbe banale). Fissiamo r perline consecutive. Le r perline successive a quelle fissate devono formare un blocco uguale alle r precedenti (dato che dopo la rotazione vanno a coincidere). In altre parole, la collana è formata da due blocchi identici consecutivi di r perline ciascuno, seguite da $p-2r$ perline. Possiamo ripetere lo stesso identico ragionamento per le ulteriori r perline successive, che devono a loro volta formare un altro blocco uguale ai due precedenti, dando luogo a 3 blocchi identici consecutivi seguiti da $p-3r$ perline. Iterando questo procedimento fino ad esaurire tutte le perline della collana senza tralasciarne nessuna, troviamo che questa è costituita da k blocchi di r perline ciascuno. In definitiva, $r \mid p$ e p non è un numero primo. □

È opportuno notare che, se p è primo, la rotazione di una collana produce una collana *diversa*, mentre questo non è vero se p non è primo, come si vede dal caso con $p = 20$ illustrato dalla Figura 2.

Per esempio, abbiamo $2^{91} \equiv 37 \bmod 91$, e quindi 91 non è un numero primo. Analogamente a quanto visto sopra per il Teorema di Wilson, questa è solo una dimostrazione "indiretta" del fatto che 91 non è primo, ed infatti non ne vengono ricavati i fattori primi. La situazione è resa più complicata dal fatto che mentre la congruenza di Wilson dà una *condizione necessaria e sufficiente* per la primalità, la congruenza di Fermat dà solo una condizione *necessaria*. In effetti, $3^{91} \equiv 3 \bmod 91$, nonostante il fatto che 91 non è un numero primo.

Osserviamo che, da un punto di vista computazionale, il calcolo di $a^n \bmod n$ è poco oneroso (si veda per esempio il §6.9.2 di [4], oppure [9]) e quindi è naturale pensare a come il Piccolo Teorema di Fermat possa essere utilizzato per la verifica della primalità di un intero.

In pratica si prova a vedere se il numero n verifica $a^n \equiv a \bmod n$ per varie scelte di $a \in \mathbb{Z}$. Notiamo che, in realtà, possiamo ridurci al caso $(a,n) = 1$, $0 \le a < n$, e verificare, in tale situazione, che $a^{n-1} \equiv 1 \bmod n$. Per analizzare il significato della risposta ci serve il seguente

Lemma 1.4 *Se n è composto ed esiste $b \in \mathbb{Z}$ con $(b,n) = 1$ e $0 \le b < n$ tale che $b^{n-1} \not\equiv 1 \bmod n$, allora $a^{n-1} \not\equiv 1 \bmod n$ per almeno la metà degli interi $a \in \mathbb{Z}$ con $(a,n) = 1$ e $0 \le a < n$.*

Allora, dopo il primo a usato, possiamo concludere che o n è *probabilmente* un numero primo con probabilità maggiore o uguale a $1 - 1/2$ o n è un numero composto che verifica $a^{n-1} \equiv 1 \bmod n$ per tale a.

Ripetendo il test k volte cambiando a ogni volta, si ottiene che o n è primo con probabilità maggiore o uguale a $1 - (1/2)^k$ oppure n è composto e verifica la congruenza $a^{n-1} \equiv 1 \bmod n$ per tutti gli a utilizzati.

A prima vista questa situazione pare non essere troppo svantaggiosa: abbiamo un test piuttosto facile da implementare e notevolmente performante che fornisce una risposta che sembra ragionevolmente buona. Sfortunatamente, però, esistono interi composti n per cui $a^{n-1} \equiv 1 \bmod n$ per ogni $a \in \mathbb{Z}$ con $(a,n) = 1$. Tali interi sono detti numeri di *Carmichael*; ad esempio $561 = 3 \cdot 11 \cdot 17$ è un numero di Carmichael. Quindi esistono interi composti che "fingono" di essere primi rispetto alla congruenza del Piccolo Teorema di Fermat per ogni possibile scelta di a. Il fatto è spiacevole, ma se i numeri di Carmichael fossero finiti potremmo ancora ottenere un algoritmo di primalità molto buono precalcolandoli tutti. Purtroppo, nel 1994, Alford, Granville e Pomerance hanno dimostrato che esistono infiniti numeri di Carmichael e quindi la congruenza del Piccolo Teorema di Fermat non può essere utilizzata per caratterizzare algoritmicamente i numeri primi.

In altre parole, un intero a tale che $n \nmid a$ ed $a^{n-1} \not\equiv 1 \bmod n$ è una *prova certa* del fatto che n non è un numero primo (se n fosse primo si avrebbe $a^{n-1} \equiv 1 \bmod n$ per il Piccolo Teorema di Fermat, contraddizione) mentre un intero a tale che $n \nmid a$ ed $a^{n-1} \equiv 1 \bmod n$ fornisce solo un *indizio* della primalità di n, ed in questo caso non è vero che tre indizi fanno una prova a causa dei numeri di Carmichael...

È possibile, però, utilizzare alcune varianti più sofisticate del Piccolo Teorema di Fermat. Esse utilizzano un insieme finito di congruenze della stessa tipologia di quelle viste poco sopra ma, a differenza del caso precedente, per esse è dimostrato che, se n è composto, esiste un a per cui tali congruenze non sono valide (ossia per tale insieme di congruenze non esiste un concetto analogo a quello dei numeri di Carmichael).

Senza entrare nel dettaglio, essenzialmente si "estraggono" tutte le possibili radici quadrate di $a^{n-1} \bmod n$ e, se n è primo, si osserva che tali radici quadrate devono essere tutte uguali a 1 o a -1. Nel caso in cui una di esse non sia ± 1

allora n è composto. Anche in questo caso si può valutare probabilisticamente la correttezza della risposta al variare di a.

Il fatto che questo test (algoritmo di Miller-Rabin) sia anch'esso computazionalmente molto performante e che, nel caso in cui n sia composto, esista certamente un "testimone" a di tale proprietà, consente di utilizzare in pratica il metodo di Miller-Rabin per verificare con "alta" probabilità che un intero è primo. Maggiori dettagli si trovano, ad esempio, nel §3.8 di [4].

Abbiamo quindi uno strumento, basato sulle congruenze, che è affidabile e veloce e che consente di "ridurre" la probabilità che un intero possa essere composto.

Vogliamo anche fare notare che il recente risultato (2002) di Agrawal-Kayal-Saxena, che dimostra la possibilità di verificare la primalità di un intero con una quantità di calcoli dipendente in modo polinomiale dal numero di cifre di n, è anch'esso basato sulla verifica di una serie di congruenze (sebbene esse siano effettuate nell'anello dei polinomi a coefficienti interi $\mathbb{Z}[x]$ e non in $\mathbb{Z}$).

In conclusione, al giorno d'oggi esistono algoritmi che consentono di provare la primalità di un intero n eseguendo un numero di calcoli essenzialmente del tipo $(\log n)^6$ operazioni effettuate sui bit e, da un punto di vista pratico, le loro implementazioni consentono di "produrre" in pochi secondi, utilizzando hardware facilmente accessibile in commercio, numeri primi di forma generale (si veda il paragrafo successivo) aventi 400-500 cifre decimali (ossia di grandezza più che sufficiente per le attuali applicazioni).

Ben diversa è la situazione per gli algoritmi di fattorizzazione. È immediato osservare che, provando a dividere un intero n per tutti gli interi minori o uguali di $\sqrt{n}$, si ottiene un algoritmo che determina un fattore di n eseguendo un numero di calcoli che, nel caso peggiore, è circa $\sqrt{n}$ operazioni effettuate sui bit; ossia effettua un calcolo estremamente più oneroso di quelli relativi alla primalità. Sebbene esistano algoritmi molto più sofisticati della *divisione per tentativi* sopra descritta, il problema della fattorizzazione sembra essere computazionalmente più "difficile" della primalità. Infatti l'algoritmo di fattorizzazione più efficiente noto al giorno d'oggi (il *Crivello dei Campi di Numeri* di Pollard e Lenstra) per determinare un fattore di n effettua un numero di calcoli che è circa pari a

$$e^{(\log n)^{1/3}(\log\log n)^{2/3}}$$

operazioni effettuate sui bit. Chiaramente anche questa verifica è estremamente più onerosa di quella relativa alla primalità.

Per esemplificare la velocità con cui cresce la funzione esponenziale ricorriamo al seguente esempio. Prendiamo un foglio di carta da $0,1$ mm e cominciamo a piegarlo su se stesso in due parti uguali. Il foglio ha ora spessore doppio ($0,2$ mm). Eseguiamo un'altra piegatura: il foglio ora ha spessore quadruplo rispetto all'inizio ($0,4$ mm). In definitiva, con ogni piegatura raddoppiamo lo spessore del foglio

stesso. Orbene, se fossimo capaci di piegarlo in tal modo 42 volte, otterremmo uno spessore maggiore della distanza Terra-Luna! Infatti, dopo aver ricordato che la distanza "media" Terra-Luna è pari a 384000 km (356410 km al perigeo e 384700 km all'apogeo), è sufficiente osservare che $2^{42} = 4398046511104$ e quindi lo spessore ottenuto è pari a 4398046511104 decimillimetri ossia $439804,6511104$ km.

È chiaro quindi che il "costo computazionale" della fattorizzazione è notevolmente maggiore rispetto a quello della primalità. È proprio su questa notevole differenza di "costo computazionale" che si fonda la crittografia a chiave pubblica: verrà sfruttata la capacità di generare primi per costruire un metodo crittografico efficiente e facilmente usabile mentre la difficoltà di violare tale sistema verrà fatta dipendere dalla "alta onerosità computazionale" di determinare un fattore di un intero.

Si faccia attenzione che queste affermazioni sono corrette nel caso si cerchi di fattorizzare un intero di forma "generale" ossia per cui non sia nota alcuna struttura. Ad esempio se è noto che l'intero n ha almeno un fattore primo p "piccolo" (avente ordine di grandezza del tipo $\log^A n$, $A > 0$ fissato) l'algoritmo di divisione per tentativi determina tale p effettuando un numero di calcoli sui bit che è polinomiale sul numero di cifre di n; oppure se n è il prodotto di esattamente due fattori primi p e q entrambi "quasi" uguali a $\sqrt{n}$ una strategia efficiente è quella di cercare di scrivere $n = X^2 - Y^2 = (X-Y)(X+Y)$ perché in tal caso Y sarà piccolo e verificando quando $n+Y^2$ è un quadrato perfetto si svolgono all'incirca Y radici quadrate di numeri aventi essenzialmente la stessa grandezza di n.

Quindi quello che sappiamo è che non siamo in grado di risolvere *il caso peggiore* della fattorizzazione in modo efficiente e che esistono *casi particolari* in cui essa è risolubile in maniera estremamente performante. Nelle applicazioni, bisognerà quindi cercare di "stare lontani" dai casi particolari in cui è noto che la fattorizzazione è efficiente per non rischiare di compromettere, ad esempio, la sicurezza di un metodo crittografico. Concretamente, non è opportuno usare i numeri primi di Mersenne (ne parliamo nel §2) come fattori della chiave pubblica n in RSA perché questi hanno una forma troppo speciale e sono di dominio pubblico. Abbiamo discusso tutte queste cose in dettaglio in [4], ma consigliamo di approfondire l'argomento consultando il libro di Crandall & Pomerance [1].

In conclusione, osserviamo che da un punto di vista psicologico, può non apparire del tutto soddisfacente sapere che un certo intero non è primo, senza conoscerne i fattori primi. Dal punto di vista pratico, invece, quando si cercano numeri primi per le applicazioni è di enorme importanza avere metodi veloci per determinare la primalità o meno, dato che non sono ancora noti metodi di fattorizzazione parimente efficienti (perlomeno nel caso generale). Le cose cambierebbero radicalmente se si scoprisse un algoritmo di fattorizzazione competitivo con i criteri di primalità, ma questo non ci sembra molto probabile sebbene esistano risultati in tal

senso che però fanno uso di un metodo di computazione (il cosiddetto "computer quantistico") che, al momento, non pare essere di prossima realizzazione.

2 Criteri di primalità elementari e numeri primi di forma speciale

Oltre ai già citati metodi basati sul Teorema di Fermat esistono altri metodi che sono basati sul tentativo di costruire un "viceversa" di tale teorema. Per fare ciò è necessario aggiungere delle ipotesi sulla struttura di n; ad esempio, nel caso si conosca la fattorizzazione di $n-1$, il seguente Teorema di Lucas fornisce un metodo efficiente. Per poterne fornire una semplice dimostrazione dobbiamo prima introdurre una definizione

Definizione 2.1 (Ordine di un elemento) *Si dice* ordine *di $a \in \mathbb{Z}_n^*$ il* minimo *intero positivo m tale che $a^m \equiv 1 \bmod n$, e lo si indica con $o_n(a)$.*

e fornire i due enunciati seguenti:

Teorema 2.2 (Eulero) *Se $n \geq 2$ ed $(a,n) = 1$ allora si ha $a^{\varphi(n)} \equiv 1 \bmod n$.*

Teorema 2.3 (Lagrange) *Per ogni $a \in \mathbb{Z}_n^*$ si ha $o_n(a) \mid \varphi(n)$.*

Le dimostrazioni dei Teoremi 2.2-2.3 possono essere trovate, in una forma più generale, in [4], per esempio.

Come conseguenza del Teorema 2.2 abbiamo che l'ordine di un qualunque elemento di $\mathbb{Z}_n^*$ (cioè di un elemento invertibile di $\mathbb{Z}_n$) divide $\varphi(n) = \mathrm{card}(\mathbb{Z}_n^*)$: si veda il Lemma A.3. Usando questo fatto possiamo facilmente dimostrare il seguente

Teorema 2.4 (Lucas) *Se $a^d \not\equiv 1 \bmod n$ per ogni $d \mid n-1$ tale che $d < n-1$ ed inoltre $a^{n-1} \equiv 1 \bmod n$, allora n è primo.*

Dim. Un tale elemento $a \in \mathbb{Z}_n$ ha ordine esattamente $n-1$ in $\mathbb{Z}_n^*$, e questo può accadere se e solo se n è primo: infatti l'ordine di a in $\mathbb{Z}_n^*$ divide $\varphi(n)$, e $\varphi(n) \leq n-2$ se $n \geq 4$ non è primo. □

Si può anche notare che in realtà è sufficiente verificare la congruenza dell'enunciato del Teorema di Lucas solamente per tutti i divisori di $n-1$ della forma $(n-1)/p$, dove p è un fattore *primo* di $n-1$. Chiaramente questo metodo è applicabile solo per interi n di forma particolare; quelli per cui siano noti questi fattori primi. Due di questi casi particolari sono i numeri di Fermat e di Mersenne (per i numeri di Mersenne serve la fattorizzazione di $n+1$) cosí chiamati perché nel XVII secolo, Fermat e Mersenne li introdussero per proporre "formule" che producessero primi: purtroppo le loro congetture si rivelarono sbagliate.

Definizione 2.5 *Per $n \in \mathbb{N}$ si chiama n-esimo* numero di Fermat *il numero $F_n = 2^{2^n}+1$. Per $n \in \mathbb{N}^*$ si chiama n-esimo* numero di Mersenne *il numero $M_n = 2^n - 1$.*

Le relazioni note tra i numeri di Fermat e di Mersenne e la primalità sono le seguenti: le due dimostrazioni sono piuttosto simili e si basano, sostanzialmente, su proprietà di divisibilità di opportuni polinomi.

Teorema 2.6 *Se il numero 2^m+1 è primo, allora $m = 2^n$ per qualche intero n.*

Dim. Se m non fosse una potenza di 2, allora esisterebbero interi a e b tali che $m = ab$, con $b > 1$ dispari. Osservando che il polinomio $x^b + 1$ è divisibile per il polinomio $x+1$ ed applicando tale fatto al caso particolare $x = 2^a$, si ha che $2^a + 1 \mid 2^{ab} + 1$ e quindi quest'ultimo non può essere un numero primo. □

La stessa dimostrazione prova che se $c^m + 1$ è primo e $c > 1$, allora c è pari ed $m = 2^n$ per qualche intero n.

Teorema 2.7 *Se il numero M_n è primo, allora n è primo.*

Dim. Se n fosse composto allora esisterebbero $1 < a, b < n$ tali che $n = ab$. Di conseguenza $2^a - 1$ sarebbe un fattore di M_n perché $2^{ab} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{a(b-1)})$. □

Per esempio, $2^5 + 1$ è divisibile per $3 = 2^1 + 1$, mentre $2^6 - 1$ è divisibile per $3 = 2^2 - 1$, e quindi non sono primi. Fermat congetturò che tutti i numeri F_n fossero primi, ma questo è vero solo per $n = 0, \ldots, 4$, e falso per $n = 5, \ldots, 32$. Un criterio fondamentale che è stato usato (da Eulero per primo) per provare che tali numeri sono composti è il seguente

Teorema 2.8 *Per ogni $n \geq 2$, $n \in \mathbb{N}$, ogni fattore primo p di F_n verifica $p \equiv 1 \bmod 2^{n+2}$.*

Chiaramente questo è un criterio di fattorizzazione per i numeri di Fermat. Esso fu usato da Eulero per determinare un fattore di F_5. In effetti qualche semplice calcolo ci consente di ottenere che esistono al più 512 interi candidati ad essere fattori di F_5 perché essi devono verificare la congruenza $p \equiv 1 \bmod 128$ e $\lfloor \sqrt{F_5} \rfloor = 2^{16} = 65536$. È sufficiente fermarsi a $\lfloor \sqrt{F_5} \rfloor$ perché ogni intero composto ha almeno un fattore non banale non superiore alla propria radice quadrata. Impostando un semplice algoritmo si trova dopo solo cinque tentativi che il numero 641 (che è un primo) è un fattore di F_5. Volendo raffinare l'analisi ci si può ridurre ai primi minori o uguali di 2^{16} (che sono 6542) e che possono essere facilmente precomputati, per esempio, tramite il crivello di Eratostene. Di essi solamente 99 sono congruenti ad 1 modulo 128. In tal caso il fattore 641 viene determinato al secondo tentativo.

VERIFICA CHE F_5 È COMPOSTO

```
1  function verificaF5()
2  F5 = 2^32 + 1
3  for (i = 129 to 65536 step 128 )
4        d = F5 mod i
5        if (d = 0) then
6              begin
7                    print(i,"divide il quinto numero di Fermat",F5)
8                    return
9               end
10       endif
11 endfor
```

Figura 3: Algoritmo di verifica che F_5 è composto.

Per questo numero speciale esiste anche una dimostrazione brevissima (di Eulero), che di nuovo fa uso di opportuni polinomi: ricordiamo che $x+1$ divide x^4-1. Nel caso particolare $x = 5\cdot 2^7$ abbiamo che $641 = x+1 \mid x^4-1 = 2^{28}\cdot 5^4 - 1 = A$. Inoltre $641 = 2^4+5^4 \mid 2^{28}\cdot(2^4+5^4) = 2^{32}+2^{28}\cdot 5^4 = B$, e quindi $641 \mid B-A = F_5$.

A titolo di esempio inseriamo lo pseudocodice di due programmi che abbiamo utilizzato per eseguire questi conti. In origine tali programmi sono stati scritti utilizzando il software Pari/Gp (`http://pari.math.u-bordeaux.fr`).

In Figura 3 trovate le verifiche fatte per provare che F_5 è composto.

Per calcolare il numero di primi minori o uguali di 2^{16} che sono congruenti a 1 mod 128 abbiamo usato lo pseudocodice di Figura 4. In esso utilizziamo la funzione `isprime` che risponde `vero` se i è primo e `falso` se i è composto.

Esistono però anche criteri di primalità *ad hoc* per i numeri di Fermat che hanno permesso di dimostrare che i numeri F_n con $n = 5,\ldots,32$ sono composti, nella maggior parte dei casi senza poterne esibire esplicitamente un fattore primo. Essi sono basati sul seguente teorema (variante del Teorema di Lucas) che conduce ad un algoritmo molto efficiente per verificare la primalità di un numero di Fermat.

Teorema 2.9 (Pepin) *Per $n \geq 1$, il numero $F_n = 2^{2^n}+1$ è primo se e solo se $3^{(F_n-1)/2} \equiv -1 \bmod F_n$.*

La dimostrazione del Teorema 2.9, sebbene semplice, utilizza alcuni concetti relativi al riconoscimento dei quadrati in $\mathbb{Z}_n$ di cui non abbiamo parlato in questo ambito. Il Lettore interessato può trovarla nell'Appendice A.

CALCOLO DEL NUMERO DEI PRIMI $\leq 2^{16}$ CONGRUENTI A 1 mod 128

```
1 function congrprimi
2 s = 0
3 for (i = 129 to 65536 step 128 )
4       if (isprime(i) = vero) then s ← s + 1
5       endif
6 endfor
7 print s
```

Figura 4: Calcolo del numero dei primi congruenti a 1 mod 128.

Per esempio nel caso di F_5 va verificato se $3^{(2^{31})} \equiv -1 \bmod F_5$. Sfruttando il Teorema 2.2, si ottiene che $3^{\varphi(F_5)} \equiv 1 \bmod F_5$ e quindi è sufficiente verificare se $3^r \equiv -1 \bmod F_5$, dove $r \equiv 2^{31} \bmod \varphi(F_5)$. Si ottiene che $r = 2147483648$ e che $3^r \equiv 10324303 \bmod F_5$, provando così, in un nuovo modo, che F_5 non è primo.

Prima di passare ai numeri di Mersenne, facciamo una breve digressione per mostrare un'interessante proprietà dei numeri di Fermat: infatti, non è difficile dimostrare per induzione che per ogni $n \geq 0$ si ha

$$F_{n+1} = F_0 F_1 F_2 \dots F_n + 2.$$

Nel caso particolare $n = 3$ abbiamo $F_4 = 65537 = 3 \cdot 5 \cdot 17 \cdot 257 + 2$. Una conseguenza di questo fatto è che $F_n \mid (F_{n+k} - 2)$ per ogni $k \geq 1$: utilizzando l'algoritmo di Euclide con F_n ed F_{n+k}, questa relazione implica che $(F_n, F_{n+k}) \mid 2$ e quindi il massimo comun divisore fra due numeri di Fermat distinti vale necessariamente 1, dato che sono tutti numeri dispari.

Da questo deduciamo in una nuova maniera che esistono infiniti numeri primi: infatti, per il Teorema Fondamentale dell'Aritmetica (il Teorema 3.1 di [5]) ogni numero di Fermat ha una sua scomposizione in fattori primi, e i fattori primi che compaiono nella fattorizzazione di un certo F_n *non possono* apparire nella scomposizione di altri numeri di Fermat.

Anche per i numeri di Mersenne abbiamo un risultato simile al Teorema 2.8: gli eventuali fattori primi di un numero di Mersenne soddisfano una speciale relazione di congruenza.

Teorema 2.10 *Se p e q sono numeri primi e $p \mid M_q$, allora $p \equiv 1 \bmod 2q$.*

Dim. Certamente p è dispari. Sia r l'ordine di 2 in $\mathbb{Z}_p^*$, cioè il minimo intero positivo per cui $2^r \equiv 1 \bmod p$. Evidentemente $r > 1$ poiché $2^1 = 2 \not\equiv 1 \bmod p$. Inoltre, per ipotesi, $2^q \equiv 1 \bmod p$ e quindi $r \mid q$, per l'osservazione che segue il

Teorema di Lagrange 2.3, o per il Lemma A.3. Dato che q è un numero primo, queste due cose insieme implicano che $q = r$. Infine, per il Teorema di Lagrange abbiamo che $r \mid p-1$, e cioè $p \equiv 1 \bmod q$. □

Nel caso $p = 11$, gli eventuali fattori primi di $M_{11} = 2047$ sono necessariamente $\equiv 1 \bmod 22$, ed un breve calcolo mostra che, in effetti, $2047 = 23 \cdot 89$.

In altri casi si può avere a disposizione solamente una fattorizzazione parziale di $n-1$ e riuscire comunque ad ottenere un buon algoritmo di primalità per interi di quel tipo. Come esempio rappresentativo di questi risultati, citiamo un Teorema di Pocklington (la cui dimostrazione è analoga a quella del Teorema di Lucas), poi esteso ulteriormente da Brillhart, Lehmer e Selfridge: si veda per esempio Crandall & Pomerance [1, §4.1.2].

Teorema 2.11 (Pocklington) *Sia $n > 1$ un intero, e siano dati interi a ed F tali che $F > n^{1/2}$, $F \mid n-1$, ed*

$$a^{n-1} \equiv 1 \bmod n, \qquad \left(a^{(n-1)/q} - 1, n\right) = 1 \qquad \textit{per ogni primo } q \mid F.$$

Allora n è primo.

Il caso in cui è nota la fattorizzazione di $n-1$ non è l'unico in cui una forma "speciale" di numeri strettamente parenti ad n conducono ad algoritmi particolarmente efficienti. Altri casi "speciali" sono quelli in cui è nota la fattorizzazione di $n+1$ o di n^2-1. Nel caso $n+1$ ricadono i numeri di Mersenne di cui può essere quindi verificata la primalità mediante il metodo di Lucas-Lehmer (Teorema 4.2.6 di Crandall & Pomerance [1]). In tal modo si è potuto verificare che la lista di numeri primi p fornita da Mersenne per i quali M_p è primo presenta vari errori ed omissioni. Non presentiamo in questa sede questi metodi basati sulla fattorizzazione di $n+1$ o di n^2-1 perché coinvolgono strumenti leggermente più sofisticati di quelli che vogliamo usare e rimandiamo il lettore interessato al testo di Crandall & Pomerance [1, §4.2].

Dobbiamo rilevare che tutti i numeri primi di forma "speciale" non sono di rilevanza crittografica perché, sebbene la loro primalità sia verificabile con estrema facilità, la loro particolare struttura può condurre a debolezze nel metodo crittografico che li utilizza (ad esempio il numero $n = pq$ utilizzato in RSA potrebbe essere fattorizzabile più facilmente che nel caso "generale").

3 Forme generali e speciali di numeri primi

3.1 Una formula per la funzione π

Usando il Teorema di Wilson 1.1 è possibile scrivere una formula esatta per $\pi(x)$, il numero dei numeri primi $\leq x$, e da questa è possibile, in linea di principio, ricavare una "formula" per l'n-esimo numero primo. Naturalmente, queste formule non sono utilizzabili nella pratica, perché richiedono troppi calcoli, più di quelli necessari ad eseguire il Crivello di Eratostene, ed inoltre non appaiono molto "naturali" ma anzi hanno un aspetto piuttosto artificioso.

Cominciamo osservando che il Teorema di Wilson 1.1 ci dà un modo relativamente semplice per distinguere fra numeri primi e numeri composti. Iniziamo da questi ultimi: se $n \geq 6$ non è un numero primo allora $n \mid (n-2)!$. Per dimostrare questo fatto, osserviamo che possiamo certamente trovare interi a e b tali che $n = ab$ con $1 < a \leq b < n$. Dobbiamo distinguere due casi: se $n = p^2$ dove $p \geq 3$ è un numero primo, allora $a = b$. Per ottenere la tesi è sufficiente osservare che tra i fattori di $(n-2)!$ vi sono certamente p e $2p$, e quindi p^2 divide $(n-2)!$. Nell'altro caso, possiamo trovare a e b come sopra, ma con $a < b$: dunque a e b sono fattori *distinti* di $(n-2)!$ e quindi $n \mid (n-2)!$.

La situazione è più semplice per i numeri primi: per il Teorema di Wilson, se p è primo allora $(p-2)! \equiv 1 \bmod p$. Infatti il Teorema di Wilson ci assicura che $(p-1)! \equiv -1 \bmod p$ e, poiché $(p-1) \equiv -1 \bmod p$ e $(p-1, p) = 1$, possiamo "semplificare" la congruenza (perché $p-1$ è invertibile modulo p) ed ottenere quindi $(p-2)! \equiv 1 \bmod p$. Indicando d'ora in poi rispettivamente con $\{x\}$ e $\lfloor x \rfloor$ la parte frazionaria e la parte intera di x (ossia $\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}$ e $x = \lfloor x \rfloor + \{x\}$), possiamo concludere che la quantità

$$n \left\{ \frac{(n-2)!}{n} \right\}$$

vale 0 se $n \geq 6$ è un numero composto, e vale 1 se n è un numero primo. Quindi, per $x \geq 5$ si ha

$$\pi(x) = 2 + \sum_{5 \leq n \leq x} n \left\{ \frac{(n-2)!}{n} \right\}.$$

Questa formula è poco più di una curiosità: infatti, dal punto di vista pratico, la quantità di calcoli necessari supera di gran lunga quelli che servono per eseguire il Crivello di Eratostene.

3.2 Formule per i numeri primi

Se abbiamo bisogno di generare numeri primi, possiamo desiderare di avere a disposizione una "formula" semplice per costruirne. In effetti una formula di questo

tipo è stata un po' la "pietra filosofale" dei matematici, finché Gauss, genialmente, non capí che ciò che conta davvero per uno studio approfondito dei numeri primi è la conoscenza accurata della funzione $\pi(x)$: i numeri primi sono distribuiti in modo molto irregolare, mentre la funzione $\pi(x)$ ha un comportamento più "ordinato".

3.2.1 Numeri primi e polinomi

Vogliamo dunque parlare di "formule" che permettono, in qualche modo, di generare numeri primi: a causa della loro forma, i polinomi in una variabile hanno diritto alla prima menzione in questa discussione.

Ricordiamo che se $f \in \mathbb{Z}[x]$ è un polinomio non costante, allora $|f(x)| \to +\infty$ per $x \to \pm\infty$, e quindi, in particolare, per $x \in \mathbb{N}$ sufficientemente grande si ha $f(x) \neq 0$. Più precisamente, ricordiamo che per ogni $c \in \mathbb{R}$, l'equazione $f(x) = c$ ha al massimo $\deg(f)$ soluzioni reali, e, *a fortiori*, intere. La stessa cosa vale anche se consideriamo l'equazione $f(x) \equiv 0 \bmod p$, purché p sia un numero primo. Questo è il Teorema 2.3.15 di [4].

La formula più semplice possibile è un polinomio di grado 1, dunque della forma $f(x) = qx + a$, per opportuni interi $q \geq 1$ ed $a \in \mathbb{Z}$. L'immagine di tale funzione f viene detta *progressione aritmetica* di ragione q e resto a. Non è difficile rendersi conto che se $d = (q,a) > 1$, allora *tutti* i valori $f(x)$, quando $x \in \mathbb{N}$, sono divisibili per d, e quindi, per x sufficientemente grande, $f(x)$ non è un numero primo.

Viceversa, scorrendo la lista dei numeri primi minori di 1000 che trovate nella Tabella 1 si notano facilmente alcune regolarità. Per esempio, si nota che circa $\frac{1}{4}$ dei numeri primi sono $\equiv 1 \bmod 10$, e lo stesso vale per i primi congrui rispettivamente a 3, 7 o 9 mod 10. In effetti, a parte i numeri primi 2 e 5 (si ricordi il Lemma 5.1 in [5]), gli altri 166 primi minori di 1000 sono cosí ripartiti nelle 4 classi: 40 sono $\equiv 1 \bmod 10$, 42 sono $\equiv 3 \bmod 10$, 46 sono $\equiv 7 \bmod 10$ ed infine 38 sono $\equiv 9 \bmod 10$. È del tutto evidente dalla discussione qui sopra che vi può essere al massimo un numero primo in ciascuna delle classi di congruenza 0, 2, 4, 5, 6, 8 mod 10, ma non è affatto ovvio che debbano esistere infiniti numeri primi in ciascuna delle altre classi di congruenza, o che debbano essere approssimativamente equiripartiti fra le classi stesse.

Teorema 3.1 (Dirichlet) *Dati $q \in \mathbb{N}^*$ ed $a \in \mathbb{Z}$, se $(q,a) = 1$ allora il polinomio $f(x) = qx + a$ assume valori primi per infiniti valori di $x \in \mathbb{N}$.*

In realtà è possibile, con tecniche di analisi complessa che sono una sofisticazione di quelle utilizzate per dimostrare il Teorema dei Numeri Primi (si veda il §4 di [5]), dimostrare una versione quantitativa del Teorema 3.1 in cui si prova che i

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997

Tabella 1: Lista dei primi minori di 1000.

numeri primi sono asintoticamente equamente ripartiti tra le classi di congruenza ammissibili modulo q. Per enunciare questo teorema introduciamo la funzione che "conta" il numero di primi in una progressione aritmetica:

$$\pi(x;q,a) = \mathrm{card}(\{p \le x : p \equiv a \bmod q\}).$$

Teorema 3.2 (Teorema dei Numeri Primi nelle Progressioni Aritmetiche) *Data una progressione aritmetica di ragione $q \in \mathbb{N}^*$ e resto $a \in \mathbb{Z}$, se $(q,a) = 1$, allora*

$$\pi(x;q,a) \sim \frac{1}{\varphi(q)} \frac{x}{\log x} \quad \text{per } x \to +\infty.$$

La dimostrazione del Teorema 3.2 richiede lo studio di alcune proprietà analitiche di funzioni di una variabile complessa che sono generalizzazioni della funzione ζ di Riemann. Analogamente a quanto abbiamo fatto nel primo lavoro di questa serie, sorvoliamo su questi aspetti.

Esistono casi particolari del Teorema di Dirichlet 3.1 che possono essere dimostrati senza la necessità di fare ricorso a matematica superiore: ne diamo due esempi, ma prima abbiamo bisogno di esplicitare una nuova conseguenza del Piccolo Teorema di Fermat.

Lemma 3.3 *Se p è un numero primo e $p \mid n^2+1$ per qualche $n \in \mathbb{N}$, allora $p = 2$ oppure $p \equiv 1 \bmod 4$.*

Dim. Supponiamo per assurdo che $p \equiv -1 \bmod 4$. Evidentemente l'ipotesi equivale ad $n^2 \equiv -1 \bmod p$ e per il Piccolo Teorema di Fermat 1.2 abbiamo anche $n^{p-1} \equiv 1 \bmod p$. Poiché $p-1 = 4m+2$ per qualche $m \in \mathbb{N}$, si ha

$$1 \equiv n^{p-1} = n^{4m+2} \equiv \left(n^2\right)^{2m+1} \equiv -1 \bmod p,$$

che è evidentemente assurdo. □

Teorema 3.4 *Esistono infiniti numeri primi in ciascuna delle progressioni aritmetiche* $4n+1$ *e* $4n-1$.

Dim. Supponiamo che esistano solo un numero finito di primi $p_i \equiv 1 \bmod 4$. Poniamo $N := (2p_1 \cdots p_k)^2 + 1$. Se q è un fattore primo di N, per il Lemma 3.3 $q \equiv 1 \bmod 4$, ma $q \nmid N$, cioè c'è almeno un nuovo numero primo $\equiv 1 \bmod 4$.

Se esistessero solo un numero finito di numeri primi $p_i \equiv -1 \bmod 4$, posto $N := 4p_1 \cdots p_k - 1$, si avrebbe $N \equiv -1 \bmod 4$, ed evidentemente non è possibile che tutti i fattori primi di N siano congrui a $1 \bmod 4$. □

Non è difficile dimostrare che nessun polinomio in una variabile non costante può assumere solo valori primi (ma esistono polinomi in più variabili che hanno questa proprietà: si veda Ribenboim [8, §3.III]). Si può anzi dimostrare (vedi per esempio [10]) che i polinomi assumono valori composti per "quasi tutti" i valori dell'argomento: in effetti, l'evento in cui un dato polinomio non costante assume valore primo per un valore intero del suo argomento è relativamente raro, e la dimostrazione dipende da una variante quantitativa dell'argomentazione euristica che abbiamo presentato nell'Appendice A di [5].

In compenso, se guardiamo ai valori non nulli di un polinomio non costante e consideriamo l'insieme dei loro fattori primi, quest'ultimo non può essere troppo "piccolo", nel senso che è necessariamente infinito: è un risultato di Schur del 1912, del quale diamo la dimostrazione originale che è basata su proprietà algebriche dei polinomi, mentre una dimostrazione più complessa basata sul conteggio si trova nell'Appendice B.

Teorema 3.5 *Se* $f \in \mathbb{Z}[x]$ *assume valore primo per ogni intero, allora* f *è un polinomio costante.*

Dim. Sia $f \in \mathbb{Z}[x]$ un polinomio che assume solo valori primi e sia $p := f(1)$. Si ha ovviamente $f(1+np) \equiv f(1) \equiv 0 \bmod p$ per ogni $n \in \mathbb{Z}$. Dunque $p \mid f(1+np)$ per ogni $n \in \mathbb{Z}$ e quindi $f(1+np) = \pm p$ poiché deve essere un numero primo, ma questo è assurdo se f non è costante, perché l'equazione $f(x) = \pm p$ ha al massimo $2\deg(f)$ soluzioni. □

Dunque un polinomio può assumere *solo* valori primi nel caso piuttosto banale in cui sia un polinomio costante: d'altra parte esistono polinomi, come x^2+x+41

che assumono moltissimi valori primi. In generale, si congettura che, escludendo una certa classe di polinomi che sono certamente da scartare, ogni polinomio a coefficienti interi assuma valore primo per infiniti valori della sua variabile intera. Purtroppo, al momento attuale il Teorema di Dirichlet 3.1 è l'unico caso in cui questa congettura è stata dimostrata.

Quali sono dunque i polinomi da escludere? Per prima cosa, escludiamo tutti i polinomi *riducibili*, cioè quelli che si scompongono in fattori che sono a loro volta polinomi a coefficienti interi. Si tratta di una generalizzazione del principio che abbiamo adoperato nella dimostrazione dei Teoremi 2.6 e 2.7. Per esempio, non ci possiamo ragionevolmente aspettare che il polinomio $n^5-1=(n-1)(n^4+n^3+n^2+n+1)$ assuma valore primo per $n\geq 3$ dato che il suo valore è decomposto algebricamente come prodotto di interi entrambi maggiori di 1. Naturalmente, consideriamo riducibili anche i polinomi come $f(n)=3n^3+6n^2-9$, che si decompongono in fattori di cui uno è una costante intera maggiore di 1.

Un'altra classe di polinomi di scartare è quella dei polinomi che hanno un *fattore primo fisso*: per esempio, il polinomio n^2+n+4, che non è riducibile come prodotto di polinomi a coefficienti interi di grado più basso, assume solamente valori pari, e quindi può essere primo solo nel caso in cui assuma esattamente il valore 2. L'osservazione fatta all'inizio del paragrafo ci dice che questo può avvenire al massimo per 2 valori di n.

In generale, dato un polinomio $f\in\mathbb{Z}[x]$, per ogni numero primo p poniamo

$$\rho_f(p)=\operatorname{card}(\{h \bmod p\colon\ f(h)\equiv 0 \bmod p\})$$

ossia il numero di radici modulo p dell'equazione polinomiale legata a f. Se $\rho_f(p)=p$ per qualche numero primo p, allora il polinomio f ha il fattore primo fisso p, e quindi non ci possiamo aspettare che assuma valori primi per più di $\deg(f)$ valori della sua variabile intera. Qui stiamo sfruttando la *periodicità* modulo p dei valori del polinomio f, una proprietà tanto elementare quanto importante.

Osserviamo che questa condizione può essere verificata in un numero *finito* di passi: infatti, $\rho_f(p)\leq\deg(f)$ per ogni p primo perché, come abbiamo notato prima, l'equazione $f(n)\equiv 0 \bmod p$ ha al più $\deg(f)$ soluzioni qualunque sia p. Dunque abbiamo la certezza che $\rho_f(p)<p$ non appena $p>\deg(f)$, e quindi è sufficiente determinare $\rho_f(p)$ per tutti i primi $\leq\deg(f)$. Per esempio, consideriamo il polinomio $f(n)=n^3-n+9$. Sappiamo che $\rho_f(p)\leq 3$ per ogni numero primo p, e quindi, in particolare, che $\rho_f(p)<p$ per ogni $p\geq 5$. Non resta che determinare $\rho_f(2)$ e $\rho_f(3)$: un breve calcolo mostra che valgono rispettivamente 0 e 3, e quindi il polinomio f deve essere scartato.

In due parole, possiamo dire che, una volta eliminati i polinomi che *certamente* non possono assumere infiniti valori primi, per tutti gli altri ci si aspetta che questa cosa debba succedere.

Passiamo ora ad un altro risultato interessante che lega numeri primi a polinomi: il Teorema di Schur.

Teorema 3.6 (Schur) *Sia $f \in \mathbb{Z}[x]$ un polinomio non costante. L'insieme $\mathfrak{P}_f := \{p\colon$ esiste $n \in \mathbb{N}$ tale che $f(n) \neq 0$ e $p \mid f(n)\}$ è infinito.*

Dim. Sia $f(x) = a_r x^r + \cdots + a_0$ con $a_r \neq 0$. Se $a_0 = 0$ allora $f(x) = x(a_r x^{r-1} + \cdots + a_1)$ e quindi il numero primo p divide $f(np)$, che non è nullo per $n \in \mathbb{N}$ sufficientemente grande, cioè $p \in \mathfrak{P}_f$. In questo caso, dunque, $\mathfrak{P}_f$ è l'insieme di tutti i numeri primi.

Possiamo ora supporre $a_0 \neq 0$. Per assurdo, sia $\mathfrak{P}_f = \{p_1, \ldots, p_k\}$, e sia $c \in \mathbb{Z}$ tale che $|f(ca_0 p_1 \cdots p_k)| > |a_0|$. Ma $(1/a_0) f(ca_0 p_1 \cdots p_k) \equiv 1 \bmod p_1 \cdots p_k$, e quindi esiste un numero primo $p \notin \mathfrak{P}_f$ tale che $p \mid (1/a_0) f(ca_0 p_1 \cdots p_k)$. □

Per i polinomi di grado 1 e 2 è possibile determinare esplicitamente l'insieme $\mathfrak{P}_f$, utilizzando alcune proprietà non completamente elementari: si vedano gli esempi B.1 ed B.2 nell'Appendice B.

Concludiamo il paragrafo menzionando un risultato curioso ma di scarsa utilità pratica: è stato dimostrato che esiste un numero reale $A > 1$ tale che $\lfloor A^{3^n} \rfloor$ è primo per tutti gli $n \in \mathbb{N}$. Si conosce anche un valore approssimato per $A \approx 1{,}3064\ldots$, ma i valori di questa funzione sono molto rapidamente crescenti, rendendo di fatto inutile questa conoscenza. Per saperne di più si veda [8, §3.II].

4 Come convincere della primalità di un intero

Come abbiamo fatto notare nel primo di questa serie di lavori, può accadere che un utente abbia la necessità di utilizzare un metodo crittografico ma non abbia la possibilità di costruire autonomamente i dati fondamentali richiesti dal metodo stesso. Nel caso di sistemi basati sulla primalità di interi (RSA, metodo di Rabin) si è dimostrato che è possibile fornire ad un qualunque utente un numero primo ed allegare ad esso una certificazione con la quale l'utente stesso possa verificare l'effettiva primalità del numero fornito. Il certificato deve consentire la verifica della primalità mediante una serie di calcoli computazionalmente non onerosi. In tal modo, l'"acquirente" ha a disposizione una verifica semplice e rapida del fatto che il "venditore" gli abbia effettivamente fornito quanto richiesto: un numero primo. L'effettiva possibilità di avere un siffatto strumento è stata provata nel 1975 da V. Pratt. Egli ha introdotto il concetto di "certificato di primalità succinto" per indicare una breve dimostrazione della primalità di un intero. Il risultato su cui è basata la sua analisi è una modifica del Teorema di Lucas 2.4.

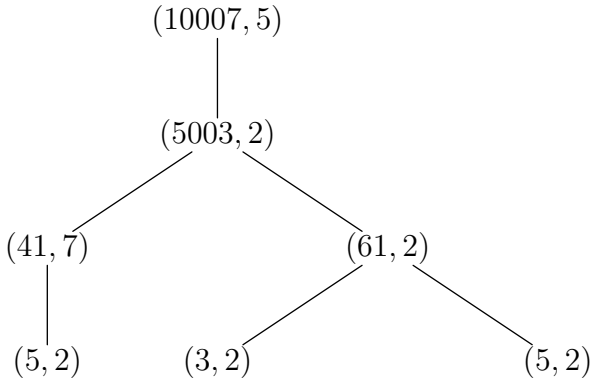

Figura 5: Il certificato di primalità succinto per $p = 10007$: ogni nodo contiene una coppia (q,a) dove q è un numero primo, ed a è un intero per cui è verificato il Teorema 4.1. Ogni nodo (q,a) è collegato ad altri nodi di livello inferiore che contengono a loro volta coppie (q_i,a_i) tali che $q_i \mid q-1$. In sostanza, per convincere qualcuno che 10007 è effettivamente primo, è sufficiente esibire l'intero $a = 5$ che soddisfa il Teorema 4.1 per tutti i fattori primi dispari di $p-1 = 10006$. A questo punto bisogna che sia primo a sua volta $q_1 = 5003$, e per questo è necessario l'intero $a_1 = 2$. Per dimostrare che $q_1 = 5003$ è primo si cercano i fattori primi dispari di $q_1 - 1 = 5002$; otteniamo così le coppie $(41,7)$ e $(61,2)$ per le quali bisogna ripetere iterativamente gli stessi passi, fino a giungere al livello più basso della figura.

Teorema 4.1 *Sia p un intero dispari, e sia a un intero tale che*

$$\begin{cases} a^{(p-1)/2} \equiv -1 \bmod p \\ a^{(p-1)/2q} \not\equiv -1 \bmod p \quad \textit{per ogni fattore primo dispari } q \mid p-1. \end{cases}$$

Allora p è un numero primo. Viceversa, se p è primo, questa condizione è soddisfatta da ogni generatore di $\mathbb{Z}_p^*$.

Dim. Se $a^{(p-1)/2} \equiv -1 \bmod p$ allora ovviamente $a^{p-1} \equiv 1 \bmod p$. Per il Teorema di Lucas 2.4 è sufficiente dimostrare che $a^{(p-1)/q} \not\equiv 1 \bmod p$ per ogni fattore primo dispari q di $p-1$. Sia $m = a^{(p-1)/2q}$: per quanto detto abbiamo $m^q \equiv -1 \bmod p$. Se $m^2 = a^{(p-1)/q}$ fosse $1 \bmod p$ avremmo $m \equiv -1 \bmod p$, contro l'ipotesi. Il viceversa è immediato. □

Questo è il punto di partenza di un algoritmo iterativo (descritto nei dettagli in Crandall & Pomerance [1, §4.1.3]): per dimostrare che i fattori q di $p-1$ sono effettivamente numeri primi si usa lo stesso risultato, e così via. Lo stesso Pratt ha dimostrato che il numero totale di moltiplicazioni di elementi di $\mathbb{Z}_p$ necessario per effettuare la verifica richiesta dal Teorema 4.1 non supera $2(\log p)^2/(\log 2)^2$. Questo è un fatto fondamentale perché ci assicura che la quantità di calcoli neces-

sari alla verifica è inferiore a quella di un algoritmo di primalità (anche delle più sofisticate e recenti versioni del metodo di Agrawal-Kayal-Saxena).

Il certificato di primalità di Pratt consiste quindi nel fornire un insieme di dati rappresentabile come uno schema ad albero, vedi Figura 5, in cui ogni nodo contiene una coppia (q,a) dove q è un primo e a è un intero per cui è verificato il verificato il Teorema 4.1. Ogni nodo (q,a) è collegato ad altri nodi di livello inferiore che contengono a loro volta coppie (q_i,a_i) tali che $q_i \mid q-1$ e per cui vale il Teorema 4.1 con q_i al posto di q ed a_i al posto di a. Per controllare il certificato l'"acquirente" segue l'albero a ritroso (dalle foglie alla radice) calcolando ad ogni passo delle potenze modulari e delle congruenze (calcoli poco onerosi). Ad ogni passo viene provata la primalità di un q_i e ciò viene sfruttato al passo successivo per provare la primalità di q_{i-1}. Il calcolo totale è computazionalmente "facile" grazie al risultato di Pratt, ossia la dimostrazione che il numero massimo di rami (cioè di collegamenti tra due nodi) compresi tra la radice e le foglie è $O\big(\log^2 p\big)$, dove p è il primo numero presente nella radice dell'albero.

5 Progetti di ricerca di primi in internet

Con l'avvento della rete internet si sono anche moltiplicati i siti che contengono riferimenti ai numeri primi. Purtroppo, tra essi ve ne sono alcuni che hanno contenuto non totalmente affidabile e quindi è necessario essere in grado di distinguere quelli che contengono informazioni consistenti dagli altri. Vogliamo qui segnalare alcuni siti utili agli appassionati e anche fissare qualche idea sui progetti di ricerca di "grandi" primi.

Il primo sito che menzioniamo è il "Prime Page" di C. Caldwell raggiungibile al link: `http://www.utm.edu/research/primes/`.

In esso sono raccolte molte informazioni sullo stato dell'arte nella ricerca della primalità; l'autore inoltre pone molta attenzione a distinguere le varie tipologie di ricerca a seconda della finalità dei primi ricercati.

Sono presenti varie sezioni in cui sono riportate anche una serie di informazioni sulle tecniche matematiche utilizzate per lo studio dei numeri primi e di problemi collegati oltre ad una buona bibliografia; ad esempio parti del sito sono dedicate a presentare problemi aperti e congetture in Teoria dei Numeri, al Teorema dei Numeri Primi, a quali siano le strategie da utilizzare per verificare la primalità di un intero, ecc.

Riteniamo dunque che il "Prime Page" rappresenti una buona sorgente di informazioni (non troppo tecniche) per gli appassionati non professionisti del settore.

Il secondo sito riguarda un progetto di calcolo dei valori della funzione $\pi(N)$ per valori sempre più grandi di N: `http://numbers.computation.free.fr/`

Constants/Primes/Pix/pixproject.html. In particolare, il miglior risultato noto al momento è il valore

$$\pi(4\cdot 10^{22}) = 783\,964\,159\,847\,056\,303\,858 \approx 7,83\cdot 10^{20}.$$

La strategia utilizzata è quella del *progetto di calcolo distribuito*. In pratica ad ogni partecipante viene assegnato un intervallo di interi su cui eseguire i calcoli mediante un particolare programma (anch'esso fornito) da installare. Usualmente tale software viene eseguito durante i periodi di inattività (in gergo: "sleep") della macchina.

Nella categoria "ricerca del più grande primo noto" menzioniamo GIMPS (Great Internet Mersenne Prime Search): http://www.mersenne.org/prime.htm.

Tale sito riporta i risultati ottenuti da un progetto di calcolo distribuito sulla ricerca di numeri primi della forma 2^p-1, dove p è anch'esso un primo. Abbiamo introdotto i numeri di Mersenne ed alcune loro proprietà nel §2. Nel software distribuito in questo sito viene utilizzata un'ottimizzazione del già menzionato algoritmo di Lucas-Lehmer.

Al momento il più grande primo noto è proprio un primo di Mersenne la cui primalità è stata dimostrata tramite GIMPS nel febbraio 2005; esso è $2^{25964951}-1$ (che ha 7816230 cifre decimali).

Come abbiamo già notato precedentemente l'interesse nella ricerca del "record" di grandezza è, dal nostro punto di vista, molto relativa perché, ad esempio, questi interi non hanno applicazioni crittografiche e quindi, in pratica, questo tipo di risultato non rappresenta altro che lo stato dell'arte nella capacità di calcolo dei moderni microprocessori in commercio.

Progetti di calcolo distribuito analoghi da un punto di vista informatico riguardano l'analisi delle radiazioni cosmiche alla ricerca di un segnale proveniente da una intelligenza non umana (SETI@home: http://setiathome.ssl.berkeley.edu/) ed il calcolo dei punti di azzeramento della funzione ζ di Riemann al fine di verificarne computazionalmente la loro dislocazione sulla retta $\Re(s)=\frac{1}{2}$ (Ipotesi di Riemann) (ZetaGrid: http://www.zetagrid.net/).

A Gruppi ciclici, Residui quadratici, Simbolo di Legendre

Come abbiamo già fatto nel primo lavoro di questa serie, a questo punto includiamo una piccola appendice in cui collezioniamo risultati di ordine più generale sperando di fornire una più ampia prospettiva al nostro discorso.

A.1 Gruppi ciclici

Cominciamo con il definire in generale i gruppi ciclici.

Definizione A.1 (Gruppo ciclico) *Un gruppo G si dice* ciclico *se esiste $g \in G$ tale che, per ogni $h \in G$, esiste $n \in \mathbb{Z}$ per cui $h = g^n$. Un tale elemento g si dice* generatore *di G perché ogni elemento di G si può esprimere in termini di g.*

Ricordiamo che è consueto scrivere ng in luogo di g^n nei gruppi additivi.

Osserviamo che $\mathbb{Z}_n$ è un *gruppo ciclico*: in effetti $g = 1$ genera $\mathbb{Z}_n$ qualunque sia $n \in \mathbb{N}^*$. Un problema interessante è dunque la determinazione dei generatori di $\mathbb{Z}_n$: non è difficile convincersi del fatto che g genera $\mathbb{Z}_n$ se e solo se $(g,n) = 1$ ossia se e solo se g è *invertibile* modulo n e quindi esiste $h \in \mathbb{Z}_n$ tale che $hg \equiv 1 \bmod n$. Infatti, se $(g,n) = d > 1$ allora tutti i numeri mg sono divisibili per d e quindi $d \mid (mg + kn)$ per ogni $k \in \mathbb{Z}$: dunque $1 \in \mathbb{Z}_n$ non è della forma mg e cioè g non è un generatore di $\mathbb{Z}_n$. È possibile trasformare questa osservazione in una dimostrazione rigorosa e provare così che l'insieme dei generatori di $\mathbb{Z}_n$ è formato da tutti e soli gli elementi di $\mathbb{Z}_n^*$.

Resta per il momento aperto il problema di sapere quali sono, se ne esistono, i gruppi ciclici del tipo $\mathbb{Z}_n^*$. Per fare ciò ci serve enunciare qualche risultato e qualche definizione di cui abbiamo già visto una forma particolare.

Per prima cosa diamo la definizione di ordine di un elemento in un gruppo generale.

Definizione A.2 *Diciamo ordine $o_G(g)$ di un elemento $g \in G$ il minimo $n \in \mathbb{N}^*$ tale che $g^n = e$, o in notazione additiva, $ng = e$.*

Inoltre è valido il seguente

Lemma A.3 *Se d è l'ordine di $g \in G$, allora $g^n = e$ se e solo se $d \mid n$.*

Dim. Dato che $g^n = e$ e $g^d = e$ per ipotesi, si ha anche $g^{\lambda n + \mu d} = e$ per ogni λ, $\mu \in \mathbb{Z}$. Grazie al Teorema di Euclide (si veda per esempio il Teorema 2.2.1 di [4]) si può esprimere (n,d) come combinazione lineare intera di d e n ossia esistono $a,b \in \mathbb{Z}$ tali che $(n,d) = an + bd$. Si ha quindi $g^{(n,d)} = e$. Ma $(n,d) \leq d$ e quindi, per la minimalità di d, deve essere $(n,d) = d$, cioè $d \mid n$. □

Abbiamo già visto l'utilità dei Teoremi di Eulero 2.2 e di Lagrange 2.3. In realtà questi risultati valgono, nelle seguenti forme, in un ambito più generale che consente loro una più ampia applicazione.

Teorema A.4 (Lagrange) *Se G è un gruppo finito, allora per ogni $g \in G$ si ha $o_G(g) \mid \mathrm{card}(G)$.*

Corollario A.5 (Eulero) *Se G è un gruppo finito e $g \in G$, allora $g^{\mathrm{card}(G)} = e$.*

Dim. Posto $d = o_G(g)$ si ha $\mathrm{card}(G)/d \in \mathbb{N}$ per il Lemma A.3 e quindi $g^{\mathrm{card}(G)} = \left(g^d\right)^{\mathrm{card}(G)/d} = e$. □

A questo punto torniamo ad esaminare il problema della ciclicità degli insiemi $\mathbb{Z}_p^*$. Abbiamo il seguente risultato.

Teorema A.6 (Gauss) *Se p è un numero primo, allora $\mathbb{Z}_p^*$ è un gruppo moltiplicativo ciclico, cioè esiste $g = g_p \in \mathbb{Z}_p^*$ tale che ogni elemento di $\mathbb{Z}_p^*$ è una potenza di g_p.*

La dimostrazione del Teorema A.6 non è semplice; per esempio potete trovarla in [4, §3.6]. Vediamo qui solo un esempio: il caso del numero primo $p = 13$. Possiamo facilmente calcolare le potenze successive degli elementi di $\mathbb{Z}_{13}^*$: soltanto in 4 casi accade che queste potenze assumano tutti i valori possibili modulo 13. In altre parole, il gruppo moltiplicativo $\mathbb{Z}_{13}^*$ è generato da $g_1 = 2$, $g_2 = 6 = g_1^5$, $g_3 = 7 = g_1^{-1}$, $g_4 = 11 = g_2^{-1} = g_1^7$.

In realtà è possibile classificare completamente i gruppi $\mathbb{Z}_n^*$ che sono ciclici (si veda, per esempio, [4, §3.6]) grazie a questa generalizzazione del teorema precedente.

Teorema A.7 (Gauss) *Il gruppo moltiplicativo $\mathbb{Z}_n^*$ è ciclico per $n = 1, 2, 4$, e per $n = p^\alpha, 2p^\alpha$, dove p è un numero primo dispari ed $\alpha \geq 1$, e per nessun altro valore di n.*

A.2 Residui quadratici e Simbolo di Legendre

Una particolare importanza (anche in ambito applicativo) hanno quegli elementi di $\mathbb{Z}_p^*$ che sono il quadrato di altri elementi.

Definizione A.8 (Residuo quadratico) *Sia p un numero primo ed $a \in \mathbb{Z}$. Diremo che a è un* residuo quadratico modulo p *se e solo se la congruenza $x^2 \equiv a \bmod p$ ammette soluzioni.*

Per comodità notazionale si usa introdurre un simbolo compatto il cui valore indichi se a è un residuo quadratico o meno.

Definizione A.9 (Simbolo di Legendre) *Sia p un numero primo ed a un intero qualsiasi. Poniamo*

$$\left(\frac{a}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{se } p \nmid a \text{ e l'equazione } x^2 \equiv a \bmod p \text{ è risolubile.} \\ 0 & \text{se } p \mid a. \\ -1 & \text{se } p \nmid a \text{ e l'equazione } x^2 \equiv a \bmod p \text{ non è risolubile.} \end{cases}$$

Per comodità tipografica, nel testo scriviamo il simbolo di Legendre nella forma $(a \mid p)$.

D'ora in poi potremo anche dire che a è un *residuo quadratico modulo* p se $(a \mid p) = 1$ e che a è un *non-residuo quadratico* se $(a \mid p) = -1$.

Osserviamo ora che, grazie alla ciclicità di $\mathbb{Z}_p^*$, possiamo caratterizzare i residui quadratici in modo molto semplice.

Lemma A.10 *Sia $p \geq 3$ un numero primo e sia g un qualsiasi generatore di $\mathbb{Z}_p^*$. Dato $a \in \mathbb{Z}_p^*$, sia $r = r_a \in \mathbb{Z}_{p-1}$ tale che $g^r \equiv a \bmod p$. Allora $(a \mid p) = 1$ se e solo se r è pari.*

Dim. L'equazione $x^2 \equiv a \bmod p$ può essere riscritta nella forma $g^{2m} \equiv g^r \bmod p$, dove $g^m = x$, e cioè $g^{2m-r} \equiv 1 \bmod p$. Ma per il Lemma A.3 questo può accadere se e solo se $p-1 \mid 2m-r$, e dato che nelle nostre ipotesi $p-1$ è pari, questo implica che $2m-r$ è pari, e quindi che r è pari. □

Il fatto interessante è che i residui ed i non residui quadratici realizzano una partizione di $\mathbb{Z}_p^*$ in due sottoinsiemi aventi la stessa cardinalità. Per provare ciò osserviamo per prima cosa che le congruenze quadratiche modulo un primo hanno esattamente due soluzioni.

Lemma A.11 *Sia $a \in \mathbb{Z}$. Se p è primo, l'equazione $x^2 \equiv a^2 \bmod p$ ha solo le soluzioni $x \equiv a \bmod p$ e $x \equiv -a \bmod p$.*

Dim. Se p è un numero primo, dal fatto che $x^2 - a^2 = (x-a)(x+a) \equiv 0 \bmod p$ segue che $p \mid (x-a)$ oppure $p \mid (x+a)$ ricordando che se $p \mid \alpha\beta$ allora $p \mid \alpha$ oppure $p \mid \beta$. Quindi $x \equiv a \bmod p$ oppure $x \equiv -a \bmod p$. □

Sfruttando tale Lemma possiamo ora provare la seguente

Proposizione A.12 *Poniamo*

$$R_p \stackrel{\text{def}}{=} \left\{ x \in \mathbb{Z}_p^* \colon \left(\frac{x}{p}\right) = 1 \right\}, \qquad N_p \stackrel{\text{def}}{=} \left\{ x \in \mathbb{Z}_p^* \colon \left(\frac{x}{p}\right) = -1 \right\}.$$

Per $p \geq 3$ si ha $\operatorname{card}(R_p) = \operatorname{card}(N_p) = \frac{1}{2}(p-1)$.

Dim. Consideriamo $f \colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ definita da $f(x) = x^2 \bmod p$, e osserviamo che $\operatorname{card}(f^{-1}(a)) = 0$ se $a \in N_p$, ed $\operatorname{card}(f^{-1}(a)) = 2$ se $a \in R_p$, perché in questo caso l'equazione $x^2 \equiv a \bmod p$ per definizione ha almeno una soluzione x_0 (e quindi anche $-x_0 \neq x_0$ è soluzione), e non può averne più di 2 per il Lemma A.11. Abbiamo dunque ripartito $\mathbb{Z}_p^*$ in $\operatorname{card}(R_p)$ sottoinsiemi disgiunti di cardinalità 2, da cui $2\operatorname{card}(R_p) = p-1$, e la tesi segue. □

Osserviamo adesso che il simbolo di Legendre ha alcune interessanti proprietà che consentono di calcolarlo piuttosto agilmente. Per prima cosa ci serve il seguente

Lemma A.13 *Dato $a \in \mathbb{Z}_n$, se $(a,n) = 1$ allora l'applicazione $f_a \colon \mathbb{Z}_n \to \mathbb{Z}_n$ definita da $f_a(x) := ax \bmod n$ è una biiezione, con inversa $f_{a^{-1}}$.*

Dim. Se $ax_1 \equiv ax_2 \bmod n$ ed $(a,n) = 1$, è sufficiente moltiplicare ambo i membri della congruenza per a^{-1} per ottenere $x_1 \equiv x_2 \bmod n$, e quindi f_a è iniettiva. Inoltre $f_a(x) = b$ per $x = a^{-1}b$, e quindi f_a è anche suriettiva. □

Inoltre ci serve la seguente caratterizzazione delle funzioni biiettive tra insiemi di cardinalità finita di cui diamo due formulazioni equivalenti.

Teorema A.14 (Principio dei cassetti)
Prima forma:
Siano A e B due insiemi finiti di cardinalità a e b rispettivamente. Se $a > b$ non esistono funzioni iniettive $f \colon A \to B$.
Seconda forma:
Siano A e B due insiemi finiti con la stessa cardinalità. Se $f \colon A \to B$ è una funzione iniettiva, allora è anche suriettiva.

Il Teorema, che in realtà si può dimostrare essere equivalente al Principio di Induzione, prende il proprio (pittoresco) nome dalle seguenti due formulazioni "intuitive":
Prima forma:
se a calzini sono disposti in b cassetti ed $a > b$, allora c'è almeno un cassetto che contiene almeno due calzini.
Seconda forma:
se a calzini sono disposti in a cassetti, e nessun cassetto contiene più di un calzino, allora ogni cassetto contiene esattamente un calzino.

Facciamo dunque uso del principio dei cassetti per mostrare che il simbolo di Legendre si comporta in modo "buono" rispetto al prodotto.

Proposizione A.15 *Qualunque siano $a, b \in \mathbb{Z}$ si ha*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Dim. Se $p = 2$ non c'è niente da dimostrare. Se $p \mid ab$ entrambi i membri sono nulli. Se $\left(a \mid p\right) = \left(b \mid p\right) = 1$ è ovvio che l'equazione $x^2 \equiv ab \bmod p$ abbia soluzione. Se invece, per esempio, $\left(a \mid p\right) = 1$ e $\left(b \mid p\right) = -1$, sia y una soluzione di $y^2 \equiv a \bmod p$. L'equazione $x^2 \equiv ab \bmod p$ diventa $\left(xy^{-1}\right)^2 \equiv b \bmod p$, che quindi non ha soluzione. Resta il caso in cui $\left(a \mid p\right) = \left(b \mid p\right) = -1$. Poniamo $f \colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $f(x) = ax \bmod p$. Per quanto appena visto si ha $f(R_p) = N_p$ e quindi, per il Lemma A.13, $f(N_p) = R_p$, dato che R_p ed N_p hanno la stessa cardinalità

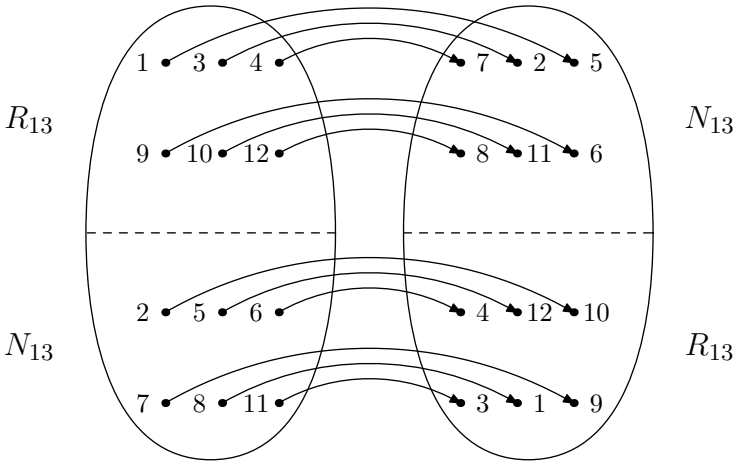

Figura 6: Poiché $\left(5 \mid 13\right) = -1$, l'applicazione $f_5(x) = 5x \bmod 13$, che è una biiezione, "scambia" l'insieme $R_{13} = \{1,\ 3,\ 4,\ 9,\ 10,\ 12\}$ dei residui quadratici modulo 13 con l'insieme $N_{13} = \{2, 5, 6, 7, 8, 11\}$ dei non-residui quadratici. In altre parole, $f(R_{13}) = N_{13}$ ed $f(N_{13}) = R_{13}$.

per la Proposizione A.12. Dunque *ab* è un residuo quadratico, per il principio dei cassetti del Teorema A.14. □

Nella Figura 6 rappresentiamo, nel caso $p = 13$ e $a = 5$, la funzione f usata nell'ultima parte della dimostrazione della precedente Proposizione.

In alternativa, per il Lemma A.10, dato un generatore g del gruppo ciclico $\mathbb{Z}_p^*$, e determinati $\alpha, \beta \in \mathbb{Z}_{p-1}$ tali che $a = g^\alpha$ e $b = g^\beta$, il Lemma A.15 equivale all'affermazione che *ab* è un quadrato in $\mathbb{Z}_p^*$ se e solo se $\alpha + \beta$ è pari.

La seconda fondamentale proprietà del simbolo di Legendre consente di esprimere in modo compatto una relazione di reciprocità di un primo rispetto ad un altro.

Teorema A.16 (Legge di Reciprocità Quadratica (Gauss)) *Se p e q sono primi dispari distinti, allora*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}, \qquad \textit{mentre} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

La legge di reciprocità quadratica è uno dei risultati più famosi e celebrati di Gauss. Di essa esistono molteplici dimostrazioni che, purtroppo, richiedono un insieme di nozioni che non possiamo sviluppare in questa sede: rimandiamo il Lettore interessato al testo di Hardy e Wright [3, Theorem 98].

Osserviamo comunque che, per quanto riguarda l'utilizzo "pratico" del Teorema A.16, ciò che conta è solamente la parità dell'esponente di (-1). È facile

osservare che, se almeno uno fra p e q è $\equiv 1 \bmod 4$, allora il primo esponente è pari e quindi $p \bmod q$ e $q \bmod p$ o sono entrambi residui quadratici o sono entrambi non-residui quadratici. D'altra parte, esaminando p modulo 8, abbiamo che il secondo esponente è pari se e solo se $p \equiv \pm 1 \bmod 8$ e quindi $2 \bmod p$ è un residuo quadratico solo in questo caso. Dunque

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot \begin{cases} -1 & \text{se } p \equiv q \equiv 3 \bmod 4; \\ +1 & \text{altrimenti.} \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} +1 & \text{se } p \equiv \pm 1 \bmod 8; \\ -1 & \text{se } p \equiv \pm 3 \bmod 8. \end{cases}$$

La legge di reciprocità quadratica e la completa moltiplicatività del simbolo di Legendre espressa dal Teorema A.16 consentono di sviluppare un algoritmo avente complessità polinomiale in $\log p$ per calcolare il simbolo di Legendre e capire in tal modo se $x^2 \equiv a \bmod p$ ha soluzione, si veda per esempio Crandall & Pomerance [1, §2.3.1]. Le idee fondamentali dell'algoritmo sono contenute nel seguente esempio in cui vogliamo determinare se la congruenza $x^2 \equiv 42 \bmod 47$ ha soluzione. Si può procedere come segue:

1) $\left(42 \mid 47\right) = \left(2 \mid 47\right)\left(3 \mid 47\right)\left(7 \mid 47\right)$ per la Proposizione A.15;

2) per la legge di reciprocità quadratica A.16, si ha $\left(2 \mid 47\right) = 1$, $\left(3 \mid 47\right) = (-1)\left(47 \mid 3\right)$ e $\left(7 \mid 47\right) = (-1)\left(47 \mid 7\right)$. Quindi $\left(42 \mid 47\right) = \left(47 \mid 3\right)\left(47 \mid 7\right)$;

3) osserviamo che $\left(47 \mid 3\right) = \left(2 \mid 3\right)$ e $\left(47 \mid 7\right) = \left(5 \mid 7\right)$ perché $47 \equiv 2 \bmod 3$ e $47 \equiv 5 \bmod 7$. Allora $\left(42 \mid 47\right) = \left(2 \mid 3\right)\left(5 \mid 7\right)$;

4) per la legge di reciprocità quadratica A.16, si ha $\left(2 \mid 3\right) = -1$ e $\left(5 \mid 7\right) = \left(7 \mid 5\right) = \left(2 \mid 5\right)$ perché $7 \equiv 2 \bmod 5$. Allora $\left(42 \mid 47\right) = -\left(2 \mid 5\right)$;

5) in conclusione, per la legge di reciprocità quadratica A.16, $\left(2 \mid 5\right) = -1$ da cui segue $\left(42 \mid 47\right) = 1$ ossia: $x^2 \equiv 42 \bmod 47$ ha soluzione.

Purtroppo non esiste un metodo diretto altrettanto efficiente per determinare esplicitamente una soluzione di una congruenza quadratica. Nell'esempio precedente, si dimostra, con qualche calcolo, che le soluzioni sono $x \equiv \pm 18 \bmod 47$.

Un ingrediente fondamentale della dimostrazione della legge di reciprocità quadratica A.16 è sufficientemente semplice ed interessante da meritare una menzione, anche perché viene utilizzato nella dimostrazione del Teorema di Pepin 2.9.

Teorema A.17 (Eulero) *Se $p \geq 3$ è un numero primo e $p \nmid a$, allora $\left(a \mid p\right) \equiv a^{(p-1)/2} \bmod p$.*

Dim. Poniamo $x = a^{(p-1)/2}$; per il Piccolo Teorema di Fermat 1.2 sappiamo che $x^2 \equiv 1 \bmod p$, e per il Lemma A.11 abbiamo dunque $x \equiv \pm 1 \bmod p$. Sia ora g un generatore di $\mathbb{Z}_p^*$ e sia $r \in \mathbb{Z}_{p-1}$ tale che $a \equiv g^r \bmod p$. Osserviamo che $x = g^{r(p-1)/2} \equiv 1 \bmod p$ se e solo se $p-1 \mid \frac{1}{2}r(p-1)$ per il Lemma A.3, e questo accade se e solo se r è pari. Possiamo ora concludere per il Lemma A.10. □

Il Teorema A.17 può anche essere utilizzato, insieme al calcolo polinomiale del simbolo di Legendre, per costruire un altro metodo di pseudoprimalità; tale algoritmo (detto di Solovay-Strassen) è però più debole di quello di Miller-Rabin di cui abbiamo parlato nel §1 di questo articolo.

Sfruttiamo ora quanto detto fino a questo punto per fornire una dimostrazione del Teorema di Pepin 2.9.

Dim. del Teorema di Pepin 2.9. Se la congruenza dell'enunciato è valida allora F_n è primo. Infatti è sufficiente fissare $a = 3$ nel Teorema di Lucas 2.4 e fare giocare a F_n il ruolo di n. Viceversa, supponiamo che F_n sia primo; allora $F_n \equiv 2 \bmod 3$ perché $2^{2^n} \equiv 1 \bmod 3$. Quindi F_n non è un quadrato modulo 3, cioè $\left(F_n \mid 3\right) = -1$. Siccome $F_n \equiv 1 \bmod 4$, la legge di reciprocità quadratica A.16 fornisce $\left(3 \mid F_n\right) = \left(F_n \mid 3\right) = -1$ cioè 3 non è un quadrato modulo F_n. Grazie al Teorema A.17, abbiamo quindi che $3^{(F_n-1)/2} \equiv -1 \bmod F_n$. □

Come ultima applicazione mostriamo come si possono calcolare le radici quadrate di -1 in $\mathbb{Z}_p^*$.

Lemma A.18 *Se p è un numero primo $\equiv 1 \bmod 4$ ed $a \in \mathbb{Z}$ soddisfa $\left(a \mid p\right) = -1$, allora $x_0 = a^{(p-1)/4}$ è una soluzione dell'equazione $x^2 + 1 \equiv 0 \bmod p$.*

Dim. Per il Lemma A.11 si ha $x_0^2 \equiv \pm 1 \bmod p$. Sia g un generatore di $\mathbb{Z}_p^*$, e sia $r \in \mathbb{N}$ tale che $a = g^r$: dunque $x_0 = g^{r(p-1)/4}$. Per il Lemma A.10, r è dispari e quindi $p-1 \nmid \frac{1}{2}r(p-1)$; questo implica che $x_0^2 + 1 \equiv 0 \bmod p$. □

Evidentemente, se g genera $\mathbb{Z}_p^*$, allora si può scegliere $a = g$, ma il Lemma qui sopra implica che è sufficiente avere un non-residuo quadratico.

B Formule per i numeri primi, II

Diamo una nuova dimostrazione del Teorema di Schur 3.6 che richiede qualche conoscenza di analisi matematica: varie generalizzazioni ed altre dimostrazioni si possono trovare nell'articolo di Morton [7].

Dimostrazione alternativa del Teorema 3.6. Per assurdo, sia $\mathfrak{P}_f = \{p_1, \ldots, p_k\}$. Se $f(x) = a_r x^r + \cdots + a_0$ con $a_r \neq 0$, poniamo $U(x) := \{m \leq x\colon m \in f(\mathbb{N})\}$; si ha $\operatorname{card}(U(x)) \sim \left(x/|a_r|\right)^{1/r}$ per $x \to +\infty$. Invece, posto $V(x) := \{m \leq x\colon p \mid m \Rightarrow p \in \mathfrak{P}_f\}$, si ha $m \in V(x)$ se e solo se esistono $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ tali che $m =$

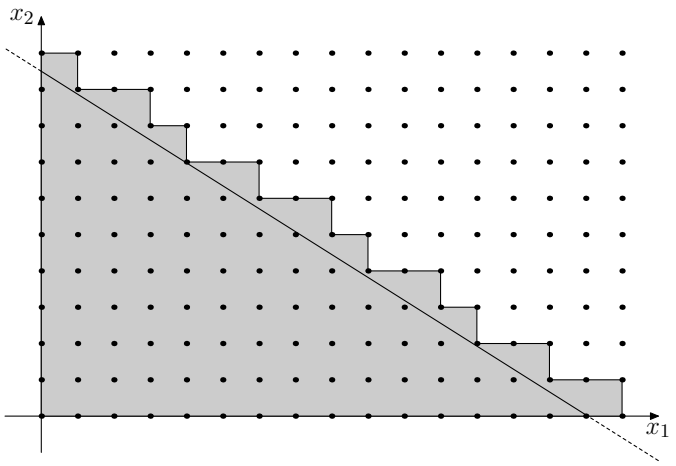

Figura 7: La dimostrazione del Teorema di Schur 3.6 nel caso in cui $k = 2$ e $\mathfrak{P}_f = \{2, 3\}$. L'area colorata è uguale a $|V(x)|$.

$p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ e quindi $\log m = \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k \le \log x$. Questo significa che

$$0 \le \alpha_i \le \frac{\log x}{\log p_i} \le \frac{\log x}{\log 2}$$

per $i = 1, 2, \ldots, k$. Dobbiamo dunque contare quanti sono gli interi α che soddisfano la disuguaglianza $0 \le \alpha \le y$, dove $y = (\log x)/\log 2$: questi sono $1 + \lfloor y \rfloor \le 2 + y$. Infatti, ci sono esattamente $\lfloor y \rfloor$ interi nell'intervallo da 1 ad y, poi dobbiamo aggiungere un'altra unità per contare anche 0, e per concludere ricordiamo che, per sua stessa definizione, $\lfloor y \rfloor \le y$ per ogni numero reale y. In definitiva

$$\mathrm{card}(V(x)) \le \left(2 + \frac{\log x}{\log p_1}\right) \cdots \left(2 + \frac{\log x}{\log p_k}\right) \le \left(2 + \frac{\log x}{\log 2}\right)^k.$$

Per x sufficientemente grande, questa cosa è in contraddizione con il fatto che $U(x) \subseteq V(x)$ e quindi $\mathrm{card}(U(x)) \le \mathrm{card}(V(x))$. □

La Figura 7 illustra il caso $k = 2$ e $\mathfrak{P}_f = \{2, 3\}$ della dimostrazione. La cardinalità di $V(x)$ è uguale al numero di punti a coordinate intere nel triangolo delimitato dagli assi cartesiani e dalla retta di equazione $x_1 \log 2 + x_2 \log 3 = \log x$. Assegniamo ad ogni punto $(a_1, a_2) \in \mathbb{N}^2$ che soddisfa questa disuguaglianza il quadrato di vertici opposti (a_1, a_2), $(a_1 + 1, a_2 + 1)$. Il numero di questi punti è uguale all'area colorata, cioè all'area del triangolo con un errore dell'ordine del perimetro del triangolo stesso, e l'area vale $(\log x)^2/(2 \log 2 \log 3) + O(\log x)$.

Calcoliamo ora l'insieme $\mathfrak{P}_f$ in due casi particolari: $f(x) = qx + a$ e $f(x) = x^2 + 1$.

Esempio B.1 *Sia $f(x) = qx + a$ con a, $q \in \mathbb{Z}$, e $q \neq 0$. Se $(a,q) = 1$ allora il Lemma A.13 implica che $\mathfrak{P}_f = \{p\colon p \nmid q\}$ perché in tal caso $x \equiv -aq^{-1} \bmod p$ è l'unica soluzione di $f(x) \equiv 0 \bmod p$. Se $(a,q) > 1$, allora $\mathfrak{P}_f = \{p\colon p \nmid q\} \cup \{p\colon p \mid (a,q)\}$ perché in tal caso $qx \equiv -a \bmod p$ è equivalente a $x \equiv -aq^{-1} \bmod p$ se $(p,q) = 1$ e a $(q/p)x \equiv -(a/p) \bmod 1$ se $p \mid (a,q)$.*

Esempio B.2 *Se $f(x) = x^2 + 1$, allora il Lemma A.18 implica che $\mathfrak{P}_f = \{2\} \cup \{p\colon p \equiv 1 \bmod 4\}$. Più in generale, se $f(x) = ax^2 + bx + c$ con $a \neq 0$, sia $\Delta = b^2 - 4ac$ il discriminante di f: se $\Delta \neq 0$, per il Lemma A.13 e la Definizione A.9 in questo caso $\mathfrak{P}_f = A \cup \{p\colon \left(\Delta \mid p\right) = 1\}$, dove A è un sottoinsieme dell'insieme dei divisori primi di $2a\Delta$. Infatti, se $p \nmid 2a$ l'equazione $f(x) \equiv 0 \bmod p$ è equivalente a $4a^2x^2 + 4abx + b^2 \equiv \Delta \bmod p$, cioè $(2ax + b)^2 \equiv \Delta \bmod p$ e questa è risolubile se e solo se $\left(\Delta \mid p\right) = 1$. Inoltre $2 \in \mathfrak{P}_f$ se e solo se $c(a+b+c) \equiv 0 \bmod 2$. Infine, se $p \mid a\Delta$ oppure se $\Delta = 0$ ricadiamo nel caso descritto nell'Esempio B.1.*

B.1 La formula di Gandhi

Torniamo alle formule per i numeri primi: ne diamo una (non elementare, ma non particolarmente complicata) che è stata scoperta nel ventesimo secolo. Per poterla enunciare e dimostrare abbiamo prima bisogno di una definizione e di un Lemma.

Definizione B.3 (Funzione di Möbius) *Poniamo $\mu(1) = 1$. Se $n \geq 2$ ha la fattorizzazione canonica $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ poniamo*

$$\mu(n) = \begin{cases} (-1)^k & \text{se } \alpha_1 = \alpha_2 = \cdots = \alpha_k = 1; \\ 0 & \text{se qualche } \alpha_i \text{ è} \geq 2. \end{cases}$$

Lemma B.4 *Poniamo*

$$I(n) = \sum_{d \mid n} \mu(d),$$

dove la somma è fatta su tutti i divisori positivi di n. Allora $I(1) = 1$ ed $I(n) = 0$ per $n \geq 2$.

Dim. Se $n = 1$ la somma si riduce ad un solo addendo che vale 1. Se $n \geq 2$ ha la fattorizzazione canonica $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, dalla definizione B.3 si vede che gli addendi non nulli della somma sono in corrispondenza biunivoca con i sottoinsiemi di $\{p_1, p_2, \ldots, p_k\}$ con la convenzione che il sottoinsieme vuoto corrisponde al divisore $d = 1$. Inoltre, la stessa definizione implica che se un tale sottoinsieme ha m elementi, allora il corrispondente addendo vale $(-1)^m$. Ricordiamo che un insieme con k elementi ha esattamente $\binom{k}{m}$ sottoinsiemi con m elementi: quindi

$$\sum_{d \mid n} \mu(d) = 1 + \sum_{m=1}^{k} (-1)^m \binom{k}{m} = (1-1)^k = 0.$$

$$
\begin{array}{rr}
d=1 & 0\,.\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\ldots \\
d=2 & -0\,.\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\ldots \\
d=3 & -0\,.\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\ldots \\
d=5 & -0\,.\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\ldots \\
d=6 & 0\,.\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\ldots \\
d=10 & 0\,.\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\ldots \\
d=15 & 0\,.\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\ldots \\
d=30 & -0\,.\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\ldots \\
\hline
S_3= & 0\,.\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\ldots
\end{array}
$$

Figura 8: La formula di Gandhi B.5 "corrisponde" a fare un crivello con i fattori primi di P_n, scrivendo in binario le quantità $\mu(d)/(2^d-1)$ e sommando in colonna, bit per bit. Per esempio, il termine con $d=3$ vale $-1/7$, che, scritto in base 2, vale $-0,\overline{001}$. Si noti che la quantità S_3 vale $\frac{1}{2}+2^{-7}+\ldots$ e quindi $p_4=7$.

L'ultima uguaglianza segue dallo sviluppo della potenza $(x+y)^k$ con $x=1$ ed $y=-1$, sfruttando il "triangolo di Tartaglia." □

Nel caso $n=60=2^2\cdot 3\cdot 5$, gli addendi non nulli nella somma in questione provengono da $d=1,\ 2,\ 3,\ 5,\ 6,\ 10,\ 15,\ 30$. Raggruppando questi numeri a seconda del numero di divisori primi che hanno, come nella dimostrazione qui sopra, abbiamo

$$\sum_{d|60}\mu(d)=1+(-1)\cdot\binom{3}{1}+(-1)^2\binom{3}{2}+(-1)^3\binom{3}{3}=0.$$

Teorema B.5 (Formula di Gandhi) *Sia p_n l'n-esimo numero primo. Poniamo $P_n:=p_1\cdot p_2\cdots p_n$. Allora per $n\geq 0$ si ha*

$$p_{n+1}=\left\lfloor 1-\log_2\Big(-\frac{1}{2}+\sum_{d|P_n}\frac{\mu(d)}{2^d-1}\Big)\right\rfloor,$$

dove con $\lfloor x\rfloor$ indichiamo la parte intera di x.

Dim. Per $n=0$ si ha $P_0=1$ e quindi la formula dà $p_1=2$. Per $n\geq 1$, ricordando lo sviluppo della serie geometrica di ragione 2^{-d}, si ha

$$S_n\stackrel{\text{def}}{=}\sum_{d|P_n}\frac{\mu(d)}{2^d-1}=\sum_{k\geq 1}\sum_{d|P_n}\frac{\mu(d)}{2^{kd}}=\sum_{m\geq 1}\frac{1}{2^m}\sum_{\substack{d|m\\ d|P_n}}\mu(d)=\sum_{m\geq 1}\frac{1}{2^m}I\big((m,P_n)\big)$$

dove I è la funzione definita nel Lemma B.4. Ma $(m,P_n)=1$ se e solo se $m=1$ oppure tutti i fattori primi di m superano p_n. Non è difficile convincersi che

il più piccolo intero maggiore di 1 che ha *tutti* i fattori primi maggiori di p_n è esattamente p_{n+1}. Dunque

$$S_n = \frac{1}{2} + \frac{1}{2^{p_{n+1}}} + \cdots$$

Vogliamo stimare S_n dall'alto e dal basso: una stima dal basso si ottiene facilmente prendendo in considerazione solo i due addendi qui indicati, e omettendo tutti i termini successivi. Una stima dall'alto si ottiene includendo nella somma qui sopra tutti gli addendi del tipo 2^{-m} per $m \geq p_{n+1}$, ed utilizzando di nuovo la formula per la somma della serie geometrica di ragione $\frac{1}{2}$. Dunque, se $n \geq 1$ otteniamo

$$\frac{1}{2} + \frac{1}{2^{p_{n+1}}} < S_n < \frac{1}{2} + \frac{1}{2^{p_{n+1}}} \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots\right) = \frac{1}{2} + \frac{2}{2^{p_{n+1}}}.$$

Da questo segue che

$$1 - \log_2\left(S_n - \frac{1}{2}\right) \in (p_{n+1}, p_{n+1} + 1)$$

da cui si ottiene la tesi. □

La Figura 8 illustra il caso $n = 3$ della dimostrazione. Per ulteriori discussioni sulla formula di Gandhi si veda, in particolare, Golomb [2].

Riferimenti bibliografici

[1] R. Crandall, C. Pomerance, *Prime numbers. A computational perspective*, Springer-Verlag, Berlin, Heidelberg, New York, 2001.

[2] S. W. Golomb, "A direct interpretation of Gandhi's formula", *Amer. Math. Monthly*, 81, pagine 752-754, 1974.

[3] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, Oxford, quinta edizione, 1979.

[4] A. Languasco, A. Zaccagnini, *Introduzione alla Crittografia*, Ulrico Hoepli Editore, Milano, 2004.

[5] A. Languasco, A. Zaccagnini, "Alcune proprietà dei numeri primi, I", *Sito web Bocconi-Pristem*, 2005, disponibile sul sito `http://matematica.uni-bocconi.it/LangZac/home.htm`.

[6] S. Mortola, "Elogio delle dimostrazioni alternative", in A. Abbondandolo, M. Giaquinta, F. Ricci (a cura di), *Ricordando Franco Conti*, pagine 273–276, Scuola Normale Superiore, Pisa, 2004.

[7] P. Morton, "Musings on the prime divisors of arithmetic sequences", *Amer. Math. Monthly*, 97, pagine 323-328, 1990.

[8] P. Ribenboim, *The New Book of Prime Numbers Records*, Springer-Verlag, Berlin, Heidelberg, New York, 1996.

[9] A. Zaccagnini, "L'importanza di essere primo", in A. Abbondandolo, M. Giaquinta, F. Ricci (a cura di), *Ricordando Franco Conti*, pagine 343-354, Scuola Normale Superiore, Pisa, 2004.

[10] A. Zaccagnini, Lezioni di Teoria dei Numeri, 2005, Dispense del Corso di *Teoria dei Numeri*, A. A. 2004-2005. Disponibili all'indirizzo `http:/www.math.unipr.it/~zaccagni/psfiles/lezioni/tdn2005.pdf`.

Alessandro Languasco
Dipartimento di Matematica Pura e Applicata,
via Belzoni 7, 35131 Padova
e-mail: languasco@math.unipd.it
pagina web: http://www.math.unipd.it/~languasc

Alessandro Zaccagnini
Dipartimento di Matematica,
Parco Area delle Scienze, 53/a – Campus Universitario, 43100 Parma
e-mail: alessandro.zaccagnini@unipr.it
pagina web: http://www.math.unipr.it/~zaccagni/home.html