

Block Notes Matematico

I numeri primi di Mersenne ed il Free Project Mersenne's Gap

ing. Rosario Turco¹, prof. Maria Colonnese,

Abstract

In questo articolo viene presentato il lavoro svolto dagli autori nell'ambito del Free Project Mersenne's Gap (FPMG).

L'articolo presenta proprietà e congetture legate ai numeri primi di Mersenne e del software sviluppato all'uopo dagli stessi autori.

Verranno analizzate la congettura di Cramer e la congettura di Cramer-Granville, come pure segnalate nuove congetture.

Infine si accenna alla nuova congettura di Mersenne, dimostrata dagli autori in [1]. La comprensione di questo articolo è legata alla lettura dell'articolo "Tecniche di primalità" [1].

mailto:rosario_turco@virgilio.it



¹ Rosario Turco è un ingegnere elettronico presso Telecom Italia (Napoli) ed ideatore di "Block Notes Matematico" insieme alla prof. Maria Colonnese del Liceo Classico "De Bottis" di Torre del Greco, provincia di Napoli.

INDICE

.....	
Definizioni.....	3
Obiettivi del Free Project Mersenne's Gap (FPMG).....	3
Congettura di Cramer	3
Congettura di Cramer-Granville.....	4
Analisi dei risultati per le Congetture Cramer e Cramer-Granville	4
Crivello di Eratostene e congettura Cramer-Granville.....	5
Numeri primi di Mersenne e Congettura del numero primo successivo	7
Lemmi sui numeri primi di Mersenne.....	9
Nuova congettura di Mersenne (o Congettura di Bateman, Selfridge e Wagstaff).....	10
Considerazioni sulla esperienza tratta dal software	10
Invito al proseguimento del Free Project Mersenne's Gap	11
Qualche problema interessante.....	11
Sorgenti e dati disponibili.....	11
<i>Riferimenti</i>	11

Definizioni

Simbolo e/o Formula	Descrizione
p	numero primo
$M_p=2^p-1$	numero primo di Mersenne associato a p
p_{n+1}	numero primo immediatamente successivo a M_p
$gM = p_{n+1} - M_p$	<i>gap di Mersenne</i>
$\gamma = \lim_{n \rightarrow \infty} \left\{ 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \log n \right\}$	costante di <i>Eulero-Mascheroni</i>
$M_g = 2 \cdot \exp(-\gamma) = 1.1229\dots$	costante della congettura di <i>Cramer-Granville</i> trascendentale
M_{ge}	costante di Granville effettiva
$R_p = p_{n+1} - M_p / (\log p)^2$	costante della <i>congettura di Cramer</i>

Obiettivi del Free Project Mersenne's Gap (FPMG)

Il progetto è nato con i seguenti semplici obiettivi:

- Utilizzare i numeri primi di Mersenne per poter arrivare velocemente su valori alti di numeri primi ("Al tendere all'infinito i numeri primi si diradano")
- Sviluppare del software con PARI/GP con le seguenti caratteristiche: a partire da un numero primo p e da un gap desiderato, il software deve individuare il numero primo di Mersenne M_p associato a p ed il numero primo p_{n+1} immediatamente successivo a M_p , verificandone: gM , R_p , il fattore di Merito, M_g ed M_{ge} , il $\gcd(p, gM)$, $\gcd(M_p, gM)$. Se il gap non fosse quello desiderato il software deve ripetere il procedimento per un nuovo numero primo successivo a p .
- Scegliere test di primalità adeguati e veloci, superando i limiti di elaborazione circa le operazioni di potenze, modulo e di numero di cifre in gioco (scelta di PARI/GP con script e compilabili con gp2c)
- Tracciare i dati su un log
- Valutare i dati: verificare le congettura di Cramer e la congettura di Cramer-Granville (se esistessero contro-esempi)
- Verificare l'esistenza una possibile dimostrazione matematica di qualche congettura
- Valutare i dati: formulare nuove ipotesi (congetture)

Conggettura di Cramer

Cramer ipotizzò (vedi [2]) che:

$$\lim_{n \rightarrow \infty} \sup \frac{p_{n+1} - p_n}{(\log p_n)^2} = 1 \quad (1)$$

Se definiamo $R_p = \frac{p_{n+1} - p_n}{(\log p_n)^2}$ la (1) equivale a:

$$\lim_{n \rightarrow \infty} \sup R_p = 1 \quad (2)$$

Tale congettura nacque da un modello probabilistico sui numeri primi che assume che la probabilità di un numero naturale x di essere primo è circa $1/\log x$.

Questa congettura porta cioè a pensare che il più grande gap esistente tra p_{n+1} e p_n sia circa $(\log p_n)^2$.

Nel FPMG si assume $p_n = Mp$.

Congettura di Cramer-Granville

Granville propose una più debole congettura rispetto a Cramer ma più efficace e verificabile:

$$p_{n+1} - p_n < M (\log p_n)^2 \quad (3)$$

Equivalente alla:

$$\frac{p_{n+1} - p_n}{(\log p_n)^2} < M \quad (4)$$

con $M=2*\exp(-\gamma)=1.1229\dots$ e γ =costante di Eulero-Mascheroni (in PARI/GP γ =Euler)

Nel progetto FPMG $p_n = Mp$.

Analisi dei risultati per le Congetture Cramer e Cramer-Granville

Per la congettura di Cramer ci si è concentrati sui valori di R_p , che per l'intervallo esaminato, non ha mai raggiunto il valore dell'unità. L'impressione è che tale congettura sia difficile a verificarsi e da dimostrare e che, invece, dovrebbe essere maggiormente presa in considerazione la *congettura di Cramer-Granville*.

La costante nella (4) è:

$$M_g = 2\exp(-\text{Euler}) \quad (5)$$

M_g è, quindi, il valore massimo ottenibile.

Dai dati disponibili in dati-fpmg.zip sul sito, difatti si è verificato che è valida la seguente "formula di Granville effettiva (R. Turco, M. Colonnese)":

$$M_{ge} = 2^{(\pm c)}\exp(-\text{Euler}) \quad (6)$$

con c numero intero che assume valori $c=1,0,-1,-2,\dots$;

Dalla (5) per $c=1 \Rightarrow M_g = M_{ge}$.

Se si verificano i dati prodotti dal FPMG ci si accorge che il tutto è equivalente a dire che:

$$R_p < M_{ge} \leq M_g.$$

Proprio dai dati si osserva la validità della (5) e della (6) e di conseguenza anche che la congettura di Cramer-Granville non ha contro-esempi e, quindi, è vera.

Una possibile *dimostrazione della congettura di Cramer-Granville* coinvolge il crivello di Eratostene e volendo anche con un crivello in *versione analitica*, tramite la *zeta di Riemann*.

Il crivello di Eratostene è noto come una delle iniziali guide per i test di primalità. Ad esempio dal crivello di Eratostene discende un possibile test del Trial Division Test (TDT vedi [1]) dove è sufficiente vedere (oltre al caso semplice se esiste almeno un numero primo divisore) se esiste un numero primo divisore fino alla radice del numero stesso da verificare².

Crivello di Eratostene e congettura Cramer-Granville

Partiamo con un esempio del crivello di Eratostene. Scriviamo come esempio tutti i numeri da 1 a $n=30$ (vedi [1] per esempio completo):

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Sono in totale $x=30$ numeri.

- L'1 non lo consideriamo.
- Il 2 è un primo ($p=2$) e lo coloriamo di verde.
- Eliminiamo tutti i suoi multipli (cioè i pari) e coloriamoli di rosso.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Sono rimasti in nero solo 15 numeri.

Adesso prendiamo il primo numero disponibile dopo il 2: è il 3 che va considerato numero primo ($p=3$) e che coloriamo di verde; ora eliminiamo i suoi multipli e sappiamo già che i multipli minori del numero di cui 3 è radice ($3^2=9$) sono già stati eliminati (il 6, cioè fino al quadrato di 3 già sono stati eliminati) ed eliminiamo i successivi:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Sono rimasti in nero solo 9 numeri, etc.

Generalizziamo il risultato del crivello di Eratostene.

Se i numeri vanno da 1 a x , abbiamo un totale di x numeri. Dopo aver eliminato il 2 e i suoi multipli rimangono: $x - x/2 = (1 - 1/2)x$ con un errore ± 1 . Col 3, inoltre, il totale che ci era rimasto precedentemente era: $(1 - 1/2)x$, adesso ne sono stati eliminati almeno $1/3$ circa; per cui il totale rimanente è circa $(1 - 1/3)(1 - 1/2)x$ con un errore ± 2 . Quindi poiché ci è sufficiente tirare fuori (setacciare) i numeri primi p fino alla radice di x , allora se continuiamo col procedimento è evidente che:

$$\prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) \cdot x \quad (7)$$

Con un errore potenziale di $\pm 2^{(k-1)}$ dove k è il numero di primi trovati. Ad esempio se il nostro numero è 81 la sua radice è 9. Per cui il setaccio deve arrivare fino a 9 per trovare i primi. Quando ne trova? $k=4$ perché rimangono 2,3,5,7.

Nel 1874 *Mertens* dimostrò che:

² ad esempio se $x=9$ è sufficiente vedere i numeri primi 2 e 3; difatti 3 è la radice di 9; quindi 9 è composto

$$\prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x} \quad (8)$$

Da qui poiché i primi che setacciamo fino alla radice di x sono eventi indipendenti da x e tenendo presente la (7) allora Granville ipotizzò:

$$\prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) x \sim \frac{e^{-\gamma} x}{\frac{1}{2} \log x} = 2 \frac{e^{-\gamma} x}{\log x} \quad (9)$$

Dove nella (9) si è ipotizzato che poiché setacciamo fino a $x^{1/2}$ allora il contributo è solo circa di metà degli elementi.

Nella (9) si vede la presenza di $Mg=2 \cdot \exp(-\text{Euler})$, mentre $x/\log x$ riporta al Teorema dei numeri primi (TNP).

Dal TNP è comunque valida la *disuguaglianza di Brun-Tichmarsh*:

Se $x > 0$ e $y > 1$ allora è:

$$\pi(x+y) - \pi(x) \leq \frac{2y}{\log y}$$

Per il TNP inoltre deve essere:

$$\lim_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\log p_n} \geq 1$$

Dove è

$$\text{Merit} = (p_{n+1} - p_n) / \log p_n$$

Il crivello di Eratostene lo si ritrova in versione analitica anche attraverso la zeta di Riemann; difatti:

$$\zeta(z) = \sum_{n=1}^{\infty} n^{-z} = \prod_p \frac{1}{1-p^{-z}} \quad (10)$$

Dove $z=a+ib$ con $z \in \mathbb{C}$ ovvero numero complesso, mentre il produttorio è sviluppato all'infinito rispetto a tutti i numeri primi. Se $z=1$ allora la parte destra della (10) equivale alla (8).

La parte destra della (10) esprime che la funzione zeta di Riemann è una serie costituita dalla "potenza complessa" di tutti i numeri naturali; mentre la parte sinistra della (1), ricavata già da Eulero in campo reale \mathbb{R} , mostra il legame esistente tra la serie ed il prodotto dei numeri primi; questo in sostanza perché anche i numeri primi fanno parte dell'insieme dei numeri naturali.

La dimostrazione di come si giunge alla parte sinistra è mostrata di seguito con i passaggi (a)(b)(c)(d). Difatti è:

$$\zeta(z) = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \frac{1}{4^z} + \dots \quad (a)$$

Se nella (a) si moltiplica per $\frac{1}{2^z}$ si ottiene:

$$\frac{1}{2^z} \zeta(z) = \frac{1}{2^z} + \frac{1}{4^z} + \frac{1}{6^z} + \frac{1}{8^z} + \dots \quad (b)$$

Se alla (a) si sottrae la (b) si ottiene:

$$\left(1 - \frac{1}{2^z}\right) \zeta(z) = 1 + \frac{1}{3^z} + \frac{1}{5^z} + \frac{1}{7^z} \quad (c)$$

Se si ripete il procedimento all'infinito anche per $1/3^z$, $1/5^z$, $1/7^z$ etc, si ottiene:

$$\left(1 - \frac{1}{2^z}\right) \left(1 - \frac{1}{3^z}\right) \dots \zeta(z) = 1 \quad (d)$$

Dalla (d) discende rapidamente la (10) osservando di avere a che fare con numeri primi. In ogni caso torniamo attraverso alla zeta ad una tecnica di "crivello analitico" già osservata col crivello di Eratostene. Per cui la (9) e la (10) sono legate; il che riconferma che TNP e zeta di Riemann sono fortemente legate e così anche la congettura di Cramer-Granville al TNP e zeta di Riemann.

Numeri primi di Mersenne e Congettura del numero primo successivo

In [1] sono state mostrate Tecniche di primalità per i numeri primi di Mersenne e le classiche proprietà legati a questi ultimi. In questo paragrafo vedremo ulteriori proprietà e congetture su essi.

Si è notato sui dati che è sempre:

$$\gcd(M_p, gM) = 1 \quad (11)$$

e che è:

$$\gcd(p, gM) = 1 \quad \text{oppure} \quad \gcd(p, gM) = p \quad (12)$$

La (11) è dimostrabile per il fatto che M_p è primo e col Teorema di Dirichlet e/o la GRH⁽³⁾; difatti una sequenza di numeri individua numeri primi se $a + d, a + 2d$, etc è tale che $\gcd(a, d) = 1$.

La (12) è "intrigante". Nei casi per cui è vero che $\gcd(p, gM) = p$, una condizione più stringente per cui è vera la (12) (vedi anche dati) è:

$$p = gM \quad (13)$$

Nei casi per cui è vera la (12), e rispettata quindi la (12), succede che:

$$gM = dM - 1 = p_{n+1} - Mp - 1 = p \quad (14)$$

Inoltre dalla (14) si ottiene che:

³ $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ (vedi [2])

$$p_{n+1} - p = Mp + 1 = 2^p - 1 + 1 = 2^p \quad (15)$$

e che, tenendo presente che non sempre $\text{gcd}(p, gM) = p$, allora una nostra "Congettura del numero primo immediatamente successivo al numero primo di Mersenne" è che:

$$p_{n+1} \sim p + 2^p \pm \varphi(p) \quad (16)$$

$$\varphi(p) = p - 1 = |2k|_{\max} < p \quad (17)$$

Dove $\varphi(p)$ è la funzione totiente di Eulero.

Per cui per essere certi di trovare p_{n+1} occorre ciclare

$$\text{da: } 2^p + p - (p - 1) = 2^p + 1 = Mp + 2$$

$$\text{a: } 2^p + p + (p - 1) = 2^p + 2p - 1 = Mp + 2p$$

il che dimostra che è giusta perché equivale a incrementare Mp di 2 ogni volta e verificare se abbiamo trovato un numero primo a partire da Mp nell'intervallo tra 2 e $2p$.

Per individuare p_{n+1} un metodo potrebbe essere quello di sfruttare la (4) e la (6) ma con Mge . Il problema però del Mge è di trovare come ricavare la c .

Analisi dei dati ottenuti nel progetto FPMG (Vedi $Rp < Mge$)

$$p=3$$

$$\text{gcd}(p, gM) = p$$

$$p_{n+1} = 2^3 + 3 = 11$$

$$k=0$$

$$Rp = 0.7922745188711325010641242440$$

$$Mge = 1.122918967133770339648286430 \cdot 2^{(1)} \cdot \exp(-\text{Euler})$$

$$p=5$$

$$\text{gcd}(p, gM) = p$$

$$p_{n+1} = 2^5 + 5 = 37$$

$$k=0$$

$$Rp = 0.4240066413753902461169380233$$

$$Mge = 0.5614594835668851698241432148 \cdot 2^{(0)} \cdot \exp(-\text{Euler})$$

$$p=7$$

$$\text{gcd}(p, gM) = 1$$

$$p_{n+1} \approx 2^7 + 7 = 135$$

$$p_{n+1} = 131 \quad k=2 \quad \text{errore} = 2 \cdot 2$$

$$Rp = 0.1278437318481178426375904524$$

$$Mge = 0.1403648708917212924560358037 \cdot 2^{(-2)} \cdot \exp(-\text{Euler})$$

$$p=13$$

$$\text{gcd}(p, gM) = 1$$

$p_{n+1} \approx 2^{13} + 13 = 8205$
 $p_{n+1} = 8209 \quad k=2 \quad \text{errore} = 2 \cdot 2$
 $R_p = 0.2093741504456730655501213712$
 $M_{ge} = 0.2807297417834425849120716074 \cdot 2^{(-1)} \cdot \exp(-\text{Euler})$

$p=17$
 $\text{gcd}(p, gM) = 1$
 $p_{n+1} \approx 2^{17} + 17 = 131089$
 $p_{n+1} = 131101 \quad k=6 \quad \text{errore} = 2 \cdot 6$
 $R_p = 0.2088573654360368096340482064$
 $M_{ge} = 0.2807297417834425849120716074 \cdot 2^{(-1)} \cdot \exp(-\text{Euler})$

$p=19$
 $\text{gcd}(p, gM) = 1$
 $p_{n+1} \approx 2^{19} + 19 = 524307$
 $p_{n+1} = 524309 \quad k=1 \quad \text{errore} = 2 \cdot 1$
 $R_p = 0.1210769010016337052155069961$
 $M_{ge} = 0.1403648708917212924560358037 \cdot 2^{(-2)} \cdot \exp(-\text{Euler})$

Lemmi sui numeri primi di Mersenne

E' possibile, infine, notare sui dati alcune proprietà che ci portano a dimostrare i seguenti Lemmi. Molti altri sono stati mostrati in [1].

Lemma forma $4k+3$ dei numeri primi di Mersenne

Tutti i numeri primi di Mersenne sono di forma $4k+3$.

Dimostrazione

Supponiamo per assurdo che i numeri primi di Mersenne siano di forma $4k+1$.

$$M_p = 2^p - 1 \Rightarrow M_{p+1} = 2^p$$

$$\text{se } M_p = 4k + 1 \Rightarrow 4k + 1 + 1 = 2^p$$

allora:

$$2(2k + 1) = 2^p \Rightarrow 2k + 1 = 2^{p-1} \Rightarrow \text{assurdo : un dispari uguale ad un pari !}$$

$$\text{se } M_p = 4k + 3 \Rightarrow 4k + 3 + 1 = 2^p$$

allora:

$$4(k + 1) = 2^p \Rightarrow k + 1 = 2^{p-2} \Rightarrow k = 2^{p-2} - 1 \text{ il che } k \text{ è dispari e ciò è possibile}$$

Corollario

Se $\text{gcd}(p, gM) = 1$ e $\text{gcd}(M_p, gM) = 1 \Rightarrow \text{gcd}(p, M_p) = 1$

Ovvero il corollario dice che poiché già sapevamo che p e M_p sono primi che è possibile anche $\gcd(p, gM)=1$.

Corollario

Se M_p è di forma $4k+3$, p e $p+1$ sono entrambi della stessa forma: $4n+1$ oppure $4n+3$.

Nuova congettura di Mersenne (o Congettura di Bateman, Selfridge e Wagstaff)

Accenniamo anche a tale nuova congettura adatta alla realizzazione di test di primalità.

La congettura afferma che per ogni numero naturale dispari p , se almeno due delle seguenti affermazioni sono vere, allora lo sarà anche la terza:

- $p = 2^k \pm 1$ o $p = 4^k \pm 3$ per un qualche k naturale.
- $2^p - 1$ è primo (Numero primo di Mersenne)
- $(2^p + 1) / 3$ è primo (*Numero primo di Wagstaff*).

Se p è un numero dispari composto, allora, anche $2^p - 1$ e $(2^p+1)/3$ lo sono. Questa è l'unica condizione necessaria per testare valori primi (test di primalità) che soddisfino la congettura.

Interessante è la dimostrazione matematica di tale congettura che secondo gli autori è vera (vedi [1]).

Renaud Lifchitz ha dimostrato che la nuova congettura di Mersenne è vera fino a 12,441,900 testando sistematicamente tutti i numeri primi per cui è noto che vale almeno una delle condizioni (vedi <http://www.primenumbers.net/rl/nmc/>).

La parte sfruttabile di questa congettura in ambito FPMG è che se p è primo, si può valutare la primalità di M_p , attraverso un numero più piccolo di M_p , ovvero con i numeri primi di Wagstaff!

Considerazioni sulla esperienza tratta dal software

Spesso il problema non è il test di primalità: ne esistono diversi validi e "abbastanza veloci"; ma il tempo maggiore è speso nel determinare il `nextprime()`. Questo porta alla considerazione che potrebbe essere più efficace sostituire `nextprime()` con un ciclo che verifica la primalità di $M_p=M_p+2$, appena i tempi di attesa su `nextprime()` si allungano.

I numeri primi di Mersenne generati col software fornito possono andare al di là delle 6000 cifre (vedi `dati-fpmg.zip`). La primalità dei numeri di Mersenne può essere fatta con vari tipi di *test*: *Miller-Rabin*, *AKS*, *Piccolo Teorema di Fermat* e *Lucas-Lehmer*, a scelta.

Il software consente di valutare la primalità dei numeri di Mersenne attraverso i *numeri primi di Wagstaff* più piccoli e, quindi, consente di valutare numeri di Mersenne di dimensioni 3 volte maggiori a parità di tempo di verifica della primalità. Inoltre scarta rapidamente, attraverso una tecnica suggerita dai numeri primi di Sophie Germain quei numeri primi che non consentirebbero di giungere a dei numeri primi di Mersenne.

La peculiarità del software è che si può interrompere segnandosi il numero primo ultimo usato per poter ricominciare successivamente.

GAP di Mersenne

E' stato trovato nell'ambito del FPMG un gap di Mersenne delle dimensioni di **gM=8884** con $M_p=2^p-1$ dove $p = 5807$.

Invito al proseguimento del Free Project Mersenne's Gap

Sul sito sono disponibili i dati attuali del FPMG oppure richiedibili all'autore dell'articolo. Il lettore che voglia partecipare può scaricarsi il software e elaborare ulteriori dati, segnalando poi al sito sia record dei gap di Mersenne ottenuti che nuove congetture o segnalazioni di contro-esempi o di errata corrice.

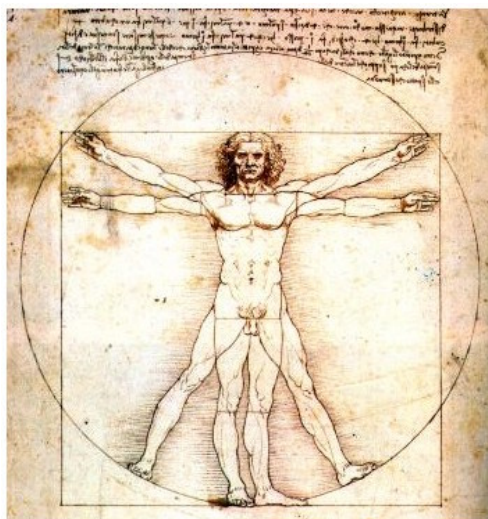
Qualche problema interessante

Esiste un metodo algoritmico che permetta con una regola calcolare c della (6)? Se sì arriveremo più velocemente a calcolare p_{n+1} attraverso la (4).

Avremo un miglioramento del TNP e del termine di errore in tal caso?

Sorgenti e dati disponibili

I sorgenti sono disponibili sul sito con **sources-fpmg.zip**; mentre i dati disponibili del progetto sono in **dati-fpmg.zip**



Riferimenti

[1] Tecniche di primalità - ing. Rosario Turco

[2] Sulle spalle dei giganti - Rosario Turco, Michele Nardelli, Giovanni Di Maria, Francesco Di Noto, Annarita Tulumello, Maria Colonnese – CNR SOLAR

Siti vari

CNR SOLAR

<http://150.146.3.132/>

Aladdin's Lamp (ing. Rosario Turco)

www.geocities.com/SiliconValley/Port/3264 MISC sezione MATEMATICA

gruppo ERATOSTENE

<http://www.gruppoeratostene.com>

dott. Michele Nardelli

<http://xoomer.alice.it/stringtheory/>

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.