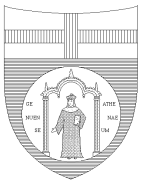


Università degli studi di Genova

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso Di Laurea In Matematica

Tesi Di Laurea

CODICI A CHIAVE PUBBLICA ED ALGORITMI DI PRIMALITA'

Relatore: Prof. Alberto Perelli

Correlatore: Prof. Ferdinando Mora

Candidato: Alessandro Languasco

Anno Accademico 1988/1989

Elenco argomenti

Capitolo 1

Introduzione

L'argomento presentato in questa Tesi di Laurea prende spunto da recenti sviluppi all'interno della disciplina della crittografia. Nel 1976 Rivest, Shamir ed Adleman inventarono un metodo di codifica di messaggi rivoluzionario rispetto ai precedenti. La principale caratteristica di tale metodo è quella di basarsi, da una parte, sulla "facilità" di "costruire" primi grandi e, dall'altra parte, dalla "difficoltà" di ottenere la fattorizzazione di interi. Tale situazione venne allora sfruttata per ottenere un sistema crittografico che fosse adatto ad essere utilizzato da un vasto numero di utenti (perché le chiavi usate nel sistema sono pubbliche) e che legasse la propria sicurezza alla fattorizzazione di interi.
Questo metodo crittografico (denominato R.S.A.), per una descrizione del quale si rimanda a D. Bazzanella [5], risvegliò l'interesse della comunità matematica e delle industrie verso la ricerca di algoritmi di primalità e di fattorizzazione sempre migliori.
Ciò ha rinnovato l'attenzione sulla classica disciplina della Teoria dei Numeri, sia per quanto riguarda la Teoria Algebrica, sia per quanto riguarda la Teoria Analitica. Infatti entrambi tali settori sono coinvolti nella ricerca di algoritmi di primalità e di fattorizzazione perché la parte algebrica è necessaria per "costruire" gli algoritmi, mentre la parte analitica è importante per potere ottenere una corretta valutazione della complessità computazionale degli algoritmi stessi. Ultimamente, però, nella costruzione di algoritmi, si è riusciti ad utilizzare risultati riguardanti lo studio delle curve ellittiche. Tale fatto ha consentito di osservare che l'argomento di studio può essere affrontato da diversi, ma egualmente interessanti, punti di vista.
Nella presente Tesi vengono prima esposti (Capitolo 2-3) alcuni risultati fondamentali di Teoria Algebrica ed Analitica dei Numeri senza i quali non è possibile procedere ad un esame approfondito dei migliori algoritmi di primalità oggi conosciuti.
Tali argomenti riguardano, per la parte algebrica, soprattutto lo studio delle proprietà di fattorizzazione di ideali primi in estensioni di campi di numeri e, per la parte analitica, le caratteristiche fondamentali delle funzioni di base della Teoria Analitica dei Numeri ed un piccolo paragrafo sulla funzione zeta di Riemann.
Nel Capitolo 4 si passerà ad esaminare alcuni test di primalità "veloci" basati su risultati classici (Piccolo Teorema di Fermat, caratterizzazione del Simbolo di Legendre) ed il test di primalità di Goldwasser e Kilian basato sulle curve ellittiche.
Nel Capitolo 5 verrà esaminato, con dovizia di particolari, il migliore algoritmo di primalità oggi conosciuto (test di Adleman, Pomerance e Rumely) non limitandosi a presentare le versioni più aggiornate e semplificate ottenute da Lenstra, ma analizzando in dettaglio anche il lavoro compiuto da Adleman, Pomerance e Rumely.
Attualmente i migliori risultati ottenuti nel campo degli algoritmi di primalità sono: la dimostrazione che il numero $2^{216091}-1$ (che ha 65050 cifre !) è primo ed il fatto che una versione migliorata e velocizzata dell'algoritmo di Adleman, Pomerance e Rumely impiega una media di 68 secondi per provare la primalità di numeri di 200 cifre.

Capitolo 2

Elementi Di Teoria Algebrica Dei Numeri

2.1. CONGRUENZE

Ricordiamo brevemente tre risultati fondamentali della teoria delle congruenze.

Proposizione 2.1.1:
Data una congruenza lineare $ax \equiv b \pmod m$ (x incognita) si ha che :

i) se $(a,m)=1$ allora esiste ed é unica modulo m, una soluzione $x_0=a^{-1}b$;

ii) se $(a,m)=d>1$ allora esistono soluzioni se e solo se $d \mid b$. In tal caso la congruenza precedente equivale a

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

Dim: cfr. Koblitz [17], pag. 18, Teorema 1.3.1. ●

Proposizione 2.1.2: (Piccolo Teorema di Fermat)
Sia p un primo di $\mathbb{Z}$ e sia $a \in \mathbb{Z}$. Allora $a^p \equiv a \pmod p$ e se inoltre $p \nmid a$ si ha che $a^{p-1} \equiv 1 \pmod p$.

Dim: cfr. Koblitz [17], pag 19, Teorema 1.3.2. ●

Proposizione 2.1.3: (Teorema Cinese dei Resti)
Supponiamo di dovere risolvere il seguente sistema di congruenze:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \cdots\cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

Supponiamo che $(m_i,m_j)=1$ per $i \neq j$.

Allora esiste una unica soluzione $\bar{x} \pmod M$, dove $M=\prod_{i=1}^{r} m_i$.

Dim: cfr. Koblitz [17], pag. 19, Teorema 1.3.3. ●

2.2. RESIDUI QUADRATICI

Supponiamo che p sia un primo dispari (p>2). Vogliamo sapere quali tra gli elementi di $F_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ sono dei quadrati (ricordiamo che F_p^* é ciclico di ordine p-1). Investigheremo quindi il problema di determinare quando un $a \in F_p^*$ é un quadrato, cioè quando esiste un elemento $b \in F_p^*$ che verifica $b^2=a$. Ovviamente se $b \in F_p^*$ verifica $b^2=a$, allora anche -b verifica la stessa equazione. Notiamo che ogni elemento di F_p^* ha al più due radici quadrate , infatti se esistessero $b_1, b_2 \in F_p^*$ tali che $b_1 \neq \pm b_2$ e che $b_1^2 \equiv b_2^2 \equiv a \pmod p$ allora si avrebbe che $p \mid (b_1^2 - b_2^2) = (b_1 - b_2)(b_1 + b_2)$ e quindi $p \mid (b_1 - b_2)$ oppure $p \mid (b_1 + b_2)$ cioè $b_1 \equiv b_2 \pmod p$ oppure $b_1 \equiv -b_2 \pmod p$ in contraddizione con l'ipotesi assurda.

Gli elementi $\pm b \in F_p^*$ sono detti RADICI QUADRATE di a in F_p^*.

I quadrati in F_p^* possono quindi essere tutti determinati calcolando $b^2 \pmod p$ al variare di $b=1,2,..,(p-1)/2$ (perché gli altri interi da (p-1)/2 a p-1 sono congrui a -b per uno dei b sopra scritti).

Da ciò segue che in F_p^* si hanno (p-1)/2 RESIDUI QUADRATICI ed altrettanti nonresidui quadratici.

Nel caso di conoscere un generatore g di F_p^*, i residui quadratici di F_p^* stesso si possono determinare osservando che essi sono tutti e soli gli elementi di F_p^* del tipo g^j con j pari.

Introduciamo adesso un simbolo che ci consente di determinare in modo semplice se un elemento di F_p^* é un residuo quadratico modulo p.

Definizione 2.2.1: *Definiamo il SIMBOLO DI LEGENDRE* $\left(\frac{\cdot}{p}\right)$.

Sia $a \in \mathbb{Z}$, *p primo, p>2 allora*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se a residuo quadratico} \\ -1 & \text{se a non residuo quadratico} \\ 0 & \text{se } p \mid a \end{cases}$$

Proposizione 2.2.1: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$.

Dim: Abbiamo due casi distinti:

i) se $p \mid a$ allora entrambi i membri della congruenza dell'enunciato sono $\equiv 0 \pmod p$;

ii) se $p \nmid a$ allora, poiché F_p^* é ciclico di ordine p-1, si ha che $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p$ e quindi $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ (perché ± 1 sono le uniche radici quadrate di 1).

Sia g un generatore di F_p^* e sia $a=g^j$. Allora $a^{\frac{p-1}{2}} = g^{\frac{j(p-1)}{2}}$ é uguale ad 1 se e solo se $(p-1) \mid \frac{j(p-1)}{2}$ e cioè se e solo se j é pari. Quindi entrambi i membri della congruenza della tesi sono uguali ad 1 in F_p^* (cioè ognuno é congruo ad 1 modulo p) se e solo se j é pari; altrimenti sono entrambi congrui a -1. ●

Proposizione 2.2.2: *Il simbolo di Legendre soddisfa le seguenti proprietà:*

1) $\left(\frac{a}{p}\right)$ *dipende solo dal residuo di a modulo p;*

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *;*

3) se (b,p)=1 allora $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ *;*

4) $\left(\frac{1}{p}\right)=1$ *e* $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Dim: 1) è ovvio dalla definizione stessa del simbolo di Legendre;
2) dipende dalla Proposizione 2.2.1;
3) é conseguenza di 2);
4) $\left(\frac{1}{p}\right)=1$ perché $1^2 \equiv 1 \pmod p$. La seconda parte é conseguenza immediata della Proposizione 2.2.1. •

Proposizione 2.2.3:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod 8 \\ -1 & \text{se } p \equiv \pm 3 \pmod 8 \end{cases}.$$

Dim: cfr. Koblitz [17], pag. 43, Proposizione 2.2.4. •

Proposizione 2.2.4: Legge di reciprocità quadratica.
Siano p,q>2, primi allora si ha che:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{se } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{p}{q}\right) & \text{altrimenti} \end{cases}$$

Dim: cfr. Koblitz [17], pag. 44-45, Proposizione 2.2.5. •

La proposizione precedente é utile perché, siccome il simbolo di Legendre $\left(\frac{a}{p}\right)$ é definito solo modulo p, si può assumere che i fattori primi q di a siano minori di p e quindi, riconducendo il calcolo di $\left(\frac{q}{p}\right)$ al calcolo di $\left(\frac{p}{q}\right)$, si semplifica il calcolo (perché si lavora in F_q^*, con q<p, anziché in F_p^*).

Tutta la trattazione precedente riguardante il simbolo di Legendre può essere generalizzata al caso in cui al posto di un primo p si considera un qualunque intero n. Come risulterà chiaro in seguito, non si potrà però più utilizzare le informazioni ottenute dal simbolo generalizzato per decidere se siamo in presenza di un residuo quadratico o di un nonresiduo quadratico.

Definizione 2.2.2: Simbolo di Jacobi.

Sia $a \in \mathbb{Z}$ *e sia n un intero dispari positivo. Se* $n=\prod_{i=1..r} p_i^{a_i}$ *allora definiamo il Simbolo di Jacobi come segue:*

$$\left(\frac{a}{n}\right)=\prod_{i=1..r}\left(\frac{a}{p_i}\right)^{a_i}$$

dove gli $\left(\frac{a}{p_i}\right)$ *sono i simboli di Legendre.*

Come esempio del fatto che il legame con i residui quadratici viene a cadere, osserviamo che: $\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)(-1)=1$, ma 2 non é un residuo quadratico modulo 15 perché gli unici residui quadratici modulo 15 sono 1 e 4.

Presentiamo adesso due proposizioni sul simbolo di Jacobi che generalizzano, rispettivamente, la Proposizione 2.2.3 e la Proposizione 2.2.4.

Proposizione 2.2.5:
Se n intero dispari positivo si ha che :

$$\left(\frac{2}{n}\right)=(-1)^{(n^2-1)/8}$$

Dim: cfr. Koblitz [17], pag 46-47, Proposizione 2.2.6. ●

Proposizione 2.2.6: *Se m,n sono interi dispari positivi allora si ha che:*

$$\left(\frac{m}{n}\right)=(-1)^{\frac{(n-1)(m-1)}{4}}\left(\frac{n}{m}\right).$$

Dim: cfr. Koblitz [17], pag 46-47, Proposizione 2.2.7. ●

E' possibile compiere un ulteriore passo di generalizzazione rispetto alla Proposizione 2.2.6 considerando non solo interi dispari positivi, bensì interi dispari di segno qualunque (cfr. Hasse [15], pag. 114-127).

Proposizione 2.2.7: Legge di reciprocità quadratica generalizzata:
Siano a,b interi dispari, (a,b)=1, allora si ha che:

$$\left(\frac{a}{b}\right)=(-1)^{\frac{(a-1)(b-1)}{4}+\frac{\sigma(a)-1}{2}\cdot\frac{\sigma(b)-1}{2}}\left(\frac{b}{a}\right) \quad , \text{ dove } \sigma(a)=\frac{a}{|a|}.$$

Dim: cfr. Hasse [15] , pag. 122-123. ●

2.3. RADICI PRIMITIVE DELL'UNITA'

Dato un campo finito F_q, dove q intero positivo, studiamo il problema di determinare se esistono e quante sono in F_q le soluzioni dell'equazione $x^n=1$.

Definizione 2.3.1: *Le soluzioni dell'equazione $x^n=1$ in F_q vengono dette "radici n-esime dell'unità in F_q ".*

Ricordiamo inoltre che F_q^* è ciclico di ordine q-1.

Proposizione 2.3.1: *Sia g un generatore di F_q^* .*
Allora g^j è una radice n-esima dell'unità se e solo se $nj\equiv 0 \pmod{q-1}$.
Il numero delle radici n-esime dell'unità è (n,q-1).

Dim: Ogni elemento di F_q^* può essere scritto come potenza del generatore g. Notiamo che una potenza del generatore g é uguale ad 1 se e solo se l'esponente di tale potenza é divisibile per q-1. Allora g^j è una radice n-esima dell'unità se e solo se $nj \equiv 0 \pmod{q-1}$. Sia adesso d=(n,q-1). Per la Proposizione 2.1.1 abbiamo che l'equazione $nj \equiv 0 \pmod{q-1}$ (in cui j é l'incognita) é equivalente all'equazione $\frac{n}{d}j \equiv 0 \pmod{\frac{q-1}{d}}$. Poiché $\frac{n}{d}$ é primo con $\frac{q-1}{d}$, é allora necessario che $\frac{q-1}{d} \mid j$. In altre parole le d distinte potenze di $g^{\frac{q-1}{d}}$ sono esattamente le radici n-esime dell'unità. •

Definizione 2.3.2: *Diremo che F_q ha una radice primitiva n-esima dell'unità se esistono n radici n-esime dell'unità ed esiste $\xi \in F_q$, radice n-esima dell'unità, tale che le sue potenze generino tutte le radici n-esime dell'unità.*

Proposizione 2.3.2: *F_q ha una radice primitiva n-esima dell'unità se e solo se $n \mid (q-1)$.*

Inoltre, se ξ è una radice primitiva n-esima dell'unità in F_q , allora ξ^j è anch'essa una radice primitiva n-esima dell'unità se e solo se (j,n)=1.

Dim: Dalla Proposizione 2.3.1 abbiamo che esistono n radici n-esime dell'unità se e solo se $n \mid (q-1)$. Sia (con le notazioni della Proposizione 2.3.1) $\xi = g^{\frac{q-1}{n}}$. Allora ξ é radice n-esima dell'unità e genera tutte le altre radici n-esime (cfr. dimostrazione della Proposizione 2.3.1). Ciò prova la prima parte dell'asserto.

Consideriamo adesso una ξ radice primitiva n-esima dell'unità e prendiamo ξ^j. Allora $\xi^j=1$ se e solo se $n \mid j$ e quindi $\xi^{kj}=1$ se e solo se $kj \equiv 0 \pmod{n}$. Si prova facilmente che ξ^j ha ordine n se e solo se j è primo con n. •

2.4. CAMPI DI NUMERI ALGEBRICI

Ricordiamo per prima cosa la nozione di elemento algebrico:

Definizione 2.4.1: *$\alpha \in \mathbb{C}$ é detto ALGEBRICO su $\mathbb{Q}$ se e solo se soddisfa una equazione polinomiale (non banale) a coefficienti in $\mathbb{Q}$.(o equivalentemente $[\mathbb{Q}(\alpha):\mathbb{Q}]$ è finito).*

Nel seguito indicheremo con A l'insieme dei numeri algebrici su $\mathbb{Q}$. Si noti che A è sotto-campo di $\mathbb{C}$.
Possiamo adesso dare la definizione di Campo di Numeri:

Definizione 2.4.2: *Sia K sottocampo di $\mathbb{C}$. Diremo che K è un CAMPO DI NUMERI se $[K:\mathbb{Q}]$ è finito.*

Esempio: $K=\mathbb{Q}(\sqrt{2})$ è un campo di numeri perché $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$

Dalla Definizione 2.4.2 si ha che ogni elemento di K è algebrico su $\mathbb{Q}$ e quindi che $K \subseteq A$. Inoltre $K=\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$ per un opportuno numero finito n di numeri algebrici α_i.
Prima di continuare ad esaminare le proprietà dei campi di numeri, ci occupiamo di particolari estensioni di un campo di numeri.
Supponiamo di aver K,L due campi di numeri $K \subseteq L$, $[L:K]=n$, allora si hanno i seguenti risultati:

Teorema 2.4.1: *Ogni immersione di K in $\mathbb{C}$ si estende esattamente a $[L:K]$ immersioni di L in $\mathbb{C}$.*

Dim: cfr. Marcus [24], pag. 259, Appendice 2, Teorema 1. ●

Corollario: *Esistono esattamente $[L:K]$ immersioni di L in $\mathbb{C}$ che tengono fissato K in modo puntuale.*

Definizione 2.4.3: *L si dice NORMALE su K se e solo se contiene tutti i coniugati degli elementi di K.*

Teorema 2.4.2: *L normale su K se e solo se ogni immersione di L in $\mathbb{C}$ che tengono fissato K in modo puntuale é un automorfismo di L in L.*

Dim: cfr. Marcus [24], pag. 260, Appendice 2, Teorema 3. ●

Teorema 2.4.3: *Se $L=K[\alpha_1,..\alpha_r]$ e L contiene tutti i coniugati degli α_i, allora L é normale su K.*

Dim: cfr. Marcus [24], pag. 260, Appendice 2, Teorema 4. ●

Definizione 2.4.4: *Diremo gruppo di Galois Gal(L/K) il gruppo degli automorfismi di L in sé che fissano puntualmente K. L'operazione di gruppo è la composizione di applicazioni.*

Un importante teorema sui campi di numeri è il seguente:

Teorema 2.4.4: *Sia K un campo di numeri, allora K=$\mathbb{Q}(\vartheta)$ per qualche numero algebrico ϑ.*

Dim: cfr. Stewart-Tall [42], capitolo 2, pag. 40-41. •

A tal punto ricordiamo un metodo per calcolare [K:$\mathbb{Q}$].

Teorema 2.4.5: *Se L estende un campo K e $\alpha \in L$, allora α è algebrico su K se e solo se K(α) è estensione finita di K.*
In tal caso [K(α):K]=grado(f), dove f è il polinomio minimo di α su K e K(α)=K[α].

Dim: cfr. Stewart-Tall [42], Teorema 1.8, pag. 23-24. •

Altro importante concetto che ci servirà nel seguito é:

Definizione 2.4.5: *$\vartheta \in \mathbb{C}$ si dice INTERO ALGEBRICO su $\mathbb{Q}$ se $\exists$ p(t)$\in \mathbb{Z}$[t], monico, tale che p(ϑ)=0.*

Esempi:
a) $\vartheta = \sqrt{-2} = i\sqrt{2}$ è un intero algebrico perché è soluzione di $t^2+2=0$;
b) ϕ= 22/7 non è un intero algebrico.

Nel seguito indicheremo con B l'insieme degli interi algebrici su $\mathbb{Q}$. Si noti che B è sottoanello di A (cfr. Stewart-Tall [42], Teorema 2.8, pag 47).

Definizione 2.4.6: *Dato un campo di numeri K indicheremo con $O_K = K \cap B$ l'ANELLO DEGLI INTERI ALGEBRICI di K.*

Ovviamente O_K è sottoanello di K (perché K e B sono sottoanelli di $\mathbb{C}$) ed inoltre, siccome $\mathbb{Z} \subseteq \mathbb{Q} \subseteq$K e $\mathbb{Z} \subseteq$B, si ha $\mathbb{Z} \subseteq O_K$.
Presentiamo adesso alcuni risultati sugli interi algebrici:

Teorema 2.4.6: *Se $\vartheta \in \mathbb{C}$ soddisfa una equazione polinomiale monica i cui coefficienti sono interi algebrici, allora ϑ è un intero algebrico.*

Dim: cfr. Stewart-Tall [42], Teorema 2.8, pag. 47. •

Lemma 2.4.1: *Se $\alpha \in K$ allora $\exists$ $c \in \mathbb{Z}$, $c \neq 0$, tale che $c\alpha \in O_K$.*
Dim: Per ipotesi abbiamo che $\exists$ p(t)$\in \mathbb{Q}$[t] tale che:

$$p(\alpha) = 0 = \frac{a_0}{b_0} + \frac{a_1}{b_1}\alpha + \ldots + \frac{a_n}{b_n}\alpha^n .$$

Sia $m = m.c.m\{b_0;\ldots;b_n\}$.

Sia $q(t) = mp(t) = a_0\frac{m}{b_0} + a_1\frac{m}{b_1}t + \ldots + a_n\frac{m}{b_n}t^n =$

$c_0 + c_1 t + \ldots + c_n t^n$ (dove $\frac{m}{b_i} \in \mathbb{Z}$). Ovviamente q($\alpha$)=0.

Sia $r(t)=c_n^{n-1}q(t)= c_n^{n-1}c_0+c_n^{n-2}c_1(c_nt)+...+ c_{n-1}(c_nt)^{n-1} + (c_nt)^n$. Posso allora riscrivere tale ultimo polinomio come $r(y)=c_n^{n-1}c_0+c_n^{n-2}c_1y+...+ c_{n-1}y^{n-1} + y^n$ e notare che $r(y)\in\mathbb{Z}[t]$, che è monico, e che le sue radici sono uguali a c_n volte le radici di q(t). Allora ponendo $c=c_n$ si ha che $r(c\alpha)=0$ e quindi $c\alpha\in O_K$. •

Questo semplice Lemma precedente consente di affermare che :

Corollario: *Sia K un campo di numeri, allora $K=\mathbb{Q}(\vartheta)$ con $\vartheta\in O_K$.*

Dim: Sappiamo dal Teorema 2.4.3 che $\exists$ ϕ algebrico tale che $K=\mathbb{Q}(\phi)$. Per il Lemma 2.4.1 abbiamo che $\exists$ $c\in\mathbb{Z}$, $c\neq0$, tale che $c\phi\in O_K$. La tesi si ottiene osservando che, se $\vartheta=c\phi$, $\mathbb{Q}(\vartheta)=\mathbb{Q}(\phi)$. •

A tal punto è necessario osservare che, a meno di casi particolari (tra cui quello dei campi ciclotomici, cfr. Paragrafo 5), se $K=\mathbb{Q}(\vartheta)$, non è detto che $O_K=\mathbb{Z}[\vartheta]$. Infatti sicuramente vale $\mathbb{Z}[\vartheta]\subseteq O_K$ perché O_K è un anello contenente ϑ e $\mathbb{Z}$, mentre $\mathbb{Z}[\vartheta]$ è, per definizione, il minimo sottoanello contenente ϑ e $\mathbb{Z}$.
L'altra inclusione può non valere:

Esempio: Se $K=\mathbb{Q}(\sqrt{5})$ abbiamo che $\sqrt{5}$ e $\frac{1+\sqrt{5}}{2}$ appartengono a $O_{\sqrt{5}}$ perché soddisfano rispettivamente le equazioni $t^2-5=0$ e $t^2-t-1=0$, ma $\frac{1+\sqrt{5}}{2}\notin\mathbb{Z}[\sqrt{5}]$ e quindi abbiamo che $\mathbb{Z}[\sqrt{5}]\subset O_{\sqrt{5}}$.

Passiamo adesso ad esaminare il concetto di Discriminante di un campo di numeri K.
Partiamo col definire il discriminante di una base.

Definizione 2.4.7: *Sia K un campo di numeri, $K=\mathbb{Q}(\vartheta)$, $[K:\mathbb{Q}]=n$ e sia $\{\alpha_1,...,\alpha_n\}$ una base di K come $\mathbb{Q}$-spazio vettoriale. Diremo DISCRIMINANTE di $\{\alpha_1,...,\alpha_n\}$ la quantità:*

$$\Delta[\alpha_1,...,\alpha_n]=\{det(\sigma_j(\alpha_i)\}^2.$$

(dove $\sigma_j: K\to\mathbb{C}$, $j=1,..,n$, sono omomorfismi iniettivi tali che $\sigma_j(\vartheta)=\vartheta_j$, con ϑ_j che sono gli zeri in $\mathbb{C}$ del polinomio minimo di ϑ su $\mathbb{Q}$, cioè i coniugati di ϑ).

Si noti che, se $\{\beta_1,...,\beta_n\}$ è un'altra base di K come $\mathbb{Q}$-spazio vettoriale, allora

$$\Delta[\alpha_1,...,\alpha_n]=\{det(c_{ik})\}^2\Delta[\beta_1,...,\beta_n] \quad \text{dove } \alpha_k=\sum_{i=1}^{n}c_{ik}\beta_i \quad \text{e } c_{ik}\in\mathbb{Q} .$$

Teorema 2.4.7: *Il discriminante di ogni base di K è razionale e non nullo.*

Dim: cfr. Stewart-Tall [42], Teorema 2.6, pag. 44-45. •

Passiamo adesso ad esaminare l'anello degli interi. Sappiamo che $(O_K,+)$ è un gruppo abeliano contenente $\mathbb{Z}$ e definiamo allora:

Definizione 2.4.8: *Diremo BASE INTERA di K una $\mathbb{Z}$-base di O_K.*

Abbiamo ovviamente che $\{\alpha_1,...,\alpha_s\}$ è base intera per K se e solo se $\alpha_i \in O_K$ e $\forall$ elemento di O_K è esprimibile in modo unico nella forma $a_1\alpha_1+...+a_s\alpha_s$ dove $a_i \in \mathbb{Z}$.
Si noti che, per il Lemma 2.4.1, ogni base intera è anche una $\mathbb{Q}$-base e quindi, in particolare, si ha s=n.
Non é però banale provare che una tale base intera esiste; infatti non basta avere una base formata da interi algebrici per avere una base intera: ad esempio $\{1,\sqrt{5}\}$ è una base di interi di $\mathbb{Q}(\sqrt{5})$, ma non è una base intera di $O_{\sqrt{5}}$ perché $\frac{1+\sqrt{5}}{2} \in O_{\sqrt{5}}$, ma $\frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$ = sp($\{1,\sqrt{5}\}$).

Abbiamo però il seguente risultato:

Teorema 2.4.8: *Ogni campo di numeri K ha una base intera e $(O_K,+)$ è un gruppo abeliano libero di rango uguale al grado di K su $\mathbb{Q}$.*

Dim: cfr. Stewart-Tall [42], Teorema 2.15, pag. 51. •

Inoltre si ha che, se $\{\alpha_1,...,\alpha_n\}$ e $\{\beta_1,...,\beta_n\}$ sono due basi intere di K, allora $\Delta[\alpha_1,...,\alpha_n]=(\pm1)^2\Delta[\beta_1,...,\beta_n]=\Delta[\beta_1,...,\beta_n]$ (cfr. Stewart-Tall [42], Lemma 1.11), e quindi il discriminante delle basi intere è un valore caratteristico del campo di numeri K.

Definizione 2.4.9: *Diremo DISCRIMINANTE di K il valore comune Δ_K del discriminante di tutte le basi intere di K.*

Prima di proseguire la trattazione dobbiamo soffermarci ad introdurre il concetto di derivata formale di un polinomio e di norma di un elemento di un campo di numeri.

Definizione 2.4.10: *Dato un anello R diremo DERIVATA FORMALE l'applicazione $D:R[t]\to R[t]$ tale che, se $f=\sum_{i=0}^{r} a_i t^i$, allora:*

$$Df=\sum_{i=1}^{r} i a_i t^{i-1}.$$

Definizione 2.4.11: *Definiamo NORMA di un elemento $\alpha \in K$, $K=\mathbb{Q}(\vartheta)$, $[K:\mathbb{Q}]=n$, la quantità $N(\alpha)=\prod_{i=1}^{n-1}\sigma_i(\alpha)$ con $\sigma_i \in Gal(K/\mathbb{Q})$ dati da $\sigma_i(\vartheta)=\vartheta_i$.*

Teorema 2.4.9:
Sia K un campo di numeri, $K=\mathbb{Q}(\vartheta)$, e sia p(t) il polinomio minimo di ϑ di grado n.
La $\mathbb{Q}$-base $\{1,\vartheta,..,\vartheta^{n-1}\}$ ha discriminante

$$\Delta[1,\vartheta,..,\vartheta^{n-1}]=(-1)^{n(n-1)/2}\,N(D(p(\vartheta)))$$

dove $D(p(\vartheta))$ è la derivata formale di p(t) calcolata in ϑ.

Dim: cfr. Stewart-Tall [42], Proposizione 2.17, pag. 55 . ●

Passiamo adesso a studiare altre proprietà dell'anello degli interi O_K di un campo di numeri.

Definizione 2.4.12: *Diremo DOMINIO DI DEDEKIND un dominio R verificante le seguenti proprietà:*
1) R noetheriano (ogni suo ideale é finitamente generato);
2) Ogni suo ideale primo è massimale;
3) R è integralmente chiuso nel suo campo delle frazioni H,

$$H=\{\alpha/\beta\ :\ \alpha,\beta\in R,\ \beta\neq 0\}.$$

La condizione 3) significa che, se $(\alpha/\beta)\in H$ è una radice di un polinomio monico in R[x], allora si ha $(\alpha/\beta)\in R$ cioè $\beta|\alpha$ in R.
In un dominio di Dedekind si hanno gli importanti risultati seguenti:

Teorema 2.4.10: *Ogni ideale non nullo di un dominio di Dedekind R può essere scritto come prodotto di ideali primi di R stesso. Tale prodotto è unico a meno dell'ordine dei fattori.*

Dim: cfr. Marcus [24], Teorema 16, pag. 59 . ●

Teorema 2.4.11: *Sia I un ideale in un dominio di Dedekind R e sia $\alpha\in I$, $\alpha\neq 0$. Allora $\exists\ \beta\in I$ tale che $(\alpha,\beta)=I$.*

Dim: cfr. Marcus [24], Teorema 17, pag. 61 . ●

Teorema 2.4.12: *Ogni anello degli interi O_K di un campo di numeri K è un dominio di Dedekind.*

Dim: cfr. Marcus [24], Teorema 14, pag. 56 . ●

Abbiamo introdotto una nozione di fattorizzazione in ideali primi perché O_K non è in generale un anello fattoriale (non è detto che sia verificata l'unicità della decomposizione).
Ricordiamo adesso alcune proprietà degli anelli fattoriali:

Teorema 2.4.13: *Se D dominio Noetheriano, allora D ammette fattorizzazione in irriducibili (cioè $\exists\ x\in D$, $x\neq 0$, x non invertibile, può essere scritto come prodotto di un numero finito di elementi irriducibili di D).*

Dim: cfr. Stewart-Tall [42], Teorema 4.6, pag. 80. ●

Non è però detto che tale fattorizzazione sia unica. Ad esempio in $\mathbb{Q}(\sqrt{-5})$ abbiamo che : $6 = 2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$ che sono irriducibili (cfr. Stewart-Tall [42], Teorema 4.10, pag. 82-83). Inoltre ricordiamo che vi sono delle relazioni tra elementi primi ed elementi irriducibili:

Teorema 2.4.14: *Un primo in un dominio D è sempre irriducibile.*

Dim: Sia $x\in D$, x primo e si abbia $x=a\cdot b$. Poiché x primo, si ha che $x|a$ oppure $x|b$. Se $x|a$ allora $a=x\cdot c$ per un certo $c\in D$ e quindi $x=x\cdot c\cdot b$. Per la proprietà di cancellazione si ha che $1=c\cdot b$ e quindi b invertibile. Ragionando in modo analogo se $x|b$ si ha la tesi. •

Nel caso in cui la fattorizzazione in irriducibili sia possibile abbiamo una condizione necessaria e sufficiente per l'unicità della decomposizione:

Teorema 2.4.15: *Sia D un dominio che ammette la fattorizzazione in irriducibili. Allora tale fattorizzazione è unica se e solo se ogni irriducibile è primo.*

Dim: cfr. Stewart-Tall [42], Teorema 4.13, pag. 88-89. •

Ricordiamo inoltre che :

Teorema 2.4.16: *Ogni dominio principale è fattoriale.*

Dim: cfr. Stewart-Tall [42], Teorema 4.15, pag. 91. •

Teorema 2.4.17: *In O_K la fattorizzazione in irriducibili è unica se e solo se O_K è principale.*
Dim: cfr. Stewart-Tall [42], Teorema 5.15, pag. 127. •

Passiamo adesso ad esaminare il problema detto SPLITTING DEI PRIMI.
Siano K,L due campi di numeri, $K\subseteq L$, ed O_K, O_L i rispettivi anelli degli interi algebrici e sia P un ideale primo di O_K.
Il nostro problema è studiare la decomposizione in ideali primi di P in O_L.
Per procedere oltre è però necessario introdurre una nozione di divisibilità tra ideali (che viene anche utilizzata nella dimostrazione del Teorema 2.4.10).

Definizione 2.4.13: *Dato R un dominio di Dedekind e dati A,B due ideali in R diremo che $A|B$ se e solo se $\exists$ un ideale C tale che $AC=B$.*

Una importante caratterizzazione della divisibilità è la seguente:

Lemma 2.4.2: *Dati A,B ideali in un dominio di Dedekind R si ha che $A|B \Leftrightarrow B\subseteq A$.*

Dim: $\boxed{\Rightarrow}$ banale;
$\boxed{\Leftarrow}$ bisogna usare il fatto che in un dominio di Dedekind, dato un ideale A esiste un ideale J tale che AJ è principale (cfr. Marcus [24], Teorema 15, pag. 57). Quindi $AJ=(\alpha)$.

Consideriamo ora l'insieme $C=\frac{1}{\alpha}JB$ che è banalmente un ideale in R. La tesi si ottiene notando che $AC=\frac{1}{\alpha}AJB=\frac{1}{\alpha}(\alpha)B=RB=B$. •

Diremo inoltre che:

Definizione 2.4.14: *Se P è un ideale primo di O_K e Q è un ideale primo di O_L, diremo che Q STA SOPRA P (e P STA SOTTO a Q) se e solo se vale una delle seguenti condizioni equivalenti:*
1) $Q|PO_L$;
2) $PO_L \subseteq Q$;
3) $P \subseteq Q$;
4) $Q \cap O_K = P$;
5) $Q \cap K = P$.

(l'equivalenza delle condizioni 1)-5) è provata in Marcus [24], Teorema 19, pag. 63).

Esponiamo adesso alcuni risultati che verranno utilizzati nel Capitolo 5:

Teorema 2.4.18: *Ogni primo Q di O_L sta sopra ad un unico primo P di O_K. Ogni primo P di O_K sta sotto ad almeno un primo Q di O_L.*
Dim: cfr. Marcus [24], Teorema 20, pag. 63. •

Mantenendo le notazioni precedentemente usate diremo che:

Definizione 2.4.15: *Indicheremo e(Q|P) e chiameremo INDICE DI RAMIFICAZIONE l'esponente con cui compare Q nella decomposizione di P in ideali primi di O_L.*

Definizione 2.4.16: *Indicheremo f(Q|P) e chiameremo GRADO INERZIALE il grado di $O_{L/Q}$ come estensione di grado finito di $O_{K/P}$.*

Nota: Si noti che sia $O_{L/Q}$ che $O_{K/P}$ sono campi finiti (cfr. Marcus [24], pag. 56, dimostrazione del Teorema 14) che vengono detti CAMPI RESIDUI.

La più importante proprietà che lega insieme e(Q|P) e f(Q|P) è data da:

Teorema 2.4.19: *Sia [L:K]=n, siano $Q_1,\dots,Q_r$ ideali primi di O_L che stanno sopra a P (ideale primo di O_K). Siano $e_1,\dots,e_r$ ed $f_1,\dots,f_r$ i rispettivi indici di ramificazione e gradi inerziali. Allora si ha che* $\sum_{i=1}^{r} e_i f_i = n$.

Dim: cfr. Marcus [24], Teorema 21, pag.65. •

Un caso particolare, ma importante, del teorema precedente è quello in cui L sia una estensione normale di K. In tal caso vale:

Teorema 2.4.20: *Sia L normale su K e siano Q e Q' due ideali primi di O_L che stanno sopra allo stesso ideale primo P di O_K. Allora $\exists\ \sigma \in Gal(L/K)$ tale che $\sigma(Q)=Q'$.*

Dim: cfr. Marcus [24], Teorema 23, pag. 70-71. ●

Corollario: *nelle ipotesi del Teorema 2.4.17, si ha che e(Q|P)=e(Q'|P) e che f(Q|P)=f(Q'|P).*

Dim: La prima affermazione dipende dalla proprietà di decomposizione unica, mentre la seconda si ottiene osservando che s induce un isomorfismo tra $O_{L/Q}$ e $O_{L/Q'}$ dato da $\bar{\sigma}: O_{L/Q} \to O_{L/Q'}$ definito come segue :

$$\bar{\sigma}(\alpha+Q)=\bar{\sigma}(\alpha)+Q' \quad \text{e} \quad \bar{\sigma}(\alpha Q)=\bar{\sigma}(\alpha)Q'. \bullet$$

Nota: Grazie a tale corollario possiamo notare che, nel caso di estensione normale, un primo P di O_K splitta in $(Q_1 \cdots Q_r)^e$, dove i Q_i sono ideali primi distinti aventi lo stesso grado inerziale f. Per il Teorema 2.4.19, si ha anche che ref=[L:K]=n.

Definizione 2.4.17: *Con le definizioni precedenti diremo che un primo P di O_K è RAMIFICATO in O_L se e solo se e(Q|P)>1 per qualche primo Q di O_L che sta sopra a P (cioè P non square-free).*

Ci occupiamo adesso di caratterizzare la ramificazione dei primi di $\mathbb{Z}$, che ci servirà poi nel Capitolo 5.

Teorema 2.4.21: *Sia p un primo di $\mathbb{Z}$ e sia p ramificato in un anello di interi O\s\do6(K) . Allora $p|\Delta_K$.*
Dim: cfr. Marcus [24], Teorema 24, pag. 72. ●

Corollario: *Se $\alpha \in O_K$, $K=\mathbb{Q}(\alpha)$, g è il polinomio monico su $\mathbb{Z}$ tale che $g(\alpha)=0$ e p primo di $\mathbb{Z}$ tale che $p \nmid N(D(g(\alpha)))$ allora p non ramifica in K.*

Dim: dipende dal Teorema 2.4.9. ●

Ci occupiamo adesso di determinare gli ideali che stanno sopra ad un certo primo p di $\mathbb{Z}$.
Supponiamo di avere K,L campi di numeri, $K \subseteq L$, [L:K]=n. Fissiamo $\alpha \in O_L$ tale che abbia grado n su K (cosicché $L=K[\alpha]$). In generale $O_K[\alpha]$ è sottogruppo additivo di O_L e comunque $O_{L/O_K[\alpha]}$ è finito perché come gruppi abeliani liberi O_L ed $O_K[\alpha]$ hanno lo stesso rango uguale a mn, dove m=[K:$\mathbb{Q}$] (cfr. Stewart-Tall [42], Teorema 1.13, pag. 32)).
Sia g il polinomio monico irriducibile a coefficienti in K che ha α come radice. Poiché α è un intero algebrico, allora i coefficienti di g stanno in O_K essendo espressi in termini degli interi

algebrici coniugati di α. Quindi si ha che $g \in O_K[x]$ e possiamo considerare $\bar{g} \in (O_K/P)[x]$, dove P è un ideale primo di O_K. Poiché $(O_K/P)[x]$ è un dominio fattoriale, possiamo scrivere

$\bar{g}=\bar{g}_1 \cdots \bar{g}_r$ dove i $\bar{g}_i$ sono polinomi monici irriducibili distinti.

Teorema 2.4.22: *Con le notazioni precedenti, sia $p \in \mathbb{Z}$ un primo tale che $p \nmid \#(O_L/O_K[\alpha])$ e che sta sotto a P. Allora la decomposizione di PO_L è data da $Q_1^{e_1} \cdots Q_r^{e_r}$ dove $Q_i=(P,g_i(\alpha))$ (in O_L). Inoltre $f(Q_i|P)=grado(g_i)$.*

Dim: cfr. Marcus [24], Teorema 27, pag. 79-82. ●

Concludiamo adesso l'analisi delle proprietà della ramificazione, osservando che vale il viceversa del Teorema 2.4.21:

Teorema 2.4.23: *Sia K un campo di numeri, O_K sia il suo anello degli interi e p un primo di $\mathbb{Z}$. Se $p|\Delta_K$ allora p ramificato in K.*

Dim: cfr. Marcus [24], Teorema 34, pag.112. ●

Esaminiamo adesso il problema dei primi che splittano completamente:

Definizione 2.4.18: *Dati due campi di numeri K,L tali che $K \subseteq L$, diremo che un ideale primo P di K SPLITTA COMPLETAMENTE in L se e solo se il numero degli ideali primi di L che stanno sopra a P stesso è [L:K] (con le notazioni usate precedentemente si può anche dire che P splitta completamente se e solo se r= [L:K]).*

Il risultato che ci interessa nei Capitoli successivi si riferisce alle estensioni normali e ci fornisce la densità dell'insieme degli ideali primi di K che splittano completamente.

Lemma 2.4.3:
Sia L normale su K. Allora l'insieme dei primi P di K che splittano completamente in L ha densità pari a $\frac{1}{[L:K]}$.

Dim: cfr. Narkiewicz [25] , Capitolo 7 , Corollario 4 , pag. 324. ●

2.5. CAMPI CICLOTOMICI.

Un campo ciclotomico è un campo del tipo $\mathbb{Q}(\xi_m)$ con m intero positivo e $\xi_m = e^{\frac{2\pi i}{m}}$ una radice primitiva m-esima dell'unità.
Nel seguito supporremo sempre m=p con p primo dispari.

Lemma 2.5.1: *Il polinomio minimo di $\xi_p = e^{\frac{2\pi i}{p}}$, p primo dispari, su $\mathbb{Q}$ è dato da*

$$f_p(t) = t^{p-1} + \ldots + t + 1.$$

Il grado di $\mathbb{Q}(\xi_p)$ su $\mathbb{Q}$ è p-1.

Dim: Abbiamo che $f_p(t) = \frac{t^p - 1}{t-1}$ e, poiché $\xi_p - 1 \neq 0$ e $\xi_p{}^p = 1$ si ha che $f_p(\xi_p) = 0$ e quindi basta provare che f_p irriducibile. Osserviamo che $f_p(t+1) = \frac{(t+1)^p - 1}{t} = \sum_{r=1}^{p} \binom{p}{r} t^{r-1}$.

Però abbiamo che $p \mid \binom{p}{r}$ per $1 \leq r \leq p-1$ e $p^2 \nmid \binom{p}{1}$ cosicché per il criterio di Eisenstein [(1)], abbiamo che $f_p(t+1)$ è irriducibile e quindi $f_p(t)$ irriducibile.
Poiché grado(f)=p-1, abbiamo che $[\mathbb{Q}(\xi_p):\mathbb{Q}] = p-1$ per il Teorema 2.4.5. •

Si noti inoltre che, per il Teorema 2.4.3, si ha che $\mathbb{Q}(\xi_p)$ è normale su $\mathbb{Q}$ e quindi che esistono $[\mathbb{Q}(\xi_p):\mathbb{Q}] = p-1$ automorfismi di $\mathbb{Q}(\xi_p)$ in sé che fissano puntualmente $\mathbb{Q}$.

Definizione 2.5.1:

Diremo TRACCIA di un elemento $\alpha \in \mathbb{Q}(\xi_p)$ la quantità $T(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha)$ con $\sigma_i \in Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ e $\sigma_i(\xi_p) = \xi_p{}^i$ per ogni i=1,...,p-1.

---

(1) **Criterio di Eisenstein:** *Sia $f \in \mathbb{Z}[t]$, $f(t) = a_0 + a_1 t + \ldots + a_n t^n$.*
Se $\exists$ q primo tale che :
a) $q \nmid a_n$;
b) $q \mid a_i$ $\forall$ i=0,...,n-1;
c) $q^2 \nmid a_0$.
Allora, a meno di fattori costanti, f è irriducibile su $\mathbb{Z}$ e quindi anche su $\mathbb{Q}$.

Dim: cfr. Stewart-Tall [42], Teorema 1.15, pag. 20 . •

Abbiamo le seguenti relazioni che ci serviranno nel seguito: (per le dimostrazioni cfr. Stewart-Tall [42], pag. 62-65)

1) $N(\xi_p^{\,i})=1 \quad \forall\, i=1,...,p-1 \quad (\text{e } N(\xi_p^{\,s})=1 \ \forall\, \sigma\in\mathbb{Z})$;

2) $T(\xi_p^{\,i}) = -1 \qquad \forall\ i=1,...,p-1$

$$(\text{e } T(\xi_p^{\,s}) = \begin{cases} -1 & \text{se } s \not\equiv 0 \pmod p \\ p-1 & \text{se } s \equiv 0 \pmod p \end{cases} \quad \forall\sigma\in\mathbb{Z});$$

3) $N(a)=a^{p-1} \qquad \forall\ a \in \mathbb{Q}$;

4) $T(a)=(p-1)a \qquad \forall a \in \mathbb{Q}$;

5) $T(\alpha)=T(\sum_{i=0}^{p-2} a_i\xi_p^{\,i}) = pa_0 - \sum_{i=0}^{p-2} a_i$;

6) $N(1-\xi_p)=p$.

Passiamo adesso ad esaminare come si presentano in questo caso particolare i concetti già esposti nel Paragrafo 4.

Teorema 2.5.1:
L'anello degli interi algebrici di $\mathbb{Q}(\xi_p)$ è $\mathbb{Z}[\xi_p]$.

Dim: Sia $\alpha=a_0+a_1\xi_p+...+a_{p-2}\xi_p^{\,p-2}\in O_{\xi_p}$ un intero algebrico di $\mathbb{Q}(\xi_p)$. Dobbiamo dimostrare che $a_i\in\mathbb{Z}$, $\forall$ i=0,...,p-2. Osserviamo intanto che l'elemento $\alpha\xi_p^{-i}-\alpha\xi_p$, i=0,...,p-2, è un intero algebrico (perché ξ_p e α lo sono e O_{ξ_p} è anello) e quindi la sua Traccia è un elemento di $\mathbb{Z}$ (per la proprietà 5).

$$T(\alpha\xi_p^{-i}-\alpha\xi_p) = T(a_0\xi_p^{-i}+...+a_i+a_{p-2}\xi_p^{\,p-i-2}-a_0\xi_p-...-a_{p-2}\xi_p^{\,p-1}) =$$
$$= pa_i-(a_0+a_1+...+a_{p-2})-(-a_0-a_1-...-a_{p-2}) = pa_i \in \mathbb{Z}.$$

Definiamo $b_i = pa_i$ e $\lambda=1-\xi_p$.

Allora **1** $p\alpha = b_0+b_1\xi_p+...+b_{p-2}\xi_p^{\,p-2} = c_0+c_1\lambda+...+c_{p-2}\lambda^{p-2}$ dove si ha:

$$c_j = \sum_{i=j}^{p-2} (-1)^r \binom{r}{j} b_r \in \mathbb{Z}$$

e, simmetricamente,

$$b_j = \sum_{i=j}^{p-2} (-1)^r \binom{r}{j} c_r \quad .$$

Proviamo che tutti i c_j sono divisibili per p. Procedendo per induzione, possiamo assumere che sia vero per tutti i c_j con $j\le i-1$ dove $0\le i\le p-2$ (Si noti che per i=0 l'asserto della prova per induzione é banalmente vero).

Notiamo che, per la proprietà 6), $p = N(1-\xi_p) = \prod_{r=1}^{p-1}\left(1-\xi_p^{\,r}\right) =$

$= (1-\xi_p)^{p-1}\prod_{r=1}^{p-1}(1+\xi_p+...+\xi_p^{\,r-1}) = \lambda^{p-1}\gamma$ dove $\gamma\in\mathbb{Z}[\xi_p]\subseteq O_{\xi_p}$.

Considerando adesso la **1** come una congruenza modulo (λ^{i+1}) e ricordando che, per quanto appena visto, $p\equiv 0 \pmod{(\lambda^{i+1})}$, si ottiene che **2** $c_i\lambda^i \equiv 0 \pmod{(\lambda^{i+1})}$ perché, per ipotesi induttiva, i termini da c_0 a $c_{i-1}\lambda^{i-1}$ svaniscono nel passaggio alla congruenza.
La **2** significa che $\exists\ \mu\in O_{\xi_p}$ tale che $c_i\lambda^i=\mu\lambda^{i+1}$, ossia $c_i=\mu\lambda$.
Passando a calcolare le norme abbiamo, per le proprietà precedentemente descritte, che :
$c_i^{\,p-1}=N(c_i)=N(\mu\lambda)=N(\mu)N(\lambda)=pN(\mu)$; quindi $p|c_i^{\,p-1}$ e quindi $p|c_i$.
Allora, per induzione, $p|c_i\ \ \forall i$ ed allora, per la **1**, $p|b_i\ \forall\ i$. Possiamo allora concludere che $a_i\in\mathbb{Z}$ e quindi che $O_{\xi_p} = \mathbb{Z}[\xi_p]$. ●

Nota: Tale risultato vale in generale per tutti i campi ciclotomici, cioè per tutti i $\mathbb{Q}(\xi_m)$ con m intero positivo e $\xi_m = e^{\frac{2\pi i}{m}}$. (cfr. Marcus [24], Corollario 2 del Teorema 12, pag. 35).

Teorema 2.5.2: *Il discriminante di $\mathbb{Q}(\xi_p)$ è $(-1)^{\frac{p-1}{2}}p^{p-2}$.*

Dim: Poiché per il Teorema 2.5.1 abbiamo che $O_{\xi_p}=\mathbb{Z}[\xi_p]$, allora una base intera di $\mathbb{Q}(\xi_p)$ è data da $\{1,\xi_p,...,\xi_p^{\,p-2}\}$. Per il Teorema 2.4.9 abbiamo che :

$$\Delta[1,\xi_p,...,\xi_p^{\,p-2}]=(-1)^{\frac{(p-1)(p-2)}{2}}\,N(D(f_p(\xi_p)))\ .$$

Poiché p è dispari, il primo fattore del 2° membro si riduce a $(-1)^{\frac{p-1}{2}}$. Calcoliamo il secondo fattore:
poiché f\s\do6(p)(t)(t-1)=t\s\up6(p)-1 allora D(f\s\do6(p)(t))(t-1) + f\s\do6(p)(t) = pt\s\up6(p-1) e quindi si ha che $D(f_p(\xi_p)) = \frac{p\xi_p^{\,p-1}}{1-\xi_p}$ e quindi $N(D(f_p(\xi_p))) = \frac{N(p)\,N(\xi_p)^{p-1}}{N(1-\xi_p)} = \frac{p^{p-1}}{p} = p^{p-2}$. ●

Ricordiamo che, per il Teorema 2.4.12, $\mathbb{Z}[\xi_p]$ è di Dedekind e per, il Teorema 2.4.11, sappiamo che ogni ideale $\mathbb{Z}[\xi_p]$ è generato al più da due elementi. In generale in $\mathbb{Q}(\xi_p)$ non ab-

biamo la fattorizzazione unica in irriducibili perché, $\mathbb{Z}[\xi_p]$ non è principale (cfr. Teorema 2.4.17): infatti $(2,\xi_p)$ è un ideale di $\mathbb{Z}[\xi_p]$ non principale.

Passando al problema dello splitting abbiamo che, poiché $\mathbb{Q}(\xi_p)$ è normale su $\mathbb{Q}$, vale la Nota al Teorema 2.4.20 e quindi che e,f sono unici e ref=p-1.

Inoltre, per il Teorema 2.4.23 e il Teorema 2.4.21, abbiamo che l'unico primo di $\mathbb{Z}$ che ramifica in $\mathbb{Z}[\xi_p]$ è p stesso.
Vale inoltre il seguente:

Teorema 2.5.3: *Sia p un primo di $\mathbb{Z}$, sia $m=p^k t$ con $p \nmid t$. Allora, in $\mathbb{Q}(\xi_m)$, si ha che $e=\varphi(p^k)=p^k-p^{k-1}$ ed f è l'ordine di p in $(\mathbb{Z}/m\mathbb{Z})^*$.*

Dim: cfr. Marcus [24], Teorema 26, pag.76 . •

Corollario:
Se $p \nmid m$, allora p splitta in $\varphi(m)/f$ ideali primi distinti di $\mathbb{Z}[\xi_m]$, dove $f=\operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^*}(p)$.

Dim: Poiché $p \nmid m$ si ha che k=0 (con le notazioni del Teorema 2.5.3) e quindi e=1. Allora per il Teorema 2.4.19 si ha che rf=φ(m). •

Per determinare gli ideali di $\mathbb{Q}(\xi_m)$ che stanno sopra un certo p di primo di $\mathbb{Z}$, basta applicare il Teorema 2.4.22 a tale caso particolare.
Notiamo inoltre che la densità dell'insieme dei primi di $\mathbb{Z}$ che splittano completamente in $\mathbb{Z}[\xi_m]$ è data da $\frac{1}{\varphi(m)}$ per il Lemma 2.4.3.

2.6. I NUMERI P-ADICI.

I numeri p-adici vengono introdotti mediante l'assegnazione a $\mathbb{Q}$ di un valore assoluto diverso da quello usuale.
Vediamo in generale alcune proprietà dei valori assoluti e delle valutazioni.

Definizione 2.6.1: *Sia K un campo. Definiamo VALORE ASSOLUTO su K una applicazione* $|\ |: K \to \mathbb{R}^+$ *tale che verifichi le seguenti proprietà:*
1) $|x|=0 \Leftrightarrow x=0$;
2) $|xy|=|x|\ |y| \quad \forall x,y \in K$;
3) $\exists\, c>0$ *tale che* $|x+y| \le c \max\{|x|;|y|\} \quad \forall x,y \in K$.

Il campo K viene così ad essere uno spazio topologico metrico con la metrica indotta dal valore assoluto $|\ |$ e definita da d(x,y)=|x-y|.
All'interno dei valori assoluti si può quindi introdurre una relazione di equivalenza.

Definizione 2.6.2: *Due valori assoluti su K si dicono equivalenti se e solo se le rispettive topologie indotte sono equivalenti.*

E' possibile introdurre anche la nozione di norma di un valore assoluto :

Definizione 2.6.3: *Definiamo NORMA di un valore assoluto* $|\ |$ *su K la quantità:*
$N(|\ |)=\inf\{ c>0 \text{ tali che } |x+y| \le c\max\{|x|;|y|\} \ \forall x;y \in K\}$.

Si può provare che $N(|\ |)\ge 1$ e che tale inf é un minimo. Infatti se esistesse c' tale che $0<c'<1$ e che verifica 3) della Definizione 2.6.1, allora si avrebbe che, $\forall x \in K,\ x\neq 1,\ |x| = |x+0| \le c'\max\{|x|;|0|\} = c'\max\{|x|;0\} = c'|x| < |x|$ e quindi si ottiene un assurdo.
Ciò implica che $N(|\ |)\ge 1$.
Per provare che tale inf è in realtà un minimo, osserviamo che esiste una successione di reali c_n, verificanti la 3) della Definizione 2.6.1, tale che $\lim_{n\to+\infty} c_n = N(|\ |)$.
Allora abbiamo una serie di disuguaglianze, al variare di n, date da :

$$|x+y| \le c_n \max\{|x|;|y|\}$$

e, passando al limite su n ed applicando il Teorema del confronto, quindi si ottiene :

$$|x+y| \le N(|\ |)\ \max\{|x|;|y|\},$$

cioè $N(|\ |)$ è un minimo.

La norma dei valori assoluti può essere usata per compiere una ulteriore classificazione dei valori assoluti stessi.

Definizione 2.6.4: *Diremo ARCHIMEDEO un valore assoluto* $|\ |$ *tale che* $N(|\ |)>1$ *e diremo NON ARCHIMEDEO un valore assoluto* $|\ |$ *tale che* $N(|\ |)=1$.

Un concetto collegato a quello di valore assoluto è quello di valutazione.

Definizione 2.6.5: *Sia K un campo. Definiamo VALUTAZIONE REALE in K una applicazione* $v : K \to \Gamma$ *(* Γ *sottogruppo additivo di* $\mathbb{R}\cup\{+\infty\}$ *) tale che verifichi le seguenti proprietà:*
1) v/K^* *è omomorfismo di gruppi;*

2) $v(0)=+\infty$ e $v(x)\neq+\infty$ $\forall\, x\neq 0$;
3) $v(x+y) \geq inf\{v(x);v(y)\}$ $\forall\, x,y\in K$.

Nel caso in cui si abbia Γ isomorfo, come gruppo additivo, a $\mathbb{Z}$ la valutazione viene detta DISCRETA anziché reale.

Definiamo adesso alcuni oggetti algebrici collegati alle valutazioni.

Definizione 2.6.6:
Diremo ANELLO DELLA VALUTAZIONE l'anello $O_v=\{x\in K$ tale che $v(x)\geq 0\}$.

Si può provare che tale anello ha solo due ideali primi: l'ideale nullo e l'ideale $M_V=\b\bc\{(x\in K$ tale che $v(x)>0)$ (cfr. Cassels [8], pag.41). Abbiamo allora che M_V é massimale per O_V e, poiché non vi sono altri ideali, abbiamo che M_V é l'unico ideale massimale di O_V (cioè O_V é ANELLO LOCALE).
Il gruppo degli elementi invertibili di O_V è dato da $U_V=\{x\in K$ tale che $v(x)=0\}=O_V\backslash M_V$.

Esiste inoltre uno stretto legame tra valori assoluti non archimedei e valutazioni reali.
Infatti: se $|\ |: K\rightarrow \mathbb{R}^+$ è un valore assoluto non archimedeo e $b\in(0,1)$ una costante arbitraria, allora possiamo definire una valutazione reale $v: K\rightarrow\mathbb{R}$, $v(x)=lg_b(|x|)$ (dove per lg_b si intende il logaritmo in base b). Viceversa, se $v: K\rightarrow \mathbb{R}$ è una valutazione reale, allora possiamo definire un valore assoluto $|\ |: K\rightarrow \mathbb{R}^+$, $|x|=b^{v(x)}$. Nel caso di fissare una costante arbitraria $b>1$, si prende rispettivamente $v(x)=-lg_b(|x|)$ e $|x|=b^{-v(x)}$.
In tal modo si può parlare di valutazioni reali equivalenti perché tale nozione di equivalenza viene scaricata sui corrispondenti valori assoluti indotti.
Si può dimostrare anche che :
1) i campi finiti ammettono solo la valutazione banale definita da $v: K^*\rightarrow\{0\}$ e $v(0)=+\infty$ (Cassels [8], pag. 13, Corollario 4 della Definizione 2.1);
2) i campi di caratteristica $p>0$, p primo, ammettono solo valori assoluti non archimedei.
(cfr. Cassels [8], pag.16, Corollario 2 del Lemma 1.5).

Nel caso particolare di aver $K=\mathbb{Q}$ si può provare che esistono solo tre tipi diversi di valori assoluti (cfr. Cassels [8], Teorema 2.1 (Ostrowsky), pag. 16-18):
a) il valore assoluto banale definito da $|x|=1$ $\forall\ x\neq 0$ e $|x|=0 \Leftrightarrow x=0$;
b) se $|\ |$ é il valore assoluto usuale, allora sono ammessi tutti i valori assoluti del tipo $|\ |^s$, con $s>0$, e sono tutti archimedei.
c) valori assoluti non archimedei.

I valori assoluti su $\mathbb{Q}$ del tipo c) sono quelli che consentono di definire i numeri p-adici.

Definizione 2.6.7:
Fissato p primo, diremo VALUTAZIONE P-ADICA la valutazione v_p: $\mathbb{Q}\rightarrow\mathbb{Z}$ tale che, se $x\in\mathbb{Q}$ viene scritto $x=\frac{a}{b}=\frac{m}{n}p^{\alpha}$ con $(p,m)=1=(p,n)$, $\alpha\in\mathbb{Z}$, si ha $v_p(x)=\alpha$.

Da quanto precedentemente detto, abbiamo che v_p é discreta e che tale valutazione induce su $\mathbb{Q}$ un valore assoluto, che indicheremo $|\ |_p$, e chiameremo VALORE ASSOLUTO P-ADICO, definito da $|x|_p=\left(\frac{1}{p}\right)^{v_p(x)}$.

Consideriamo adesso $(\mathbb{Q},|\ |_p)$ e notiamo che:

a) $O_{v_p} = O_p = \left\{ x\in\mathbb{Q} \text{ tale che } v_p(x)\geq 0 \right\} = \left\{\frac{m}{n}\in\mathbb{Q} \text{ tali che } n\neq 0 \text{ e } p\not| n\right\} = \mathbb{Z}_{(p)}$

(dove con tale ultima notazione si intende $\mathbb{Z}$ localizzato nel proprio ideale (p)).

b) $M_{v_p} = M_p = \left\{ x\in\mathbb{Q} \text{ tale che } v_p(x)>0 \right\} =$

$= \left\{\frac{m}{n}\in\mathbb{Q} \text{ tali che } n\neq 0;\ p\not| n \text{ e } p| m\right\} = p\mathbb{Z}_{(p)}$ (cioè l'ideale generato da p in $\mathbb{Z}_{(p)}$).

c) $U_{v_p} = U_p = \mathbb{Z}_{(p)}\backslash p\mathbb{Z}_{(p)} = \left\{\frac{m}{n}\in\mathbb{Q} \text{ tali che } n\neq 0;\ p\not| n \text{ e } p\not| m\right\}$.

Definizione 2.6.8: *Definiamo CAMPO DEI NUMERI P-ADICI $\mathbb{Q}_p$ il completamento di $(\mathbb{Q},|\ |_p)$ rispetto a $|\ |_p$ stesso.*
(da Cassels [8], Teorema 4.1, pag. 24, sappiamo che tale completamento esiste ed è unico a meno di isomorfismi)

Inoltre estendiamo per continuità $|\ |_p$ su $\mathbb{Q}_p$ in modo da ottenere su quest'ultimo la struttura di spazio topologico metrico.

Indicheremo col simbolo $\mathbb{Z}_p$ l'anello della valutazione di $(\mathbb{Q}_p,|\ |_p)$. L'ideale massimale di $\mathbb{Z}_p$ é dato da $p\mathbb{Z}_p$. Si noti inoltre che vale la seguente catena di isomorfismi di campi:

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}\ .$$

Per il primo isomorfismo confrontare con Cassels [8], Lemma 1.1, pag. 41, mentre il secondo é una facile applicazione del Primo Teorema di Omomorfismo per Anelli.
Possiamo adesso caratterizzare gli elementi di $\mathbb{Q}_p$ (cfr. Cassels [8], Lemma 1.4 e rispettivo Corollario, pag. 44-45) come tutti e soli gli elementi del tipo:

$$x=\sum_{n=n_0}^{+\infty} a_n p^n = \frac{a_{n_0}}{p^{n_0}} + a_0 + ... + a_n p^n + ... \quad \text{dove } n_0\in\mathbb{Z} \text{ e } a_n \in(\mathbb{Z}/p\mathbb{Z}).$$

Tale serie é convergente rispetto a $|\ |_p$ ed inoltre si noti che $v_p(x)=n\backslash s\backslash do4(0)$ perché $x=\frac{1}{p^{n_0}}(a_{n_0} + \cdots + a_0 p^{n_0} + ...)= \frac{1}{p^{n_0}}\omega$ con $\omega\in\mathbb{Q}_p$ e $p\not|\omega$.

Da tale ultima osservazione si ottiene che :

a) $x\in\mathbb{Z}_p \Leftrightarrow x = \sum_{n=n_0}^{+\infty} a_n p^n$ con $n_0\geq 0$;

b) $x \in U_p \Leftrightarrow x = \sum_{n=0}^{+\infty} a_n p^n$;

c) $x \in \mathbb{Q}_p \Leftrightarrow x = t+y$ con $y \in \mathbb{Z}_p$ e $t \in \mathbb{Z}[p^{-1}]$;

d) $x \in \mathbb{Q}_p \Leftrightarrow x = \frac{1}{p^{v_p(x)}} u$ dove $u \in U_p$.

Capitolo 3

Elementi Di Teoria Analitica Dei Numeri

3.1. FUNZIONI BASE DELLA TEORIA ANALITICA DEI NUMERI.

Nella Teoria Analitica dei Numeri esistono alcune funzioni aritmetiche molto usate che ci serviranno nei capitoli successivi.

Definizione 3.1.1: Funzione μ di MÖBIUS:

Definiamo $\mu:\mathbb{N}\to\mathbb{N}$ *tale che* $\mu(1)=1$ *e, posto* $n=\prod_{i=1..r} p_i^{a_i}$, *che*

$$\mu(n)=\begin{cases}(-1)^r & \text{se } a_i = 1\ \forall\ i = 1..r\\ 0 & \text{altrimenti}\end{cases}.$$

Definizione 3.1.2: Funzione φ di EULERO:

Definiamo $\varphi:\mathbb{N}\to\mathbb{N}$ *tale che* $\varphi(n)=\#\{k\in\mathbb{N}$ *t.c.* $1\le k\le n$ *e* $(k,n)=1\}$.

Alternativamente si può scrivere $\varphi(n)=\sum_{\substack{k=1..n\\(k,n)=1}} 1$ cioè φ è la funzione che conta quanti sono gli interi k relativamente primi con n.

Vediamo adesso alcune proprietà di φ e di μ.

Teorema 3.1.1: $\sum_{d\mid n}\mu(d) = \begin{cases}1 & \text{se } n = 1\\ 0 & \text{se } n > 1\end{cases}$.

Dim: Se n=1 allora la formula é banalmente vera;

se n>1 ed $n=\prod_{i=1..r} p_i^{a_i}$, possiamo notare che nella somma gli unici termini non nulli sono quelli per cui d=1 oppure d é square-free. Allora si ha :

$$\sum_{d\mid n}\mu(d)=\mu(1)+\mu(p_1)+..+\mu(p_r)+\mu(p_1p_2)+...+\mu(p_{r-1}p_r)+...+\mu(p_1\cdots p_r)=$$

$$=1+\binom{r}{1}(-1)+\binom{r}{2}(-1)^2+...+\binom{r}{r}(-1)^r=(1-1)^r=0. \quad \bullet$$

Teorema 3.1.2: $\sum_{d|n} \varphi(d) = n.$

Dim: Sia S={1..n}. Definiamo A(d)={ k∈ℕ t.c. 1≤k≤n e (k,n)=d} ∀d|n. Gli insiemi A(d) sono tra loro disgiunti e la loro unione fornisce tutto S. Definiamo adesso f(d)=#A(d). L'affermazione precedente sugli A(d) può essere quindi scritta come $\sum_{d|n} f(d)=n$.

Però sappiamo che (k,n)=d ⇔ $(\frac{k}{d}, \frac{n}{d})=1$ e che $0<k\le n \Leftrightarrow 0<\frac{k}{d} \le \frac{n}{d}$. Poniamo adesso $q=\frac{k}{d}$. Per quanto detto sopra abbiamo una biiezione tra A(d) e gli interi q soddisfacenti $0<q\le\frac{n}{d}$ e $(q,\frac{n}{d})=1$. Quindi abbiamo $f(d)=\varphi(\frac{n}{d})$ ed allora $\sum_{d|n} \varphi(\frac{n}{d})=n$. Ma tale scrittura é equivalente alla tesi perché se d varia in tutti i divisori di n, allora anche $\frac{n}{d}$ varia in tutti i divisori di n. •

Teorema 3.1.3: $\varphi(n)= \sum_{d|n} \mu(d)\frac{n}{d}$.

Dim: Dalla definizione si ha che $\varphi(n)= \sum_{k=1..n} \left[\frac{1}{(k,n)}\right]$ .Per il Teorema 3.1.1, si ha che $\varphi(n)= \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d)$. Fissiamo adesso un divisore d di n e notiamo che la somma precedente viene effettuata solo sugli interi k multipli di d compresi nell'intervallo 1≤k≤n. Poniamo allora k=qd ed osserviamo allora che $1\le k\le n \Leftrightarrow 1\le q<\frac{n}{d}$. La doppia sommatoria precedente può allora essere scritta:

$$\varphi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d)\frac{n}{d} \quad . \bullet$$

Teorema 3.1.4: $\varphi(n) = n \prod_{\substack{p|n \\ p \text{ primo}}} (1-\frac{1}{p})$.

Dim: Se n=1 abbiamo che il prodotto viene effettuato sull'insieme vuoto. In tal caso assegniamo al prodotto il valore 1.

Se n>1 e $n=\prod_{i=1..r} p_i^{a_i}$, con $p_i \neq p_j$ per i≠j, allora abbiamo che :

$$\prod_{\substack{p\mid n\\ p\text{ primo}}}\left(1-\frac{1}{p}\right) = \prod_{i=1..r}\left(1-\frac{1}{p_i}\right) = 1-\sum_{i=1..r}\frac{1}{p_i} + \sum_{i\neq j}\frac{1}{p_ip_j} - \ldots\ldots\ldots + \frac{(-1)^r}{p_1p_2\ldots\ldots p_r}\ .$$

Si noti che ogni termine del membro di destra é della forma $\pm\frac{1}{d}$ dove d é un divisore di n (d può essere soltanto o 1 oppure un square-free). Il segno ± 1 viene determinato da $\mu(d)$ e, poiché $\mu(d)=0$ se d non è square-free, allora possiamo concludere che tale membro non è altro che $\sum_{d\mid n}\frac{\mu(d)}{d}$. •

Da tale teorema si possono dedurre alcune importanti proprietà della funzione φ di Eulero .

Teorema 3.1.5: *La φ di Eulero verifica le seguenti proprietà:*
a) $\varphi(p^a)=p^a-p^{a-1}$ con p primo e a>1;
b) $\varphi(mn)=\varphi(m)\varphi(n)$ se (m,n)=1.

Dim: a) dipende dal Teorema 3.1.4 con $n=p^a$;
b) dal Teorema 3.1.4 abbiamo che $\frac{\varphi(mn)}{mn} = \prod_{\substack{p\mid mn\\ p\text{ primo}}}\left(1-\frac{1}{p}\right)$. Osservando che m ed n non hanno divisori comuni e che, siccome p é primo, se p|mn, allora p|m oppure p|n, possiamo allora scrivere:

$\frac{\varphi(mn)}{mn} = \prod_{\substack{p\mid m\\ p\text{ primo}}}\left(1-\frac{1}{p}\right)\prod_{\substack{p\mid n\\ p\text{ primo}}}\left(1-\frac{1}{p}\right) = \frac{\varphi(m)}{m}\frac{\varphi(n)}{n}$ da cui si ottiene banalmente la tesi. •

Nota: La proprietà b), unitamente alla condizione φ non identicamente nulla, viene anche enunciata dicendo che φ è una FUNZIONE MOLTIPLICATIVA.

Le funzioni moltiplicative godono di alcune importanti proprietà:

Teorema 3.1.6: *Se f, g funzioni moltiplicative allora la funzione $h:\mathbb{N}\to\mathbb{N}$; $h(n)=\sum_{d\mid n} f(d)g(\frac{n}{d})$*

è anch'essa moltiplicativa.

Dim: Siano m,n due interi positivi primi tra loro, allora $h(mn)=\sum_{c\mid n} f(c)g(\frac{mn}{c})$. Però ogni divisore c di mn può essere espresso nella forma c=ab dove a|m, b|n, (a,b)=1, $(\frac{m}{a}, \frac{n}{b})=1$ perché m

ed n sono primi tra loro. Abbiamo quindi una corrispondenza biunivoca tra l'insieme dei prodotti ab ed i divisori c di mn. Possiamo allora scrivere che:

$$h(mn) = \sum_{\substack{a|m \\ b|n}} f(ab)g(\frac{mn}{ab}) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g(\frac{m}{a})g(\frac{n}{b}) = \sum_{a|m} f(a)g(\frac{m}{a}) \sum_{b|n} f(b)g(\frac{n}{b}) = h(m)\,h(n)\ .$$ •

Nota: La funzione h(n) è anche detta Prodotto di Dirichlet di f e g e tale prodotto si indica $h=f*g$.

Abbiamo enunciato e provato tali proprietà per poter dimostrare una formula che consente di passare da un particolare prodotto di Dirichlet ad un prodotto usuale effettuato sui primi. Tale formula è importante perché è di uso comune all'interno della Teoria Analitica dei Numeri.

Teorema 3.1.7:

Se f moltiplicativa allora $\sum_{d|n} \mu(d)f(d) = \prod_{p|n} (1-f(p))$.

Dim: Sia $g(n)=\sum_{d|n} \mu(d)f(d)$. Per il Teorema 3.1.6 g è moltiplicativa e quindi per calcolare g(n) basta conoscere $g(p^a)$.

Però $g(p^a)= \sum_{d|p^a} \mu(d)f(d) = \mu(1)f(1)+...+\mu(p)f(p) = 1-f(p)$.

Quindi $g(n)= \prod_{p|n} g(p^a) = \prod_{p|n} (1-f(p))$.

Nota: Il primo membro dell'equazione provata in questo teorema è il Prodotto di Dirichlet tra la funzione moltiplicativa $t(n)=\mu(n)f(n)$ (é una funzione moltiplicativa perché μ è moltiplicativa ed il prodotto di due funzioni moltiplicative è moltiplicativo) e la funzione $u(n)=1\ \forall\ n\geq 1$. Quindi tale teorema si può anche enunciare come segue:

$$(\mu f)*u= \prod_{p|n} (1-f(p)).$$

Passiamo adesso a definire alcune altre importanti funzioni della Teoria Analitica dei Numeri.

Definizione 3.1.3:

Definiamo $\pi(x)$ la funzione che conta il numero dei primi nell'intervallo [2,x].

Alternativamente possiamo anche scrivere $\pi(x)= \sum_{\substack{p\leq x \\ p \text{ primo}}} 1$.

Definizione 3.1.4: Funzione ϑ di Cebicev.

Definiamo $\vartheta(x) = \sum_{\substack{p \le x \\ p \text{ primo}}} lgp$.

Tali due funzioni sono legate dalle relazioni :

$$\vartheta(x) = \pi(x)\lg x - \int_2^x \frac{\pi(t)}{t}\,dt \qquad\qquad \pi(x) = \frac{\vartheta(x)}{\lg x} + \int_2^x \frac{\vartheta(t)}{t\lg^2 t}\,dt$$

la cui dimostrazione si trova su Ramanujan [32], pag. 83 .

Entrambe queste due ultime funzioni sono importanti per studiare la distribuzione asintotica dei numeri primi.
Una prima osservazione utile per studiarne le caratteristiche é data dal fatto che $\lim_{x\to+\infty} \pi(x) = +\infty$ (perché vi sono infiniti primi), ma la relazione fondamentale è data dal seguente

Teorema 3.1.8: Teorema dei Numeri Primi.

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

Dim: cfr. Apostol [2], Capitolo 13. •

Il Teorema dei numeri primi ci consente di affermare che, per x molto grande, il rapporto tra $\pi(x)$ e $\frac{x}{\lg x}$ è circa uguale ad 1.
Si noti che, per quanto abbiamo detto sulle relazioni tra $\pi(x)$ e $\vartheta(x)$, si ha, come enunciato equivalente del Teorema dei Numeri Primi, che $\lim_{x\to+\infty} \frac{\vartheta(x)}{x} = 1$ (cfr . Apostol [2], capitolo 4, Teorema 4.4, pag 79).

Un problema simile a quello precedente, ma un po' più complesso, è quello di studiare la distribuzione dei primi nelle progressioni aritmetiche. A priori non si sa neanche se una progressione aritmetica del tipo qn+a, n=0,1,... , contiene un numero infinito di primi. Dirichlet (Apostol [2], pag. 154) ha provato che condizione necessaria e sufficiente affinché la progressione aritmetica precedente contenga infiniti primi è che (q,a)=1.
In tal caso possiamo definire la funzione che conta il numero di primi appartenenti alla progressione:

Definizione 3.1.5: $\pi(x;q,a) = \sum_{\substack{p \le x \\ p \equiv a \,(mod\, q) \\ p \text{ primo}}} 1$.

Come per il problema precedente esiste un risultato sulla distribuzione :

Teorema 3.1.9: Teorema dei Numeri Primi nelle progressioni.

$$\lim_{x \to +\infty} \frac{\pi(x;q,a)\varphi(q)\lg x}{x} = 1.$$

Dim: cfr. Davenport [11], capitolo 22, pag. 133. ●

Tale teorema ci consente di affermare che, per x molto grande, il rapporto tra $\pi(x;q,a)$ e $\frac{x}{\lg x}$ è circa dato da $\frac{1}{\varphi(q)}$.

Sempre nell'ambito della distribuzione dei numeri primi nelle progressioni, enunciamo adesso un risultato che utilizzeremo nel seguito (Capitolo 5):

Teorema 3.1.10: Disuguaglianza di Brun-Titchmarsh.
Se x>1 e y>3q allora si ha che :

$$\pi(x+y;q,a)-\pi(x;q,a) \leq \frac{2y}{\varphi(q)\lg(y/q)}$$

Dim: cfr. Bombieri [7], pag. 22. ●

3.2. L'IPOTESI DI RIEMANN E L'IPOTESI DI RIEMANN GENERALIZZATA.

Con i termini utilizzati nel titolo del presente paragrafo si intendono due congetture (entrambe ancora non provate) sulla distribuzione degli zeri di due particolari funzioni della Teoria Analitica dei Numeri.
Tali congetture giocano un ruolo molto importante all'interno della Teoria Analitica dei Numeri perché consentono di ottenere i risultati ottimali sulla distribuzione dei primi nelle progressioni aritmetiche.

Definizione 3.2.1:
Chiameremo Funzione Zeta di Riemann la funzione :

$$\zeta(s)=\sum_{n=1}^{+\infty}\frac{1}{n^s} \quad , \text{ con } s=\sigma+it \text{ e } \sigma>1.$$

La funzione $\zeta(s)$ si estende come funzione meromorfa in $\mathbb{C}$. (cfr. Apostol [2], Teorema 12.5, pag. 255).

Alcune proprietà fondamentali della funzione $\zeta(s)$ sono :
1) $\zeta(s)\neq 0$ in $\sigma>1$;
2) Gli zeri di z(s) in $s<0$ sono zeri semplici in s=-2,-4,-6,...
3) Gli zeri di z(s) in $0\leq s\leq 1$ sono simmetrici rispetto alla retta $\sigma=\frac{1}{2}$ ed all'asse reale (cioè sono simmetrici rispetto $s=\frac{1}{2}$).

Queste tre proprietà derivano da proprietà di convergenza della serie $\sum_{n=1}^{+\infty}\frac{1}{n^s}$ (cfr. Apostol [2], Capitolo 12, Teorema 12.1, pag. 251), dal Prodotto di Eulero ($\zeta(s)=\prod_p (1-\frac{1}{p^s})^{-1}$; cfr. Apostol [2], Capitolo 11, Teorema 11.6, pag. 230) e dall'equazione funzionale seguente:

$$\pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2})\zeta(s)=\pi^{-\frac{(1-s)}{2}}\Gamma(\tfrac{(1-s)}{2})\zeta(1-s)$$

(dove $\Gamma(s)=\int_0^{+\infty} e^{-y}y^{s-1}\,dy$; cfr. Apostol [2], pag. 250 e Teorema 12.7, pag. 259-260).

Grazie a quanto detto in precedenza possiamo procedere a dare una classificazione degli zeri di $\zeta(s)$:
gli zeri di $\zeta(s)$ in s=-2,-4,-6,... sono detti zeri BANALI;

gli zeri non banali di $\zeta(s)$ sono dunque compresi nella striscia $0\le\sigma\le1$ (detta STRISCIA CRITICA), mentre la retta $s=\frac{1}{2}$ viene detta LINEA CRITICA.

Possiamo adesso enunciare l'**Ipotesi di Riemann** (1859) :

Gli zeri non banali di $\zeta(s)$ appartengono tutti alla linea critica.

L'Ipotesi di Riemann ha interessato moltissimi matematici che, purtroppo, sono riusciti solo a provare dei risultati parziali: nel 1914 Hardy [14] dimostrò che infiniti zeri di $\zeta(s)$ appartengono alla linea critica, nel 1942 Selberg [39] provò che gli zeri nel segmento $[\frac{1}{2},\frac{1}{2}+iT]$ sono almeno ATlgT per un certo A>0 se T abbastanza grande, nel 1974 Levinson [23] dimostrò che la frazione degli zeri appartenenti alla linea critica è almeno $\frac{1}{3}$ del totale e recentemente (1989) Conrey [10] ha provato che almeno i $\frac{2}{5}$ appartengono alla linea critica. Inoltre alcuni calcoli effettuati con l'ausilio elaboratori elettronici hanno provato che i primi $1.5\cdot10^{9}$ zeri di $\zeta(s)$ appartengono alla linea critica.

L'orientamento attuale dei matematici è quello di considerare il problema dell'Ipotesi di Riemann dal punto di vista positivo, cioè si pensa che essa sia effettivamente vera.

Prima di poter parlare dell'Ipotesi di Riemann Generalizzata dobbiamo introdurre la seguente:

Definizione 3.2.2: L-serie di Dirichlet.

Diremo L-serie di Dirichlet la funzione $L(s,\chi)=\sum_{n=1}^{+\infty}\frac{\chi(n)}{n^s}$ *dove* χ *è un carattere di Dirichlet e* $\sigma>1$.

Un carattere di Dirichlet (modulo q), q intero, è una applicazione $\chi:\mathbb{Z}\to\mathbb{C}$ *che estende un omomorfismo* $\bar{\chi}:(\mathbb{Z}/q\mathbb{Z})^*\to\mathbb{C}$ *nel modo seguente:*

a) se $n\in(\mathbb{Z}/q\mathbb{Z})\setminus(\mathbb{Z}/q\mathbb{Z})^*$ *allora* $\chi(n)=0$;

b) se $n\equiv\bar{n}\pmod q$ *allora* $\chi(n)=\bar{\chi}(\bar{n})$.

Le funzioni $L(s,\chi)$ godono di proprietà molto simili a quelle di $\zeta(s)$.

Possiamo adesso enunciare l'**Ipotesi di Riemann Generalizzata**:

Gli zeri non banali di $L(s,\chi)$ appartengono tutti alla linea critica.

Capitolo 4

Test Di Primalità

Introduzione al problema:

Il problema di decidere la primalità di un intero ha sempre affascinato i matematici. Per molto tempo si é cercato di trovare dei metodi che permettessero di produrre facilmente tavole di numeri primi (ad esempio il crivello di Eratostene), oppure consentissero di "costruire" primi dotati di una forma "speciale". Molti di tali metodi, essendo essenzialmente calcolativi, si prestavano male ad essere usati con carta e penna, e, quindi, venivano commessi diversi errori.
Con l'avvento degli elaboratori elettronici, la situazione é radicalmente mutata. Infatti, l'avere a disposizione uno strumento capace di svolgere calcoli elementari molto più velocemente e precisamente di una mente umana, ha sia permesso di raggiungere una maggiore sicurezza nei calcoli, sia fornito impulso allo studio di algoritmi sempre più facilmente implementabili ed efficienti. Negli ultimi anni, inoltre, lo sviluppo della crittografia a chiave pubblica ha portato notevole interesse al problema della primalità ed alla ricerca di test di primalità "veloci".
Allo stato attuale dei fatti, il maggiore problema che si presenta negli algoritmi di primalità non é tanto ottenere una risposta, bensì provare la correttezza della risposta stessa.
A tal scopo é utile mettere in risalto la differenza esistente tra algoritmi di primalità probabilistici e deterministici. Col termine "probabilistico" si intende, generalmente, un algoritmo la cui esecuzione può non terminare (vi é la possibilità di un loop infinito). Bisognerà allora, al momento di valutare la complessità computazionale, indicare, oltre alla complessità vera e propria, anche con che probabilità l'esecuzione termina in un certo numero di passi. Con lo stesso termine indicheremo, però, anche quegli algoritmi che, pur terminando con certezza e pur essendo in grado di provare che un intero é composto, sono solo in grado di affermare che un intero é "probabilmente" primo (ossia quelli che concludono che tale intero ha un'opportuna probabilità di essere effettivamente un numero primo).
Con il termine "deterministico" si intende un algoritmo che termina con certezza e che prova la primalità di un intero.
Alcuni dei test di primalità più importanti sono da ritenersi probabilistici. Vi sono anche dei test che, supponendo la correttezza di alcune congetture non provate (fino ad oggi !) di Teoria dei Numeri, diventano, da probabilistici, deterministici (ad esempio : l'algoritmo probabilistico di MILLER-RABIN, che viene presentato nel presente capitolo, diventa deterministico se si assume che l'IPOTESI DI RIEMANN GENERALIZZATA sia vera).
Un altro importante fattore di classificazione e di valutazione degli algoritmi é dato dalla complessità computazionale (ossia, in termini un poco rozzi, dal numero di operazioni elementari necessarie per eseguire l'algoritmo). Più la complessità computazionale é "piccola", più l'algoritmo é efficiente. Nel seguito indicheremo col termine "polinomiale" quegli algoritmi che hanno complessità computazionale maggiorata da un polinomio nella variabile "numero delle cifre dell'intero testato". Poiché il numero delle cifre di un intero n é circa dato da lgn, avremo che gli algoritmi polinomiali hanno complessità maggiorata da un polinomio in lgn. Da tale punto di vista il migliore algoritmo deterministico di primalità conosciuto (test di Adleman-Pomerance-Rumely [1], cfr. Capitolo 5) presenta una complessità "quasi-polinomiale" data da $O((\lg n)^{c \lg\lg\lg n})$ con c costante positiva.
Un risultato molto importante sulla complessità computazionale del problema della primalità è stato ottenuto nel 1975 da Pratt [31] . Egli ha provato che, per ogni primo p, esiste un algoritmo polinomiale che certifica la primalità, ma il determinare tale algoritmo può avere complessità

esponenziale nel numero delle cifre dell'intero, ossia complessità maggiorata da una potenza dell'intero testato.
Nel presente capitolo verranno presentati alcuni degli algoritmi di primalità più classici e verrà anche fatto un accenno a qualche nuovo sviluppo del settore che riguarda soprattutto l'impiego delle curve ellittiche.

4.1. PSEUDOPRIMALITA' E TEST DI PRIMALITA'

Nel presente paragrafo vengono esposti alcuni semplici test basati su risultati classici.

4.1.1 TEST DI FERMAT

Ricordiamo l'enunciato del ben noto piccolo teorema di Fermat già visto nel Capitolo 2 (Proposizione 2.1.2) :

Teorema 4.1.1 : *Sia p un numero primo e sia b un intero tale che (b,p)=1. Allora si ha che:*

$$b^{p-1} \equiv 1 \pmod{p} \quad (4.1.1).$$

Tale teorema fornisce solo una condizione necessaria di primalità ; infatti esistono interi n composti per cui vale $b^{n-1} \equiv 1 \pmod{n}$ per qualche b primo con n, ad esempio n=91, b=3 verificano la (4.1.1) anche se n non è primo perché $n=13 \cdot 7$ (cfr. Koblitz [17], Capitolo 5, pag.113).

Definizione 4.1.1 *Sia n dispari composto e sia* $b \in (\mathbb{Z}/n\mathbb{Z})^*$ *tale che* $b^{n-1} \equiv 1 \pmod{n}$. *Allora n si dice PSEUDOPRIMO di FERMAT in base b.*

Si noti che esistono degli interi dispari che sono pseudoprimi di Fermat in base b rispetto a tutti i $b \in (\mathbb{Z}/n\mathbb{Z})^*$; ad esempio 561 é pseudoprimo di Fermat in tutte le basi b di $(\mathbb{Z}/561\mathbb{Z})^*$ (cfr. Koblitz [17], cap 5, pag.115) . Una analisi delle proprietà di tali interi verrà esposta nel seguito del presente paragrafo quando si cercherà di valutare la risposta dell'algoritmo di Fermat (la presentazione dell'algoritmo di Fermat é fatta nell' argomento successivo al presente).
Un possibile test di primalità si può "costruire" a partire dal Teorema 4.1.1 come segue:

ALGORITMO DI FERMAT

a) prendere n in input;
b) scegliere un $b \in (\mathbb{Z}/n\mathbb{Z})^*$;
c) calcolare b^{n-1} e controllare se $b^{n-1} \equiv 1 \pmod{n}$.
d) se tale congruenza non vale allora si conclude che n è composto, se invece la congruenza vale si conclude che n è o primo o pseudoprimo di Fermat in base b.

Ovviamente un tale algoritmo non fornisce molte informazioni su n . Possiamo pensare di valutare la congruenza per diversi valori di b e poi sfruttare la seguente:

Proposizione 4.1.1: *Sia n non pseudoprimo di Fermat in base b. Allora n non è pseudoprimo di Fermat in base b per almeno la metà dei* $b \in (\mathbb{Z}/n\mathbb{Z})^*$.

Dim: Serve un fatto di banale dimostrazione :
Sia n pseudoprimo di Fermat in basi b_1 e b_2, allora n pseudoprimo di Fermat in basi $b_1 b_2$ e $b_1 (b_2)^{-1}$ (segue immediatamente dalle proprietà delle congruenze).

Sia adesso D={b∈ $(\mathbb{Z}/_{n\mathbb{Z}})^*$ t.c. n sia pseudoprimo di Fermat in base b}. Se D=Ø allora la tesi é banale; altrimenti si ha D={b_1,...,b_S}. Sia $\bar{b}$ una base per cui n non é pseudoprimo di Fermat, cioè $\bar{b}\notin$D. Per assurdo supponiamo che n sia pseudoprimo di Fermat per una base del tipo $\bar{b}b_i$; allora n é pseudoprimo di Fermat per la base $\bar{b}=\bar{b}b_i(b_i)^{-1}$ che é assurdo . Quindi n non é pseudoprimo di Fermat per ogni elemento di $\bar{b}$D. La proposizione segue allora dal fatto che gli elementi di $\bar{b}$D sono ovviamente tutti distinti.

VALUTAZIONE PROBABILISTICA DELLA RISPOSTA

Il risultato della Proposizione 4.1.1 ci permette quindi di affermare che, se ∃ b per cui n non é pseudoprimo di Fermat in base b, abbiamo almeno il 50% di probabilità che n non sia pseudoprimo di Fermat per una scelta casuale di b∈ $(\mathbb{Z}/_{n\mathbb{Z}})^*$. Possiamo allora modificare l'algoritmo precedente sostituendo al punto d) il seguente :
d') se la congruenza $b^{n-1}\equiv 1 \pmod n$ non vale, allora si conclude che n è composto; se invece la congruenza vale si torna al punto b). L'esecuzione dell'algoritmo termina quando si é provato che n é composto oppure dopo che sono state effettuate k scelte al punto b) (dove k é un intero positivo fissato a priori).

Se l'algoritmo non termina dichiarando che n é composto, si ha che n é o primo o pseudoprimo di Fermat nelle k basi testate e, quindi, la probabilità che n sia in realtà composto é minore di $\frac{1}{2^k}$ (sempre che n non abbia la speciale proprietà di verificare la congruenza (4.1.1) per ogni b∈ $(\mathbb{Z}/_{n\mathbb{Z}})^*$).
Bisogna a tal punto investigare la struttura dei numeri di Carmichael, definiti da :

Definizione 4.1.2 : U*n intero n si dice di Carmichael se é pseudoprimo di Fermat per ogni base b di* $(\mathbb{Z}/_{n\mathbb{Z}})^*$.

Presentiamo alcuni risultati sui numeri di Carmichael:

Proposizione 4.1.2: *Sia n un intero dispari composto, allora valgono :*
***a**) se n non é square-free, allora n non é un numero di Carmichael;*
***b**) se n è square-free, allora n é di Carmichael se e solo se (p-1)|(n-1) per ogni primo p tale che p|n.*

Dim: **a**) Supponiamo che $p^2|$ n . Sia g una radice primitiva modulo p^2 (cioè un generatore di $(\mathbb{Z}/_{p^2\mathbb{Z}})^*$) [1] . Sia m il prodotto di tutti i primi che dividono n e che sono diversi da p. Per il

[1] : é noto che $(\mathbb{Z}/_{p^m\mathbb{Z}})^*$ ha radici primitive, vedi Apostol [2], Capitolo 10.

Teorema Cinese dei Resti (Proposizione 2.1.3), esiste un intero b che verifica le seguenti congruenze : $b \equiv g \pmod{p^2}$ e $b \equiv 1 \pmod{m}$. Allora b é, come g, una radice primitiva modulo p^2 ed inoltre si ha (b,n)=1. Proviamo che n non é pseudoprimo rispetto a tale b. Per assurdo, se avessi $b^{n-1} \equiv 1 \pmod{n}$ avrei, poiché $p^2 | n$, $b^{n-1} \equiv 1 \pmod{p^2}$. In tal caso avrei che $p(p-1) | (n-1)$ perché $p(p-1)$ é l'ordine di b in $(\mathbb{Z}/p^2\mathbb{Z})^*$. Ma $p | n$, quindi $p \nmid (n-1)$; assurdo. Tale contraddizione prova **a**).

b) $\boxed{\Leftarrow}$ Supponiamo che $(p-1) | (n-1)$ per ogni p primo tale che $p | n$.

Sia $b \in (\mathbb{Z}/n\mathbb{Z})^*$; allora per ogni primo $p | n$ si ha che b^{n-1} é una potenza di $b^{p-1} \equiv 1 \pmod{p}$.) Quindi $b^{n-1}-1$ é diviso da tutti i fattori primi p di n ed allora si ha che $n | (b^{n-1}-1)$. Ciò prova la prima implicazione.

$\boxed{\Rightarrow}$ Supponiamo per assurdo che esista un p primo tale che $p | n$ e $(p-1) \nmid (n-1)$.

Sia g una radice primitiva di $(\mathbb{Z}/p\mathbb{Z})^*$. Sappiamo che esiste un intero b tale che $b \equiv g \pmod{p}$ e $b \equiv 1 \pmod{\frac{n}{p}}$ perché possiamo agire come già fatto nella parte **a**) .

Allora (b,n)=1 e $b^{n-1} \equiv g^{n-1} \pmod{p}$.

Ma $g^{n-1} \not\equiv 1 \pmod{p}$ perché $(p-1) \nmid (n-1)$.

Quindi si ha che $p \nmid (b^{n-1}-1)$ ed allora n non é di Carmichael. •

Proposizione 4.1.3: *Un numero di Carmichael deve essere il prodotto di almeno tre primi distinti.*

Dim: Per la Proposizione 4.1.2 sappiamo che un numero di Carmichael deve essere il prodotto di primi distinti. Investighiamo il caso n=pq con p e q primi distinti. Supponiamo che p<q ; allora, se n fosse di Carmichael, si avrebbe $n-1 \equiv 0 \pmod{(q-1)}$ (per il punto **b**) della Proposizione 4.1.2). In tal caso si ha $n-1 = p(q-1+1)-1 \equiv p-1 \pmod{(q-1)}$; ma $p-1 \not\equiv 0 \pmod{(q-1)}$ perché $0<p-1<q-1$. •

A questo punto, per poter dare maggiori informazioni sulla primalità dell'intero sottoposto al test precedente, bisogna cercare di avere delle informazioni sulla distribuzione dei numeri di Carmichael.
Nel 1984 Pomerance [27] ha provato che :

Teorema 4.1.2: *se* $C(x)=\#\{n \le x \text{ t.c. } n \text{ di Carmichael}\}$*, si ha che:*

$$C(x) \le x e^{-\left(\frac{\lg x}{\lg_2 x}\right)\left(\lg_3 x+\lg_4 x+\frac{(\lg_4 x-1)}{\lg_3 x}+O\left(\left(\frac{\lg_4 x}{\lg_3 x}\right)^2\right)\right)}$$

dove per lg_i *si intende il logaritmo iterato i volte .*

Tale risultato ci permette di osservare come, in realtà, i numeri di Carmichael siano "pochi" rispetto ai numeri primi. Infatti, ricordando che, per il Teorema dei Numeri Primi (cfr. Capitolo 3, Teorema 3.1.8), se $\pi(x)=\#\{n \le x \text{ t.c. } n \text{ primo}\}$, si ha che $\forall\ \varepsilon > 0\ \pi(x) \ge \frac{(1-\varepsilon)x}{\lg x}$ per $x > x_0(\varepsilon)$ ed allora si può valutare :

$$\frac{C(x)}{\pi(x)} \le \frac{\lg x}{1-\varepsilon} e^{-\left(\frac{\lg x}{\lg_2 x}\right)\left(\lg_3 x+\lg_4 x+\frac{(\lg_4 x-1)}{\lg_3 x}+O\left(\left(\frac{\lg_4 x}{\lg_3 x}\right)^2\right)\right)}$$

per $x>x_0(\varepsilon)$. Da ciò deriva $\lim_{x\to+\infty} \frac{C(x)}{\pi(x)} = 0$, e quindi si può affermare che la densità dei probabili primi (cioè degli interi che passano il test precedente) che sono in realtà composti diventa molto piccola al crescere di x.

Esempio: con la maggiorazione precedente si può calcolare che se $x=10^{20}$ allora $\frac{C(x)}{\pi(x)} \le 7.2\cdot10^{-5}$ e che se $x=10^{50}$ allora $\frac{C(x)}{\pi(x)} \le 5.7\cdot10^{-16}$ (cfr. Riesel [34], capitolo 4, pag. 102).

Quindi, se si cerca di provare la primalità di interi "grandi", si può trascurare l'influenza dei numeri di Carmichael . Ritornando quindi a considerare la valutazione probabilistica della primalità dell'algoritmo di Fermat, notiamo che le precedenti osservazioni ci permettono, nel caso in cui n sia o primo o pseudoprimo di Fermat nelle k basi testate, di considerare n primo con probabilità maggiore di $1-\frac{1}{2^k}$ (perché le osservazioni precedenti mi consentono di passare, con probabilità 1, da numeri di Carmichael a primi).

COMPLESSITA' DELL'ALGORITMO DI FERMAT

Per valutare la complessità dell ' algoritmo di Fermat é necessario calcolare il numero di operazioni elementari richieste per il calcolo di $b^{n-1}(\text{mod } n)$. Un metodo che consente di realizzare tale calcolo con complessità polinomiale in lgn é quello dei "quadrati ripetuti" che esponiamo nel seguito:
Siano $u_0,...,u_t$ le cifre dell'espansione binaria di n-1 .

Allora abbiamo che $b^{n-1}= b^{u_0}b^{u_1}\cdots b^{u_t}$.
Se $u_0=0$ allora si pone a=1, altrimenti si pone a=b . Dopodiché calcoliamo $b_1=b^2 \text{ (mod } n)$. Se $u_1= 1$ allora calcolo $ab_1 \text{ (mod } n)$ e tale risultato lo pongo in a, altrimenti a rimane invariato.

Al j-esimo passo ($j\le t$) calcolo $b_j=b^{2^j} \text{ (mod } n)$. Se $u_j =1$ allora calcolo $ab_j \text{ (mod } n)$ e tale risultato lo pongo in a, altrimenti a rimane invariato. Al t-esimo passo abbiamo che $a\equiv b^{n-1} \text{ (mod } n)$. Poiché ad ogni passo vengono effettuate una o due moltiplicazioni di numeri minori od uguali a n^2, si ha che ogni passo presenta una complessità $O(\lg^2(n^2))=O(\lg^2(n))$. Siccome il numero di cifre di n-1 é $O(\lg(n-1))=O(\lg n)$, si ha che la complessità di calcolo di $b^{n-1}(\text{mod } n)$ é $O(\lg^3 n)$.
Poiché il procedimento é ripetuto al più k volte, si ha che la complessità dell'algoritmo é data da $O(k(\lg^3 n))$.

Possiamo, quindi, concludere che l'algoritmo di Fermat termina in k passi, ha complessità $O(k(\lg^3 n))$ e prova che n é composto oppure che la probabilità che n sia primo é maggiore di $1-\frac{1}{2^k}$ anche se é necessario ricordarsi dell'esistenza dei numeri di Carmichael).

4.1.2. TEST DI SOLOVAY-STRASSEN.

Presentiamo un test che permette di evitare il problema dei numeri di Carmichael e che é basato sul seguente :

Teorema 4.1.3: *Sia n un intero dispari. Allora condizione necessaria e sufficiente perché n sia primo é che* $\exists\, b \in (\mathbb{Z}/n\mathbb{Z})^*$ *valga la congruenza :*

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

(dove per $\left(\frac{b}{n}\right)$ si intende il simbolo di Jacobi, cfr. Capitolo 2, Definizione 2.2.2).

Dim: cfr. Koblitz [17], pag. 46.

La proposizione seguente ci consente di provare che, per una scelta casuale di b, se n non é primo, ho almeno il 50% di probabilità che la congruenza del Teorema 4.1.3 non valga.

Proposizione 4.1.4: *Sia n un intero composto : allora la congruenza del Teorema 4.1.3 non vale per almeno la metà dei* $b \in (\mathbb{Z}/n\mathbb{Z})^*$.

Dim: E' analoga alla dimostrazione della Proposizione 4.1.1. ●

Seguendo la linea espositiva del paragrafo precedente definiamo un altro tipo di pseudoprimo:

Definizione 4.1.3: *Sia n intero composto per cui vale:*

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

per un opportuno $b \in (\mathbb{Z}/n\mathbb{Z})^*$.
Allora tale intero viene detto PSEUDOPRIMO di EULERO in base b.

Vediamo adesso, col seguente semplice Lemma, quale relazione intercorre tra pseudoprimi di Fermat e pseudoprimi di Eulero:

Lemma 4.1.1: *Sia n un pseudoprimo di Eulero in base b allora n è pseudoprimo di Fermat in base b.*

Dim: basta elevare al quadrato entrambi i membri di $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod n$. ●

Un possibile test di primalità si può "costruire" a partire dal Teorema 4.1.3 come segue:

ALGORITMO DI SOLOVAY-STRASSEN

a) prendere n in input;
b) scegliere un $b \in (\mathbb{Z}/n\mathbb{Z})^*$;
c) calcolare $b^{\frac{n-1}{2}}$ e $\left(\frac{b}{n}\right)$;
d) controllare se $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod n$;

e) se tale congruenza non vale allora si conclude che n è composto, se invece la congruenza vale si torna al punto b). L'esecuzione dell'algoritmo termina quando si é provato che n é composto oppure dopo che sono state fatte k scelte al punto b) (dove k é un intero positivo fissato a priori).

VALUTAZIONE DELLA RISPOSTA E DELLA COMPLESSITA'

Se l'algoritmo non termina dichiarando che n é composto, si ha che n o é primo o é pseudoprimo di Eulero nelle k basi testate e, quindi la probabilità che n sia primo é maggiore di $1-\frac{1}{2^k}$.

Dal punto di vista della complessità computazionale si ha che, per quanto detto nel paragrafo precedente, calcolare $b^{\frac{n-1}{2}}$ costa $O(\lg^3 n)$. Dobbiamo adesso valutare la complessità del calcolo di $\left(\frac{b}{n}\right)$. Il metodo che usiamo si basa sulla Legge di Reciprocità Quadratica Generalizzata per il simbolo di Jacobi (cfr. Capitolo 2, Proposizione 2.2.7), che afferma:
se r,s sono interi dispari, allora si ha

$$\left(\frac{r}{s}\right) = (-1)^{\left(\frac{(r-1)(s-1)}{4}\right)+\left(\frac{(\sigma(r)-1)(\sigma(s)-1)}{4}\right)}\left(\frac{s}{r}\right),$$

dove $\sigma(r)=\frac{r}{|r|}$.

Inoltre sfrutteremo il fatto che, se $r \equiv s \pmod n$, allora $\left(\frac{r}{n}\right) = \left(\frac{s}{n}\right)$.

Inoltre sappiamo calcolare $\left(\frac{2}{n}\right)=(-1)^{(n^2-1)/8}$, (per la Proposizione 2.2.5) ed allora cercheremo di ricondurci a tale ultima formula. Sia adesso $b \in (\mathbb{Z}/n\mathbb{Z})^*$. Per prima cosa isoliamo tutte le potenze di 2 in b (cioé calcoliamo f tale che $b=2^f b_1$ e b_1 dispari) e calcoliamo

$$(-1)^{f(n^2-1)/8},$$

Dopodiché, applicando la Legge di Reciprocità Generalizzata, abbiamo che :

$$\left(\frac{b_1}{n}\right) = (-1)^{\left(\frac{(b_1-1)(n-1)}{4}\right)+\left(\frac{(\sigma(b_1)-1)(\sigma(n)-1)}{4}\right)}\left(\frac{n}{b_1}\right).$$

Il calcolo dell'esponente ha complessità $O(\lg^2 n)$, mentre si ha anche che $\b\bc\((\f(n,b_1))=\left(\frac{n_1}{b_1}\right)$ con $-\frac{b_1}{2}\le n_1\le\frac{b_1}{2}$ e $n\equiv n_1 \pmod{b_1}$. Il caso peggiore si ha quando b é dispari e $b=\left[\frac{n}{2}\right]$, perché in tal caso n_1 ha modulo più grande possibile. Quindi, riapplicando la Legge di Reciprocità Quadratica Generalizzata, posso al più ogni volta dimezzare i residui, e quindi, dopo h applicazioni della reciprocità, avrò i residui $\le\frac{n}{2^h}$. Per ricondursi alla formula per $\left(\frac{2}{a}\right)$, basta prendere h=lgn. In definitiva, si eseguono lgn iterazioni di un calcolo di complessità $O(\lg^2 n)$, e quindi il calcolo di $\left(\frac{b}{n}\right)$, utilizzando la legge di reciprocità quadratica generalizzata, ha complessità $O(\lg^3 n)$.

Allora l'algoritmo di Solovay-Strassen presenta complessità $O(k(\lg^3 n))$ come l'algoritmo di Fermat precedentemente descritto.

In definitiva, possiamo affermare che l'algoritmo di Solovay-Strassen, [41], termina in k passi, ha complessità $O(k(\lg^3 n))$ e prova che n é composto oppure che la probabilità che n sia primo é maggiore di $1-\frac{1}{2^k}$.

Abbiamo quindi che, dal punto di vista della complessità e della valutazione probabilistica della risposta, gli algoritmi di Fermat e di Solovay-Strassen si equivalgono, ma il secondo si fa preferire, sia dal punto di vista teorico che dal punto di vista pratico, perché non si presenta il problema dei numeri di Carmichael.

4.1.3. ALGORITMO DI MILLER-RABIN.

L'algoritmo di Miller-Rabin si basa sulla seguente definizione (che introduce un terzo tipo di pseudoprimalità):

Definizione 4.1.4: *Sia n un intero dispari composto e si ponga $n-1=2^s t$ con t dispari. Sia $b\in(\mathbb{Z}/_n\mathbb{Z})^*$ .Allora se n e b verificano una delle due seguenti condizioni :*

i) $b^t \equiv 1 \pmod n$

ii) $\exists$ *r t.c.* $0 \le r < s$ *per cui vale* $b^{2^r t} \equiv -1 \pmod n$;

si dice che n é PSEUDOPRIMO FORTE in base b.

Tale definizione trova la propria giustificazione nel ragionamento seguente: sappiamo che, se n è primo, allora, per il piccolo Teorema di Fermat (Proposizione 2.1.2), si ha $b^{n-1}\equiv 1 \pmod n$; consideriamo adesso $b^{\frac{n-1}{2}}$. Tale numero può essere congruente solo a ±1 modulo n perché in $(\mathbb{Z}/_n\mathbb{Z})^*$ le uniche radici quadrate dell'unità sono 1 e -1 (cfr. Capitolo 2, Proposizione 2.3.1).

Se siamo nel caso in cui $b^{\frac{n-1}{2}} \equiv 1 \pmod n$ allora $b^{\frac{n-1}{4}}$ può essere congruente solo a ±1 modulo n per quanto visto sopra.

Se ripetiamo tale ragionamento per tutti i numeri del tipo:

$b^{\frac{n-1}{2^r}}$, $0<r\leq s$, notiamo che i residui possono essere o tutti 1 (caso **i**) della Definizione 4.1.4) oppure il primo residuo diverso da 1 che si ottiene é -1 (caso **ii**) della Definizione 4.1.4).

Come abbiamo già fatto in precedenza, studiamo la relazione con i precedenti tipi di pseudoprimalità:

Lemma 4.1.2: *Sia n pseudoprimo forte in base b. Allora n pseudoprimo di Eulero in base b.*

Dim: cfr. Koblitz [17], Capitolo 5, pag. 117. •

Presentiamo allora un algoritmo basato sulle osservazioni precedenti :

ALGORITMO DI MILLER-RABIN

a) prendere n in input
b) scegliere un $b\in(\mathbb{Z}/n\mathbb{Z})^*$
c) calcolare $b^t \pmod n$ (col metodo dei quadrati ripetuti) e testare se $b^t\equiv\pm1 \pmod n$. Se tale congruenza non vale, allora si esegue il punto d); altrimenti si esegue il punto b)
d) per ogni r, $0<r<s$, si calcoli $b^{2^r t} \pmod n$ e si controlli che tale numero sia congruo a -1 (mod n). Se nessuna di tali congruenze vale, allora si conclude che n é composto; altrimenti si torna al punto b).
L'esecuzione dell'algoritmo termina quando si é provato che n é composto, oppure dopo che sono state fatte k scelte al punto b) (dove k é un intero positivo fissato a priori).

VALUTAZIONE DELLA RISPOSTA E DELLA COMPLESSITA'

L'interesse del test di Miller-Rabin deriva dal fatto che la valutazione della probabilità di primalità viene migliorata, rispetto a quella degli algoritmi già presentati, grazie alla seguente :

Proposizione 4.1.5: *Sia n composto e dispari; allora n é pseudoprimo forte in base b per al più il 25% dei* $b\in(\mathbb{Z}/n\mathbb{Z})^*$.

Dim: cfr. Koblitz [17], pag. 117. •

Abbiamo quindi che, dopo k scelte casuali di basi b, (se l'algoritmo non é terminato dichiarando n composto) n può essere o primo o pseudoprimo forte nelle k basi testate. La probabilità che n sia primo é allora, in virtù della Proposizione 4.1.5, maggiore di $1-\frac{1}{4^k}$.

Passando alla valutazione della complessità computazionale si potrebbe erroneamente concludere che essa, pur essendo sempre $O(k(\lg^3 n))$, contempli una costante s volte maggiore di quella presente nell'algoritmo di Solovay-Strassen o di Fermat, perché, per ogni b, vengono effettuate s elevazioni a potenza, invece che una sola. In realtà, però, la costante non cambia perché le varie elevazioni necessarie vengono ottenute come risultati parziali del metodo dei quadrati ripetuti. Quindi basta "tener nota" di tali risultati parziali per effettuare l'algoritmo di Miller-Rabin in $O(k(\lg^3 n))$ con la stessa costante degli algoritmi precedenti.

In definitiva, si ha che l'algoritmo di Miller-Rabin termina in k passi, ha complessità $O(k(\lg^3 n))$ e prova che n é composto oppure che la probabilità che n sia primo é maggiore di $1-\frac{1}{4^k}$.

OSSERVAZIONI
Sull'algoritmo di Miller-Rabin si possono fare alcune interessanti osservazioni :

1) In pratica non é necessario scegliere un gran numero di basi b per essere "quasi sicuri" che n sia primo. Infatti é stato calcolato che (cfr. Pomerance-Selfridge-Wagstaff [30]) $\exists!$ n composto, $n<2.5\cdot 10^{10}$, (n=3215031751) che é pseudoprimo forte nelle basi 2,3,5,7.

2) se si suppone che l'ipotesi di Riemann generalizzata (cfr. Capitolo 3) sia vera, l'algoritmo di Miller-Rabin diviene deterministico, pur rimanendo a complessità polinomiale. Infatti é stato provato il seguente teorema :

Teorema 4.1.5: *Se l'Ipotesi di Riemann Generalizzata é vera ed n é un intero composto dispari, allora* $\exists b \in (\mathbb{Z}/n\mathbb{Z})^*$ *t.c.* $b<2\cdot\lg^2 n$ *per cui n non pseudoprimo forte in base b.*
Dim: Vedi Bach [4]. •

Sfuttando tale risultato, si ottiene un algoritmo polinomiale $O(\lg^5 n)$ e deterministico (basta effettuare i calcoli descritti precedentemente nell'algoritmo per tutti i $b<2\cdot\lg^2 n$).
Rimane comunque il problema costituito dal fatto che, al giorno d'oggi, l'ipotesi di Riemann generalizzata é solamente una congettura (anche se vi sono diverse evidenze calcolative favorevoli).

3) Sia l'algoritmo di Miller-Rabin che quello di Solovay-Strassen divengono deterministici se si sceglie $k=\varphi(n)$, cioé se testo le rispettive congruenze per tutti gli elementi di $(\mathbb{Z}/n\mathbb{Z})^*$. Purtroppo, però, applicando tale strategia, si ha che la complessità diviene esponenziale in lgn e quindi tali algoritmi vengono a perdere la loro caratteristica di efficienza computazionale.

4.2. ALGORITMI BASATI SULLA FATTORIZZAZIONE DI N-1

Da quanto abbiamo visto nel precedente paragrafo, non siamo in grado, a questo punto, di provare la primalità di un intero in tempo polinomiale. Il problema principale incontrato nel paragrafo precedente é l'esistenza di pseudoprimi.
Nel seguito vediamo come si può eliminare tale problema, almeno a livello teorico, mediante l'aggiunta di alcune condizioni sulla struttura di n-1. Si ha però, come conseguenza, che il funzionamento degli algoritmi derivati da tali teoremi é efficiente solo per interi n con la proprietà di avere n-1 uguale al prodotto di piccoli primi conosciuti a priori, mentre gli algoritmi del paragrafo precedente hanno la caratteristica di funzionare in modo indipendente dalla "forma" di n. Se la fattorizzazione di n-1 non é conosciuta a priori, allora bisogna risolvere il problema di fattorizzare n-1. Poiché la fattorizzazione di interi é un problema molto più "difficile" della primalità (cfr. Bazzanella [5]), non é quindi conveniente utilizzare questo tipo di algoritmi per provare la primalità di interi n di cui non si conosce a priori la fattorizzazione di n-1.
Ad esempio, gli algoritmi seguenti possono essere usati per cercare di stabilire un record di grandezza per i numeri primi testando i numeri di Fermat che hanno la forma : $2^{2^k}+1$.

Inoltre, dal punto di vista delle applicazioni alla crittografia, non é molto utile avere dei primi grossi ma dalla forma speciale, perché il ruolo di chi cerca di "rompere" il codice risulta facilitato (poiché conosce già la struttura dei divisori dell'intero che cerca di fattorizzare).

Presentiamo adesso dei risultati classici che "tentano" di costruire un "viceversa" del piccolo teorema di Fermat, che sappiamo essere falso.

Teorema 4.2.1: (LEHMER) *Sia* $n-1=\prod_{j=1..s} q_j^{\beta_j}$ *con* q_j *primi distinti.*

Se $\exists$ *a intero t.c. valgano :*
i) $a^{(n-1)/q_j} \not\equiv 1 \pmod n \quad \forall j=1..s$ *e*
ii) $a^{n-1} \equiv 1 \pmod n$
allora n é primo.

Dim: Notiamo che ii) implica che (a,n)=1. Sia d=ord $_{(\mathbb{Z}/n\mathbb{Z})^*}$(a). Da ii) abbiamo che d|(n-1). Supponiamo che d<n-1. Poiché ogni divisore proprio di n-1 divide almeno uno dei $(n-1)/q_j$, si ha allora che almeno uno dei $a^{(n-1)/q_j}\equiv 1$ (mod n) in contraddizione con la i). Allora si ha d=n-1. Dal teorema di Eulero-Fermat [(2)] , abbiamo anche che d|φ(n) (dove φ(n) é la funzione di Eulero, cfr. Capitolo 3), ovvero (n-1)| φ(n) da cui si ha φ(n)=n-1, cioé n primo. •

A commento del precedente teorema, osserviamo che le condizioni i) e ii) sono equivalenti ad affermare che a é elemento di $(\mathbb{Z}/n\mathbb{Z})^*$ di ordine n-1 e quindi a dire che n è primo.

---

(2) : **Teorema di Eulero-Fermat :**

Sia n intero positivo e sia $a\in(\mathbb{Z}/n\mathbb{Z})^*$. *Allora* $a^{\varphi(n)} \equiv 1 \pmod n$.

Dim: cfr. Koblitz [17], Capitolo 1, Proposizione 1.3.5. •

ALGORITMO DI LEHMER

L'idea base su cui si basa l'algoritmo di Lehmer é quella di cercare di determinare un elemento a di $(\mathbb{Z}/n\mathbb{Z})^*$ di ordine n-1.
Una descrizione dell'algoritmo é la seguente:

a) dato in input n e la fattorizzazione di n-1 (i fattori primi di n-1 siano dati in ordine crescente $q_1<...<q_s$).
b) scegliere casualmente a in $(\mathbb{Z}/n\mathbb{Z})^*$
c) per ogni j=1,...,s calcolare $a^{(n-1)/q_j}$ e testare la congruenza $a^{(n-1)/q_j} \not\equiv 1 \pmod n$. Se almeno una di tali congruenze non é verificata si torna al punto b), altrimenti si controlla se vale $a^{n-1} \equiv 1 \pmod n$. Se tale ultima congruenza é vera, allora n é primo; altrimenti si ritorna al punto b).

ANALISI DELL'ALGORITMO

Per prima cosa, osserviamo che, al contrario degli algoritmi del paragrafo precedente, se forziamo la terminazione dell'algoritmo di Lehmer dopo k scelte random di a (senza essere riusciti a provare che n é primo), non siamo in grado di dare nessun tipo di valutazione della probabilità che n sia primo.
Quello che possiamo fare é solo supporre che n sia primo e valutare con quale probabilità l'algoritmo termina in T passi, provando la primalità di n.

Per fare ciò ci sevono alcune osservazioni riguardanti il numero degli elementi di ordine n-1 in $(\mathbb{Z}/n\mathbb{Z})^*$, con n primo (cioé il numero dei generatori di $(\mathbb{Z}/n\mathbb{Z})^*$).

Osservazione:

a) Notiamo che, poiché $\exists\ \varphi(n-1)$ generatori di $(\mathbb{Z}/n\mathbb{Z})^*$ (cfr. Koblitz [17], Capitolo 2, Proposizione 2.1.2) e $\varphi(n-1)=(n-1)\prod_{j=1..s}(1-\frac{1}{q_j})$ (per la moltiplicatività di φ, cfr. Capitolo 3), quanto più piccoli sono i divisori di n-1, tanto più piccolo é il numero dei generatori.

b) Inoltre osserviamo che la densità dell'insieme costituito dagli $a\in(\mathbb{Z}/n\mathbb{Z})^*$ tali che $a^{(n-1)/q_j}\equiv 1 \pmod n$ é $\frac{1}{q_j}$.

Infatti sia $A_j=\left\{ a\in(\mathbb{Z}/n\mathbb{Z})^* \text{ tali che } a^{(n-1)/q_j}\equiv 1 \pmod n \right\}$ e sia g un generatore modulo n .

Allora $\forall\ a\in A_j$ si ha che $\exists$ i tale che $2\le i\le n-1$ e $g^i=a$. Quindi $a^{(n-1)/q_j} = g^{i(n-1)/q_j}\equiv 1 \pmod n$, allora $(n-1)\mid i(\frac{(n-1)}{q_j})$ e quindi $q_j\mid i$. Notiamo che se $q_j\mid i$ allora $a=g^i\in A_j$.

Quindi $\#A_j = \#\{\text{i t.c. } 2\le i\le n-1 \text{ e } q_j\mid i\}=\frac{(n-1)}{q_j}$ ed allora la densità cercata é data da $\frac{1}{q_j}$.

Le osservazioni precedenti ci consentono dunque di affermare che é conveniente testare la congruenza in questione a partire dal divisore minore perché, in tale modo, ho probabilità maggiore di fallire al primo calcolo. L'algoritmo di Lehmer quindi si comporta in modo da minimizzare il più possibile la propria complessità.
A tal punto valutiamo la probabilità che l'algoritmo termini con successo dopo T scelte di a.
Partiamo dal considerare la probabilità che il primo "a" scelto abbia ordine n-1:
per quanto detto sopra tale probabilità é data da $\varphi(n-1)/n-1$.
La probabilità di avere successo al secondo tentativo é allora data da : $(\varphi(n-1)/n-2)$.
Allora la probabilità che si abbia un successo al T-esimo tentativo ($T \geq 1$)é data da:
$(\varphi(n-1)/n-T)$. (4.2.1)

Osserviamo però che tale algoritmo può non terminare perché non abbiamo nessuna condizione che ci assicuri di ottenere il risultato desiderato dopo un certo numero T , $T<n-\varphi(n-1)$,di scelte random di a (cfr. Riesel [34], pag. 106 e Koblitz [17], Capitolo 2, Proposizione 2.1.3). Nel caso in cui $T=n-\varphi(n-1)$ abbiamo che sicuramente l'elemento scelto ha ordine n-1. Come per gli algoritmi del paragrafo precedente, tale caso non é molto interessante perché la complessità, come si vede nell'immediato seguito, diviene esponenziale in lgn.
Dal punto di vista della complessità computazionale, abbiamo che, se l'algoritmo di Lehmer termina in T passi e per ogni scelta di a vengono eseguite s+1 elevazioni a potenza (caso peggiore), essa é data da $O(T(s+1)\lg^3 n)$.
In conclusione, abbiamo che l'algoritmo di Lehmer é probabilistico (nel senso che può non terminare anche se n é primo) e notiamo anche che, se n composto, sicuramente non termina. Inoltre la probabilità di terminare in T passi é data dalla formula (4.2.1), e se l'algoritmo termina in T passi la complessità computazionale é $O(T(s+1)\lg^3 n)$.

OSSERVAZIONE

Per cercare di migliorare un poco la situazione, si può cercare di indebolire l'ipotesi relativa alla completa fattorizzazione di n-1, sostituendola con una che contempli solo una parziale fattorizzazione di n-1.

Teorema 4.2.2: (Lehmer-Pocklington)
Sia $n-1=R\cdot F=R\cdot \prod_{j=1..s} q_j^{\beta_j}$ *con* q_j *primi distinti e* $(R,F)=1$.
Se $\exists$ *a intero t.c. valgano :*
i) $(a^{(n-1)/q_j}-1,n)=1 \ \forall j=1..s$ *e*
ii) $a^{n-1} \equiv 1 \pmod n$
allora ogni fattore primo p di n ha la forma $p=Fm+1$ *e se inoltre* $F>\sqrt{n}$ *si ha che n é primo.*

Dim: Sia p|n, p primo. Poniamo $b=a^R$ ed allora $b^F \equiv 1 \pmod n$ e quindi $b^F \equiv 1 \pmod p$. Però abbiamo anche che $b^{F/q_j} \not\equiv 1 \pmod p$ $\forall j=1..s$ e quindi ord (b)=F. Per il Piccolo Teorema di Fermat si ha allora che F |(p-1) e quindi $\exists$ m intero t.c. p=Fm+1 . Supponiamo adesso che $F > \sqrt{n}$. In tal caso ho $\sqrt{n} < F < p$ e quindi n primo.

L'algoritmo che deriva dal Teorema 4.2.2 é analogo al precedente, solo che può essere applicato anche ad interi di cui si conosce una fattorizzazione parziale anziché completa. Alla luce degli

ultimi risultati sulle curve ellittiche (vedi paragrafo seguente), assume però un ruolo più importante perché risulta essere, in una versione adattata al nuovo contesto, il teorema base su cui costruire degli algoritmi.

4.3. PRIMALITA' CON CURVE ELLITTICHE.

Il principale vantaggio che si ottiene dall'uso delle curve ellittiche su campi finiti, sia negli algoritmi di primalità che in quelli di fattorizzazione (cfr. Bazzanella [5]), é che é possibile variare il gruppo di punti su cui si lavora finché non si riesce a determinarne uno la cui cardinalità sia facilmente fattorizzabile. Nell'impostazione più classica, fin qui adottata, si lavora solo su $(\mathbb{Z}/_{n\mathbb{Z}})^*$ e quindi non é evidentemente possibile variare la cardinalità. Presentiamo nel seguito un algoritmo di primalità probabilistico (nel senso che può non terminare).

4.3.1 Generalita' sulle curve ellittiche definite su campi finiti:

Dobbiamo quindi dare una veloce presentazione delle curve ellittiche definite su campi finiti e dei metodi utili a calcolare la somma di due punti della curva e per calcolare i multipli di un punto della curva stessa.

Dato un campo finito F_r, r intero positivo, $char(F_r)\neq 2,3$, definiamo :

Definizione 4.3.1: *Dicesi CURVA ELLITTICA $E(F_r)$ l'insieme dei punti $(x:y:z)\in\mathbb{P}^2(F_r)$ tali che verificano l'equazione $y^2z=x^3+Axz^2+Bz^3$, dove $A,B\in F_r$ e verificano $4A^3+27B^2\neq 0$ (condizione di non singolarità della curva).*

Passiamo adesso a definire la legge di somma di due punti. Tale legge viene data in modo da avere il punto O=(0:1:0) come elemento neutro del gruppo costituito da $(E(F_r),+)$.

Definizione 4.3.2:

Dati due punti $L=(x_1:y_1:z_1)$, $M=(x_2:y_2:z_2)\in E(F_r)$, entrambi diversi da O, (cioè $z_1=1=z_2$), indicato $L+M=(x_3:y_3:z_3)$, abbiamo tre casi distinti:

i) Se $(x_1=x_2)$ e $(y_1=-y_2)$ allora $L+M=O$ (cioé $z_3=0$);

ii) Se $(x_1=x_2)$ e $(y_1=y_2)$ allora si pone $\lambda = \dfrac{3x_1^2+A}{2y_1}$;

iii) Se $(x_1\neq x_2)$ allora si pone $\lambda = \dfrac{y_2-y_1}{x_2-x_1}$;

Posto $\beta=y_1-\lambda x_1$ si definisce $L+M=(\lambda^2-x_2-x_1: -(\lambda x_3+\beta):1)$.

Nel caso in cui uno dei due addendi sia uguale ad O, ad es. L=O, si definisce L+M=M.

Si noti anche che, in conseguenza della definizione adottata, si ottiene:

- l'inverso di O é O stesso;
- l'inverso di L=(x:y:z), L≠O, è -L:=(x,-y,z).

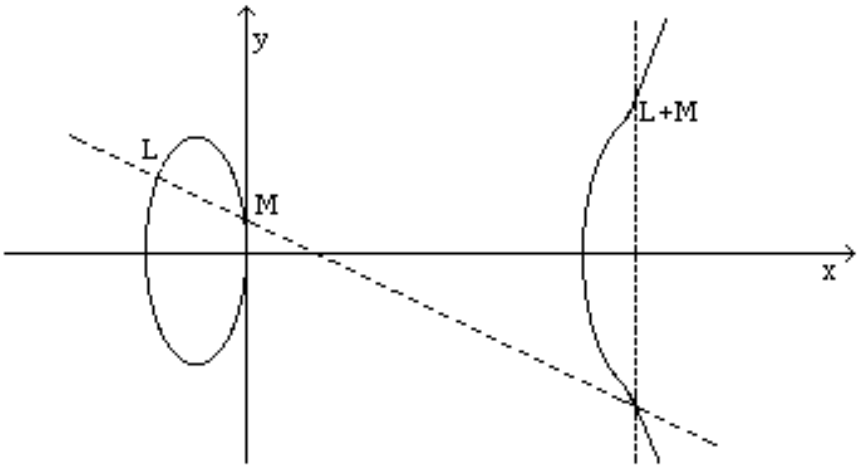
Al fine di poter dare una idea intuitiva del processo di somma, osserviamo che, nel caso di avere una curva ellittica sui reali la casistica della Definizione 4.3.2 può essere descritta come segue:

Dati due punti L, M∈E(ℝ), entrambi diversi da O, prendiamo la retta che li congiunge, oppure la retta tangente se L=M, e abbiamo che :

$$L+M=\begin{cases} O & \text{se la retta è vericale} \\ Q & \text{altrimenti} \end{cases}$$

dove Q é il riflesso rispetto all'asse x del punto ottenuto mediante intersezione tra la retta scelta e la curva ellittica.

Esempio:



curva ellittica $y^2 = x^3 \cdot x$

Diamo adesso un algoritmo che realizza quanto detto sopra:

Algoritmo di somma:

1) Sia $L=(x_1:y_1:z_1)$, $M=(x_2:y_2:z_2)$, $L+M=(x_3:y_3:z_3)$;
2) Se $(z_1=0)$ allora $x_3=x_2, y_3=y_2, z_3=z_2$ (cioé L+M=M);
3) Se $(z_2=0)$ allora $x_3=x_1, y_3=y_1, z_3=z_1$ (cioé L+M=L);
4) Se $(x_1=x_2)$ e $(y_1=-y_2)$ allora L+M=O (cioé $z_3=0$);
5) Se $(x_1\neq x_2)$ allora si pone $\lambda=\dfrac{3x_1^2+A}{2y_1}$,

altrimenti si pone $\lambda=\dfrac{y_2-y_1}{x_2-x_1}$;

6) Sia $\beta=y_1-\lambda x_1$, $x_3=\lambda^2-x_2-x_1$, $y_3=-(\lambda x_3+\beta)$, $z_3=1$.

Tale algoritmo, la cui complessità é $O(lg^2 r)$, fornisce la somma di due punti di una curva ellittica definita su un campo di caratteristica $k\neq 2,3$ (in questi casi si può comunque generalizzare l'algoritmo (cfr. H.W.Lenstra [21])) .

Passiamo adesso ad esaminare il problema di determinare il multiplo di un punto di una curva ellittica.

Definizione 4.3.3: *Sia q intero, $q\geq 0$, $M\in E(F_r)$ allora definiamo :*

$$\begin{cases} 0M = O \\ qM = (q-1)M + M \quad (q \text{ dispari}). \\ qM = \frac{q}{2}M + \frac{q}{2}M \quad (q \text{ pari}) \end{cases}$$

Da ciò si ricava un algoritmo analogo all'algoritmo dei quadrati ripetuti presentato nel calcolo della complessità dell'algoritmo di Fermat.
Abbiamo quindi una complessità di $O(\lg r)$ addizioni in $E(F_r)$, cioé $O(lg^3 r)$ perchè una somma in $E(F_r)$ ha complessità $O(lg^2 r)$.

In molti casi, come vedremo in seguito nell'algoritmo presentato al punto 3.3, si deve però lavorare su anelli anzichè su campi finiti. La definizione di curva ellittica, di somma e di multiplo di un punto (questo problema é importante in quei casi in cui la somma in E(A), A anello, non è associativa come, ad esempio, in $E(\mathbb{Z}/n\mathbb{Z})$, con n composto) viene allora data in modo analogo a quanto presentato in precedenza, ma deve però prestare attenzione all'esistenza degli elementi inversi coinvolti nel calcolo. Ad esempio in $(\mathbb{Z}/n\mathbb{Z})$, dove n composto, bisogna avere l'esistenza di $(2y_1)^{-1}$ oppure di $(x_2-x_1)^{-1}$. Ciò può essere controllato facilmente in $(\mathbb{Z}/n\mathbb{Z})$ utilizzando un algoritmo di massimo comun divisore esteso (cfr. Schoof [38], pag. 53). E' comunque possibile generalizzare gli algoritmi precedentemente descritti in modo da lavorare anche su curve definite su anelli (cfr. H.W.Lenstra [21]).

Passiamo adesso ad esaminare alcune caratteristiche fondamentali di $E(F_r)$.
Il punto fondamentale su cui si basano tutti gli algoritmi di primalità che utilizzano le curve ellittiche é il calcolo della cardinalità del gruppo di punti di una curva ellittica $E(F_r)$.

Il risultato fondamentale per il calcolo di $\#(E(F_r))$ con F_r campo finito é il seguente:

Teorema 4.3.1 : (Hasse) *Sia $E(F_r)$ una curva ellittica definita su F_r e sia $char(F_r)\neq 2,3$. Allora si ha che $\#(E(F_r))=r+1-t$; $|t|\leq 2\sqrt{r}$, con t che dipende dalla particolare curva.*

Dim. cfr. Silverman [40], pag. 131. ●

Inoltre si può notare che, se n é composto, per calcolare $\#(E(\mathbb{Z}/n\mathbb{Z}))$ basta, almeno teoricamente, saper calcolare $\#(E(F_r))$ con F_r campo finito, perché si può dimostrare (Lenstra [21]) che :

$$\frac{\#(E(\mathbb{Z}/n\mathbb{Z}))}{n} = \prod_{\substack{p \mid n \\ p \text{ primo}}} \frac{\#(E(F_p))}{p} \quad .$$

Ciò sembra risolvere il problema di calcolare $\#(E(\mathbb{Z}/n\mathbb{Z}))$, però, ovviamente, per sfruttare la formula precedente bisogna conoscere già la fattorizzazione di n, e quindi avere a priori conoscenza delle informazioni che stiamo, invece, ricercando.

Seguiremo quindi un approccio diverso al problema e quindi cercheremo di calcolare algoritmicamente $\#(E(F_r))$.

4.3.2 ALGORITMI PER IL CALCOLO DI $\#(E(F_r))$

Supponiamo di essere sempre nel caso in cui F_r sia un campo finito: allora il problema di calcolare $\#(E(F_r))$ si riduce a determinare t, per il Teorema 4.3.1 (di Hasse).
Esistono diversi algoritmi (cfr. Lenstra [21]) che realizzano tale calcolo, ma quello che presentiamo é il migliore attualmente conosciuto ed é stato sviluppato da Schoof. Le sue caratteristiche principali sono quelle di essere deterministico e polinomiale, anche se, all'atto pratico, risulta di difficile implementazione.

L'algoritmo di Schoof sfrutta alcune proprietà degli endomorfismi di campi finiti che elenchiamo nel seguito:

1) Sia K la chiusura algebrica di F_r e sia $\Phi : E(K) \rightarrow E(K)$ l'endomorfismo (di Frobenius) di gruppi definito da $\Phi(x:y:z)=(x^r:y^r:z^r)$.
Si noti che, poiché vale che $E(F_r) = \{P \in E(K) \text{ t.c. } \Phi(P)=P\}$ (perché l'endomorfismo di Frobenius genera il gruppo di Galois $Gal(K/F_r)$, cfr. Silverman [40], pag. 131), allora $E(F_r)$ é sottogruppo di E(K) .

2) Sfrutteremo nell'algoritmo una proprietà base di tale endomorfismo: $\Phi^2 - t\Phi + r = 0$ in End(E(K)). (dipende dal fatto che il polinomio caratteristico di Φ é dato da $\det(X-\Phi)=X^2-tX+r$ e quindi $0=\det(\Phi-\Phi)=\Phi^2-t\Phi+r$ (cfr. Silverman [40], pag. 135)).

3) Osserviamo inoltre che, per calcolare t, basta conoscere i valori di t (mod q) per ogni q primo dispari minore od uguale di un opportuno L (in tal caso L deve essere scelto in modo che si abbia sia $q \neq \text{char}(F_r)$ sia $\prod_{q \leq L} q > 4\sqrt{r}$). Infatti, se si conoscono tutti i t (mod q), allora, applicando il Teorema Cinese dei Resti, si può determinare t (mod $(\prod_{q \leq L} q)$). Però, per il Teorema di Hasse, la conoscenza di t (mod $(\prod_{q \leq L} q)$) é equivalente a conoscere t e quindi a poter calcolare $\#(E(F_r))$.

4) Sia $\Psi_q(X) = q \prod_{x \in H}(X-x)$ dove si ha :

$$H=\{ u \in K \text{ t.c. } \exists v \in K \text{ per cui } (u:v:1) \in E(K) \text{ e ha ordine } q \}.$$

Si noti che l'insieme sopra descritto é non vuoto perché l'insieme dei punti di ordine q di una curva ellittica é, in questo caso, isomorfo a $(\mathbb{Z}/_q\mathbb{Z})x(\mathbb{Z}/_q\mathbb{Z})$ (cfr. Silverman [40], pag. 89). E' possibile anche dare una definizione induttiva di $\Psi_q(X)$ (cfr. Lang [18], pag. 33). Tali polinomi hanno la proprietà di annullarsi solo nei punti di ordine q e permettono di calcolare qP, $\forall P \in E(\mathbb{Z}/_n\mathbb{Z})$. In pratica tali polinomi, detti "polinomi divisori", verranno calcolati tutti, mediante la definizione induttiva, in una precomputazione e ci serviranno per calcolare t (mod q). Si prova, a partire dalla definizione induttiva, che (cfr. Lang [18], Schoof [37]) grado($\Psi_q(X)$)=$(q^2-1)/2$ e che $\Psi_q(X) \in F_r[X]$.

ALGORITMO DI SCHOOF:

a) Per ogni q primo, q≤L, si consideri :
l'anello $T=F_r[X,Y]/(\Psi_q(X),Y^2-X^3+aX-b)$ in cui ogni elemento ha rappresentazione unica data da :

$$\sum_{i=0}^{(q^2-3)/2} \sum_{j=0..1} a_{ij} \bar{X}^i \bar{Y}^j$$

con $a_{ij} \in F_r$ e $\bar{X},\bar{Y}$ che sono l'immagine di X,Y in T secondo la proiezione canonica.

A tal punto consideriamo $Q=(\bar{X}:\bar{Y}:1) \in E(T)$ e definiamo l'applicazione (che é in realtà un omomorfismo) :

$$\sigma: E(T) \rightarrow E(T) \text{ t.c. } \sigma(x:y:z)=(x^r:y^r:z^r).$$

Se si riesce a provare che Q e $\sigma(Q)$ hanno ordine q e che $\sigma^2-t\sigma+r=0$ in End(E(T)), allora abbiamo che t (mod q) é caratterizzato in modo ovvio dall'equazione $\sigma^2(Q)+rQ=t\sigma(Q)$.
Il metodo più banale per calcolare t (mod q) é allora quello di calcolare $\sigma^2(Q)+rQ$ e confrontarlo poi con $0 \cdot s(Q)$, $1 \cdot s(Q)$,... finché non si realizza una uguaglianza.

Nota: I calcoli su E(T) vanno eseguiti tenendo presente che T é a priori un anello e, quindi, bisogna usare la legge di addizione per punti di una curva ellittica definita su anelli.

b) Applichiamo il Teorema Cinese dei Resti per calcolare t.

GIUSTIFICAZIONE DELL'ALGORITMO DI SCHOOF

Proviamo le proprietà di Q e σ indicate in precedenza.
Sia $V=\{ P \in E(K) \text{ t.c. } ord(P)=q \}$ e sia $P=(x_p:y_p:1) \in V$. Abbiamo allora che $\exists!$ un omomorfismo di anelli $T \rightarrow K$ (lineare su F_r) tale che l'immagine di $\bar{X},\bar{Y}$ sia x_p,y_p. Si costruisce allora automaticamente un omomorfismo di anelli $T \rightarrow \prod_{P \in V} K$, di cui si può facilmente verificare l'iniettività (dipende dall'unicità dell'omomorfismo precedente).

A tal punto si può considerare E(T) come sottogruppo di $\prod_{P\in V} E(K)$. Da ciò discende immediatamente che l'ordine di Q é q (perché Q corrisponde a $(P)_{P\in V}$) e che $\sigma^2-t\sigma+r=0$ (perché σ non é altro che la restrizione a E(T) dell'automorfismo di $\prod_{P\in V} E(K)$ in cui ogni coordinata é data da Φ). Inoltre σ é chiaramente iniettiva (restrizione di una applicazione iniettiva) e quindi σ(Q) ha ordine q.

VALUTAZIONE DELLA COMPLESSITA' DELL'ALGORITMO DI SCHOOF

Per quanto riguarda la complessità computazionale, é importante valutare quanto é "grande" L. Per fare ciò ci si basa sul Teorema dei Numeri Primi (cfr. Capitolo 3), da cui discende l'esistenza di una costante calcolabile e positiva c per cui si ha $\prod_{q\le L} q > c\cdot e^L$, con q primo, $q\neq 2,p$.

Se si considera L=O(lgr), si ha la maggiorazione richiesta nell'algoritmo ed, inoltre, si ha che anche tutti gli q, che intervengono nel precedente prodotto, sono O(lgr)).
Si osserva anche che tutti i calcoli eseguiti in F_r possono essere svolti considerando un polinomio irriducibile f di grado uguale a $[F_r:F_p]$, con p primo, p≤r, e considerando gli elementi di F_r come elementi del quoziente $F_p[X]/(f)$.
Inoltre si ha che il calcolo di $\sigma^2(Q)+rQ=t\sigma(Q)$ costa $O(lg^7r)$ (viene eseguito tramite un massimo comun divisore di polinomi che ha complessità, se i due polinomi hanno grado ≤ d, $O(d^2lg^3r)$),e quindi tutto l'algoritmo ha complessità $O(lg^8r)$.

Tale argomentazione conclude la descrizione dell'algoritmo di Schoof.

4.3.3 TEST DI PRIMALITÀ DI GOLDWASSER-KILIAN:

L'algoritmo di Schoof appena esposto viene usato nel seguito in un test di primalità che sfrutta il seguente :

Teorema 4.3.2: (Pocklington "ellittico")
Sia $n\in\mathbb{Z}$ tale che (n,6)=1, $E(\mathbb{Z}/n\mathbb{Z})$ una curva ellittica su $(\mathbb{Z}/n\mathbb{Z})$ e $m,s\in\mathbb{Z}$, m,s>0 ed s|m.
Sia $P\in E(\mathbb{Z}/n\mathbb{Z})$ verificante:

1) mP=O ;

2) $\exists$ q primo, q|s, se $\frac{m}{q}P=(x_q:y_q:z_q)$, si abbia $(z_q,n)=1$.

Allora $\exists$ p primo, p|n, si ha $\#(E(\mathbb{Z}/p\mathbb{Z}))\equiv 0 \pmod s$ ed inoltre, se $s>(\sqrt[4]{n}+1)^2$, si ha che n é primo.

Dim: Sia p un divisore primo di n e sia $Q=(m/s)P \in E(\mathbb{Z}/n\mathbb{Z})$. Con Q_p denotiamo l'immagine di Q in $E(\mathbb{Z}/p\mathbb{Z})$. Notiamo che, dall'ipotesi mP=O, si ha che sQ=O e quindi $ord(Q_p)|s$.
Consideriamo adesso q divisore primo di s e valutiamo $(s/q)Q_p= (x_q \bmod p: y_q \bmod p: z_q \bmod p)$ che non può essere O perché, per ipotesi $p\nmid z_q$. Quindi l'ordine di Q_p non é un divisore di s/q per ogni q che divide s ed allora l'ordine di Q_p deve essere s stesso . A tal punto possiamo concludere che $s|\#(E(\mathbb{Z}/p\mathbb{Z}))$. Ciò prova la prima parte della tesi. Se inoltre vale $s>(\sqrt[4]{n}+1)^2$ allora, poiché per il Teorema di Hasse si ha $\#(E(\mathbb{Z}/p\mathbb{Z})) \le(\sqrt{p}+1)^2$, si ha $p >\sqrt{n}$ e quindi n primo. ●

A tal punto siamo in grado di "costruire" un algoritmo di primalità basato sul Teorema 4.3.2 e sull'algoritmo di Schoof.
Tale algoritmo è stato sviluppato nel 1986 da Goldwasser e Kilian [13].

Descrizione dell'algoritmo di Goldwasser-Kilian:

Diamo adesso una descrizione schematica dell'algoritmo di Goldwasser-Kilian. Nel seguito si considererà sempre s=q e supponiamo che n sia un intero positivo dispari.
a) selezioniamo una curva ellittica su $(\mathbb{Z}/n\mathbb{Z})$ e un intero m positivo tale che verifichi:

i) $m<(\sqrt{n}+1)^2$ e, se n è primo, $\#(E(\mathbb{Z}/n\mathbb{Z}))=m$;

ii) $\exists\ q>(\sqrt[4]{n}+1)^2$ tale che $m=2\cdot q$ e che q é "probabilmente primo".

Un metodo per fare ciò é il seguente:

1) si scelgono due interi random $a,b\in(\mathbb{Z}/n\mathbb{Z})$ in modo che $4a^3+27b^2\neq 0$ (é la condizione che la curva ellittica sia non singolare). Ciò accade con probabilità $1-\frac{1}{n}$ (se n é veramente primo). Si controlla poi che $(n,4a^3+27b^2)=1$ (é vero se n é realmente primo). Nel caso che almeno una di tali condizioni non sia verificata, si riesegue il punto 1).

Si usa poi l'algoritmo di Schoof per calcolare m. Se l'algoritmo di Schoof non termina in tempo polinomiale in lgn, allora n composto e l'algoritmo di Goldwasser-Kilian termina.
Se accade che $m \geq (\sqrt{n}+1)^2$, allora si riesegue il punto 1).

L'ultima affermazione riguardante la terminazione dell'algoritmo di Schoof può sembrare in contrasto col fatto che é un algoritmo deterministico, ma, in realtà nell'algoritmo di Goldwasser-Kilian, non si é certi che $(\mathbb{Z}/_{n\mathbb{Z}})$ sia un campo finito e quindi, sebbene i calcoli dell'algoritmo di Schoof possano essere eseguiti ugualmente, non é detto che l'algoritmo riesca a terminare e quindi a fornire la cardinalità del gruppo di punti della curva.

2) Dopo aver verificato i) si divide m per 2 e si controlla se q é probabilmente primo (ad esempio si può attivare ricorsivamente lo stesso algoritmo su q). Se m non é divisibile per 2 o se q risulta essere composto, si riesegue il punto 1).

Nota : altri algoritmi di primalità (ad esempio il test di Atkin, cfr. Lenstra [21]) sostituiscono la ii) con una condizione più generale :
ii') $\exists$ k>1, $q > (\sqrt[4]{n}+1)^2$ tale che $m=k \cdot q$ e che q é "probabilmente primo".
A tal punto, per verificare ii') si può sottoporre m ad un algoritmo di fattorizzazione che sia efficiente per determinare piccoli fattori primi; porre k uguale al prodotto di tali fattori e poi porre $q=\frac{m}{k}$. Inoltre l'algoritmo di Atkin (cfr. Lenstra [21]) si differenzia da quello qui presentato, sebbene mantenga la stessa struttura, perché utilizza curve ellittiche di tipo "speciale" (cioé curve ellittiche in cui a=0 oppure b=0 e definite sfruttando particolari proprietà di $\mathbb{Q}(\sqrt{\delta})$ con δ = discriminante di campi quadratici immaginari).

b) Supponiamo di aver terminato con successo il punto **a**) e quindi di avere E,m,q. Si sceglie allora un punto random P in $E(\mathbb{Z}/_{n\mathbb{Z}})$ e lo indichiamo $(x_p:y_p:1)$. Un metodo per fare ciò é quello di selezionare x random in $(\mathbb{Z}/_{n\mathbb{Z}})$ finchè non si ha che x^3+ax+b é un quadrato in $(\mathbb{Z}/_{n\mathbb{Z}})$. Ricordiamo che, se n è primo, x^3+ax+b é un quadrato in $(\mathbb{Z}/_{n\mathbb{Z}})$ se e solo se $\left(\frac{x^3+ax+b}{n}\right)=1$ (simbolo di Jacobi). A tal punto si usa un algoritmo per il calcolo di y t.c. $y^2=x^3+ax+b$. (Ad esempio si può usare l'algoritmo di calcolo di radici quadrate modulo n presentato nel Koblitz [17], Capitolo 2, §2, pag. 47-49. E' un algoritmo polinomiale $O(lg^4 n)$ se si conosce un nonresiduo quadratico (cioé un $v \in (\mathbb{Z}/_{n\mathbb{Z}})$ t.c. $\left(\frac{v}{n}\right)=-1$). Si noti che, se non si assume la validità dell'Ipotesi di Riemann, non si conosce un algoritmo che permette di determinare un nonresiduo quadratico modulo n in tempo polinomiale) .

Si calcoli adesso Q=2P e si controlli se $Q \neq O$ (si può provare che ciò é vero per più della metà dei P se n é veramente primo: dipende dal fatto che tutti e soli i punti di ordine 2 sono quelli per cui y=0 (cfr. Pomerance [29], pag. 318).
Se Q=O allora si ritorna al punto **a**) finché non se ne determina uno per cui $Q \neq O$. A tal punto si controlla se qQ=O (come deve essere se n è primo). Si noti che la condizione (z,n)=1 (indicando Q=(x:y:z)) é equivalente alla condizione $Q \neq O$.

c) Tale passo consiste nel provare che q é primo. Può essere fatto o con una applicazione ricorsiva dell'algoritmo oppure, se q é abbastanza piccolo, utilizzando un metodo più diretto (ad esempio uno di quelli presentati in precedenza).

Si noti che la lunghezza della ricorsione é O(lgn) perché $q<\frac{1}{2}(\sqrt{n}+1)^2$.

Se **a**),**b**),**c**) sono stati portati a termine con successo allora si ha la prova che n é primo, perché si é riusciti a determinare una curva ellittica e un punto P di tale curva che verificano le ipotesi del Teorema 4.3.2, e perché $q>(\sqrt[4]{n}+1)^2$.

COMPLESSITA' COMPUTAZIONALE DI GOLDWASSER-KILIAN

La valutazione precisa della complessità computazionale dell'algoritmo risulta essere un problema piuttosto complesso che richiede l'utilizzo di metodi di Teoria Analitica dei Numeri. Il problema é riuscire a valutare quante prove bisogna fare per riuscire a verificare i) e ii) del punto **a**). Purtroppo,però,tale problema é collegato alla distribuzione dei primi nell'intervallo $(n-\sqrt{n},n+\sqrt{n})$. Fino ad oggi non si é riusciti a provare che tale distribuzione é regolare (cioé 1/lgn). Esistono però due risultati che ci consentono di dare una stima della complessità di tale algoritmo:

Teorema 4.3.3: *Supponiamo che esistamo due costanti positive c_1,c_2 tali che per tutti i numeri reali $x\geq 2$ si abbia che il numero dei primi p nell'intervallo $[x,x+\sqrt{2x}]$ sia almeno $c_1\sqrt{x}\cdot(lgx)^{-c_2}$. Allora l'algoritmo di Goldwasser-Kilian, con in input un intero n primo, prova la primalità di n, se termina, in $O((lgn)^{10+c_2})$.*

Dim. cfr. Goldwasser-Kilian [13], pag. 324-325. •

Il significato del Teorema 4.3.3 é che, se é vera una certa congettura standard di Teoria Analitica dei Numeri e se n é primo, allora l'algoritmo é probabilistico e termina con complessità polinomiale.

Teorema 4.3.4 : *Esistono due costanti positive c_3,c_4 tali che per tutti gli interi $k\geq 2$ la frazione dell'insieme dei primi n che hanno k cifre binarie e per cui l'algoritmo di Goldwasser-Kilian termina con complessità $\leq c_3k^{11}$ é almeno*

$$1-c_4 2^{-k^{\frac{1}{lglgk}}}.$$

Dim. : cfr. Goldwasser-Kilian [13], pag. 326-328. •

Questo secondo teorema asserisce che il sottoinsieme dei primi per cui l'algoritmo precedente prova la primalità in modo probabilistico e polinomiale é "molto grande".

Si noti che i Teoremi 4.3.3 e 4.3.4 sono stati qui enunciati con una leggera miglioria rispetto alla versione originale. Tale miglioria é conseguenza del fatto che é stata usata una versione dell'algoritmo di Schoof più recente.

Nota: Il Teorema 4.3.4 non fornisce informazioni sull'esistenza di un insieme infinito di primi la cui primalità sia provabile in modo deterministico e polinomiale. La risposta a tale questione è stata recentemente (1989) trovata da Pintz-Steiger-Szeremedi [26] i quali sono riusciti a costruire un insieme infinito di primi di densità $\frac{cn^{2/3}}{\lg n}$ la cui primalità viene provata con un algoritmo deterministico e polinomiale $O(\lg^9 n)$.
Rimane ancora ovviamente aperto il problema di sapere se è possibile provare in modo deterministico e polinomiale la primalità di tutti gli interi.
La migliore risposta disponibile a tale ultima questione è presentata nel capitolo seguente.

Capitolo 5

Test Di Adleman-Pomerance-Rumely

Nel presente capitolo verranno presentate due diverse versioni dello stesso algoritmo: la prima é la versione originale dovuta ai tre autori sopra menzionati; la seconda fa riferimento ai miglioramenti apportati da Lenstra e Cohen alla versione precedente.
Nel 1980 Adleman, Pomerance e Rumely, [1], inventarono un test di primalità che, oltre ad affermare se un intero passa o fallisce il test, ha l'importante capacità di fornire ulteriori informazioni sulla struttura dell'intero testato. Utilizzando tali informazioni si riesce a provare "velocemente" (con complessità "quasi-polinomiale" in lgn) la primalità o la non primalità di n.

5.1. VERSIONE ORIGINALE

IDEA BASE DELL'ALGORITMO

L'idea base dell'algoritmo é quella di selezionare due diversi insiemi di numeri primi in modo da sfruttare alcune loro proprietà particolari.

Definizione 5.1.1: *Fissato un arbitrario insieme di primi I, detto dei primi INIZIALI, definiamo un insieme E di primi, detto dei primi EUCLIDEI, tale che q∈E se e solo se q-1 é squarefree e ogni suo fattore primo appartiene ad I.*

Tali insiemi verranno costruiti all'interno dell'algoritmo stesso.
Al fine di ottenere un algoritmo efficiente, é necessario porre due condizioni sulla struttura di I=I(n) ed E=E(n) :

i) $\prod_{q\in E(n)} q > \sqrt{n}$

ii) $\prod_{p\in I(n)} p$ sia il più piccolo possibile .

La condizione i) serve per poter concludere sulla primalità di n, mentre la condizione ii) serve per ottenere una buona complessità computazionale perchè essa è, come vedremo nel prosieguo, polinomiale in tale prodotto.
Inoltre si prova che se n>100 allora si può scegliere I(n) in modo che $\prod_{p\in I(n)} p > (\lg n)^{c\lg_3 n}$ (é un risultato di Teoria Analitica dei Numeri che proveremo nel paragrafo 3. riguardante la complessità computazionale calcolata con metodi analitici).

Diamo adesso uno schema del ragionamento seguito nell'algoritmo.

Sia r un divisore primo di n .
Cerchiamo di determinare r (mod q) $\forall q\in E(n)$. Se si riesce a fare ciò, allora si può determinare r usando il Teorema Cinese dei Resti (Proposizione 2.1.3) per la condizione i) sopra scritta.
Notiamo, però, che per conoscere r (mod q) $\forall q\in E(n)$ basta riuscire a determinare $Ind_q(r)$ $\forall q\in E(n)$ (dove per $Ind_q(r)$ si intende ciò che segue :
data t_q radice primitiva di $(\mathbb{Z}/_{q\mathbb{Z}})^*$ si ha che

$$\mathrm{Ind}_q(r)=\min\left\{\text{a tale che } r\equiv t_q^a \pmod q\right\} .$$

Il problema é quindi quello di determinare $\mathrm{Ind}_q(r)$ $\forall q\in E(n)$. Il modo che é stato scelto é quello di determinare $\mathrm{Ind}_q(r)$ (mod p) con $p\in I(n)$ e poi usare il Teorema Cinese dei Resti . In quest'ultimo passo si é aiutati dal fatto che, come vedremo nel seguito, basta conoscere $\mathrm{Ind}_q(r)$ (mod p) per un solo p, perché tutti gli altri vengono determinati in dipendenza dell'unico conosciuto.
Infine si provano sistematicamente tutti i possibili valori per $\mathrm{Ind}_q(r)$ (mod p) (con q=q(p) particolare primo euclideo scelto in un modo che vedremo) per ogni p in I(n). Calcoliamo, quindi, $\prod_{p\in I(n)} p$ valori.
In tal modo costruiamo e testiamo ogni possibile divisore primo di n e, quindi, possiamo decidere la primalità o meno di n.

La versione originale dell'algoritmo sfrutta alcune proprietà dei campi ciclotomici :

FATTI RILEVANTI DI TEORIA ALGEBRICA DEI NUMERI

Campi ciclotomici:
(per maggiori dettagli vedere il Capitolo 2).

Sia p un primo, p∤n, e sia $\xi_p=e^{\frac{2\pi i}{p}}$ una radice primitiva p-esima dell'unità. Il suo polinomio minimo su $\mathbb{Q}$ é dato da $f_p(x)=x^{p-1}+x^{p-2}+...+1$.
Ricordiamo che l'anello degli interi algebrici di $\mathbb{Q}(\xi_p)$ é dato da $\mathbb{Z}[\xi_p]$.
Ci interessano in modo particolare le proprietà della fattorizzazione di ideali in $\mathbb{Z}[\xi_p]$.
Ricordiamo che, se q è primo, allora (q) é ramificato in $\mathbb{Z}[\xi_p]$ se e solo se p=q (infatti abbiamo che $(p)=(1-\xi_p)^{p-1}$). Altrimenti (q) fattorizza nel prodotto di $g=\frac{p-1}{f}$ ideali primi distinti (dove f é l'ordine di q in $(\mathbb{Z}/_{p\mathbb{Z}})^*$ cioé $(q)=I_1\cdot...\cdot I_g$. La norma di ogni tale ideale primo I_i che divide (q) é data da $NI_i=\#(\mathbb{Z}[\xi_p]/I_i)=q^f\equiv 1 \pmod p$.

Consideriamo adesso il polinomio $f_p(x)$ (mod q). Notiamo che, siccome $(\mathbb{Z}/_{q\mathbb{Z}})[X]$ é fattoriale, il polinomio $f_p(x)$ (mod q) fattorizza, in modo unico, come segue:

$$f_p(x) \equiv \prod_{i=1..g} h_i(x) \pmod q$$

dove gli $h_i(x)$ sono polinomi distinti, monici, di grado f ed irriducibili in $(\mathbb{Z}/_{q\mathbb{Z}})[X]$. Usando tale fattorizzazione e ricordando che ogni ideale in $\mathbb{Z}[\xi_p]$ ha al più due generatori, si ha la seguente:

Proposizione 5.1.1 : *Gli ideali primi di $\mathbb{Z}[\xi_p]$ sopra (q) sono dati da $I_i=(q,h_i(\xi_p))$ i=1..g.*

Dim: cfr. Teorema 2.4.22. ●

Inoltre, se sappiamo che n é un intero composto che si comporta "quasi" come un primo, la seguente proposizione risulta utile:

Proposizione 5.1.2 : *sia* $n\geq 2$, $f=\underset{(\mathbb{Z}/p\mathbb{Z})^*}{ord}(n)$, $g=\frac{p-1}{f}$.

Supponiamo che $f_p(x) \equiv \prod_{i=1..g} h_i(x) \pmod n$ *dove gli* $h_i(x)$ *sono monici di grado f e consideriamo gli ideali* $J_i=(n,h_i(\xi_p))$ *in* $\mathbb{Z}[\xi_p]$.

Allora se $r|n$, *r primo, si ha che, in* $\mathbb{Z}[\xi_p]$, $(r)=\prod_{i=1..g}(r,J_i)$.

Inoltre il numero di ideali primi di $\mathbb{Z}[\xi_p]$ *che stanno sopra a* (r) *e che dividono* (r,J_i) *non dipende da i.*

Dim: Sia $f_p(x) \equiv \prod_{j=1..k} v_j(x) \pmod r$ la decomposizione di $f_p(x)$ in fattori irriducibili di $(\mathbb{Z}/_{r\mathbb{Z}})[X]$. Notiamo che non ci sono fattori ripetuti (poiché $p\neq r$ si ha che (r) non ramifica). Per la Proposizione 5.1.1 abbiamo che gli ideali primi sopra a (r) sono dati da $H_j=(r,v_j(\xi_p))$ $j=1..k$. Però ogni $h_i(x)$ é prodotto modulo r (in modo unico) di certi $v_j(x)$ ed ogni $v_j(x)$ é divisore modulo r di qualche $h_i(x)$ perché $(\mathbb{Z}/_{r\mathbb{Z}})$ é un campo. Allora ogni (r,J_i) é precisamente il prodotto di quegli H_j corrispondenti ai $v_j(x)$ che dividono $h_i(x) \pmod r$. Allora, poiché ogni $v_j(x)$ ha grado t (uguale al grado inerziale di r), abbiamo che $h_i(x)=\prod_{j\in S_i} v_j(x)$ per ogni $i=1..g$ con $S_i\subseteq\{1..k\}$ opportuno. Poniamo $s_i=\#S_i$ ed allora si ha $f=ts_i$ $\forall i=1..g$. Da ciò segue $s_i=s$ e quindi ogni (r,J_i) é diviso esattamente dallo stesso numero di ideali primi che stanno sopra a (r).
Inoltre si ha la formula $(r)=\prod_{i=1..g}(r,J_i)$ perché abbiamo sia $tk=p-1=gf$ che $f=ts$; da ciò segue $tk=gst$ e quindi $k=gs$. ●

Nota:
Se $d|n$, d non necessariamente primo allora $(d)=\prod_{i=1..g}(d,J_i)$. Infatti: sia $d=r_1\cdot\ldots\cdot r_u$ la fattorizzazione di d in primi, allora :

$$(r_1)=\prod_{i=1..g}(r_1,J_i) \,,\ldots,\, (r_u)=\prod_{i=1..g}(r_u,J_i).$$

Però ho anche che :

$$(d) = (r_1\cdot\ldots\cdot r_u) = (r_1)\cdot\ldots\cdot(r_u) = (\prod_{i=1..g}(r_1,J_i))\cdot\ldots\cdot(\prod_{i=1..g}(r_u,J_i)) = \prod_{i=1..g}(r_1\cdot\ldots\cdot r_u,J_i) = \prod_{i=1..g}(d,J_i).$$

Legge di reciprocità p-esima:

Nel campo di numeri algebrici $\mathbb{Q}(\xi_p)$ si formula una legge di reciprocità tra simboli residuali (analoghi al simbolo di Jacobi e di Legendre entrambi definiti nel Capitolo 2).
Sia I un ideale primo non nullo di $\mathbb{Q}(\xi_p)$ tale che $p\notin I$ e sia v_I la valutazione definita da:

$$v_I(x)=a \Leftrightarrow I^a \| (x).$$

Notiamo che, per quanto visto nel Capitolo 2 e nell'argomento precedente, $p|(NI-1)$.
Sia adesso $\alpha\in\mathbb{Q}(\xi_p)$ con $v_I(\alpha)=0$.

Definizione 5.1.2: *Simbolo residuale p-esimo :*

con la notazione $\left(\frac{\alpha}{I}\right)_p$ *intendiamo l'unica radice p-esima dell'unità tale che :*

$$\left(\frac{\alpha}{I}\right)_p = \xi_p^{J} \equiv \alpha^{(NI-1)/p} \pmod{I}$$

(notiamo che $\alpha^{(NI-1)/p}$ *é radice p-esima dell'unità).*

Per tale simbolo, analogamente al simbolo di Jacobi, vale la moltiplicatività sul secondo argomento: cioé se $\gamma=I_1^{a_1}\cdot....\cdot I_r^{a_r}$ allora vale $\left(\frac{\alpha}{\gamma}\right)_p = \prod_i \left(\frac{\alpha}{I_i}\right)_p^{v_{I_i}(\gamma)}$ dove il prodotto si intende fatto sugli I_i tali che $I_i \not| (p)$, $\alpha \notin I_i$ e dove $v_{I_i}(\gamma)=a_i$.

Nel seguito ci serviranno due proposizioni:

Proposizione 5.1.3: (Legge di reciprocità per simboli residuali p-esimi)
Sia p>2 e siano a, $\gamma \in \mathbb{Q}(\xi_p)$ *relativamente primi tra loro e con 1-*ξ_p *(che nel seguito denoteremo col simbolo* λ*) .*
Allora esiste una radice p-esima dell'unità $(\alpha,\gamma)_\lambda$ *per cui vale la relazione:*

$$\left(\frac{\alpha}{\gamma}\right)_p = \left(\frac{\gamma}{\alpha}\right)_p (\alpha,\gamma)_\lambda .$$

Proposizione 5.1.4: *Se* $\alpha \equiv 1 \pmod{\lambda^{i}}$ *e* $\gamma \equiv 1 \pmod{\lambda^{j}}$ *con* $i+j \geq p+1$ *allora* $(\alpha,\gamma)_\lambda = 1$.

Inoltre $(\alpha,\gamma)_\lambda$ é moltiplicativo in entrambi gli argomenti e non varia se entrambi gli argomenti vengono moltiplicati per una potenza p-esima. (Tutti i tre fatti sopra enunciati si trovano in Artin-Tate [3], pag. 168-173).

Si noti anche che, se $\sigma \in Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$, allora si ha che:

$$\left(\frac{\sigma\alpha}{\sigma I}\right)_p = \sigma\left(\frac{\alpha}{I}\right)_p$$

Proviamo quest'ultima affermazione:
$\left(\frac{\alpha}{I}\right)_p = \xi_p^{j} \equiv \alpha^{(NI-1)/p} \pmod{I} \Rightarrow \exists\, i \in I$ tale che $\xi_p^{j} - \alpha^{(NI-1)/p} = i$ e quindi che:

$$\sigma(\xi_p^{j} - \alpha^{(NI-1)/p}) = \sigma(i) \in \sigma(I).$$

Però il primo membro non é altro che : $\xi_p^{ju} - \sigma(\alpha)^{(NI-1)/p}$ (se $\sigma(\xi_p)=\xi_p^{u}$) e, poiché NI=NσI, é uguale a $\xi_p^{ju} - \sigma(\alpha)^{(N\sigma I-1)/p} = \sigma(i)$.

Allora si ha che $\xi_p^{ju} \equiv \sigma(\alpha)^{(N\sigma I-1)/p} \pmod{\sigma I}$ e quindi, per l'unicità, si ha $\left(\frac{\sigma\alpha}{\sigma I}\right)_p = \sigma\left(\frac{\alpha}{I}\right)_p$.

Nel caso particolare in cui si abbiano due primi $p,q \in \mathbb{Z}$ che soddisfano la relazione $p|(q-1)$, consideriamo $t=t_q$ un generatore di $(\mathbb{Z}/_{q\mathbb{Z}})^*$ e calcoliamo :

$$f_p(x) \equiv \prod_{i=1}^{p-1}\left(x-\left(t^{\frac{i(q-1)}{p}}\right)\right) \pmod q$$

per quanto visto precedentemente nel punto dedicato ai campi ciclotomici (in questo caso f=1 perché q≡1 (mod p)).

Si noti che $t^{\frac{(q-1)}{p}}$ é una radice primitiva p-esima dell'unità e che é sempre possibile scegliere ξ_p in modo che ξ_p non sia uguale a $t^{\frac{(q-1)}{p}}$: infatti é noto che esistono φ(p)=p-1 radici primitive p-esime dell'unità (cfr. Capitolo 2).

Notazione: Diremo ideale primo "canonico" l'ideale $I=(q,\xi_p-t^{\frac{(q-1)}{p}})$ che sta sopra q in ($\mathbb{Z}[\xi_p]$ (un tale ideale esiste (per la Proposizione 5.1.1)) .

Vediamo adesso come la conoscenza di $\left(\frac{x}{I}\right)_p$ con x∈$\mathbb{Z}$ ci consente di calcolare $Ind_q(x)$. Infatti si ha che :

$$\left(\frac{x}{I}\right)_p \equiv x^{\frac{(q-1)}{p}} \equiv t^{Ind_q(x)\frac{(q-1)}{p}} \equiv \xi_p^{Ind_q(x)} \pmod I.$$

Somme di Jacobi:

I simboli precedentemente definiti possono essere usati per calcolare alcuni elementi di $\mathbb{Z}[\xi_p]$ che hanno la proprietà di essere facilmente calcolabili e di avere fattorizzazione in ideali primi conosciuta.
Sia I un ideale primo di $\mathbb{Q}(\xi_p)$ con p∉I, a,b∈$\mathbb{Z}$, allora:

Definizione 5.1.3: *Diremo SOMMA DI JACOBI la seguente espressione :*

$$J_{a,b}(I) = \sum{}'\left(\left(\frac{x}{I}\right)_p^a\left(\frac{(1-x)}{I}\right)_p^b\right)$$

dove col simbolo $\sum'$ *si intende la somma su tutti gli x∈*$\mathbb{Z}[\xi_p]/I$ *tranne x=0,1.*

La fattorizzazione in ideali primi di tali elementi é data da (per il Lang [19], Teorema 11, pag. 98):

Proposizione 5.1.5:
Siano a,b∈$\mathbb{Z}$ *per cui ab(a+b)≠0 (mod p).*
Per u∈$\mathbb{Z}$ *sia* $\theta_{ab}(u)=\left[\frac{a+b}{p}u\right]-\left[\frac{a}{p}u\right]-\left[\frac{b}{p}u\right]$ *, allora :*

$$J_{a,b}(I) = \prod_{u=1}^{p-1}\left(\sigma_u^{-1}(I)\right)^{\theta_{ab}(u)},$$

dove σ_u∈$Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ *tale che* $\sigma_u(\xi_p)=\xi_p^u$.

Nel seguito useremo anche il seguente risultato, dovuto a Iwasawa [16], per provare che, in qualche caso particolare, $(\alpha,\gamma)_\lambda = 1$ (dove $(\alpha,\gamma)_\lambda$ è definita nella Proposizione 5.1.3):

Proposizione 5.1.6: *$\forall\, a,b \in \mathbb{Z}$ si ha che $-J_{a,b}(I) \equiv 1 \pmod{\lambda^2}$.*

La proposizione seguente ci consentirà di utilizzare la somma di Jacobi come un "buon" surrogato dei primi in $\mathbb{Q}(\xi_p)$:

Proposizione 5.1.7:

Se $p>2$ allora $\exists\, a,b \in \mathbb{Z}$ tali che $ab(a+b) \not\equiv 0 \pmod p$ per cui $p \nmid \theta'_{ab} = \sum_{u=1}^{p-1} \theta_{ab}(u)u^{-1}$

(per u^{-1} si intende l'inverso di u modulo p).

Dim: Si noti che, se $1 \le u \le p-1$, allora $\left[\frac{u}{p}\right]=0$ e $\left[\frac{p-1}{p}u\right] = u-1$. Quindi, se si considera la sommatoria sugli elementi del tipo $\theta'_{m,1}$, si ha che:

$$\sum_{m=1}^{p-2}\theta'_{m1} = \sum_{m=1}^{p-2}\left(\sum_{u=1}^{p-1}\left[\frac{m+1}{p}u\right]-\left[\frac{m}{p}u\right]u^{-1}\right) =$$

$$= \sum_{u=1}^{p-1}\left[\frac{p-1}{p}u\right]u^{-1} = \sum_{u=1}^{p-1}(u-1)u^{-1} = \sum_{u=1}^{p-1}(1-u^{-1}) =$$

$= p-1-(\sum_{u=1}^{p-1}u) \equiv p-1 \pmod p$. Ma, ovviamente, $p-1 \not\equiv 0 \pmod p$ e quindi vi deve essere almeno una coppia del tipo (m,1) per cui $\theta'_{m,1} \not\equiv 0 \pmod p$. ●

Osservazione :
Si noti inoltre che (Cohen [9], Lemma 3.1):
$\theta'_{a,b} \equiv \frac{(a+b)^p-a^p-b^p}{p} \pmod p$ e quindi se $p<10^9$ e $p \neq 1093, 3511$ si può prendere a=b=1.

5.1.1 ALGORITMO PROBABILISTICO.

Siamo adesso in grado di descrivere il funzionamento dell'algoritmo. La versione che presentiamo nel seguito é probabilistica, perché adotta l'algoritmo probabilistico e polinomiale di Berlekamp (cfr. Berlekamp [6]) per fattorizzare polinomi in $(\mathbb{Z}/_{n\mathbb{Z}})[X]$ (l'algoritmo di Berlekamp può non terminare in tal punto anche se n é primo).
Sia n un intero che ha passato uno o più dei test di primalità del Capitolo 4. Dividiamo l'algoritmo in tre fasi:

A. FASE DI PREPARAZIONE

A.1 : Calcolare il più piccolo naturale squarefree, che denotiamo f(n) , tale che $\prod_{\substack{(q-1)|f(n)\\ q \text{ primo}}} q > \sqrt{n}$.

Definiamo

$$\mathbf{I(n)} := \{p \text{ primi tali che } p|f(n)\}$$
$$\mathbf{E(n)} := \{q \text{ primi tali che } (q-1)|f(n)\}.$$

Un metodo per determinare f(n) é quello di calcolare sequenzialmente per ogni intero squarefree k=1,2,3,5,6 , ... il prodotto $\prod_{\substack{(q-1)|k\\ q \text{ primo}}} q$ fermandosi non appena si determina un k per cui il prodotto sopra indicato é maggiore di $\sqrt{n}$. Il numero di operazioni necessarie per eseguire tale calcolo per ogni k é alpiù k^c , con c costante intera positiva opportuna, e quindi la complessità computazionale del calcolo di f(n) é $O(f(n)^{c+1})$.

A.2 : Calcolare e fissare una radice primitiva t_q per ogni primo euclideo q (ad esempio la più piccola radice primitiva), e controllare che p∤n e che q∤n.
Un metodo per calcolare una radice primitiva (cioé un elemento di ordine q-1) é stato esposto nel Capitolo 4 al Paragrafo 2. Come abbiamo fatto notare, l'algoritmo di Lehmer può non terminare anche se q é primo. Però, se in tale algorimo vengono effettuate q-1 scelte di elementi distinti di $(\mathbb{Z}/_{q\mathbb{Z}})^*$, sicuramente una radice primitiva viene ad essere determinata con complessità $O(q\lg^3 q)=O(q^2)$. Nel nostro caso, poiché q|f(n), abbiamo quindi che il calcolo di una radice primitiva modulo q é $O(f(n)^2)$.

A.3 : Per ogni p∈I(n), p>2 determinare a,b∈$\mathbb{Z}$ tali che :
0<a<p , 0<b<p , a+b ≠0 (mod p), e

$$\theta'_{ab} = \sum_{u=1}^{p-1} \theta_{ab}(u)u^{-1} .$$

Tali a,b esistono per la Proposizione 5.1.7 ed inoltre la osservazione successiva a tale proposizione ci consente di prendere a=b=1, $\theta'_{ab}=1$ se $p<10^9$ e p ≠1093, 3511.
Nel caso in cui si ha p=2 si prenda a=b= $\theta'_{ab}=1$.

A.4 : Calcoliamo $J_p(q)$ per ogni p∈I(n) e q∈E(n) per cui p|(q-1) come segue:
se p=2 allora $J_p(q) = -q$

se p>2 allora $J_p(q)= - J_{a,b}(I) =- \sum_{x=2}^{q-1} \left(\left(\frac{x}{I}\right)_p^a \left(\frac{(1-x)}{I}\right)_p^b \right)$

dove a,b sono stati calcolati in **A.3** e I é l'ideale primo "canonico" rispetto a t_q definito precedentemente da $I=(q,\xi_p - t^{\frac{(q-1)}{p}})$.
Si ha che $J_p(q) \in \mathbb{Q}(\xi_p)$.
In tale passo si pone il problema di calcolare $\left(\frac{x}{I}\right)_p = \xi_p^j$. Notiamo che, per fare ciò, basta calcolare i valori $\left(t^{\frac{i(q-1)}{p}}\right)$ i=0,1,...,p-1, calcolare $x^{\frac{(q-1)}{p}}$ e poi determinare j come abbiamo visto nel paragrafo riguardante la Legge di Reciprocità p-esima (pag. 79).
In questo caso la Legge di Reciprocità p-esima vale con $(J_p(q),r)_\lambda =1$ per ogni r intero primo con p, perché, sfruttando la proprietà che il simbolo $(.,.)_\lambda$ non varia se il secondo termine viene moltiplicato per una potenza p-esima (cfr. pag. 78), si ha :

$$(J_p(q),r)_\lambda = (J_p(q),rr^{-p})_\lambda = (J_p(q),(r^{-1})^{p-1})_\lambda .$$

Però, poiché $(r^{-1})^{p-1} \equiv 1 \pmod{\lambda^{p-1}}$ (per il Piccolo Teorema di Fermat e perché $(\lambda^{p-1})=(p)$ e $J_p(q) \equiv 1 \pmod{\lambda^2}$ (per la Proposizione 5.1.6), si ha, per la Proposizione 5.1.4, che $(J_p(q),r)_\lambda=1$.

A.5 : Per ogni $p \in I(n)$, fattorizziamo (n) in ideali di $\mathbb{Z}[\xi_p]$ come se n fosse primo.
Per p=2 non é necessario nessun calcolo.
Per p>2 si procede come segue:
Sia $f= \underset{(\mathbb{Z}/p\mathbb{Z})^*}{ord}(n)$ e sia $g=\frac{p-1}{f}$.
Cerchiamo di fattorizzare $f_p(x) = x^{p-1} + ...+x+1 \equiv \prod_{i=1..g} h_i(x) \pmod n$, dove gli $h_i(x)$ sono monici di grado f.
Se n é primo allora $f_p(x)$ ha alta probabilità di essere fattorizzato su $(\mathbb{Z}/_{p\mathbb{Z}})[X]$ coll'algoritmo di Berlekamp, ma, purtroppo, l'algoritmo di Berlekamp, anche se n é primo, può non terminare.
Se l'algoritmo di Berlekamp termina allora, in analogia con la Proposizione 5.1.2, prendiamo $I_i=(n,h_i(\xi_p))$, i=1,..,g.

B. PASSO ESTRATTIVO

Supponiamo che J sia un ideale di $\mathbb{Z}[\xi_p]$ verificante $J \not| (\lambda)$ e sia a un elemento di $\mathbb{Z}[\xi_p]$. Precedentemente abbiamo visto che, se J é primo e se $a \notin J$, allora $a^{(NJ-1)/p}$ é congruente modulo J ad una radice p-esima dell'unità.
Ciò però può accadere anche se J non é primo ed in tal modo J può essere considerato analogamente ad un pseudoprimo di $\mathbb{Z}$ (cfr. Capitolo 4). Notiamo però che, siccome $J \not| (\lambda)$, l'affermazione precedente può essere vera per alpiù una radice dell'unità, infatti se, per assurdo, si avesse :

$$a^{(NJ-1)/p} \equiv \xi_1 \pmod J$$

$$a^{(NJ-1)/p} \equiv \xi_2 \pmod J$$
$$(\xi_1 \neq \xi_2)$$

allora, ponendo per semplicità $\xi_1=\xi_p$, esiste f>1 per cui $\xi_2= \xi_p^f$. Dalle relazioni precedenti si ha che $\xi_p \equiv \xi_p^f \pmod J$ cioé $(\xi_p-\xi_p^f)\in J$.

Però $\xi_p-\xi_p^f= \xi_p(1-\xi_p^{f-1})$ ed allora distinguiamo due casi :

1) f=2 $\quad \xi_p(1-\xi_p^{f-1})=\xi_p\lambda$ ed allora $\lambda\in J$ (perché ξ_p é invertibile in $\mathbb{Z}[\xi_p]$);

2) f>2 $\quad \xi_p(1-\xi_p^{f-1})=\xi_p\lambda(1+\xi_p+.....+\xi_p^{f-2})$ ma, poiché $1+\xi_p+.....+\xi_p^{f-2} = \frac{1-\xi_p^{f-1}}{1-\xi_p}$ é un elemento invertibile in $\mathbb{Z}[\xi_p]$, allora $\lambda\in J$.

In entrambi i casi si ha una contraddizione e quindi si ha $\xi_1=\xi_2$.

Definizione 5.1.4: *Si definisce il Simbolo Residuale Fittizio p-esimo come segue :*

$$\left\langle \frac{\alpha}{J} \right\rangle_p = \xi_p^{\,j} \quad \textit{se j é tale che valga} \quad \xi_p^{\,j} \equiv \alpha^{(NJ-1)/p} \ \textit{(mod J),}$$

e

$$\left\langle \frac{\alpha}{J} \right\rangle_p = 0 \qquad \textit{in tutti gli altri casi.}$$

Si noti inoltre che, anche per il simbolo fittizio vale la seguente proprietà :

se $\sigma\in Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ allora si ha che:

$$\left\langle \frac{\sigma\alpha}{\sigma I} \right\rangle_p = \sigma \left\langle \frac{\alpha}{I} \right\rangle_p .$$

Passiamo adesso ad esaminare il passo estrattivo in dettaglio:

B.1 : Per ogni $p\in I(n)$ e $q\in E(n)$ con $p|(q-1)$ si calcoli $\left\langle \frac{J_p(q)}{I_i} \right\rangle_p$ con i=1,..,g; dove gli ideali I_i sono quelli calcolati in **A.5**.

Se almeno uno degli $\left\langle \frac{J_p(q)}{I_i} \right\rangle_p$, i=1,..,g, é nullo, allora n é composto (infatti, se n è primo, allora $\left\langle \frac{J_p(q)}{I_i} \right\rangle_p \neq 0$, $\forall$ i=1,..,g, perché in tal caso I_i é primo $\forall$ i=1,..,g).

Nella presentazione della versione deterministica dell'algoritmo (pag. 91), si farà vedere come un simbolo residuale fittizio p-esimo possa essere calcolato con complessità polinomiale in p e lgn ($\leq$f(n)). Poiché il numero di residui fittizi che dobbiamo calcolare é g$\leq$p-1 per ogni coppia di primi (p,q) con $p|(q-1)$ e poiché il numero dei primi euclidei é $\leq$f(n), allora si ha che il passo **B.1** può essere eseguito con complessità polinomiale in f(n).

B.2 : Per ogni $p\in I(n)$ si faccia ciò che segue:

a) se i simboli residuali fittizi per p non sono tutti uguali a 1, se ne scelga uno tra quelli $\neq 1$, indicato $\left\langle \frac{\gamma}{J} \right\rangle_p$, che chiameremo simbolo DISTINTO corrispondente a p.

b) se tutti i simboli residuali fittizi per p sono uguali a 1 allora si scelgano in modo casuale degli elementi $\gamma \in \mathbb{Z}[\xi_p]$ e si calcoli $\left\langle \frac{\gamma}{I_i} \right\rangle_p$, i=1,..g, finché non se ottiene uno per cui $\left\langle \frac{\gamma}{I_i} \right\rangle_p \neq 0,1$ per un certo i, lo si chiami simbolo DISTINTO e lo si indichi $\left\langle \frac{\gamma}{J} \right\rangle_p$.

Si noti che anche nel punto **b**) precedente , l'algoritmo può non terminare, ma, se n è primo, si ha che la probabilità di scegliere casualmente un $\gamma \in \mathbb{Z}[\xi_p]$ per cui $\left\langle \frac{\gamma}{I_i} \right\rangle_p \neq 0,1$ é data da $\frac{p-1}{p}$ (cfr. Capitolo 4, algoritmo di Lehmer).

B.3 : Per ogni coppia di primi (p,q) con p|(q-1) si calcoli $m_{i,q}$ tale che :

$$\left\langle \frac{\gamma}{I_i} \right\rangle_p^{m_{iq}} = \left\langle \frac{J_p(q)}{I_i} \right\rangle_p \quad 0 \leq m_{i,q} < p.$$

Un tale intero $m_{i,q}$ esiste perché $\left\langle \frac{\gamma}{I_i} \right\rangle_p$ é una radice primitiva p-esima dell'unità.

Dimostriamo adesso un importante risultato che permette di dedurre, dalla relazione sui simboli fittizi, una analoga relazione sui simboli residuali p-esimi.

Lemma 5.1.1: (Lemma di estrazione).
Siano A_1 e A_2 due ideali di $\mathbb{Z}[\xi_p]$ tali che $NA_1=NA_2$ e che p$\not|$$NA_1$. Siano B_1 e B_2 due ideali primi coniugati di $\mathbb{Z}[\xi_p]$ che dividono, rispettivamente, A_1 e A_2.

Supponiamo che $\exists\, \gamma \in \mathbb{Z}[\xi_p]$ tale che $\left\langle \frac{\gamma}{A_1} \right\rangle_p \neq 0,1$.

Allora $\forall\, \alpha \in \mathbb{Z}[\xi_p]$ la relazione :

a) $\left\langle \frac{\gamma}{A_1} \right\rangle_p^m = \left\langle \frac{\alpha}{A_2} \right\rangle_p$ *($m \in \mathbb{Z}$)*

implica la relazione:

b) $\left(\frac{\gamma}{B_1}\right)_p^m = \left(\frac{\alpha}{B_2}\right)_p$

Dim: Per ipotesi abbiamo che $\gamma^{(NA_1-1)/p} \equiv \xi_p^{\,j} \pmod{A_1}$ per qualche j tale che (j,p)=1. Allora si ha che $\gamma^{(NA_1-1)/p} \equiv \xi_p^{\,j} \pmod{B_1}$.

Proviamo adesso che $v_p(NB_1-1)>v_p\left(\frac{NA_1-1}{p}\right)$.

Osserviamo intanto che $\gamma^{NA_1-1} \equiv 1 \pmod{B_1}$ e che $NA_1 \geq NB_1$.

Inoltre so che $\gamma^{NB_1-1} \equiv 1 \pmod{B_1}$ e quindi $(NB_1-1)|(NA_1-1)$, ma $(NB_1-1) \nmid \frac{NA_1-1}{p}$. Allora $\exists$ $k \in \mathbb{N}$ tale che $k(NB_1-1)=(NA_1-1)$ e $p \nmid k$ (se $p|k$ avrei che $(NB_1-1) \mid \frac{NA_1-1}{p}$ che é assurdo) e quindi $v_p(NB_1-1) = v_p(NA_1-1) = v_p\left(\frac{NA_1-1}{p}\right)$-1 che prova quanto volevamo.

Supponiamo adesso che $B_1=B_2$; allora usando la relazione **a**) modulo B_1 e il fatto che $NA_1=NA_2$ si ha che:

$$\left(\gamma^{(NA_1-1)/p}\right)^m = \left\langle \frac{\gamma}{A_1} \right\rangle_p^m = \left\langle \frac{\alpha}{A_2} \right\rangle_p \equiv \alpha^{(NA_1-1)/p} \pmod{B_1}.$$

Poiché il gruppo moltiplicativo di un campo finito é ciclico, consideriamo una radice primitiva τ modulo B_1.

In tal modo posso allora scrivere che:

$$\tau^{(Ind(\gamma)m-Ind(\alpha))(NA_1-1)/p} \equiv 1 \pmod{B_1}.$$

Poiché l'ordine di τ é NB_1-1, allora si ha che:

$$(NB_1-1) \mid (Ind(\gamma)m-Ind(\alpha))\frac{NA_1-1}{p}.$$

Ma poiché $v_p(NB_1-1) > v_p\left(\frac{NA_1-1}{p}\right)$ allora si può dire che $p|(Ind(\gamma)m-Ind(\alpha))$ e quindi si ha che:

$$\tau^{(Ind(\gamma)m-Ind(\alpha))(NB_1-1)/p} \equiv 1 \pmod{B_1}$$

che, può anche essere scritta come $\left(\gamma^{(NB_1-1)/p}\right)^m = \alpha^{(NB_1-1)/p} \pmod{B_1}$.

Ciò prova la tesi nel caso $B_1=B_2$.

Supponiamo adesso $B_1 \neq B_2$. Poiché B_1 e B_2 sono coniugati, esiste un $\sigma \in Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ tale che $\sigma B_1=B_2$ ed allora si ha che :

$$\left\langle \frac{\alpha}{A_2} \right\rangle_p = \sigma\left(\left\langle \frac{\sigma^{-1}\alpha}{\sigma^{-1}A_2} \right\rangle_p\right) = \left\langle \frac{\sigma^{-1}\alpha}{\sigma^{-1}A_2} \right\rangle_p^j \qquad (\text{se } \sigma(\xi_p)=\xi_p^j).$$

Sfruttando quanto sopra scritto, ci si può ricondurre al caso precedente rimpiazzando a con $\sigma^{-1}\alpha$, A_2 con $\sigma^{-1}A_2$, m con mu (dove $u=j^{-1}$ é l'inverso di j modulo p) perché in tal caso si ha:

$$\left\langle \frac{\gamma}{A_1} \right\rangle_p^m = \left\langle \frac{\alpha}{A_2} \right\rangle_p = \left\langle \frac{\sigma^{-1}\alpha}{\sigma^{-1}A_2} \right\rangle_p^j \qquad \text{e quindi :}$$

$$\left\langle \frac{\gamma}{A_1} \right\rangle_p^{mu} = \left\langle \frac{\sigma^{-1}\alpha}{\sigma^{-1}A_2} \right\rangle_p.$$

Allora per quanto precedentemente detto nel caso $B_1=B_2$, poiché $NA_2=N\sigma^{-1}A_2$ e $\sigma^{-1}(B_2)=B_1$, si ha che $\left(\frac{\gamma}{B_1}\right)_p^{mu} = \left(\frac{\sigma^{-1}\alpha}{\sigma^{-1}B_2}\right)_p$ e quindi, con passaggi analoghi ai precedenti, $\left(\frac{\gamma}{B_1}\right)_p^m = \left(\frac{\alpha}{B_2}\right)_p$. •

Sfruttando tale Lemma 5.1.1, si possono, quindi, calcolare tutti i simboli residuali p-esimi utilizzando uno di essi già determinato :

sia r primo, r|n, sia p>2, p∈I(n) e sia $\left\langle \frac{\gamma}{J} \right\rangle_p$ il simbolo residuale distinto corrispondente a p. Purtroppo conoscere tale simbolo non ci consente di calcolare $\left(\frac{\gamma}{(r,J)}\right)_p$, ma comunque tale ultimo simbolo può assumere solo p possibili valori. Dopo essere riusciti a determinare il valore di $\left(\frac{\gamma}{(r,J)}\right)_p$, si é in grado di calcolare ogni $Ind_q(r)$ (mod p), con q tale che p|(q-1), come segue :

Valutiamo $\left(\frac{J_p(q)}{r}\right)_p$ in due diversi modi :

1) Per la Legge di Reciprocità p-esima ed il passo **A.4** si ha che

$$\left(\frac{J_p(q)}{r}\right)_p = \left(\frac{r}{J_p(q)}\right)_p (J_p(q),r)_\lambda = \left(\frac{r}{J_p(q)}\right)_p.$$

Però, per la Proposizione 5.1.5, si ha :

$$\left(\frac{r}{J_p(q)}\right)_p = \prod_{u=1}^{p-1} \left(\frac{r}{(\sigma_u^{-1}(I))}\right)_p^{\theta_{ab}(u)} =$$

$$= \prod_{u=1}^{p-1} (\sigma_u^{-1}\left(\frac{r}{I}\right)_p)^{\theta_{ab}(u)} = \prod_{u=1}^{p-1} \left(\frac{r}{I}\right)_p^{(\theta_{ab}(u)/u)} = \left(\frac{r}{I}\right)_p^{\theta'_{ab}(u)}$$

dove I é il primo "canonico" sopra a q.

2) D'altra parte si ha anche che:

$$\left(\frac{J_p(q)}{r}\right)_p = \prod_{i=1}^{g} \left(\frac{J_p(q)}{(r,I_i)}\right)_p = \prod_{i=1}^{g} \left(\frac{\gamma}{(r,J)}\right)_p^{m_{iq}} = \left(\frac{\gamma}{(r,J)_p}\right)^{\sum_{i=1}^{g} m_{iq}}$$

per la Proposizione 5.1.2, il passo **B.3**, e l'osservazione seguente:

Osservazione :

facciamo vedere che, se $\left\langle \frac{J_p(q)}{I_i} \right\rangle_p = \left\langle \frac{\gamma}{J} \right\rangle_p^{m_{iq}}$, allora si ha che $\left(\frac{J_p(q)}{(r,I_i)}\right)_p = \left(\frac{\gamma}{(r,J)}\right)_p^{m_{iq}}$

Siccome r divisore primo di n, abbiamo che $(r) = \prod_{j=1..k} (r, v_j(\xi_p))$ (per la Proposizione 5.1.2) con grado($v_j(x)$)=t.

Fissato i, si ha che, se con R_j indichiamo $(r,v_j(\xi_p))$, (r,J) é diviso esattamente da s ideali R_c e (r,I_i) da s ideali R_d. Poiché si ha che $J\subseteq(r,J)$ e $I_i\subseteq(r,I_i)$, allora si deduce che $R_d|I_i$ e che $R_c|J$ per ogni c,d tali che $R_c|(r,J)$ e che $R_d|(r,I_i)$ (per le proprietà di divisibilità di ideali in un anello di Dedekind quale é $\mathbb{Z}[\xi_p]$, cfr. Capitolo 2). Applicando il Lemma 5.1.1, si ottiene, siccome R_c e R_d sono coniugati (sono primi che dividono lo stesso ideale in una estensione normale di un campo di numeri, cfr. Capitolo 2), che:

$$\left(\frac{J_p(q)}{R_d}\right)_p = \left(\frac{\gamma}{R_c}\right)_p^{m_{iq}}$$

ma, poiché ho tanti R_c quanti R_d, si ottiene

$$\prod_d\prod\left(\frac{J_p(q)}{R_d}\right)_p = \prod_c\prod\left(\frac{\gamma}{R_c}\right)_p^{m_{iq}}.$$

Però il secondo membro, per la moltiplicatività di $\left(\frac{\cdot}{\cdot}\right)_p$, non é altro che $\left(\frac{\gamma}{\prod\prod R_c}\right)_p^{m_{iq}} = \left(\frac{\gamma}{(r,J)}\right)_p^{m_{iq}}$,

mentre il primo membro é invece $\left(\frac{J_p(q)}{\prod\prod R_d}\right)_p = \left(\frac{J_p(q)}{(r,I_i)}\right)_p$ e ciò conclude l'osservazione.

Confrontando allora i due risultati ottenuti in **1**) e **2**), e osservando che, se a,b sono stati scelti come in **A.3**, θ'_{ab} é invertibile modulo p e, se ω é il suo inverso modulo p, allora si ha che:

$$\left(\frac{r}{I}\right)_p = \left(\frac{\gamma}{(r,J)}\right)_p^{\omega\sum_{i=1}^{g} m_{iq}}$$

e quindi, se $\left(\frac{\gamma}{(r,J)}\right)_p = \xi_p^{\,k}$, si ha che, per quanto detto sulle somme di Jacobi,

$$\mathrm{Ind}_q(r) \equiv k\omega \sum_{i=1..g} m_{iq} \pmod p.$$

Quindi, se riusciamo a conoscere k, cioè $\left(\frac{\gamma}{(r,J)}\right)_p$, allora possiamo determinare $\mathrm{Ind}_q(r)$.

C. PASSO DI CONSOLIDAMENTO

Prima di descrivere questo passo, osserviamo che :

se $I(n)=\{p_1,...,p_S\}$ e se $\left\langle\frac{\gamma_i}{J_i}\right\rangle_{p_i}$ sono i corrispondenti simboli distinti p_i-esimi calcolati in **B.2**,

allora, se r|n e r è primo, $\exists\ k_1,..,k_S\in\mathbb{N}$ tali che $\left(\frac{\gamma_i}{(r,J_i)}\right)_{p_i} = \xi^{k_i}\ \forall\ i=1,..s$, con ξ radice p_i-esima dell'unità.

Ma in questo passo non calcoleremo ogni k_i,bensì l'unico k (definito modulo $\prod_i p_i$) tale che $\left(\frac{\gamma_i}{(r,J_i)}\right)_{p_i} = \xi^k \ \forall\ i=1,..s$ (un tale k esiste per il Teorema Cinese dei Resti).

Passiamo adesso a descrivere il passo di consolidamento:

C.1 Per ogni k,$1 \le k \le f(n)=\prod_i p_i$, si eseguano le seguenti operazioni (costruiamo e testiamo tutti i possibili divisori di n):

C.1.1 Col Teorema Cinese dei Resti calcolare, per ogni q>2, q∈E(n), gli interi I(k,q) tali che

$$I(k,q) \equiv k\omega \sum_{i=1..g} m_{iq} \pmod p \quad \text{per ogni } p|(q-1).$$

Definiamo inoltre I(k,2)=1.
Si noti che, se k é fattore primo di n, allora si ha che:

$$I(k,q) \equiv Ind_q(k) \pmod p.$$

C.1.2 Per ogni q∈E(n), calcolare il minimo intero positivo $r(k,q) \equiv t_q^{I(k,q)} \pmod q$.
Si noti che, se k é fattore primo di n, allora si ha :

$$r(k,q) \equiv r \pmod q.$$

C.1.3 Col Teorema Cinese dei Resti si calcoli il minimo intero positivo r(k) tale che :

$$\forall q \in E(n) \text{ si abbia } r(k) \equiv r(k,q) \pmod q.$$

Si noti che, se k é fattore primo di n, allora $r(k) \equiv r \pmod Q$ dove $Q=\prod_{q\in E(n)} q$ e che, se $Q>\sqrt{n}$, allora r(k)=r.

C.1.4 Controllare se r(k) divide n. Se ciò accade e r(k)≠1, allora n composto e l'algoritmo termina. Altrimenti ritorna al punto **C.1** (cioé si sceglie il k successivo e si ripetono i calcoli).

C.2 Dichiarare n primo (perché se n fosse composto avrebbe un divisore primo ≤ $\sqrt{n}$, e tale divisore verrebbe determinato in corrispondenza di un k opportuno nei passi precedenti).

ANALISI EURISTICA DELL'ALGORITMO

Da quanto detto precedentemente, abbiamo che l'algoritmo, se termina, dichiara correttamente se n é primo o composto.
Se n è primo, abbiamo che ∃ una costante $c_1>0$ tale che ∀k≥1 l'algoritmo termina in $T_k(n)$ passi, $f(n) \le T_k(n) \le kf(n)^{c_1}$, con probabilità maggiore di $1-\frac{1}{2^k}$.
Inoltre possiamo osservare che :

a) nel passo **C** sembra che in realtà si fattorizzi n e che quindi il presente algoritmo sia un algoritmo di fattorizzazione. Purtroppo, in pratica, se n è composto, l'algoritmo termina, riconoscendolo, quasi sempre al punto **B**.

b) Si vedrà in seguito, nella versione di Lenstra, che in realtà non é necessario calcolare r(k) per ogni k perché un generatore dei possibili divisori di n modulo Q é dato da n stesso.

5.1.2 ALGORITMO DETERMINISTICO

L'algoritmo appena presentato nel punto precedente non é deterministico perché in due suoi punti, come osservato durante la presentazione, si ricade nel caso probabilistico.
I due punti in questione sono : la fattorizzazione di $f_p(x)$ modulo n e la costruzione di un elemento $\gamma \in \mathbb{Z}[\xi_p]$ tale che $\left\langle \frac{\gamma}{I} \right\rangle_p$ sia non banale. Tali problemi possono essere eliminati simultaneamente rimpiazzando la fattorizzazione in ideali primi di (n) con un procedimento che coinvolge la costruzione di un massimo comun divisore di ideali. Si proverà poi una versione generalizzata del Lemma di estrazione che renderà inutile la presenza di un "γ".
Inoltre nel presente paragrafo non useremo più i simboli residuali, ma lavoreremo direttamente sulle congruenze al fine di trarne ulteriori interessanti informazioni.
D'ora in poi supponiamo anche che il passo **A** della versione probabilistica sia già stato eseguito.

Procedura di M.C.D. di ideali

Fissato $p \in I(n)$, indichiamo con f l'ordine di n in $(\mathbb{Z}/_{p\mathbb{Z}})^*$. Se n é primo e J é un ideale primo tale che $J|(n)$, allora $NJ=n^f$ (cfr. Capitolo 2). Supponiamo adesso $\alpha \notin J$ ed allora, se $\left(\frac{\alpha}{J}\right)_p = 1$ e $p^2|(n^f-1)$, abbiamo che $\alpha^{(n^f-1)/p^2}$ é una radice p-esima dell'unità modulo J, cioé esiste j tale che: $\alpha^{(n^f-1)/p^2} \equiv \xi_p^{\,j} \pmod J$.
Si può ragionare analogamente se $p^3|n^f-1$.
Più in generale, se $p^k|(n^f-1)$, allora esistono s, $1 \le s \le k$, e j tali che:

a) $\alpha^{(n^f-1)/p^s} \equiv \xi_p^{\,j} \pmod J$

b) o $\xi_p^{\,j} \neq 1$ oppure s=k.

Estendendo il ragionamento sopra esposto al caso di avere h numeri $\alpha_1,..,\alpha_h \notin J$, si ha che esistono s, $1 \le s \le k$, e $j_1,..,j_h$ tali che valgano :

i) $\alpha_i^{(n^f-1)/p^s} \equiv \xi_p^{\,j_i} \pmod J$

ii) o $\xi_p^{\,j_i} \neq 1$ oppure s=k.

Se i) e ii) valgono per diversi primi R_l che dividono (n) (cioé valgono con gli stessi numeri $s,j_1,..,j_h$), allora valgono modulo $(\prod_l R_l)=I$.

Lo scopo che ci proponiamo è quello di trovare un ideale, non banale e divisore di (n), che "giochi" il ruolo di J nel caso specifico in cui $\alpha_1,..,\alpha_h$ sono o $J_p(q)$, per $q \in E(n)$ e $p|(q-1)$, oppure le loro coniugate $\sigma J_p(q)$, $\sigma \in Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$.
Per fare ciò costruiamo una procedura di massimo comun divisore di ideali che, se non ha successo, prova che n é composto.
L'idea base che useremo é la seguente:
se n é primo, allora ogni ideale di $\mathbb{Z}[\xi_p]$ che divide n é generato da n e $h(\xi_p)$ (per la Proposizione 5.1.1). Se aggiungiamo un elemento $h_1(\xi_p)$ a $(n,h(\xi_p))$ abbiamo come risultato l'ideale generato da n e $h_2(\xi_p)$, dove $h_2 \equiv$ M.C.D.$(h \pmod n, h_1 \pmod n) \pmod n$. Tale massimo comun

divisore può essere calcolato mediante l'algoritmo di divisione euclidea per polinomi che indicheremo M.C.D. e che ha un costo di $O(d^2 \lg^3 n)$, se i gradi dei polinomi coinvolti sono $\leq d$.
Se n non é primo, ma l'algoritmo di divisione euclidea dei polinomi termina egualmente per h (mod n) e h_1 (mod n), allora abbiamo comunque che l'ideale viene sempre generato da n e $h_2(\xi_p)$.
Notiamo inoltre che, l'unica ragione per cui l'algoritmo di divisione euclidea per polinomi può non terminare é che si sia determinato, in un certo passo dell'algoritmo, un divisore comune non banale di n e di uno dei due coefficienti di grado massimo dei polinomi ottenuti in tale passo. In tal caso n é stato fattorizzato e quindi n é composto.

Illustriamo adesso in dettaglio il processo :
Sia $I_0 = (n) = n\mathbb{Z}[\xi_p]$. Supponiamo che $1 \leq i \leq h$ e che I_{i-1} sia stato determinato. Allora consideriamo gli ideali :

$$(I_{i-1}, \alpha_i^{(n^f-1)/p} - \xi_p^{\,j}) \quad \text{per } j=1..p \quad (5.1.1).$$

Tali ideali vengono costruiti usando l'algoritmo di divisione euclidea dei polinomi come sopra descritto. A tal punto, se n viene fattorizzato, o se tutti gli ideali sopra scritti sono l'ideale identità si ha che n é composto e tale procedura termina. Supponiamo allora di essere riuscito a costruire tutti gli ideali della formula (5.1.1); allora definiamo I_i il primo ideale non banale.

Dopo aver costruito I_h, se é stato possibile scegliere $\xi_p^{\,j} \neq 1$ o se $p \not| \frac{n^f-1}{p}$, si prenda $I = I_h$. Altrimenti si ripete il processo sopra descritto prendendo al posto di $\frac{n^f-1}{p}$ la quantità $\frac{n^f-1}{p^2}$.

Se, dopo aver costruito I_{2h}, é stato ottenuto qualche ideale per cui $\xi_p^{\,j} \neq 1$ o $p \not| \frac{n^f-1}{p^2}$, si prende $I = I_{2h}$.
Altrimenti si procede analogamente finché non si raggiunge qualche s per cui é stato possibile scegliere qualche $\xi_p^{\,j} \neq 1$ o $p \not| \frac{n^f-1}{p^s}$, e a tal punto si prenda $I = I_{sh}$.

Si noti che tale processo termina sicuramente se n è primo, e che, in tal caso, $s < \frac{p}{\lg p} \lg n$.

Infatti sappiamo che $p^s \| (n^f-1)$ ossia che $\exists\, t \in \mathbb{N}-\{0\}$ tale che $tp^s = n^f - 1$ e $p \not| t$. Allora $p^s = \frac{n^f-1}{t}$ e, passando al logaritmo in entrambi i membri, si ha che $s \lg p = \lg(n^f-1) - \lg t \leq f \lg n$ (perché $t \geq 1$ e perchè il logaritmo è crescente). Poiché f é l'ordine di n in $(\mathbb{Z}/p\mathbb{Z})^*$ si ha che $f \leq p-1$. Da ciò si ottiene la valutazione voluta.
Inoltre le operazioni sugli ideali che sono state sopra esposte possono essere portate a termine in tempo polinomiale in p e lgn perché le operazioni sui polinomi si possono eseguire modulo $f_p(x)$ e modulo n e perchè le elevazioni a potenza vengono condotte a termine con la stessa tecnica esposta nel Capitolo 4 negli algoritmi di pseudoprimalità.
Si noti inoltre che la procedura sopra esposta può essere usata nei passi **B.1**, **B.2** dell'algoritmo probabilistico consentendo così di effettuare il calcolo dei simboli residuali fittizi in tempo polinomiale in p e lgn.
A tal punto esponiamo il seguente:

Lemma 5.1.2: (Lemma Estrattivo Generalizzato).
Sia $f = \underset{(\mathbb{Z}/p\mathbb{Z})^*}{ord}(n)$ *e sia J un ideale di* $\mathbb{Z}[\xi_p]$ *tale che* $J \backslash (n)$.
Supponiamo che siano dati $\alpha_1,..,\alpha_h \in \mathbb{Z}[\xi_p]$ *e che esistano s,* $1 \leq s \leq k$, *e* $j_1,..,j_h$ *tali che valgano :*

i) $\alpha_i^{(n^f-1)/p^s} \equiv \xi_p^{\,j_i} \pmod J$

ii) *o* $\xi_p^{j_i} \neq 1$ *per qualche i oppure* $p \nmid \frac{n^f-1}{p^s}$.

Allora $\forall \alpha,\beta \in \{\alpha_1,..,\alpha_h\}$ *e* $\forall m \in \mathbb{Z}$ *la relazione :*

a) $\alpha^{m(n^f-1)/p^s} \equiv \beta^{(n^f-1)/p^s} \pmod J$

implica la relazione:

b) $\forall H|J$, *H primo, si ha che* $\left(\frac{\alpha}{H}\right)_p^m = \left(\frac{\beta}{H}\right)_p$.

Dim: Se H | J allora si ha che **a**) vale (mod H) cosicché, se τ é un generatore di $(\mathbb{Z}[\xi_p]/H)^*$, si ha che :

$$\tau^{(\mathrm{Ind}(\alpha)m-\mathrm{Ind}(\beta))(n^f-1)/p^s} \equiv 1 \pmod H.$$

Poiché $\mathrm{ord}(\tau)=NH-1$, abbiamo che $(\mathrm{Ind}(\alpha)m-\mathrm{Ind}(\beta))\frac{n^f-1}{p^s} = l(NH-1)$ per un certo l intero.

Adesso si noti che, poiché $p \nmid n$ e $n \in H$, si ha $p|(NH-1)$.

A tal punto, se vale che $p \nmid \frac{n^f-1}{p^s}$, allora si ha che:

$$p|(\mathrm{Ind}(\alpha)m-\mathrm{Ind}(\beta)).$$

D'altra parte, se si ha che $\xi_p^{j_i} \neq 1$ per qualche i, allora si ha che

$$(NH-1) \nmid (\mathrm{Ind}(\alpha_i)\frac{n^f-1}{p^s})$$

e anche che :

$$(NH-1) | (\mathrm{Ind}(\alpha_i)\frac{n^f-1}{p^{s-1}}).$$

Ma ciò implica che:

$$v_p(NH-1) > v_p(\frac{n^f-1}{p^s})$$ e quindi si ha che $p|(\mathrm{Ind}(\alpha)m-\mathrm{Ind}(\beta))$.

In entrambi i casi si ha che :

$$\tau^{(\mathrm{Ind}(\alpha)m-\mathrm{Ind}(\beta))(NH-1)/p} \equiv 1 \pmod H$$

e quindi:

$$\alpha^{m(NH-1)/p} \equiv \beta^{(NH-1)/p} \pmod H$$

che altro non é che **b)** scritta in modo esplicito. •

SCHEMA DELL'ALGORIMO DETERMINISTICO

Vediamo adesso come si possono sfruttare tali informazioni per costruire un algoritmo analogo a quello probabilistico, ma che presenti la caratteristica di essere deterministico.

Se nella procedura di calcolo del massimo comun divisore di ideali, si ha che vale $\xi_p^{j_i} \neq 1$ per un certo i, allora si consideri l'elemento α_i corrispondente e lo si denoti γ. Ricordiamo inoltre che gli α_i non sono altro che $\sigma(J_p(q))$, cioé i coniugati di $J_p(q)$,con p,q primi tali che $p|(q-1)$, ed indichiamo con $m(\sigma,q)$ l'intero $0<m(\sigma,q)\leq p-1$, tale che:

$$\gamma^{m(\sigma,q)(n^f-1)/p^s} \equiv \sigma(J_p(q))^{(n^f-1)/p^s} \pmod I$$

dove I é l'ideale determinato col processo di M.C.D. di ideali. Si noti che un tale $m(\sigma,q)$ esiste perché $\xi_p^{j_i}$ é una radice primitiva p-esima dell'unità.

Se, d'altra parte, ogni $\xi_p^{j_i}=1$, allora poniamo $\gamma=\alpha_1$ e poniamo $m(\sigma,q)=0 \ \forall\sigma,q$.

A tal punto possediamo tutti gli elementi per poter valutare $Ind_q(r) \pmod p$, dove r divisore primo di n. Infatti, se R é un primo che divide I e (r), e se l'ordine di r (mod p) é $d_p=d$, allora si ha che (come nel passo **B.3**) :

$$\left(\frac{J_p(q)}{r}\right)_p = \left(\frac{r}{J_p(q)}\right)_p = \left(\frac{r}{J}\right)_p^{\theta'_{ab}}$$

dove θ'_{ab} é come in **A.3** e $J=(q,\xi_p-\left(t_q^{\frac{q-1}{p}}\right))$ é il primo "canonico" su q.
D'altra parte, poiché $(r)^d=\prod_{j=1..p-1}(\sigma_j(R))$, $\sigma_j\in Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ (dipende dal fatto che r non ramifica e dal Teorema 2.5.3), si ha che, per il Lemma 5.1.2 : (se indichiamo σ_j^{-1} con ω_j)

$$\left(\frac{J_p(q)}{r}\right)_p^d = \prod_{j=1}^{p-1}\left(\frac{J_p(q)}{(\sigma_j(R))_p}\right) = \prod_{j=1}^{p-1}\sigma_j\left(\omega_j\left(\frac{J_p(q)}{R}\right)_p\right) = \prod_{j=1}^{p-1}\left(\frac{\omega_j(J_p(q))}{R}\right)_p^j =$$

$$= \prod_{j=1}^{p-1}\left(\frac{\gamma}{R}\right)_p^{jm(\omega_j,q)} = \left(\frac{\gamma}{R}\right)_p^{\sum_{j=1}^{p-1}jm(\omega_j,q)} .$$

Purtroppo non conosciamo né $\left(\frac{\gamma}{R}\right)_p$ né d, ma se $i=i_p$ é tale che $\left(\frac{\gamma}{R}\right)_p=\xi_p^i$, allora abbiamo che:

$$Ind_q(r)\equiv i(d\theta'_{a,b})^{-1}\sum_{j=1}^{p-1}jm(\omega_j,q) \pmod p.$$

Quindi possiamo concludere che $\exists$ k, $1\le k\le f(n)$, tale che :

$Ind_q(r)\equiv k(\theta'_{a,b})^{-1}\sum_{j=1}^{p-1}jm(\omega_j,q) \pmod p$ per ogni coppia p,q di primi tali che $p|(q-1)$

(chiaramente tale k verifica $k\equiv i_p d_p^{-1} \pmod p$ per ogni p ed una soluzione di tale sistema di congruenze esiste per il Teorema Cinese dei Resti).

DESCRIZIONE DELL'ALGORITMO DETERMINISTICO

A'. PASSO DI PREPARAZIONE : identico al punto **A** della versione probabilistica.

B'. PASSO ESTRATTIVO:

B'.1 Per ogni $p\in I(n)$ eseguire la procedura M.C.D. in $\mathbb{Q}(\xi_p)$ rispetto ad n e all'insieme formato dagli elementi del tipo $\sigma(J_p(q))$ con $q\in E(n)$ e $\sigma\in Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$.
In tal modo o si prova che n é composto oppure si costruisce un ideale proprio I di $\mathbb{Z}[\xi_p]$, un intero $s\ge1$ e degli interi $j(\sigma,q)$, $1\le j(\sigma,q)\le p$, tali che valgano :

i) $(\sigma(J_p(q))^{(n^f-1)/p^s} \equiv \xi_p^{j(\sigma,q)} \pmod I \quad \forall\ \sigma\in Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$

ii) o $\xi_p^{j(\sigma,q)} \neq 1$ per qualche σ oppure $p \mid \frac{n^f-1}{p^s}$

dove $f = \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^*}(n)$.

B'.2 $\forall\, p \in I(n)$ si faccia ciò che segue:
Se qualche $j(\sigma_0,q_0) \neq p$ denotiamo con γ l'elemento $\sigma_0(J_p(q_0))$. Per tutti i σ,q costruiamo poi gli interi $m(\sigma,q)$, $0 \leq m(\sigma,q) \leq p-1$, tali che :

$$\gamma^{m(\sigma,q)(n^f-1)/p^s} \equiv \sigma(J_p(q))^{(n^f-1)/p^s} \pmod{I}.$$

Se tutti i $j(\sigma,q)$ sono uguali a p, allora si fissano tutti gli $m(\sigma,q)=0$.

C' PASSO DI CONSOLIDAMENTO

Per ogni k, $1 \leq k \leq f(n)$, si eseguano i punti **C'.1-C'.4**

C'.1 Per ogni $q>2$ si usi il Teorema Cinese dei Resti per calcolare I(k,q) tale che :

$$I(k,q) \equiv k(\theta'_{a,b})^{-1} \sum_{j=1}^{p-1} j m(\omega_j,q) \pmod{p} \quad \forall p \mid (q-1).$$

Fissiamo inoltre $I(k,2)=1$.

C'.2 Per ogni $q>2$ calcolare $r(k,q) \equiv t_q^{I(k,q)} \pmod{q}$.

C'.3 Col Teorema Cinese dei Resti calcolare $r(k) \equiv r(k,q) \pmod{q}$.

C'.4 Controllare se $r(k) \mid n$. Se ciò avviene e $r(k) \neq 1$, allora n é composto e l'algoritmo termina. Altrimenti si ripete il ragionamento ripartendo da **C'.1** con un altro valore di k.

C'.5 Dichiarare n primo.

VALUTAZIONE EURISTICA DELLA COMPLESSITA'

La valutazione euristica della complessità computazionale dell'algoritmo deterministico é del tutto analoga a quella effettuata per la versione probabilistica, perché, per quanto detto all'inizio del presente paragrafo, la procedura di M.C.D. di ideali ha complessità polinomiale in f(n). Si conclude allora che, se n è primo, il tempo di esecuzione T(n) é almeno f(n), cioé $T(n) \geq f(n)$, e che, se n composto, esiste una costante $c>0$ tale che $T(n) \leq f(n)^c$.

5.2. VERSIONE DI LENSTRA

Il problema principale che si presenta nella versione originale dell'algoritmo é la difficoltà di implementazione (soprattutto per la versione deterministica) .
Un tipo di approccio diverso, basato sulle proprietà delle somme di Gauss, é stato sviluppato da Lenstra in modo da semplificare l'algoritmo e da renderlo più facilmente implementabile. L'idea base utilizzata da Lenstra é derivata dal seguente Lemma di banale dimostrazione :

Lemma 5.2.1 : *p é primo se e solo se tutti i suoi divisori sono potenze di p stesso.*

In pratica si cercherà di dimostrare che tutti i divisori di un intero n sono potenze di n stesso in un certo anello $(\mathbb{Z}/_{s\mathbb{Z}})^*$. Se $s>\sqrt{n}$, allora, per provare la primalità di n, basta controllare se nessuno degli elementi $n^2,..,n^{k-1}$ divide n stesso (k tale che $ord((\mathbb{Z}/_{s\mathbb{Z}})^*|k)$. Ovviamente l'algoritmo é efficiente se il numero dei possibili divisori da testare non é troppo grande (cioé se s é abbastanza piccolo).
Vediamo adesso l'algoritmo di Lenstra sia nella versione probabilistica che in quella deterministica.

ALGORITMO DI LENSTRA

D'ora in poi indicheremo con s il prodotto $\prod_{(q-1)|f(n)} q$, q primo, dove f(n) é come nella versione originale. Prendiamo inoltre p primo tale che p|f(n), e che, se q primo, q|s, si abbia p|(q-1). Ovviamente p e q non devono dividere n, altrimenti non ha senso continuare a investigare la primalità di n.

Definizione 5.2.1: *Definiamo CARATTERE di ordine p e conduttore q, un qualunque omomorfismo surgettivo di gruppi* $\chi : (\mathbb{Z}/_{q\mathbb{Z}})^* \rightarrow \langle \xi_p \rangle$ *(dove* ξ_p *é una radice primitiva p-esima dell'unità).*
Un carattere χ *viene detto PRINCIPALE se* $\chi(a)=1 \ \forall a \in (\mathbb{Z}/_{q\mathbb{Z}})^*$.

Definizione 5.2.2 : *Dato un carattere* χ *di ordine p e conduttore q, definiamo SOMMA DI GAUSS l'elemento di* $\mathbb{Q}(\xi_p, \xi_q)$ *dato da*

$$\tau(\chi) = -\sum_{x=1.}^{q-1} \chi(x)\xi_q^x.$$

Notiamo che, in realtà, $\tau(\chi) \in \mathbb{Z}[\xi_p, \xi_q]$.

Vediamo adesso alcune proprietà delle somme di Gauss:

Lemma 5.2.1:

1) $\tau(\chi)^p \in \mathbb{Z}[\xi_p]$

2) $\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi})$

3) $|\tau(\chi)| = \sqrt{q}$

4) *se n é primo, allora* $(\tau(\chi))^n \equiv -(\chi(n))^{-n}\ \tau(\chi^n) \pmod{n}$.

Dim: 1) sia σ_b: $\mathbb{Q}(\xi_p,\xi_q)\to \mathbb{Q}(\xi_p,\xi_q)$ l'omomorfismo determinato da $\sigma_b(\xi_q)=\xi_q^b$ e $\sigma_b/\mathbb{Q}(\xi_p)$ = identità.

Allora $\sigma_b(\tau(\chi)) = \sigma_b(-\sum_{x=1}^{q-1}\chi(x)\xi_q^x) = -\sum_{x=1}^{q-1}\chi(x)\xi_q^{bx}$ =

$$= (-\sum_{u=1}^{q-1}\chi(u)\xi_q^u)\chi(b^{-1}) = \tau(\chi)\cdot(\chi(b))^{-1}.$$

Allora $\sigma_b(\tau(\chi)^p)= (\tau(\chi)^p)\cdot(\chi(b))^{-p} = \tau(\chi)^p$ e quindi $\tau(\chi)^p\in\mathbb{Z}[\xi_p]$.

2) $\overline{\tau(\chi)}=\overline{\chi}(-1)\tau(\overline{\chi})=\chi(-1)\tau(\overline{\chi})$ perché $\chi(-1)\in\mathbb{Q}\cdot$

3) Useremo tre fatti di banale dimostrazione :

i) il coniugio di $\chi(x)$ é dato da $\chi(x)^{-1}$

ii) $\sum_{x=1}^{q-1}\chi(x)=0$

iii) $\sum_{u=1}^{q-1}\xi_q^{uw} = q-1$ se $q|w$ e $\sum_{u=1}^{q-1}\xi_q^{uw}= -1$ se $q\nmid w$.

Allora si ha che :

$|\tau(\chi)|^2 = \sum_{x=1}^{q-1}\sum_{u=1}^{q-1}\chi(x)\chi^{-1}(u)\xi_q^{x-u}$ = (sostituendo a x la quantità xu)

$= \sum_{x=1}^{q-1}\sum_{u=1}^{q-1}\chi(xu)\chi(u^{-1})\xi_q^{u(x-1)}$= (fisso x=1 e divido la doppia sommatoria)

$= (-\sum_{x=2}^{q-1}\chi(x))+(q-1)\chi(1) = \chi(1)+(q-1)\chi(1)=q.$

4) Utilizzando il fatto che, se n è primo, in $(\mathbb{Z}/_{n\mathbb{Z}})^*$ si ha che $(a+b)^n\equiv a^n+b^n \pmod n$ per ogni $a,b\in(\mathbb{Z}/_{n\mathbb{Z}})^*$, si ottiene facilmente che:

$$(\tau(\chi))^n \equiv (-\sum_{x=1}^{q-1}(\chi(x))^n.\xi_q^{nx}) \pmod n \equiv \tau(\chi^n)\cdot(\chi(n))^{-n}. \quad \bullet$$

5.2.1 ALGORITMO PROBABILISTICO DI LENSTRA

Da questo punto in poi indichiamo con R l'anello $\mathbb{Z}[\xi_p,\xi_q]$.
Costruiamo adesso un test di primalità che sfrutti le due seguenti condizioni:

1 $\exists\ \eta(\chi)\in<\xi_p>$ tale che $(\tau(\chi))^n \equiv -(\eta(\chi))^{-n}\ \tau(\chi^n) \pmod{nR}$ $\forall p,q,\chi$. (dove per $\eta(\chi)\in<\xi_p>$ si intende $\eta(\chi)$ appartenente all'immagine di $<\xi_p>$ in $\mathbb{Z}[\xi_p,\xi_q]$).

2 condizione su p (non é facilmente verificabile)

$$\forall r|n \text{ si abbia } l_p(r):=\frac{r^{p-1}-1}{n^{p-1}-1}\in\mathbb{Z}_p.$$

(dove col simbolo $\mathbb{Z}_p$ si intende l'anello degli interi p-adici, cfr. Capitolo 2).

NOTA BENE:

a) la condizione **2** é equivalente a:

2' $\forall r|n$ si abbia $v_p(r^{p-1}-1)\geq v_p(n^{p-1}-1)$

(dove per v_p si intende la valutazione p-adica).

Infatti se vale \x(**2**) allora si ha che r\s\up3(p-1)-1 = $l_p(r)\cdot$(n\s\up3(p-1)-1) e quindi v\s\do6(p)(r\s\up3(p-1)-1) = v\s\do6(p)($l_p(r)\cdot$(n\s\up3(p-1)-1)) = $v_p(l_p(r))+v_p(n^{p-1}-1)\geq v_p(n^{p-1}-1)$ perché $\mathbb{Z}_p=\{x\in\mathbb{Q}_p \text{ t.c. } v_p(x)\geq 0\}$ (cfr. Capitolo 2.).
Viceversa, se vale **2'**, allora si ha:

$$v_p(r^{p-1}-1)- v_p(n^{p-1}-1)\geq 0$$

ed allora, per le proprietà di v_p, ciò equivale a $v_p\left(\frac{r^{p-1}-1}{n^{p-1}-1}\right)\geq 0$ e quindi si ha che $\left(\frac{r^{p-1}-1}{n^{p-1}-1}\right)\in\mathbb{Z}_p$.

b) L'equivalenza provata in **a**) consente di affermare che, perché **2** sia verificata per ogni divisore di n, basta verificarla solo sui divisori primi di n.
Infatti, se si considera $l'_p(r)=l_p(r) \pmod p$, si ha che $l'_p(rr')=l'_p(r)+l'_p(r')$ e che $l'_p(r)\in(\mathbb{Z}_p/p\mathbb{Z}_p)=(\mathbb{Z}/p\mathbb{Z})$.

Proposizione 5.2.1: *Se valgono* **1** *e* **2**, *allora si ha che* $\chi(r)=(\eta(\chi))^{l_p(r)}$ $\forall r|n$. *In particolare* $\chi(n)=\eta(\chi)$ *(e quindi il teorema si potrebbe anche formulare :* $\chi(r)=(\chi(n))^{l_p(r)}$ $\forall r|n$ *).*

Dim: Consideriamo $\sigma:\mathbb{Z}[\xi_p,\xi_q]\to\mathbb{Z}[\xi_p,\xi_q]$ l'omomorfismo definito da : $\sigma(a)=a$ $\forall a\in\mathbb{Z}(\xi_q)$ e da $\sigma(\xi_p)=(\xi_p)^{n^i}$ con $i\in\mathbb{N}$.
Applicando allora σ ad entrambi i membri di **1** si ha:

$$\alpha)\ (\tau(\chi^{n^i}))^n\equiv(\eta(\chi))^{-n^{i+1}}\cdot\tau(\chi^{n^{i+1}}) \pmod{nR} \quad \forall i\in\mathbb{N}.$$

Proviamo adesso per induzione che vale la seguente congruenza :

$$\beta)\ (\tau(\chi))^{n^i}\equiv(\eta(\chi))^{-in^i}\cdot\tau(\chi^{n^i}) \pmod{nR} \quad \forall i\in\mathbb{N}.$$

Per i=0 la congruenza β) diventa $\tau(\chi)\equiv\tau(\chi) \pmod{nR}$.
Sia vera la congruenza β) per i-1, la provo per i:
per ipotesi induttiva si ha che:

$$(\tau(\chi))^{n^{i-1}}\equiv(\eta(\chi))^{-(i-1)n^{i-1}}\cdot\tau(\chi^{n^{i-1}}) \pmod{nR}$$

e si noti che :

$(\tau(\chi))^{n^i} = ((\tau(\chi))^{n^{i-1}})^n \equiv \left((\eta(\chi))^{-(i-1)n^{i-1}} \cdot \tau(\chi^{n^{i-1}})\right)^n = (\eta(\chi))^{-(i-1)n^i} \cdot (\tau(\chi^{n^{i-1}}))^n =$
(per la congruenza **α**))

$$=(\eta(\chi))^{-(i-1)n^i} \cdot (\eta(\chi))^{-n^i} \cdot \tau(\chi^{n^i}) = (\eta(\chi))^{-in^i} \cdot \tau(\chi^{n^i}) \pmod{nR}.$$

Ciò conclude la prova della congruenza **β**).
Poniamo adesso i=p-1 in **β**), allora si ha :

$$(\tau(\chi))^{n^{p-1}} \equiv (\eta(\chi))^{-(p-1)n^{p-1}} \cdot \tau(\chi^{n^{p-1}}) = (\eta(\chi))^{-pn^{p-1}} \cdot (\eta(\chi))^{n^{p-1}} \cdot \tau(\chi^{n^{p-1}}).$$

Ma poiché $\eta(\chi) \in <\xi_p>$ e $n^{p-1} \equiv 1 \pmod p$, si ha allora che:

$$(\tau(\chi))^{n^{p-1}} \equiv \eta(\chi) \cdot \tau(\chi) \pmod{nR}.$$

Osservo adesso che, siccome $|\tau(\chi)| = \sqrt{q}$, $\tau(\chi)$ é invertibile e quindi si ha:

$$(\tau(\chi))^{n^{p-1}-1} \equiv \eta(\chi) \pmod{nR}.$$

Sia ora r un divisore primo di n, allora si ha che :
$(\tau(\chi))^{n^{p-1}-1} \equiv \eta(\chi) \pmod{rR}$ e che $(\tau(\chi))^{r^{p-1}-1} \equiv \chi(r) \pmod{rR}$ e quindi si ottiene banalmente che $\chi(r) \equiv (\eta(\chi))^{l_p(r)} \pmod{rR}$, ma poiché sia $\chi(r)$ che $\eta(\chi)$ sono radici primitive p-esime dell'unità, si ha che $\chi(r) = (\eta(\chi))^{l_p(r)}$. ●

Osservazione :
Nella dimostrazione sono stati presi in considerazione solo i divisori primi di n perché, essendo $\eta(\chi)$ una radice primitiva p-esima dell'unità, il suo esponente é significativo solo modulo p e l'$_p(r)$ é moltiplicativo. Sfruttando tali proprietà si ottiene il risultato voluto per tutti i divisori di n e per n stesso.

Abbiamo già osservato che la condizione **2** non é facilmente verificabile. Cerchiamo allora di ottenere delle condizioni sufficienti per **2** .

Lemma 5.2.1: *Se $p^2 \nmid (n^{p-1}-1)$ allora* **2** *é vera.*

Dim: L'ipotesi del Lemma significa che $v_p(n^{p-1}-1)=1$. Inoltre, per il Piccolo Teorema di Fermat, si ha che $p|(n^{p-1}-1)$, e quindi $v_p(r^{p-1}-1) \geq 1$. Allora vale **2'** che é però equivalente a **2** . ●

Lemma 5.2.2: *Se la condizione* **1** *é vera con $\eta(\chi) \neq 1$, allora la condizione* **2** *é vera.*

Dim: Nella dimostrazione della Proposizione 5.2.1 abbiamo provato che:

$$(\tau(\chi))^{r^{p-1}-1} \equiv \chi(r) \pmod{rR} \ \forall r|n, \ r \text{ primo}.$$

Sia adesso ω l'ordine di $\tau(\chi)$ (mod rR) in $(R/rR)^*$. Si noti che, per la congruenza precedente, si ha $\omega | p(r^{p-1}-1)$. Sempre nella dimostrazione della Proposizione 5.2.1 abbiamo provato che:
$(\tau(\chi))^{n^{p-1}-1} \equiv \eta(\chi) \pmod{rR}$. Ma poiché $\eta(\chi) \neq 1$, si ha che $\omega | p(n^{p-1}-1)$ e che $\omega \nmid (n^{p-1}-1)$.
Abbiamo allora che $v_p(\omega) = v_p(p(n^{p-1}-1))$ e che $v_p(\omega) \leq v_p(p(r^{p-1}-1))$.
Quindi abbiamo che :
$v_p(p(n^{p-1}-1)) = 1+v_p((n^{p-1}-1)) \leq v_p(p(r^{p-1}-1)) = 1+v_p((r^{p-1}-1))$ da cui si trae la tesi. ●

Il problema che si presenta adesso é quindi quello di determinare un carattere χ per cui la $\boxed{1}$ vale con $\eta(\chi)\neq 1$. Purtroppo un metodo efficiente per determinare un tale carattere é subordinato alla validità dell'Ipotesi Generalizzata di Riemann. Si può però notare che la probabilità che un carattere χ, scelto casualmente, verifichi $\boxed{1}$ con $\eta(\chi)\neq 1$ é data da $1-\frac{1}{p}$. Infatti, da quanto detto precedentemente, possiamo valutare la probabilità che χ verifichi $\boxed{1}$ con $\chi(n)\neq 1$. Supponiamo che χ non sia principale (altrimenti $\chi(n)=1$) e consideriamo g un generatore di $(\mathbb{Z}/_{q\mathbb{Z}})^*$; allora $\chi(g)=\xi_p{}^m$, $m\in\{1...p-1\}$.

Supponiamo che $n\not\equiv 1 \pmod q$ e che $n\equiv g^j \pmod q$. Allora si ha:

$\chi(n)=\chi(g^j)=\left[\chi(g)\right]^j=\xi_p{}^{mj}\neq 1 \Leftrightarrow p\not| mj \Leftrightarrow p\not| j$.

La condizione $p|j$ equivale ad affermare che $n^{\frac{q-1}{p}}\equiv 1 \pmod q$.

Abbiamo quindi due condizioni su n (e quindi su χ) :

1) $n\not\equiv 1 \pmod q$;

2) $n^{\frac{q-1}{p}}\not\equiv 1 \pmod q$.

Notiamo però che la condizione **2**) implica la condizione **1**) e quindi la condizione significativa su χ è :

$$\boxed{*}\quad n^{\frac{q-1}{p}}\not\equiv 1 \pmod q.$$

Ricordiamo inoltre che si deve avere $q\equiv 1 \pmod p$. Tali congruenze significano che q splitta completamente in $\mathbb{Q}(\xi_p)$, ma non splitta completamente in $\mathbb{Q}(\xi_p, n^{1/p})$. Questa affermazione dipende dal Ribemboim [33], Teorema 6B, pag. 277. Dopo aver osservato che $[\mathbb{Q}(\xi_p, n^{1/p}):\mathbb{Q}(\xi_p)]=p$, basta applicare il Teorema sulla densità dei primi che splittano completamente (cfr. Capitolo 2) per ottenere che l'insieme dei primi verificanti $\boxed{*}$ e $q\equiv 1 \pmod p$ ha densità pari a $\frac{1}{p-1}\cdot\frac{p-1}{p}=\frac{1}{p}$. Allora un primo $q\in E(n)$ scelto casualmente ha probabilità di verificare $\boxed{*}$ pari a $1-\frac{1}{p}$.

A tal punto vediamo che, se vale la Proposizione 5.2.1, si può, utilizzando il Teorema Cinese dei Resti, determinare un intero l(r) tale che $l(r)\equiv -l_p(r) \pmod p$ $\forall p\in I(n)$.

Si noti che $l(r)\in[0,..,f(n)-1]$, perché $f(n)=\prod_{p\in I(n)} p$ per definizione.

Allora, poiché $\chi(n)$ é una radice primitiva p-esima dell'unità, si ha che $\chi(rn^{l(r)})=\chi(r)\cdot\chi(n)^{l(r)}=1$ e quindi $rn^{l(r)}\in Ker(\chi)$ $\forall p,q$ tali che $p|(q-1)$.

Proviamo adesso che, fissato un q, poiché q-1 é squarefree si ha

$$\bigcap_{p|(q-1)} (Ker(\chi))=1 \text{ (p primo)}.$$

Infatti, se $x\in \bigcap_{p|(q-1)} (Ker(\chi))=1$ (p primo), abbiamo che $\chi(x)=1$ $\forall p|(q-1)$, p primo. Però, se g è un generatore di $(\mathbb{Z}/_{q\mathbb{Z}})^*$ e se $x=g^{j_q}$ con $j_q\leq q-1$, abbiamo che $\chi(x)=\xi_p{}^{mj_q}$, $m\in\{1,...,p-1\}$, e

quindi $\xi_p^{j_q}=1$. Da ciò segue allora che $p|j_q \ \forall p$ e quindi che $(q-1)|j_q$. Ma allora $j_q=q-1$ e quindi $x=1$.
Abbiamo allora che $r n^{l(r)} \equiv 1 \pmod q \ \forall q \in E(n)$, ma, applicando il Teorema Cinese dei Resti, si ha $r n^{l(r)} \equiv 1 \pmod s$. Siccome $l(r)$ é definito modulo $f(n)$, si ottiene quindi che $r \equiv n^i \pmod s$, con $i=f(n)-l(r)$.

Utilizzando la trattazione sopra esposta si può allora costruire un algoritmo di primalità come segue:

SCHEMA DELL'ALGORITMO PROBABILISTICO DI LENSTRA

a) dato n in input

b) calcolare I(n), E(n),f(n) ed s in modo che $s>\sqrt{n}$. (Tale passo viene svolto in modo analogo al passo **A.1** della versione originale).

c) $\forall$ $p \in I(n)$ ripetere i passi **c1)**, **c2)**, **c3)** finché non si ha successo.

> **c1)** $\forall$ $q \in E(n)$ scegliere un carattere $\chi:(\mathbb{Z}/_{q\mathbb{Z}})^* \rightarrow <\xi_p>$.
> (Ciò può venir fatto scegliendo $\chi(t_q)$, dove t_q é una radice primitiva di $(\mathbb{Z}/_{q\mathbb{Z}})^*$ calcolata come nel passo **A.2** della versione originale).
>
> **c2)** controllare se χ verifica $\boxed{1}$. Se verifica si passa al punto **c3)**, altrimenti si ritorna al punto **c1)** e si sceglie un altro χ.
>
> **c3)** controllare se $\eta(\chi) \neq 1$. Se verifica si passa al punto **d)**, altrimenti si ritorna al punto **c1)** e si sceglie un altro χ.

d) cambiare p e ritornare al punto **c)** fino a quando non sono stati esauriti tutti gli elementi di I(n).

e) calcolare n (mod s), n^2 (mod s),..., $n^{f(n)-1}$ (mod s).

f) se nessuno dei residui calcolati al punto **e)** divide n, allora n é primo, altrimenti n è composto.

ANALISI EURISTICA DELLA COMPLESSITA' E VALUTAZIONE PROBABILISTICA

Da quanto detto precedentemente, abbiamo che l'algoritmo, se termina, dichiara correttamente se n é primo o composto. Notiamo come ogni passo dell'algoritmo precedentemente descritto possa essere calcolato, se portato a termine con successo, in tempo polinomiale in f(n). Quindi anche la versione modificata da Lenstra, ha, come entrambe le versioni originali, la caratteristica di essere polinomiale in f(n).
Si noti inoltre che il carattere probabilistico dell'algoritmo dipende solamente dalla scelta del carattere χ di ordine p e conduttore q che verifichi $\eta(\chi) \neq 1$. Tale osservazione ci consente quindi di affermare che, se n é primo, $\exists$ una costante $c_1>0$ tale che $\forall k \geq 1$ l'algoritmo termina in $T_k(n)$ passi, $f(n) \leq T_k(n) \leq k f(n)^{c_1}$, con probabilità maggiore di $1-\frac{1}{2^k}$.

Si noti che é possibile migliorare un poco l'efficienza dell'algoritmo sostituendo alla condizione $s>\sqrt{n}$ la condizione $s>\sqrt[3]{n}$. Infatti Lenstra [22] ha provato che :

Teorema 5.2.2 : *Siano r,s,n degli interi tali che $0\le r<s<n$ e $s>\sqrt[3]{n}$ e (s,r)=1. Allora esistono al più 11 divisori positivi di n che sono congrui a r (mod s) ed esiste un algoritmo polinomiale che li calcola.*

Dim: cfr. Lenstra [22]. ●

5.2.2 ALGORITMO DETERMINISTICO DI LENSTRA

L'unico punto per cui la versione precedente é da considerarsi probabilistica é il calcolo di un carattere χ di ordine p e conduttore q che verifichi **1** con $\eta(\chi)\neq 1$. Tale problema può però essere eliminato impostando i fondamenti matematici dell'algoritmo in modo un poco diverso.
Nel seguito manteniamo le notazioni utilizzate in precedenza ed inoltre consideriamo due interi h ed u tali che: $n^{p-1}-1=p^h u$ e $p^h \| (n^{p-1}-1)$ (cioé $h= v_p(n^{p-1}-1)$).
Consideriamo adesso i seguenti elementi di $\mathbb{Z}[\xi_p]$:

$$(\tau(\chi))^p u,(\tau(\chi))^{p^2} u,...,(\tau(\chi))^{p^h} u.$$

Tali elementi appartengono a $\mathbb{Z}[\xi_p]$ perché, per la proprietà **1**) del Lemma 5.2.1, si ha che $(\tau(\chi))^p \in \mathbb{Z}[\xi_p]$.
Osserviamo adesso che, se n é primo, allora, per quanto visto nella dimostrazione della Proposizione 5.2.1, si ha, se χ é un carattere di ordine p e conduttore q, che :

$$(\tau(\chi))^{p^h} u \equiv \chi(n) \pmod{nR}$$

Quindi come prima condizione (sostitutiva della **1** della versione probabilistica) si considera:

i $\exists\, \eta(\chi)\in<\xi_p>$ tale che $(\tau(\chi))^{p^h} u \equiv \eta(\chi) \pmod{nR}$.

Se **i** é vera, allora possiamo considerare

$$w(\chi)=\min\left\{ i\in\{1..h\} \text{ t.c. } \exists \eta(\chi)\in<\xi_p> \text{ t.c.} (\tau(\chi))^{p^i} u \equiv \eta(\chi) \pmod{nR} \right\}.$$

Ha senso procedere a tale operazione di minimo perché l'insieme é non vuoto (abbiamo supposto che **i** sia vera).

Diamo adesso una seconda condizione (sostitutiva della **2** della versione probabilistica):

ii se $w(\chi)\ge 2$ e $(\tau(\chi))^{p^{w(\chi)}} u \equiv 1 \pmod{nR}$, allora $\forall j\in\{0,..,h-1\}$ l'elemento :

$$b_j = (\tau(\chi))^{p^{w(\chi)-1}} u - \xi_p^{\,j} \in \mathbb{Z}[\xi_p]$$

ha, se espresso nella base $\{1,\xi_p,...,\xi_p^{p-2}\}$ di $\mathbb{Z}[\xi_p]$ su $\mathbb{Z}$, un coefficiente coprimo con n.

La condizione **ii** é giustificata dalla definizione stessa di $w(\chi)$: infatti ogni b_j ha almeno un coefficiente non divisibile per n.
La condizione **ii** può essere testata con una serie di massimi comun divisori. Nel caso in cui la condizione **ii** non valga, durante il suo test viene determinato un divisore non banale di n.

Proposizione 5.2.2:

Se **i** *e* **ii** *sono verificate allora* $\forall r|n$, *r primo, si ha che* $r^{p-1} \equiv 1 \pmod{p^{w(\chi)}}$.

Dim: Se $w(\chi)=1$ allora la tesi é vera per il Piccolo Teorema di Fermat.
Sia adesso $w(\chi)\geq 2$.
Dividiamo la dimostrazione in due casi:

se $(\tau(\chi))p^{w(\chi)}u \not\equiv 1 \pmod{nR}$, allora, ponendo con $\omega = \text{ord}\,(\tau(\chi) \pmod{rR})$, si ha che $\omega | p(r^{p-1}-1)$ perché si ha, per quanto visto nella Proposizione 5.2.1, che:

$$(\tau(\chi))r^{p-1-1} \equiv \chi(r) \pmod{rR}.$$

Inoltre, poiché $\eta(\chi) \neq 1$, si ha che $\omega | p^{w(\chi)+1}u$ e che $\omega \nmid p^{w(\chi)}u$.
Ciò significa che $v_p(p(r^{p-1}-1)) \geq v_p(\omega) = v_p(p^{w(\chi)+1}u) = w(\chi)+1$ e quindi si ottiene che $(p^{w(\chi)+1}) | p(r^{p-1}-1)$.
Poiché $w(\chi)\geq 2$, si ha che $p^{w(\chi)} | (r^{p-1}-1)$ e quindi si ha la tesi.
Se $(\tau(\chi))p^{w(\chi)}u \equiv 1 \pmod{nR}$, allora per assurdo si supponga che $p^{w(\chi)} \nmid (r^{p-1}-1)$. Allora, poiché si ha la seguente :

$$\tau(\chi)^{p(r^{p-1}-1)} \equiv 1 \pmod{rR},$$

si ha, analogamente al caso precedente, poichè $\omega | p^{w(\chi)}u$ e $\omega \nmid p^{w(\chi)-1}u$, che $v_p(p(r^{p-1}-1)) \geq v_p(p^{w(\chi)}u) = w(\chi)$ e quindi si ha che :

$$v_p(r^{p-1}-1) \geq w(\chi)-1.$$

Per l'ipotesi assurda, si ha anche che $v_p(r^{p-1}-1) < w(\chi)$ ed allora $v_p(r^{p-1}-1) = w(\chi)-1$.

Da ciò si deduce che $\exists$ t, $p \nmid t$, tale che $tp^{w(\chi)-1} = r^{p-1}-1$ e quindi si ha che $\frac{(p^{w(\chi)-1}u)}{(r^{p-1}-1)} = ut^{-1}$.
Allora, ponendo $a=ut^{-1}$ (dove per t^{-1} si intende l'inverso di t modulo p) e b un qualunque intero congruo a 1 modulo p, si ha $\frac{(p^{w(\chi)-1}u)}{(r^{p-1}-1)} = \frac{a}{b}$. Allora si ha che :

$$(\tau(\chi)p^{w(\chi)-1}u) \equiv (\tau(\chi)p^{w(\chi)-1}ub) \equiv (\tau(\chi)^{a(r^{p-1}-1)}) \equiv (\chi(r))^a = \xi_p^{\,j} \pmod{rR}$$

per un j opportuno, $j \in \{0,..,p-1\}$.
Ma allora tutti i coefficienti di tale b_j sono divisibili per r, e quindi nessuno di essi é coprimo con n. Si ha allora una contraddizione, e si conclude. ●

Supponiamo adesso che **i** sia vera e consideriamo w in intero fissato tale che $w(\chi) \leq w \leq h$ e che $r^{p-1} \equiv 1 \pmod{p^w}$ $\forall r|n$, r primo. Notiamo che , se vale **ii**, allora un tale intero esiste perché $w(\chi)$ verifica quanto chiesto sopra per la Proposizione 5.2.2.

Definiamo adesso $m_p(r):=\frac{r^{p-1}-1}{p^w u}$ (é un elemento di $\mathbb{Z}_p$ perché si ha che $v_p(m_p(r))=v_p(r^{p-1}-1)-v_p(p^w u)\geq w-w=0$).

Inoltre definiamo anche $\eta'(\chi)\in<\xi_p>$ come l'elemento determinato da :

$$(\tau(\chi)p^w u)\equiv\eta'(\chi) \pmod{nR}.$$

Proposizione 5.2.3: *Con le ipotesi e le notazioni sopra esposte si ha che* $\chi(r)=\eta'(\chi)^{m_p(r)}$ $\forall r|n$. *Inoltre si ha* $\chi(n)=\eta(\chi)$.

Dim: Supponiamo che r|n, r primo. Allora per ipotesi si ha che:

$$(\tau(\chi)p^w u) \equiv \eta'(\chi) \pmod{rR}$$

ed

$$(\tau(\chi)^{(r^{p-1}-1)}) \equiv \chi(r) \pmod{rR}.$$

Quindi abbiamo che :

$$\chi(r) \equiv (\tau(\chi)^{(r^{p-1}-1)}) = (\tau(\chi)p^w u)^{m_p(r)} \equiv (\eta'(\chi))^{m_p(r)} \pmod{rR}.$$

Ma, notando che $\chi(r)$ che $\eta'(\chi)$ sono radici primitive p-esime dell'unità, si può allora affermare che $\chi(r)= (\eta'(\chi))^{m_p(r)}$.

La tesi per ogni divisore di n si prova in modo analogo a quello della Proposizione 5.2.1.

Inoltre si ha anche che $\chi(n)=(\eta'(\chi))^{m_p(n)}$. Ma $m_p(n)=\frac{p^h u}{p^w u} = p^{h-w}$.

La tesi si ottiene notando che :

$$\eta(\chi)= (\eta'(\chi))^{p^{h-w}} . \bullet$$

Sfruttando quanto precedentemente esposto si può allora costruire un test di primalità deterministico come segue:

SCHEMA DELL'ALGORITMO DETERMINISTICO DI LENSTRA

a) dato n in input

b) calcolare I(n), E(n),f(n) ed s in modo che $s>\sqrt{n}$. (Tale passo viene svolto in modo analogo al passo **A.1** della versione originale).

c) $\forall$ $p\in I(n)$, fissato, ripetere i passi **c1), c2), c3),c4)** finché non si ha successo.

> **c1)** $\forall$ $q\in E(n)$ t.c. $p|(q-1)$, scegliere un carattere $\chi:(\mathbb{Z}/_{q\mathbb{Z}})^* \rightarrow <\xi_p>$ (ha indice p).
> (Ciò può venir fatto scegliendo $\chi(t_q)$, dove t_q é una radice primitiva di $(\mathbb{Z}/_{q\mathbb{Z}})^*$ calcolata come nel passo **A.2** della versione originale);
>
> **c2)** controllare se χ verifica **i**. Se verifica passare al punto **c3)**, altrimenti ritornare al punto **c1)**.
>
> **c3)** calcolare $w(\chi)$.

c4) calcolare il numero :

$w=\max\{ w(\chi): \chi \text{ determinato in } \mathbf{c1} \text{ e } \mathbf{c2} \ (\chi \text{ ha indice } p)\}$.

Se, per un certo p, nessun χ verifica allora tale passo non viene eseguito e non si considera tale p nel prosieguo.

d) cambiare p e ritornare a **c)** fino a che non si sono esauriti tutti gli elementi di I(n).

e) calcolare tutti gli $\eta'(\chi)$. Si noti che sono ben definiti per come é stato scelto w.

f) con il Teorema Cinese dei Resti determinare l'unico residuo ν (mod s) tale che $\chi(\nu)=\eta'(\chi)$ per ogni χ.
(Si applica il Teorema Cinese dei Resti prima sui residui modulo q (fissato p) e poi su p).

g) Calcolare gli elementi $r_i \in \mathbb{Z}$ tali che $\nu^i \equiv r_i \pmod s$ i=0,..,f(n)-1.

h) Provare a dividere n per tutti gli r_i. Se almeno un r_i divide allora n composto, altrimenti n primo.

GIUSTIFICAZIONE DELLA CORRETTEZZA DELL'ALGORITMO

Per giustificare la correttezza dell'algoritmo osserviamo che, se per assurdo un intero n composto passasse i test precedenti, allora, se r é un divisore non banale di n tale che $r \le \sqrt{n}$, si avrebbe che, per la Proposizione 5.2.3, $\chi(r)=\chi(\nu^{m_p(r)})$ per ogni carattere χ su cui viene effettuato il test. Ma allora , se si definisce $m \in \{0,..,f(n)-1\}$ come l'intero tale che $m \equiv m_p(r) \pmod p$ per ogni $p \in I(n)$, si ha che $r \equiv \nu^m \equiv r_m \pmod s$. Allora, poiché $0 \le r \le \sqrt{n} < s$ e $0 \le r_m < s$, si ha che $r=r_m$ che é in contraddizione con l'ipotesi che n passi i test contenuti nell'algoritmo.

ANALISI EURISTICA DELLA COMPLESSITA'

Da quanto detto precedentemente, abbiamo che l'algoritmo termina con certezza e dichiara correttamente se n é primo o composto. Notiamo come ogni passo dell'algoritmo precedentemente descritto possa essere calcolato, in tempo polinomiale in f(n). Quindi anche la versione deterministica modificata da Lenstra, ha, come entrambe le versioni originali, la caratteristica di essere polinomiale in f(n).

5.3. CALCOLO DELLA COMPLESSITA' UTILIZZANDO METODI ANALITICI

Da quanto esposto fino adesso abbiamo che tutte le versioni presentate dell'algoritmo di Adleman-Pomerance-Rumely hanno complessità polinomiale in f(n). Per poter dare maggiori informazioni sulla complessità computazionale di tali algoritmi bisogna conoscere in modo più dettagliato le caratteristiche della f(n).
Chiaramente la caratteristica di f(n) che ci interessa maggiormente dal punto di vista del calcolo della complessità computazionale é il suo ordine di grandezza.
Il problema che adesso si presenta é quindi quello di ottenere una valutazione dell'ordine di grandezza di tale funzione. Il risultato che proveremo é :

Teorema 5.3.1: *$\forall$ n intero, n>100, esistono due costanti c_1,c_2 positive e calcolabili tali che :*

$$(\lg n)^{c_1(\lg_3 n)} < f(n) < (\lg n)^{c_2(\lg_3 n)}.$$

Il procedimento che seguiremo si baserà su alcuni risultati di Teoria Analitica dei Numeri che ci permetteranno di valutare il numero dei divisori di un intero (fatto necessario per poter ottenere la minorazione sopra scritta) e la distribuzione di numeri primi in una progressione aritmetica (fatto necessari per poter ottenere la maggiorazione sopra scritta).
Dopo aver provato il Teorema 5.3.1, potremo allora concludere che tutte le versioni dell'algoritmo di Adleman-Pomerance-Rumely hanno complessità $O((\lg n)^{c(\lg_3 n)})$, cioè quasi-polinomiale in lgn, come abbiamo affermato all'inizio del Capitolo 5.
Per maggior chiarezza espositiva e perché verranno usati diversi risultati intermedi, la dimostrazione del Teorema 5.3.1 verrà "spezzata" in parti diverse.

Calcolo della minorazione :

Lemma 5.3.1: *$\exists$ una costante c>0 calcolabile tale che, se n>100, si ha :*

$$\lg n^{c(\lg_3 n)} < f(n).$$

Dim: La dimostrazione é basata su una maggiorazione per $d(k)=\#\{d\in\mathbb{N} \text{ tali che } d|k\}$, dove $k\in\mathbb{N}$.
Sia $k=\prod_{i=1..n} p_i^{a_i}$ dove i p_i appartengono ad un certo, opportuno, insieme di primi. Allora, attraverso banali calcoli (cfr. Ramanujan [32], pag. 80) si ha che :

$$d(k) < \frac{\left(\frac{1}{n}\lg(p_1..p_n k)\right)^n}{\lg p_1..\lg p_n}.$$

Sia adesso $k'=2^{a_1}...p^{a_n}$, dove p é l'n-esimo primo. Si noti che d(k)=d(k'). Quindi, definendo $\varpi(x) = \prod_{q\le x} \lg q$ (q primo) e notando che $\vartheta(p)\le \lg k' \le \lg k$, si ha che:

$$d(k)=d(k') < \frac{1}{\varpi(p)}\left(\frac{\lg k'+\vartheta(p)}{\pi(p)}\right)^{\pi(p)} \le \left(1+\frac{\lg k}{\vartheta(p)}\right)^{\pi(p)} \frac{1}{\varpi(p)}\left(\frac{\vartheta(p)}{\pi(p)}\right)^{\pi(p)}.$$

Diamo adesso una stima di $\frac{1}{\varpi(p)}\left(\frac{\vartheta(p)}{\pi(p)}\right)^{\pi(p)}$.
Attraverso facili calcoli si ottiene che : (cfr. Ramanujan [32], pag. 83-84)

$$\int_2^x \left(\frac{1}{u\lg^2 u}\int_2^u \frac{\pi(t)}{t}\,dt\right) du \;>\; \pi(x)\lg\left(\frac{\vartheta(x)}{\pi(x)}\right)-\lg\varpi(x) \quad e$$

$$\pi(x)\lg\left(\frac{\vartheta(x)}{\pi(x)}\right)-\lg\varpi(x) \;>\; \int_2^x \left(\frac{1}{u\lg^2 u}\int_2^u \frac{\pi(t)}{t}\,dt\right) du \;-\; \frac{1}{\vartheta(x)\lg x}\left(\int_2^u \frac{\pi(t)}{t}\,dt\right)^2.$$

Inoltre dal Teorema dei Numeri Primi (cfr. Capitolo 3) si ha che $\pi(x)=O\left(\frac{x}{\lg x}\right)$ e che $\frac{1}{\vartheta(x)}=O\left(\frac{1}{x}\right)$ e quindi, notando che

$$\int_2^x \frac{1}{\lg^a t} = O\left(\frac{x}{\lg^a x}\right) \text{ (se } a\geq 1),$$

si ha che: $\int_2^u \frac{\pi(t)}{t}dt= O\left(\frac{x}{\lg x}\right).$

Allora $\int_2^x \left(\frac{1}{u\lg^2 u}\int_2^u \frac{\pi(t)}{t}\,dt\right) du = \int_2^x \frac{1}{\lg^3 u}\,du = O\left(\frac{x}{\lg^3 x}\right).$

Analogamente si ha che:

$$\frac{1}{\vartheta(x)\lg x}\left(\int_2^u \frac{\pi(t)}{t}dt\right)^2 = \frac{1}{\vartheta(x)\lg x}O\left(\frac{x^2}{\lg^2 x}\right) = O\left(\frac{x}{\lg^3 x}\right).$$

Allora si ottiene $\frac{1}{\varpi(x)}\left(\frac{\vartheta(x)}{\pi(x)}\right)^{\pi(x)} = e^{O(x/\lg^3 x)}$.

Utilizzando tali maggiorazioni per stimare d(k) si ottiene:

$$d(k) < \left(1+\frac{\lg k}{\vartheta(p)}\right)^{\pi(p)} e^{O(p/\lg^3 p)} = \left(1+\frac{\lg k}{\vartheta(p)}\right)^{\pi(p)+O(p/\lg^3 p)}.$$

Con tecnica analoga a quella usata per le relazioni precedenti si può provare che: (cfr. Ramanujan [32], pag. 83-85)

$$\pi(p)\lg p-\vartheta(p)=O\left(\frac{p}{\lg p}\right).$$

Abbiamo allora che $\vartheta(p)=\pi(p)\left\{\lg p+O(1)\right\}=\pi(p)\left\{\lg\vartheta(p)+O(1)\right\}$ e quindi si ottiene:

$$\pi(p)=\vartheta(p)\left\{\frac{1}{\lg p}+O\left(\frac{1}{\lg^2\vartheta(p)}\right)\right\}.$$

Si ha allora $d(k)\le\left(1+\frac{\lg k}{\vartheta(p)}\right)^{\frac{\vartheta(p)}{\lg\vartheta(p)}+O\left(\frac{\vartheta(p)}{\lg^2\vartheta(p)}\right)}$ con $\vartheta(p)\le\lg k$.

Ma, poiché al crescere di k rispetto a $\vartheta(p)$ il secondo membro della disuguaglianza precedente decresce, allora il caso più sfavorevole é che k sia il più piccolo possibile rispetto a $\vartheta(p)$. Allora, se $\vartheta(p)=\lg k$, si ha :

$$d(k)\le 2^{\frac{\lg k}{\lg_2 k}+O\left(\frac{\lg k}{(\lg_2 k)^2}\right)}$$

che é la maggiorazione che desideravamo.

Allora si ha che, per un $k\le\bar{k}$ opportuno si ha che $d(k)\le(2.5)^{\frac{\lg k}{\lg_2 k}}$.

Proviamo adesso $\prod_{(q-1)|k} q > \sqrt{n}$ implica $k\ge\lg n$.

Infatti si ha che:

$$\prod_{(q-1)|k} q \le \prod_{d|k}(d+1) \le \prod_{d|k} 2d = (2\sqrt{k})^{d(k)} \le (2\sqrt{k})^{(2.5)^{\frac{\lg k}{\lg_2 k}}} <$$

$$< (2\sqrt{k})^{e^{\frac{\lg k}{\lg_2 k}}} = (2\sqrt{k})^{k^{\frac{1}{\lg_2 k}}} = e^{k^{\frac{1}{\lg_2 k}}(\lg 2+\frac{1}{2}\lg k)}.$$

Se, per assurdo si avesse $k<\lg n$, allora si potrebbe maggiorare la quantità precedente (per n abbastanza grande) con :

$$e^{(\lg n)^{\frac{1}{\lg_3 n}}(\lg 2+\frac{1}{2}\lg_2 n)} < e^{\frac{1}{2}\lg n}=\sqrt{n}$$

(ciò dipende dal fatto che $(\lg n)^{\frac{1}{\lg_3 n}} < \sqrt{\lg n}$ e che $(\lg n)^{\alpha} > \lg_2 n \ \ \forall\ \alpha>0$), in contraddizione con l'ipotesi.

Da ciò si ottiene quindi che $f(n)>\lg n$.

Proviamo adesso che $f(n)\ge\lg n^{(\lg_3 n)}$.

Allora se $n>\bar{n}$ e $k\le\lg n^{(\lg_3 n)}$ si ha che

$$\prod_{(q-1)|k} q \le \prod_{d|k}(d+1) \le \prod_{d|k} 2d = (2\sqrt{k})^{d(k)} \le$$

$$\le 2(\lg n^{(\frac{1}{2}\lg_3 n)})^{(2.5)^{(\lg_2 n)}} = \exp\left\{\left[\lg 2+\tfrac{1}{2}(\lg_2 n)(\lg_3 n)\right](\lg n)^{\lg(2.5)}\right\} < \sqrt{n}\,.$$

Poichè f(n) è definito come il minimo intero square-free per cui $\prod_{(q-1)|f(n)} q > \sqrt{n}$, allora si ha che $f(n)\ge\lg n^{(\lg_3 n)}$ se $n>\bar{n}$.

Notiamo però che vogliamo una condizione su $n>100$, ed allora introduciamo una costante $c>0$ tale che $f(n)\ge\lg n^{c(\lg_3 n)}$ se $n>100$. •

Calcolo della maggiorazione:

Possiamo allora passare a provare la maggiorazione indicata precedentemente. Il punto cruciale della dimostrazione é quello di provare che esiste qualche piccolo intero square-free con un grosso numero di divisori del tipo p-1 (dove p é un numero primo).
Ricordiamo che (cfr. Capitolo 3) $\vartheta(x;k,a) = \sum_{\substack{p\le x \\ p\equiv a(\mathrm{mod}\ k)}} \lg p$.
Ci serviamo di un importante risultato sulla distribuzione dei primi nelle progressioni aritmetiche:

Proposizione 5.3.1: *$\forall \varepsilon >0\ \exists\, x_0(\varepsilon)\ ,\delta(\varepsilon)>0$ calcolabili tali che, se $x\ge x_0(\varepsilon)$, $k,a\in\mathbb{N}$, $(k,a)=1$, $0<k<x^{\delta(\varepsilon)}$ allora:*

$$\left| \vartheta(x;k,a) - \frac{x}{\varphi(k)} \right| < \frac{\varepsilon x}{\varphi(k)}$$

tranne per quei k che sono multipli di un certo intero $k_0(x) > (\lg x)^{\frac{3}{2}}$.

Dim: dipende dalla dimostrazione del Teorema di Linnik data da Bombieri (cfr. Bombieri [7]). ●

Definiamo adesso $\vartheta_0(x;k,a)= \sum_{\substack{p\le x \\ p\equiv a(\mathrm{mod}\ k)}} \mu^2(p-1)\lg p$

dove per μ si intende la funzione di MÖBIUS (cfr. Capitolo 3).

Osserviamo che $\vartheta_0(x;k,a)$ differisce da $\vartheta(x;k,a)$ soltanto per il fatto che non conta tutti i primi, ma considera solo i primi p tali che p-1 sia square-free.

Nel seguito denoteremo con α la costante di Artin di cui ricordiamo la definizione :

$$\alpha= \prod_{p \text{ primo}} \left(\frac{p^2-p-1}{p^2-p} \right) \simeq 0.374 .$$

Definiamo inoltre la funzione $\gamma(k)$ come la funzione moltiplicativa (cfr. Capitolo 3) che verifica $\gamma(p^d) = \frac{p^2-p}{p^2-p-1}$.
Si noti che $\forall$ k si ha $\alpha \le \alpha\gamma(k) < 1$.

Possiamo adesso dimostrare un risultato analogo alla proposizione precedente, ma più utile nel prosieguo:

Proposizione 5.3.2: *$\forall \varepsilon>0\ \exists\, \delta, x_0, T>0$ calcolabili tali che se $0<k<x^{\delta}$, k square-free, $x\ge x_0$ e $k_0(x)\nmid (k^2\prod_{\substack{p<T \\ p\nmid k}} p^2)$, p primo, allora si ha :*

$$\left| \vartheta_0(x;k,1) - \frac{\alpha\gamma(k)x}{k} \right| < \frac{\varepsilon x}{k} .$$

Dim: Consideriamo le $\varphi(k)$ classi residue a_i modulo k^2, $i=1..\varphi(k)$, che verificano $a_i \equiv 1 \pmod k$ e $(\frac{a_i-1}{k},k)=1$. Notiamo che tali classi sono effettivamente $\varphi(k)$ perché solo k classi residue modulo k^2 verificano $a_i \equiv 1 \pmod k$, mentre le classi che verificano $(\frac{a_i-1}{k},k)=1$, oltre alla precedente, sono in numero pari a $\varphi(k)$.
Sia a una di tali classi residue. Se (k,J)=1 allora sia R(J) il più piccolo intero positivo che verifica:

$$R(J) \equiv a \pmod{k^2} \quad \text{e} \quad R(J) \equiv 1 \pmod J.$$

Si noti che un tale R(J) esiste per il Teorema Cinese dei Resti (Capitolo 2).
Indichiamo adesso con $\{q_i\}$, $q_i<q_{i+1}$, l'insieme dei primi che non dividono k . Si ha allora, grazie ad un ragionamento aritmetico di inclusione-esclusione, che:

$$\vartheta_0(x;k^2,a) = \vartheta(x;k^2,a) - \sum_i \vartheta(x;k^2q_i^2,R(q_i^2)) + \sum_{i<j} \vartheta(x;k^2q_i^2q_j^2,R(q_i^2q_j^2)) - ... + ...$$

Infatti notiamo che $\vartheta(x;k^2q_i^2,R(q_i^2))$ "conta" i primi p tali che $p \equiv R(q_i^2) \pmod{k^2q_i^2}$ e quindi tali che $p \equiv 1 \pmod{q_i^2}$ e che $p \equiv a \pmod{k^2}$. Nel processo sottraggo da $\vartheta(x;k^2,a)$ elementi che non hanno p-1 square-free, ma sommando su i tolgo però "troppi" di tali elementi ed é quindi necessario riaggiungerli.
Tale processo é finito poiché la funzione $\vartheta(x;r,s)$ si annulla se r>x.
Sia adesso M(T) il secondo membro dell'equazione precedente in cui però si considerano solo i $q_i<T$.
Definiamo adesso la funzione che conta il numero dei divisori primi di un intero d :

$$\omega(d) := k \text{ se } d = \prod_{i=1}^{k} p_i^{a_i} .$$

Sia inoltre $Q = \prod_{q_i<T} q_i$ ed allora abbiamo che :

$$M(T) = \sum_{d|Q} (-1)^{\omega(d)} \vartheta(x;k^2d^2,R(d^2)) \le \vartheta_0(x;k^2,a) + \sum\nolimits' \lg p \le$$

$$\le \vartheta_0(x;k^2,a) + \sum_{\substack{m \ge T \\ (m,k)=1}} \vartheta(x;k^2m^2,R(m^2)) .$$

(In tal caso col simbolo $\sum'$ si intende una somma sui primi p tali che $p \le x$ e che $q_i^2 | (p-1)$ per almeno un $q_i \ge T$ e $q_i^2 \not| (p-1)$ per tutti i $q_i < T$).

Si noti inoltre che, se $m \ge \sqrt{x}$, allora $\vartheta(x;k^2m^2,R(m^2)) = 0$ (perché in tal caso $k^2m^2>x$ e $R(m^2) \ge m^2+1>x$).

Supponiamo allora che $k < \sqrt[12]{x}$ e spezziamo l'ultima somma scritta in due parti in modo da poter usare la disuguaglianza di Brun-Titchmarsh (cfr. Capitolo 3) che é data da :

$$\vartheta(x;u,a) \le c_5 \frac{x}{\varphi(u)} \frac{\lg x}{\lg \frac{x}{u}} .$$

Nel caso di avere $m< \sqrt[4]{x}$, si ottiene $k^2m^2 < x^{\frac{2}{3}}$ e quindi si ha che

$$\frac{\lg x}{\lg\left(\frac{x}{k^2m^2}\right)} < \frac{\lg x}{\lg(\sqrt[3]{x})} = 3.$$

Allora si ha $\sum_{\substack{m\ge T \\ (m,k)=1}} \vartheta(x;k^2m^2,R(m^2)) = \left(\sum_{\substack{T\le m< \sqrt[4]{x} \\ (m,k)=1}} + \sum_{\substack{\sqrt[4]{x}\le m<\sqrt{x} \\ (m,k)=1}} \right) \vartheta(x;k^2m^2,R(m^2)) \le$

$$\le 3c_5 \left(\sum_{\substack{T\le m< \sqrt[4]{x} \\ (m,k)=1}} \frac{x}{\varphi(k^2m^2)} \right) + \lg x \left(\sum_{\substack{\sqrt[4]{x}\le m<\sqrt{x} \\ (m,k)=1}} \left(1+\frac{x}{k^2m^2}\right) \right) \le \frac{(3c_5c_6+1)x}{\varphi(k^2)T} .$$

Nella prima maggiorazione il primo termine è ottenuto applicando Brun-Titchmarsh mentre il secondo termine é ottenuto in modo banale. Nella seconda maggiorazione abbiamo sfruttato la seguente relazione per la prima somma:

$\sum_{m\ge 1} \frac{1}{\varphi(m^2)} < \frac{c_6}{T}$ (per la dimostrazione cfr. Adleman-Pomerance-Rumely [1]); mentre per la seconda somma si usa una stima banale.

Poniamo adesso $T= \frac{3}{\varepsilon}(3c_5c_6+1)$ e si ottiene :

$$0 \le M(T)-\vartheta_0(x;k^2,a) < \frac{\varepsilon x}{3\varphi(k^2)} .$$

Passiamo adesso a stimare M(T).

Sia $\varepsilon'= \frac{\varepsilon}{3c_6}$. Applichiamo la Proposizione 5.3.1 ad ε', ottenendo così $x_0,\delta>0$ tali che, se $0<k<x^{\delta}$, $x\ge x_0$ e se inoltre $k_0(x) \nmid k^2Q^2$ (condizione che assicura che, se $d|Q$, allora k^2d^2 non é multiplo di $k_0(x)$ e quindi assicura che la Proposizione 5.3.1 può essere applicata a $\vartheta(x;k^2d^2,R(d^2))$ allora vale la relazione:

$$\left| M(T)-\frac{\alpha\gamma(k)x}{\varphi(k^2)} \right| = \left| M(T)- \sum_{(d,k)=1} m^2(d)(-1)^{\omega(d)} \frac{x}{\varphi(k^2d^2)} \right| \le$$

$$\leq \left| \sum_{d|Q} (-1)^{\omega(d)} \left\{ \vartheta(x;k^2d^2,R(d^2) - \frac{x}{\varphi(k^2d^2)} \right\} \right| + \sum_{d \geq 1} \frac{x}{\varphi(k^2)\varphi(d^2)} <$$

$$< \sum_{d|Q} \frac{\varepsilon' x}{\varphi(k^2d^2)} + \frac{c_6 x}{\varphi(k^2)T} < \frac{\varepsilon' x c_6}{\varphi(k^2)T} + \frac{c_6 x}{\varphi(k^2)T} < \frac{2}{3}\frac{\varepsilon x}{\varphi(k^2)} .$$

Allora combinando le due valutazioni ottenute si ha che :

$$\left| \vartheta_0(x;k^2,a) - \frac{\alpha\gamma(k)x}{\varphi(k^2)} \right| < \frac{\varepsilon x}{\varphi(k^2)} .$$

Sommando tali stime al variare delle $\varphi(k)$ scelte possibili di a (modulo k^2), e poiché $\frac{\varphi(k)}{\varphi(k^2)} = \frac{1}{k}$, si ottiene :

$$\left| \vartheta_0(x;k,1) - \frac{\alpha\gamma(k)x}{k} \right| < \frac{\varepsilon x}{k} . \quad \bullet$$

Basandoci su quanto appena dimostrato, possiamo allora provare la seguente:

Proposizione 5.3.3:

$\exists\ c_7>0$ calcolabile tale che $\forall\ x>10\ \exists$ M, intero square-free, $M<x^2$ per cui $\sum_{\substack{(p-1)|M \\ p \text{ primo}}} 1 > e^{c_7 \frac{lgx}{lg_2 x}}$.

Dim: fissiamo $\varepsilon=\frac{1}{4}$ e utilizziamo la Proposizione 5.3.2. Sappiamo allora che $\exists\ \delta, x_0, T$ tali che, se $0<k<x^{\delta}$, k square-free, $x \geq x_0$, vale la relazione:

$$\left| \vartheta_0(x;k,1) - \frac{\alpha\gamma(k)x}{k} \right| < \frac{1}{4}\frac{x}{k}$$

provvedendo a $k_0(x) \not| (k^2 \prod_{\substack{p<T \\ p \not| k}} p^2)$, p primo.

Abbiamo quindi fissati δ, x_0, T.

Denotiamo con $k_1 = \prod_{\substack{p \leq r \\ p \text{ primo}}} p$, dove $r=\max\left\{ \frac{1}{2}\delta lgx; T \right\}$.

Notiamo che $\exists\ x_1$ tale che, se $x>x_1$, allora si ha $k_1 < x^{\delta}$. (Per calcolare effettivamente x_1 si possono usare le stime di Rosser-Schonfeld [35]).

Se $(k_1, k_0(x))$ ha un fattore primo $p_0 \geq T$, allora si pone $k=\frac{k_1}{p_0}$, altrimenti si pone $k= k_1$.

Allora $k_0(x) \not| k^2$ (in realtà se avessi $k_0(x) | k^2$ otterrei che ogni fattore primo di $k_0(x)$ sarebbe $< T$. Poichè $k_0(x) > (\lg x)^{\frac{3}{2}}$ abbiamo che $\exists$ p primo tale che $p^3 | k_0(x)$, per $x > x_2$ con x_2 opportuno, e ciò contraddirebbe $k_0(x) | k^2$.).

Se d|k allora, per la Proposizione 5.3.2, si ha che :

$$\pi_0(x;d,1) = \sum_{\substack{p \le x \\ p \equiv 1 \pmod d}} \mu^2(p-1) \ge \frac{\vartheta_0(x;d,1)}{\lg x} \ge \left(\alpha\gamma(d) - \frac{1}{4}\right) \frac{x}{d \lg x} > \frac{x}{10 d \lg x} .$$

Sia adesso A la cardinalità dell'insieme delle soluzioni della congruenza :

β) $m(p-1) \equiv 0 \pmod k$ dove $m \le x$, $p \le x$, p primo, p-1 square-free.

$\forall$ d|k sia A_d la cardinalità dell'insieme delle soluzioni di **β)** tali che inoltre valga d|(p-1) e $(m,k) = \frac{k}{d}$.

Da quanto visto precedentemente si ha che

$$\#\left\{ \text{p primi; } p \le x \text{; p-1 square-free; } d | (p-1) \right\} > \frac{x}{10 d \lg x} .$$

Inoltre si ha anche che $\#\left\{ m \le x \text{ tali che } (m,k) = \frac{k}{d} \right\} > \left[\frac{x}{k}\right] \varphi(d)$.

Allora si ha che $A_d \ge \frac{x}{10 d \lg x} \left[\frac{x}{k}\right] \varphi(d) > \frac{x^2}{20 k \lg x} \frac{\varphi(d)}{d}$. Così, se $x > \bar{x}$ opportuno, abbiamo che , siccome $\sum_{d|k} \frac{\varphi(d)}{d} = \sum_{d|k} \frac{m^2(d)\varphi(d)}{d}$ (perché k square-free), possiamo applicare il Teorema 3.1.7 ed allora otteniamo:

$$A = \sum_{d|k} A_d > \frac{x^2}{20 k \lg x} \sum_{d|k} \frac{\varphi(d)}{d} = \frac{x^2}{20 k \lg x} \prod_{\substack{p | k \\ p \text{ primo}}} \left(2 - \frac{1}{p}\right) \ge$$

$$\ge \frac{x^2}{20 k \lg x} \left(\frac{3}{2}\right)^{\omega(k)} > \frac{x^2}{20 k \lg x} \left(\frac{3}{2}\right)^{\frac{1}{4} \frac{\delta \lg x}{\lg_2 x}} .$$

L'ultima maggiorazione é ottenuta applicando il Teorema dei Numeri Primi (Teorema 3.1.8), tenendo conto del fatto che i fattori primi di k sono $\le \frac{1}{2}\delta \lg x$ e che k é square-free.

Inoltre, poichè ogni soluzione m,p di **β)** appartiene a $\left\{ n \le x^2 \text{ tali che } k | n \right\}$ e la cardinalità di tale insieme é <\f(x\s\up8(2),k), abbiamo che $\exists$ $n \le x$\s\up8(2) tale che $k | n$ ed n ha almeno $\frac{A}{(x^2/k)} > \frac{1}{20 \lg x} \left(\frac{3}{2}\right)^{\frac{1}{4} \frac{\delta \lg x}{\lg_2 x}} > > e^{c_7 \frac{\lg x}{\lg_2 x}}$ rappresentazioni come m(p-1).

Sia adesso M=il più grande divisore square-free di n, allora M ha tante rappresentazioni come m(p-1) quante ne ha n.

Per ottenere la tesi si può aggiustare la costante c_7 in modo che la maggiorazione valga per x>10 anzichè per $x>\bar{x}$.

Grazie a quest'ultima Proposizione possiamo adesso ottenere la maggiorazione del Teorema 5.3.1.

Infatti: sia $x=(\lg n)^{\frac{2}{c_7}\lg_3 n}$; allora per la Proposizione 5.3.3 abbiamo che $\exists$ M, intero square-free, $M<x^2$ per cui

$$\sum_{\substack{(p-1)|M \\ p \text{ primo}}} 1 > e^{c_7 \frac{\lg x}{\lg_2 x}} = \exp\left\{\frac{2\lg_2 n \lg_3 n}{\lg(2/c_7)+\lg_3 n+\lg_4 n}\right\} \geq \exp(\lg_2 n) = \lg n \qquad \text{(per } n>\bar{n} \text{ opportuno).}$$

Quindi $\prod_{\substack{(p-1)|M \\ p \text{ primo}}} p \geq 2^{\left(\sum_{(p-1)|M} 1\right)} \geq 2^{\lg n} > \sqrt{n}$.

Posso allora prendere $f(n) \leq M < x^2 = (\lg n)^{\frac{4}{c_7}\lg_3 n}$, se $n>\bar{n}$.

Anche in questo punto si può aggiustare la costante $\frac{4}{c_7}$ per ottenere n>100 anzichè $n>\bar{n}$. ●

Ciò conclude la dimostrazione del Teorema 5.3.1 e l'analisi computazionale con metodi analitici di tutte le versioni dell'algoritmo di Adleman-Pomerance-Rumely .

Bibliografia

[1] Adleman L., Pomerance C., Rumely R.S. :
"On distinguishing prime numbers from composite numbers", Annals of Mathematics, 1983, vol. 117, pag. 173-206.

[2] Apostol T. :
"Introduction to analytic number theory", Springer-Verlag UTM, 1976.

[3] Artin E., Tate J. :
"Class Field Theory", Benjamin, New York, 1967 .

[4] Bach E. :
"Analytic methods in the analysis and Design of Number-Theoretic Algorithms", An ACM Distinguished Dissertation 1984, The MIT Press, Cambridge, Massachusetts.

[5] Bazzanella D. :
"Codici a chiave pubblica ed algoritmi di fattorizzazione", Tesi di Laurea, Università di Genova, Corso di Laurea in Matematica, 1989.

[6] Berlekamp E.R. :
"Factoring polynomials over large finite fields", Mathematics of Computations , vol. 24, 1970, pag. 713-735.

[7] Bombieri E. :
"La grand crible dans la théorie analytique des nombres", Société Mathematique de France, 1974.

[8] Cassels J.W.S. :
"Local Fields", London Mathematical Society, Student Texts 3, 1986.

[9] Cohen H. :
"Test de primalité d'apres Adleman, Rumely, Pomerance et Lenstra", Séminaire de Theorie des Nombres, 1981, Grenoble.

[10] Conrey J.B. : "More than two fifths of the zeros of the Riemann zeta function are on the critical line", Journal fur die reine und angewandte Mathematik, Band 399, 1989.

[11] Davenport H. :
"Multiplicative Number Theory", Second Edition, Springer-Verlag, 1980.

[12] Dixon J.D.:
"Factorisation and primality tests", American Mathematical Monthly, vol. 91, 1984, pag. 333.

[13] Goldwasser S., Kilian J. :
"Almost all primes can be quickly certified", Proc. 18th Annual ACM Simpos. on Theory of Computing (STOC) Berkeley, 1986, pag. 316-329.

[14] Hardy G.H. : "Sur les zeros de la fonction $\zeta(s)$ di Riemann", Comptes rendus de l'Academie des Sciences (Paris), vol. 158, (1914), pag. 1012-1014.

[15] Hasse H. :
"Vorlesungen uber Zahlentheorie", Springer-Verlag, 1950.

[16] Iwasawa K. :
"A note on the Jacobi sums", Symposia Mathematica, vol. 15, 1975, pag. 447-459.

[17] Koblitz N. :
"A course in number theory and cryptography", Springer-Verlag, GTM 114, 1987.

[18] Lang S. :
"Elliptic Curves : Diophantine Analysis", Springer-Verlag, 1978.

[19] Lang S. :
"Algebraic Number Theory", Addison-Westley, 1968.

[20] Lenstra, H.W.Jr. :
"Primality testing algorithms (after Adleman, Pomerance, Rumely)", Seminaire Bourbaki 33 (1980/81), n°576, pag. 246-257

[21] Lenstra, H.W.Jr. : "Elliptic curves and Number Theoretic Algorithms", Proceedings of the International Congress of Mathematicians, Berkeley, California, U.S.A., 1986.

[22] Lenstra, H.W.Jr. :
"Divisors in residue classes", Mathematics of Computations vol. 42, 1984, pag. 331-340.

[23] Levinson N. :
"More than one third of zeros of Riemann's function are on $\sigma = \frac{1}{2}$", Advances Math., vol.13, pag. 383-436.

[24] Marcus D. :
"Number Fields", Springer-Verlag Universitext, 1977.

[25] Narkiewicz W. :
"Elementary and analytic Theory of algebraic numbers", P.W.N. Polish Scientific Publishers, 1974.

[26] Pintz J., Steiger W., Szeremedi E. :
"Infinite Sets of Primes with Fast Primality Tests and Quick Generation of Large Primes", Mathematics of Computations, vol. 53, 1989, pag. 399-406.

[27] Pomerance C. :
"On the distribution of pseudoprimes", Mathematics of Computations , vol. 37, 1981, pag. 587-593.

[28] Pomerance C. :
"Recent development in primality testing", Mathematical Intelligencer, vol. 3 (1981), pag. 97-105.

[29] Pomerance C. : "Very short primality proofs", Mathematics of Computations, vol. 48, 1987, pag. 315-322.

[30] Pomerance C., Selfridge J.L., Wagstaff S.S :
"The pseudoprimes to $25 \cdot 10^9$ ", Mathematics of Computations, vol. 35, 1980, pag. 1003-1026.

[31] Pratt V. :
"Every prime number has a succint certificate", SIAM Journal of Computation, vol. 4, pag. 214-220.

[32] Ramanujan S. : "Highly Composite Numbers", Proceedings of the London Mathematical Society, 2,XIV,1915, pag. 347-409 .

[33] Ribemboim P. :
"Algebraic Numbers", Pure and Applied Mathematics, vol. XXVII, 1972.

[34] Riesel H. :
"Prime numbers and Computer Method for factorisation", Birkhauser, 1985.

[35] Rosser J.B., Schonfeld L. :
"Approximate formulas for some functions of prime numbers", Illinois Journal Mathematical, vol. 6, 1962, pag. 64-94.

[36] Rumely R.S. :
"Recent Advances in Primality Testing", Notices of American Mathematical Society, agosto 1983, pag. 475.

[37] Schoof R. :
"Elliptic curves over finite fields and the computation of square roots mod p ", Mathematics of Computations, vol. 44, 1985, pag. 483-494.

[38] Schoof R. :
"Fattorizzazione e criptosistemi a chiave pubblica", Didattica delle scienze, n°137, 1989.

[39] Selberg A. :
"On the zeros of the Riemann's zeta function", Skr. Norskevid Akad., Oslo, vol. 10, 1942, pag. 1-59.

[40] Silverman J. :
"The arithmetic of Elliptic Curves", Springer-Verlag, GTM 106, 1986.

[41] Solovay R., Strassen V. :
"A fast Monte-Carlo test for primality", SIAM Journal of Computation, vol. 6, 1977, pag. 84-85.

[42] Stewart I. , Tall D. :
"Algebraic Number Theory", Chapman and Hall, 1979.

abbreviazioni usate nei riferimenti bibliografici:

ACM	Association of Computer Machinery.
MIT	Massachusetts Institute of Technology.
SIAM	Society for Industrial and Applied Mathematics.
STOC	Symposium on Theory of Computing.