UNIVERSITÀ DEGLI STUDI DI ROMA TRE
FACOLTÀ DI SCIENZE M.F.N.

Tesi di Laurea in Matematica
di
Antonio Cosentino

Applicazioni delle Leggi di Reciprocità in Crittografia

Relatore
Prof. Francesco Pappalardi

Il Candidato

Il Relatore

ANNO ACCADEMICO 2000 - 2001
NOVEMBRE 2001

Classificazione AMS : 94A60, 11T71
Parole Chiave : Residui, Reciprocità, Identificazione

L'uso di tecniche crittografiche per proteggere documenti è antico quanto la scrittura stessa. La disciplina della crittografia, che solo da pochi anni ha attirato l'attenzione degli organi di informazione e del grosso pubblico, affonda le sue radici storiche in Italia; ad esempio, nel Rinascimento, gli ambasciatori della Repubblica Veneziana e i Messi Pontifici erano i principali utilizzatori di tecniche crittografiche.
Nella crittografia classica, o a *chiave privata*, tutti i tradizionali cifrari (o crittosistemi) si comportano nella pratica come si comporta la normale serratura di una porta, che apriamo e chiudiamo con una stessa chiave. Un cifrario di questo tipo viene chiamato *simmetrico*.
Il concetto di crittografia a *chiave pubblica* fu introdotto da Whitfield Diffie e Martin Hellman e, indipendentemente, da Ralph Merkle nel 1976. Diffie ed Hellman presentarono per la prima volta questa nozione in un fondamentale lavoro teorico (vedi [33]), dove, ipotizzando di poter disporre di un cifrario *asimmetrico*, dimostravano la fattibilità di sistemi crittografici di nuovo tipo, adatti alla crittografia di massa mediante il concetto delle *chiavi pubbliche*. In pratica in un sistema di questo tipo esiste una coppia di chiavi distinte, che sono una l'inversa dell'altra: una chiave (pubblica) per codificare e l'altra (privata) per decodificare. Punto saliente del sistema è l'indipendenza delle due chiavi, ossia l'impossibilità di generare una chiave dall'altra. Dal 1976 sono stati proposti molti algoritmi di crittografia a chiave pubblica. Solo alcuni però sono risultati sicuri e pratici allo stesso tempo, come ad esempio i crittosistemi di El Gamal, di Rabin e RSA.
L'obiettivo di questa tesi è quello di proporre, sfruttando l'idea di W. D. Banks, D. Lieman, I. E. Shparlinski in [27], basata sui residui quadratici, due nuovi crittosistemi di identificazione a chiave pubblica basati rispettivamente sui residui cubici e sui residui biquadratici, e sulle relative leggi di reciprocità. È soprattutto sul primo schema, il CRIP, che concentremo la nostra attenzione, evidenziandone pregi e difetti. Useremo i risultati ottenuti come punto di partenza per una futura analisi del secondo schema, il BRIP.

Nel Capitolo 1 esponiamo la teoria dei residui quadratici e il simbolo di Legendre, definito, per ogni a intero e p primo dispari, nel seguente modo:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \text{ divide } a \\ -1 & \text{se } a \text{ è un non–residuo quadratico modulo } p \\ +1 & \text{se } a \text{ è un residuo quadratico modulo } p. \end{cases}$$

Per applicare la legge di reciprocità quadratica ed ottenere un metodo efficiente per calcolare il simbolo di Legendre, è necessario estendere la definizione di simbolo a moduli composti. Per ogni n, m interi con m dispari e tale che $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ sia la sua fattorizzazione in potenze di primi,

definiamo il simbolo di Jacobi:

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{s} \left(\frac{n}{p_i}\right)^{\alpha_i},$$

dove $\left(\frac{n}{p_i}\right)$ è l'usuale simbolo di Legendre. Richiamiamo inoltre alcune proprietà del simbolo di Jacobi, che verrano utilizzate per determinare un efficiente algoritmo per calcolarlo. Le dimostrazioni si trovano nel Capitolo 1. Abbiamo il seguente:

Teorema 1. *Siano n, n' e m interi con m positivo dispari, allora:*

- *se $n \equiv n' \pmod m$, allora $\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)$;*
- $\left(\frac{1}{m}\right) = \begin{cases} -1 & \text{se } m \equiv -1 \pmod 4 \\ +1 & \text{se } m \equiv 1 \pmod 4 \end{cases} = (-1)^{\frac{m^2-1}{8}}$;
- $\left(\frac{2}{m}\right) = \begin{cases} -1 & \text{se } m \equiv \pm 3 \pmod 8 \\ +1 & \text{se } m \equiv \pm 1 \pmod 8 \end{cases} = (-1)^{\frac{m^2-1}{8}}$;
- *Legge di reciprocità quadratica estesa:*

$$\left(\frac{n}{m}\right) = \begin{cases} -\left(\frac{m}{n}\right) & \text{se } n \equiv m \equiv 3 \pmod 4 \\ \left(\frac{m}{n}\right) & \text{altrimenti} \end{cases} = (-1)^{\frac{m-1}{2}\frac{m-1}{2}} \left(\frac{m}{n}\right).$$

Si noti come dall'identità di Eulero,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p,$$

segua che il simbolo di Legendre può essere calcolato, usando l'algoritmo dei quadrati successivi, mediante un "esponenziale modulare". Tuttavia questo richiederebbe $O(\log^3 p)$ operazioni bit. Questo fenomeno giustifica l'introduzione del simbolo di Jacobi e l'uso della legge di reciprocità.
Lo pseudocodice che segue illustra una versione ricorsiva in cui vengono applicate ripetutamente le proprietà del Teorema 1.

Algoritmo 0.0.1

JAC(x,y)= `IF` $(x = 1)$ `THEN 1`
`IF` $(2|a)$ `THEN` **JAC**$(\frac{x}{2}, y)\cdot(-1)^{\frac{y^2-1}{8}}$
`ELSE` **JAC**$(y \bmod x, x)\cdot(-1)^{\frac{x-1}{2}\frac{y-1}{2}}$

Se $M = max(x, y)$ allora il numero di operazioni bit necessarie a calcolare $\left(\frac{x}{y}\right)$ è $O(\log^2 M)$, il che equivale a dire che l'algoritmo ha complessità quadratica. Quindi, il tempo necessario per calcolare il simbolo di Jacobi di due numeri interi è dello stesso ordine di grandezza di quello necessario a moltiplicarli.
Un altro aspetto che rende l'algoritmo veloce è il fatto che utilizza molte divisioni per 2, che in un computer coincidono con un semplice *shift-bit*. Il fatto di poter calcolare i simboli di Legendre più velocemente di quanto richieda calcolare esponenziali modulari ne giustifica l'impiego in crittografia.

Nel Capitolo 2 esponiamo una breve panoramica su alcuni algoritmi fondamentali, utilizzati per produrre numeri primi. Sappiamo, da Euclide, che esistono infiniti numeri primi e, grazie al teorema dei numeri primi, la probabilità che un intero random $n \leq M$ sia primo è circa $\frac{1}{\log M}$.
Per verificare se un dato intero n è primo in teoria basta provare a dividerlo per tutti i numeri minori della sua radice quadrata. Se non si ottiene mai un resto nullo allora il numero è primo. Questo fornisce un algoritmo con complessità pari a $O(n \log^2 n)$, ed è quindi impraticabile per numeri con più di 25 cifre decimali. Insorge, dunque, la necessità di utilizzare test più veloci, basati su metodi non necessariamente deterministici.
Un *problema decisionale* è un problema in cui la domanda può avere due risposte, ad esempio "si" o "no". Un *algoritmo probabilistico* è un qualsiasi algoritmo che usi numeri random. Consideriamo la seguente definizione riguardante gli algoritmi probabilistici per problemi decisionali.

Definizione 2.0.2. *Un* algoritmo Monte Carlo polarizzato-si *è un algoritmo probabilistico per un problema decisionale in cui una risposta* "si" *è sempre corretta, mentre una risposta di tipo* "no" *potrebbe essere incorretta. Diremo che un algoritmo Monte Carlo polarizzato-si ha* probabilità di errore pari a ϵ *se, per ogni domanda la cui risposta è* "si"*, l'algoritmo dà risposta errata* "no" *con probabilità al massimo* ϵ.

I test di primalità sono una classe di algoritmi Montecarlo polarizzati-si in cui la risposta "si" significa che l'input è un numero composto, e la risposta "no" che l'input è un numero primo. Dalla definizione segue che, a patto di applicare k volte ad un input n un test di primalità con probabilità ϵ, è possibile stabilirne la primalità con probabilità minore di ϵ^k.
Discuteremo due test di primalità Montecarlo, quello di Solovay-Strassen e quello di Miller-Rabin. Entrambi sono basati sulla teoria sviluppata nel Capitolo 1.

Il Test di Solovay-Strassen è un algoritmo Monte Carlo di tipo polarizzato-si con probabilità $\frac{1}{2}$. Se l'algoritmo, applicato ad un intero n, dà una risposta "si" allora n è composto. Al contrario, se n è composto, l'algoritmo dà una risposta "si" con probabilità al massimo $\frac{1}{2}$. Sia n un intero dispari, $b \in (\mathbb{Z}/n\mathbb{Z})^*$, e sia $\left(\frac{b}{n}\right)$ il simbolo di Jacobi. Se n è primo, dal Criterio di Eulero, sappiamo che

$$\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \pmod{n} \qquad \forall\, b \in (\mathbb{Z}/n\mathbb{Z})^*.$$

D'altraparte, se n è composto, $\gcd(n, b) = 1$ e il Criterio di Eulero è verificato, allora n si dice *pseudoprimo di Eulero* per la base b. Segue l'algoritmo in pseudocodice del test di primalità di Solovay-Strassen.

Algoritmo 0.0.2

Sol-Stra(n){
  b =RANDOM$(2, n-1)$
  IF $\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \pmod{n}$ THEN
    RETURN("n è un b-EPRP")
  ELSE
    RETURN("n è composto")
}

Nel suddetto algoritmo b-EPRP indica un *probabile primo* di Eulero per la base b, cioè un intero dispari che superi un test di Solovay-Strassen per una qualsiasi base b. Si tratta di un algoritmo polinomiale con complessità pari a $O(\log^3 n)$.
Successivamente abbiamo esposto il test di primalità di Miller-Rabin, il quale ha una probabilità di errore pari a $\frac{1}{4}$. Questo test è basato sulla seguente definizione:

Definizione 2.2.1. *Sia n un intero dispari composto. Scriviamo $n-1 = 2^s t$ con t dispari e sia $b \in (\mathbb{Z}/n\mathbb{Z})^*$. Se $b^t \equiv 1 \pmod{n}$ oppure esiste un r, con $0 \leq r < s$, tale che $b^{2^r t} \equiv -1 \pmod{n}$, allora n si dice* pseudoprimo forte *per la base b.*

Per ogni intero dispari n con $n - 1 = 2^s t$ e $b \in (\mathbb{Z}/n\mathbb{Z})^*$, possiamo considerare le sequenze (di Miller-Rabin)

$$(\epsilon_0, \ldots, \epsilon_s) = (b^t \bmod n, b^{2t} \bmod n, \ldots, b^{n-1} \bmod n).$$

Dire che n è pseudoprimo forte in base b equivale a dire che la sequenza è $(1, \dots, 1)$ oppure $(\epsilon_0, \dots, \epsilon_i, -1, 1, \dots, 1)$, dove necessariamente $\epsilon_i \neq \pm 1$. Osserviamo che se n è primo allora la sequenza è necessariamente di questo tipo (cioè n è pseudoprimo forte in base b). Infatti ϵ_i è una radice quadrata di ϵ_{i+1}; quindi se $\epsilon_{i+1} = 1$ allora $\epsilon_i = \pm 1$ (± 1 sono le uniche radici quadrate di 1 nel campo $(\mathbb{Z}/n\mathbb{Z})^*$). Inoltre $\epsilon_s = 1$.
Nel caso che un intero n superi il test, lo definiamo un *probabile primo forte* per la base b (b-SPRP).
Oltre all'aver migliorato di un fattore 2 la probabilità di errore del test di Solovay-Strassen, un altro aspetto che rende preferibile questo test a quello di Solovay-Strassen è la medesima complessità, pari a $O(\log^3 n)$.

Algoritmo 0.0.3

Mil-Rab(n){
  $m = \frac{n-1}{2^k}$, con k max
  b =RANDOM$(2, n-1)$
  $a = b^m \bmod n$
  IF $a \equiv 1 \pmod n$ THEN RETURN("n è un b-SPRP")
  FOR $i = 0$ TO $k - 1$ DO{
    IF $a \equiv -1 \pmod n$ THEN RETURN("n è un b-SPRP")
    ELSE $b = b^2 \bmod n$
  }
  RETURN("n è composto")
}

Nel Capitolo 3 enunciamo e dimostriamo la legge di reciprocità cubica. Questo ci porta a considerare la nozione di residuo cubico.
Sia

$$\omega = \frac{-1 + \sqrt{-3}}{2}.$$

L'insieme $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$ è un anello con unità contenuto in $\mathbb{C}$, dunque un dominio d'integrità. Esso contiene $\mathbb{Z}$ ed è chiuso anche rispetto alla coniugazione complessa. Per ogni $\alpha \in \mathbb{Z}[\omega]$, definiamo la *norma* di α, come $N\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$ e poniamo $D = \mathbb{Z}[\omega]$.
L'insieme D è un dominio euclideo, dunque un anello ad ideali principali, quindi un anello a fattorizzazione unica. Le unità e gli elementi primi di D

sono caratterizzati dal seguente:

Teorema 2.

- *$\alpha \in D$ è un'unità se e solo se $N\alpha = 1$. Quindi le unità di D sono $\pm 1, \pm\omega, \pm\omega^2$.*
- *Se π è un primo in D, allora esiste un primo razionale p tale che $N\pi = p$ o p^2. Nel primo caso π non è associato ad alcun primo razionale, mentre nel secondo π è associato a p (cioè $\pi = (-\omega)^i p$ con $i \in \mathbb{Z}/6\mathbb{Z}$).*
- *Se $\pi \in D$ è tale che $N\pi = p$, con p primo razionale, allora π è un primo in D.*
- *Sia $p > 2$ un primo razionale.*
  - *Se $p \equiv 2 \pmod 3$ allora p è primo in D.*
  - *Se $p \equiv 1 \pmod 3$ allora $p = \pi\overline{\pi} = N\pi$ dove π è primo in D.*
  - *$3 = -\omega^2(1-\omega)^2$ e $1-\omega$ è primo in D.*

Analogamente a $\mathbb{Z}$, anche in D le classi di congruenza modulo γ sono rappresentate mediante gli elementi dell'anello $D/\gamma D$, che chiameremo *anello delle classi residuo modulo* γ. Se γ è primo in D, allora $D/\gamma D$ è un campo finito con $N\gamma$ elementi.
Sia $\pi \in D$ un primo. Il gruppo moltiplicativo di $D/\pi D$ ha ordine $N\pi - 1$. Se $\pi \nmid \alpha$, allora

$$\alpha^{N\pi-1} \equiv 1 \pmod \pi,$$

che è l'analogo del Piccolo Teorema di Fermat. Inoltre, se $N\pi \neq 3$, allora le classi residue di $1, \omega, \omega^2$ sono distinte in $D/\pi D$. Notare che $\{1, \omega, \omega^2\}$ è un gruppo ciclico di ordine 3 e, per il Teorema di Lagrange, 3 divide l'ordine di $(D/\pi D)^*$, quindi $N\pi \equiv 1 \pmod 3$. Dunque esiste un unico intero $m = 0, 1$ o 2 tale che

$$\alpha^{\frac{N\pi-1}{3}} \equiv \omega^m \pmod \pi.$$

I risultati precedenti ci permettono di definire il simbolo cubico. Siano $\alpha, \pi \in D$ con π primo e $N\pi \neq 3$, il *carattere* (o *simbolo*) *cubico* di α modulo π, $\left(\frac{\alpha}{\pi}\right)_3$, è tale che:

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & \text{se } \pi|\alpha \\ \alpha^{\frac{N\pi-1}{3}} \bmod \pi & \text{altrimenti.} \end{cases}$$

In analogia a quanto fatto con il simbolo di Jacobi nel Capitolo 1, estendiamo ora la definizione di residuo cubico in modo tale da poter lavorare con elementi non necessariamente primi di D nel denominatore. Questo è alla base dell'algoritmo per il calcolo veloce del simbolo cubico.
Siano $\alpha, \beta \in D$ con $3 \nmid N\beta$ e β non un'unità. Sia $\beta = \beta_1^{b_1}\beta_2^{b_2}\cdots\beta_s^{b_s}$ la fattorizzazione in potenze di primi distinti di D. Definiamo il *carattere (o simbolo cubico) esteso* di α modulo β, $\left(\frac{\alpha}{\beta}\right)_3$, nel seguente modo:

$$\left(\frac{\alpha}{\beta}\right)_3 = \prod_{j=1}^{s}\left(\frac{\alpha}{\beta_j}\right)_3^{b_j}.$$

Inoltre diremo che $\pi \in D$ è *primario* se $\pi \equiv 2 \pmod 3$.
L'utilità di questa definizione sta nell'eliminare l'ambiguità creata dal fatto che ogni elemento in D diverso da zero ha sei associati. Infatti, se $N\pi = p \equiv 1 \pmod 3$, si ha che, tra gli associati di π, esattamente uno è primario.
Dunque, per ogni $\beta \in D$, esistono $P(\beta), c(\beta)$ tali che:

- $P(\beta)$ è primario;
- $P(\beta) = (3P(\beta)_1 - 1) + 3P(\beta)_2\omega$;
- $c(\beta) \in \{0, 1, -1\}$;
- $\beta = \pm\omega^{c(\beta)}P(\beta)$.

Inoltre, si ha il seguente

Teorema 3. *Siano $\alpha, \gamma, \beta \in D$ con $3 \nmid N\beta$, β non è un'unità e β primario, scriviamo $\beta = (3\beta_1 - 1) + 3\beta_2\omega$. Abbiamo le seguenti proprietà:*

- *se $\alpha \equiv \gamma \pmod\beta$, allora $\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\gamma}{\beta}\right)_3$;*
- $\left(\frac{\pm 1}{\beta}\right)_3 = 1$;
- *se β e $\tilde{\beta}$ sono associati, allora $\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\alpha}{\tilde{\beta}}\right)_3$;*
- ***Legge di reciprocità cubica estesa**:*

  se $P(\alpha) = \alpha$ e $P(\beta) = \beta \in D$, allora $\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3$;
- $\left(\frac{1-\omega}{\beta}\right)_3 = \omega^{-\beta_1}$;

- $\left(\frac{\omega}{\beta}\right)_3 = \omega^{\beta_1+\beta_2}$.

Queste proprietà ci consentono di enunciare un algoritmo per il calcolo ricorsivo del simbolo cubico esteso:

Algoritmo 0.0.4

RCUB(x,y)= IF ($x = -1$ or $y = -1$) THEN 0
ELSE IF ($P(y) \neq y$) THEN **RCUB**$(x, P(y))$
ELSE IF ($(1-\omega)|x$) THEN **RCUB**$(\frac{x}{1-\omega}, y) \cdot (-y_1)$
ELSE **RCUB**$(y \bmod P(x), P(x)) \cdot (-c(x)(P(x)_1 + P(x)_2))$

Sia $D = \mathbb{Z}[\omega]$ e $\beta \in D$ tale che β non è un'unità e $3 \nmid N\beta$. Indichiamo con $RC(\beta)$ i residui cubici di $(D/\beta D)^*$ e con $SC(\beta)$ l'insieme degli elementi di $(D/\beta D)^*$ aventi simbolo cubico pari a 1. Uno *pseudocubo* modulo β è un elemento α di $(D/\beta D)^*$ che non è un cubo ma tale che $\left(\frac{\alpha}{\beta}\right)_3 = 1$.

Problema della Residuosità Cubica (PRC): *dato un elemento $\beta \in D^*$ composto tale che $3 \nmid \beta$, e $\alpha \in SC(\beta)$, decidere se α è o non è un residuo cubico modulo β, cioè se $\alpha \in RC(\beta)$* oppure no.

Sia $N\beta = n \in \mathbb{N}$. Se la fattorizzazione di n è sconosciuta, allora non esiste alcun metodo efficiente per risolvere il PRC. È opinione diffusa che il PRC abbia una difficoltà equivalente al problema di fattorizzare gli interi, anche se nessuna dimostrazione di ciò sia stata ancora scoperta.
Dai test da noi effettuati si può notare come i tempi di calcolo del simbolo cubico, mediante l'Algoritmo 0.0.4, da noi implementato, siano nettamente migliori di quelli in cui si utilizza l'esponenziale modulare. Abbiamo osservato, inoltre, un importante risultato: il nostro algoritmo ha un tempo di esecuzione quadratico, mentre per l'esponenziale, come noto, questo è cubico.
Abbiamo anche voluto mettere a confronto i tempi totali di calcolo del simbolo cubico rispetto a quello di Jacobi. Va osservato che per il calcolo del simbolo di Jacobi abbiamo utilizzato l'Algoritmo 0.0.1, mentre per il calcolo del simbolo cubico l'Algoritmo 0.0.4. Da questi confronti si evince che il calcolo del simbolo cubico, ottenuto con un' implementazione non del tutto ottimizzata, sia circa 8 volte più lento del simbolo di Jacobi. La causa di questo fatto è da imputare principalmente al calcolo della norma, in quanto con la sua complessità quadratica rimane il "collo di bottiglia" del nostro

algoritmo.

Nel Capitolo 4 ci occupiamo di simboli biquadratici e della legge di reciprocità che ne deriva. Anche qui, dopo aver definito il simbolo biquadratico esteso, formuliamo il problema della *residuosità biquadratica*.
Per definire i simboli quadratici e studiarne le proprietà, dobbiamo introdurre l'anello degli interi di Gauss, cioè l'insieme $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$. $\mathbb{Z}[i]$ è un dominio d'integrità, in quanto sottoinsieme di $\mathbb{C}$, ed è chiuso anche rispetto alla coniugazione complessa e per ogni $\alpha \in \mathbb{Z}[i]$, la *norma* di α è definita come $N\alpha = \alpha\overline{\alpha} = a^2 + b^2$.
Sia $B = \mathbb{Z}[i]$. B è un anello a fattorizzazione unica. Quindi per ogni π irriducibile di B tale che $\pi|\alpha\beta$ allora o $\pi|\alpha$ oppure $\pi|\beta$, con $\alpha, \beta \in B$.
Da adesso in poi la parola primi indicherà solamente i primi positivi in $\mathbb{Z}$, mentre ci riferiremo ai primi in B con il termine *elementi irriducibili*.
Con il seguente risultato otteniamo una classificazione completa delle unità e degli elementi irriducibili di B.

Teorema 4.

- *$\alpha \in B$ è un'unità se e solo se $N\alpha = 1$. Quindi le unità di B sono $\pm 1, \pm i$.*
- *Se π è irriducibile allora esiste un primo $p \in \mathbb{Z}$ tale che $\pi|p$.*
- *Se $\alpha \in B$ e $N\alpha$ è primo allora α è irriducibile.*
- *$1 + i$ è irriducibile e $2 = -i(1 + i)^2$ è la fattorizzazione in irriducibili di 2 in B.*
- *Se $q \equiv 3 \pmod 4$ è primo in $\mathbb{Z}$, allora q è un elemento irriducibile di B.*
- *Se $p \equiv 1 \pmod 4$, allora esistono due interi a e b, unici e positivi, tali che $a^2 + b^2 = p$. Inoltre $\pi = a + bi$ è irriducibile in B e $p = \pi\overline{\pi}$.*

Se $\pi \in B$ è irriducibile, allora $B/\pi B$ è un campo finito con $N\pi$ elementi. Inoltre, se $\pi \nmid \alpha$, allora $\alpha^{N\pi - 1} \equiv 1 \pmod \pi$, ed esiste, dunque, un unico intero $j \in \mathbb{Z}/4\mathbb{Z}$ tale che

$$\alpha^{\frac{N\pi - 1}{4}} \equiv i^j \pmod \pi.$$

Allora siano $\alpha, \pi \in B$ con π irriducibile e $N\pi \neq 2$. Il *carattere (o simbolo) biquadratico* di α modulo π, $\left(\frac{\alpha}{\pi}\right)_4$, è così definito:

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} 0 & \text{se } \pi|\alpha \\ \alpha^{\frac{N\pi-1}{4}} \pmod{\pi} & \text{altrimenti .} \end{cases}$$

Procedendo in analogia ai residui cubici e quadratici, possiamo estendere la definizione di residuo quadratico ad elementi non necessariamente irriducibili di B nel denominatore del simbolo. Siano $\alpha, \beta \in B$ con $(1+i) \nmid \beta$ e β non unità, e sia $\beta = \beta_1^{b_1}\beta_2^{b_2}\cdots\beta_s^{b_s}$ la fattorizzazione in potenze di irriducibili di B. Se $\gcd(\alpha, \beta) = 1$ definiamo il *carattere (o simbolo) biquadratico esteso* di α modulo β, nel modo seguente:

$$\left(\frac{\alpha}{\beta}\right)_4 = \prod_{j=1}^{s}\left(\frac{\alpha}{\beta_j}\right)_4^{b_j}.$$

Anche in questo caso un elemento $\alpha \in B$, non unità, viene definito primario se

$$\alpha \equiv 1 \pmod{(1+i)^3}.$$

Gli elementi primari di B soddisfano le seguenti proprietà:

- Un elemento $\alpha = a + bi \in B$ diverso dall'unità è primario se, e solo se, verifica una di queste due condizioni:
  - $a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$;
  - $a \equiv 3 \pmod 4, b \equiv 2 \pmod 4$.
- Sia $\alpha \in B$ non unità tale che $(1+i) \nmid \alpha$. Allora esiste un'unica unità u tale che $u\alpha$ sia primario.
- Un elemento primario può essere scritto come il prodotto di primari irriducibili.

Osseviamo che, per ogni $\beta \in B$, esistono $P(\beta), c(\beta)$ tali che:

- $P(\beta)$ è primario;
- $c(\beta) \in \{0, 1, 2, 3\}$;
- $z = i^{c(\beta)}P(\beta)$.

Abbiamo il seguente

Teorema 5. *Siano $\alpha, \gamma, \beta \in B$ con $(1+i) \nmid \beta$, β non è un'unità e β primario, allora i simboli biquadratici estesi soddisfano le seguenti proprietà:*

- *se $\alpha \equiv \gamma \pmod{\beta}$, allora $\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\gamma}{\beta}\right)_3$;*
- $\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\alpha}{\tilde{\beta}}\right)_4$ *se $\tilde{\beta}$ è associato di β;*
- **legge di reciprocità biquadratica estesa***:*

  $\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\beta}{\alpha}\right)_4 (-1)^{\frac{c-1}{2}\frac{a-1}{2}}$ *se $\alpha = c+di, \beta = a+bi$ sono primari e primi tra loro;*
- *Se $\beta = a+bi$ allora $\left(\frac{1+i}{\beta}\right)_4 = i^{\frac{3(a-b-b^2-1)}{4}}$;*
- $\left(\frac{i}{\beta}\right)_4 = i^{\frac{N\beta-1}{4}}$.

Queste proprietà ci consentono di enunciare un'algoritmo per il calcolo ricorsivo del simbolo cubico esteso, ponendo $z = y \bmod P(x)$:

Algoritmo 0.0.5

RBIQ(x,y)= IF $(x = -1$ or $y = -1)$ THEN 0
ELSE IF $(P(y) \neq y)$ THEN **RBIQ**$(x, P(y))$
ELSE IF $((1+i)|x)$ THEN **RBIQ**$(\frac{x}{1-i}, y) \cdot \left(\frac{-(y_1-y_2-y_2^2-1)}{4}\right)$
ELSE **RBIQ**$(z, P(x)) \cdot \left(-c(x)^{\frac{N(P(x))-1}{4}} + \frac{(z_1-1)(P(x)_1-1)}{2}\right)$

Sia $B = \mathbb{Z}[i]$ e $\beta \in B$, tale che β non sia un'unita e $2 \nmid N\beta$. Indichiamo con $RB(\beta)$ i residui biquadratici di $(B/\beta B)^*$ e con $SB(\beta)$ l'insieme degli elementi di $(B/\beta B)^*$ aventi simbolo biquadratico pari a 1.

Problema della Residuosità Biquadratica (PRB): *dato un elemento $\beta \in B^*$ composto tale che $2 \nmid \beta$, e $\alpha \in SB(\beta)$, decidere se α è o non è un residuo biquadratico modulo β, cioè se $\alpha \in RB(\beta)$* oppure no.

Sia $N\beta = n \in \mathbb{N}$. Dunque, come nel caso della residuosità cubica, è opinione diffusa che il PRB ha una difficoltà di risoluzione pari al problema

di fattorizzare gli interi.
Nel Capitolo 5 proponiamo tre *protocolli di identificazione* il cui scopo è quello di provare elettronicamente la propria identità non permettendo a nessuno di poterci sostituire nella procedura di identificazione. Tratteremo i seguenti schemi di identificazione a chiave pubblica:

- Fast Legendre Identification Protocol.
- Cubic Residue Identification Protocol.
- Biquadratic Residue Identification Protocol.

Sono tutti basati sul protocollo *sfida-e-risposta* e sono caratterizzati da una minima potenza di calcolo richiesta per effettuare una verifica.
Abbiamo condotto le implementazioni e i test usando programmi scritti in linguaggio C con l'utilizzo delle funzioni della libreria *pari.h* di PARI [53] e della libreria *cubic.h*, da noi implementata. Il sistema PARI è un pacchetto creato essenzialmente per operare in teoria dei numeri ad alta velocità.

Bibliografia

Testi di Crittografia e Programmazione

[1] B. W. Kernighan, P. J. Plauger, *Elements of Programming Style*, McGraw-Hill, 1978.

[2] B. W. Kernighan, D. M. Ritchie, *Linguaggio C*, Jackson Libri, 1989.

[3] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, seconda edizione, 1994.

[4] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, Berlin, 1998.

[5] E. Kranakis, *Primality and Cryptography*, John Wiley and Sons, 1986.

[6] A. J. Menezes, P. C. Van Oorschot e S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.

[7] B. Schneier, *Applied Cryptography*, John Wiley & Sons Inc., seconda edizione, 1996.

[8] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, FL, 1995.

[9] J. C. A. Van Der Lubbe, *Basic Methods of Cryptography*, Cambridge University Press, Cambridge, 1998.

Testi di Teoria dei Numeri

[10] D. M. Bressoud, *Factorization and Primality Testing*, UTM Springer, 1989.

[11] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1997.

[12] H. Davenport, *Aritmetica Superiore*, quinta edizione, Zanichelli, 1995.

[13] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, New York, seconda edizione, 1980.

[14] R. F. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 1994.

[15] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, The Clarendon Press Oxford University Press, New York, quinta edizione, 1979.

[16] K. Ireland e M. Rosen, *A Classical Introduction to Modern Number Theory*, seconda edizione, Springer, 1990.

[17] P. Ribenboim, *Algebraic Numbers*, Wiley, New York, 1972.

[18] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[19] H. J. Smith, *Report on Theory of Numbers*, Chelsea Publishing Company Inc., New York, 1965.

[20] J. Stillwell, *Elements of Algebra*, Springer-Verlag, New York, 1996.

Articoli di Crittografia e Teoria dei Numeri

[21] W. Adams, D. Shanks, *Strong Primality Tests That Are Not Sufficient*, Math. Comp. **39**, Nr. 159, 1982, pp. 255–300.

[22] S. D. Adhikari, The early reciprocity laws: from Gauss to Eisenstein, *Cyclotomic Fields and Related Topics*, Bhaskaracharya Pratishthana, 2000, pp. 55–74.

[23] L. Adleman, R. Mc Donnel, *An Application of Higher Reciprocity to Computational Number Theory*, Proc. of 23 IEEE Symp. on Foundation of Computer Science, 1982, pp. 100–106.

[24] L. M. Adleman, C. Pomerance, R. S. Rumely, *On Distinguishing Prime Numbers from Composite Numbers*, Ann. Math. **117**, 1983, pp. 173–206.

[25] F. Arnault, *Rabin-Miller Primality Test: Composite Numbers Which Pass It*, Math. Comp. **64** (209), 1995, pp. 355–361.

[26] R. Baille, S. Wagstaff, Jr., *Lucas Pseudoprimes*, Math. Comp. **35**, 1980, pp. 1391–1417.

[27] W. D. Banks, D. Lieman, I. E. Shparlinski, R. Steinfeld e Y. Zheng, *An Identification Scheme Based On Legendre Symbols*.

[28] D. Bleichenbacher, *Efficiency and Security of Cryptosystems Based on Number Theory*, Dissertation ETH Zurich, 1996.

[29] D. Boneh, *Twenty Years of Attacks on the RSA Cryptosystem*, preprint, 2000.

[30] H. Cohen, H. W. Lenstra, Jr., *Primality Testing and Jacobi Sums*, Math. Comp. **48**, 1984, pp. 297–330.

[31] M. J. Collisions, *The Origins of the Cubic and Biquadratic Reciprocity Laws*, Arch. Hist. Exact Sci. **17**, no. 1, 1977, pp. 63–69.

[32] I. Damgard, P. Landrock, C. Pomerance, *Average Case Error Estimates for the Strong Probable Prime Test*, Math. Comp. **61**, 1993, pp. 177–194.

[33] W. Diffie, M. E. Hellman, *Multiuser Cryptography Tecniques*, Proceedings of AFIPS National Computer Conference, 1976, pp. 644–654.

[34] W. Diffie, M. E. Hellman, *New Direction in Cryyptography*, IEEE Transaction on Information Theory, V. IT-22 no. **6**, 1976, pp. 644–654.

[35] W. Diffie, *The First Ten Years of Public-Key Cryptography*, Contemporary Cryptology, The Science of Information Integrity, IEEE Press, 1992, pp.135–175.

[36] G. Eisenstein, *Lois de réciprocitè*, Mathematische Worke, Band I, New York, 1975, pp. 53–67.

[37] J. Grantham, *A Probable Prime Test with High Confidence*, J. Number Thery **72**, 1998, pp. 32–47.

[38] G. Jaenschke, *On Strong Pseudoprimes in Several Bases*, Math. Comp. **61**, 1993, pp. 915–926.

[39] E. Lehmer, *Rational Reciprocity Laws*, Am. Math. Monthly **85**, 1978, pp. 467–472.

[40] H. W. Lenstra, Jr., *Euclid's Algorithm in Cyclotomic Fields*, J. Lond. Math. Soc. ser. 2, vol. **10**, 1975, pp. 457–465.

[41] P. Mihailescu, *Algorithms for Generating, Testing and Proving Primes: A Survey*, Progress in Computer Science and Applied Logic **20**, Birkhauser Verlag Basel, Switzerland, 2001, pp. 93–122.

[42] P. Mihailescu, *Recent Developments in Primality Proving*, Progress in Computer Science and Applied Logic **20**, Birkhauser Verlag Basel, Switzerland, 2001, pp. 93–122.

[43] S. Muller, *Carmichael Numbers and Lucas Test*, Contemporary Mathematics **225**, 1999, pp. 193–202.

[44] S. Muller, *On Strong Lucas Pseudoprimes*, Contribution to General Algebra **10**, 1998, pp. 237–249.

[45] S. Muller, *On the Combined Fermat/Lucas Probable Prime Test*, IMA-Crypto & Coding'99, LNCS 1746, Springer-Verlag, 1999, pp. 222–235.

[46] C. Pomerance, J. L. Selfridge, S. S. Wagstaff, Jr., *The Pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35**, 1980, pp. 1003–1026

[47] M. O. Rabin, *Probabilistic Algorithm for Primality Testing*, J. Number Theory **12**, 1980, pp. 128–138.

[48] R. Scheidler, *A Public-key Cryptosystem Using Purely Cubic Fields.*

[49] C. P. Schnorr, *Efficient Identification and Signatures for Smart Cards.*

[50] R. Solovay, V. Strassen, *A Fast Monte Carl Test for Primality*, SIAM J. Comput. **6**, 1977, pp. 64–85.

[51] H. C. Williams, *Edouard Lucas and Primality Testing*, Canadian Society Series of Monographs and Advanced Texts, vol. **22**, John Wiley and Sons, 1998.

[52] Y. Zheng, T. Matsumoto, H. Imai, *Cryptography Applications of* γ^{th}*-Residuosity Problem with* γ *an Odd Integer*, Symp. on Cryptography & Information Security, Japan, 1988.

Varie

[53] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, 'Pari-GP Versione 2.0.20 (beta)', **http://www.parigp-home.de**, 2001.

[54] E. Biham, D. Rawitz, *Cryptology*, Cryptology Course of 1999, Computer Science Department Technion, Haifa 32000, Israel.

[55] C. Caldwell: *The Prime Pages*, **http://www.utm.edu/research/primes**.

[56] J. Grantham's homepage: **http://www.pseudoprime.com**.