Universitá degli Studi Roma Tre

Facoltá di Scienze M.F.N.

Corso di Laurea in Matematica

Sintesi della Tesi di laurea Specialistica in Matematica

La fattorizzazione e il crivello del campo numerico

Candidato

Lucia Tiberio

Relatore

Prof. Andrea Bruno

Anno Accademico 2010-2011

Maggio 2012

Classificazione: 11Y05, 11N36, 11Y40.

Parole Chiave: CURVE ELLITTICHE, ALGORITMO, CRITTOGRAFIA

La crittografia è la disciplina che si occupa di trasmettere messaggi tra due persone (o enti) in modo tale che il messaggio sia inintelligibile a terze persone.
L'esigenza di comunicare informazioni in maniera riservata, in modo tale che solamente un numero limitato di persone autorizzate fossero in grado di accedervi, è sempre stata presente nella storia dell'umanità.
Con la diffusa proliferazione dei computer nelle abitazioni e nei posti di lavoro e con l'inarrestabile sviluppo di internet, la possibilità di effettuare comunicazioni e transazioni sicure per via telematica è diventata una questione di vitale importanza.

La crittografia è una scienza antichissima, si dice che anche Giulio Cesare per comunicare con le sue truppe in Gallia usasse un sistema crittografico. La sua tecnica consisteva nell'associare a ciascuna lettera dell'alfabeto latino, la lettera ottenuta traslando di tre. Secondo il metodo di Cesare, la cifratura del messaggio *"morte ai Galli"* era *"ptuzh dn Ldoon"*; ma essendo l'odierno alfabeto composto da 26 caratteri, con un massimo di 26 prove si riuscirebbe a rompere questo schema che quindi non è robusto.
In generale si è sempre cercato di assicurare che venissero rispettati i seguenti requisiti:

- riservatezza: i messaggi inviati devono poter essere letti solo da persone autorizzate;
- integrità: i messaggi devono giungere a destinazione senza manomissione alcuna;
- autenticità: il mittente sia identificato con certezza;
- non ripudiabilità: il mittente non possa disconoscere di aver spedito il messaggio.

Per chiarire meglio le idee sugli oggetti che si hanno a disposizione nello scambio di due messaggi definiamo cosa si intende per *crittosistema*.
Un *crittosistema* è un insieme del tipo (P,C,K,E,D) dove:

- P è l'insieme (o spazio) dei *messaggi in chiaro*
- C è l'insieme (o spazio) dei *messaggi cifrati*
- K è l'insieme (o spazio) delle *chiavi*

- E è la *funzione di cifratura*

$$\begin{aligned} E : P \times K &\longrightarrow C \\ (p, k) &\longmapsto c = E_k(p) \end{aligned}$$

- D è la *funzione di decifratura*

$$\begin{aligned} D : C \times K &\longrightarrow P \\ (c, k) &\longmapsto p = D_k(c). \end{aligned}$$

Queste funzioni sono tali che $D_k(E(p)) = p$ e viceversa, cioè devono essere l'una l'inversa dell'altra.
Lo spazio delle chiavi potrebbe essere complesso e gestito in modi diversi e in diverse circostanze.

Per questa ragione è naturale dividere la crittografia in due branche: crittografia a *chiave privata* e crittografia a *chiave pubblica*.
La differenza tra questi due volti della crittografia sta nel fatto che con un sistema a chiave privata è previsto che due soggetti, che vogliono comunicare utilizzando il sistema, debbano essersi scambiati la chiave in un momento precedente alla comunicazione.
Invece un crittosistema a chiave pubblica non richiede necessariamente che i due soggetti si siano incontrati.

Ogni crittosistema a chiave pubblica basa la propria sicurezza su un problema matematico MOLTO difficile da risolvere.

La possibilità di costruire un sistema crittografico rispondente a requisiti di sicurezza e autenticità, fu provata a livello teorico da Diffie ed Hellman nel 1976 mediante un rivoluzionario metodo a chiave pubblica. Tale idea trovò applicazione pratica due anni dopo utilizzando le proprietà dei numeri primi.

Con la nascita della crittografia a chiave pubblica (o asimmetrica), per la prima volta viene descritto un sistema crittografico in cui non solo non è necessario che si

mantenga tutto segreto, al contrario, è indispensabile che una parte dell'informazione sia addirittura resa pubblica; infatti ciascun utente sceglie una funzione crittografica che dipende da alcuni parametri, ma rende noti solo quelli che permettono di codificare i messaggi a lui diretti, mantenendo segreti quelli necessari alla decodifica.
In questo modo chiunque può spedire un messaggio all'utente in questione senza che questo, se intercettato da terzi, possa essere compreso.

Il nome "asimmetrica" deriva dal fatto che il ruolo delle chiavi di cifratura e di decifratura, a differenza di quanto accade nei casi classici, non è più speculare, essendo la seconda chiave collegata ad un problema di complessità computazionale maggiore di quello utilizzato per costruire la prima.

Per molte persone la crittografia è legata ai film di spionaggio o di guerra, in cui ci sono due parti ben distinte ed i personaggi sono quasi sempre legati da vincoli di fedeltà ad una delle due.
Questa visione della crittografia è sostanzialmente quella classica: oggi, invece, l'uso prevalente della crittografia è legato ad applicazioni molto diffuse; ma che hanno esigenza di riservatezza diverse da quelle tradizionali. Tra gli svariati esempi quotidiani ne citiamo alcuni: l'accesso ad uno sportello bancario automatico, la ricarica delle schede telefoniche o gli acquisti on line.

In questa trattazione analizzeremo varie modalità di fattorizzazione di un intero, in particolare descriveremo il *Crivello del campo numerico*, in quanto sulla difficoltà di fattorizzare un numero intero si basa, in buona sostanza, la moderna crittografia a chiave pubblica.

Nella teoria dei numeri per fattorizzazione si intende la scomposizione di un numero intero in un insieme di divisori non banali che, moltiplicati tra loro, diano il numero di partenza. In particolare scomporre un numero $n \in N$ in *fattori primi* significa trovare

quell'insieme di numeri primi $p_1, ..., p_k$ tali che:

$$\prod_{i=1}^{k} p_i = n$$

Possiamo quindi enunciare il seguente teorema:

Teorema 0.1 (Teorema Fondamentale dell'aritmetica)**.** *Sia $n \neq 0$ un intero. Allora n si può scrivere come prodotto di un numero finito di numeri primi come segue:*

$$n = c \cdot p_1 \cdots p_k$$

dove $c = \pm 1$ e i p_i sono interi primi positivi e $k \geq 0$. Questa espressione è unica a meno dell'ordine dei fattori primi.

La ricerca di un algoritmo per la determinazione di una tale fattorizzazione è uno storico problema della matematica. Tuttavia, ancora oggi, tale ricerca non ha prodotto risultati soddisfacenti, nel senso che non è ancora stato trovato un algoritmo con tempo di esecuzione *polinomiale*; cioè un algoritmo il cui numero di passi necessari per terminare è una funzione polinomiale delle cifre dell'intero da fattorizzare.
Si tratta quindi di un problema ancora aperto della teoria dei numeri e se l'algoritmo esistesse renderebbe possibile la risoluzione di altri problemi considerati decisamente complessi quali ad esempio il calcolo rapido di funzioni moltiplicative e la compressione di un insieme di numeri primi.

Non è ancora noto, infatti, se esistano degli algoritmi per computer classici che risolvano il problema della fattorizzazione in un tempo polinomiale, mentre ne è stato trovato uno, *algoritmo di fattorizzazione di Shor*, che risolve il problema per i computer quantistici (o quantici), che sono dispositivi per il trattamento ed elaborazione di informazioni che, per eseguire le classiche operazioni sui dati, utilizzano i fenomeni tipici della meccanica quantistica come la sovrapposizione degli effetti.

Nonostante ciò, negli ultimi quarant'anni sono stati fatti molti passi in avanti. Nel 1975, difatti, è stato presentato da J.Brillhart e M.A.Morrison il Metodo delle frazioni

continue, ovvero il primo algoritmo per la fattorizzazione degli interi ad avere complessità sub-esponenziale, cioè il costo dell'algoritmo per ogni $\varepsilon > 0$ è pari a $\mathcal{O}(exp(\varepsilon\ log(n)))$ operazioni elementari.
Tale algoritmo spostò il limite per il numero delle cifre decimali dell'intero da fattorizzare da 20 a 50. Da allora si è fatta molta strada. Infatti, successivamente, il Crivello quadratico, ideato da C.Pomerance nel 1982, e il Metodo delle curve ellittiche, ideato da H.W.Lenstra Jr. nel 1985, hanno più che raddoppiato tale limite.

Come detto precedentemente porremo particolare attenzione sul Crivello del campo numerico, in breve NFS (dall'inglese *Number Field Sieve*), ovvero quello che, attualmente è il più veloce algoritmo per la fattorizzazione di un generico intero con più di 150 cifre.

Il crivello del campo numerico può essere considerato un'estensione del più semplice *rational sieve*. Per fattorizzare un intero grande n, quest'ultimo algoritmo ha bisogno di trovare numeri dello stesso ordine di n che hanno fattori primi piccoli, la rarità di questi numeri rende di fatto inutilizzabile il *rational sieve*.
Per ovviare a questo problema, il crivello del campo numerico sposta il problema negli anelli degli interi di alcuni campi numerici.
Questo approccio, pur introducendo alcune complicazioni teoriche, rende sufficiente cercare gli interi con fattori primi piccoli tra i numeri di ordine $n^{1/d}$, ove d è un intero maggiore di 1. Dato che i numeri più piccoli hanno generalmente fattori primi più piccoli, questa modifica aumenta notevolmente l'efficienza del metodo.

In particolare l'idea chiave che sta alla base di questo algoritmo è l'utilizzo di numeri *lisci* o B-*numeri* in un opportuno anello numerico diverso da $\mathbb{Z}$. Tale idea è stata proposta per la prima volta da John Pollard nel 1988. Da allora molti matematici hanno contribuito con vari suggerimenti allo sviluppo di tale algoritmo.

L'NFS è, senza dubbio, un algoritmo molto *complicato*. Strutturalmente è simile al crivello quadratico (potremmo quasi dire che ne è una generalizzazione) ma, a differenza di quest'ultimo, fa uso di molti parametri da ottimizzare e, inoltre, poggia su una teoria

molto meno elementare.
Difatti, per dimostrarne la validità (così come per comprenderne il funzionamento) avremo bisogno di richiamare alcuni risultati di Algebra Commutativa e Teoria Algebrica dei Numeri.

In teoria, non vi è alcuna differenza fra teoria e pratica.
In pratica ce n'è.

Da un punto di vista più pratico, possiamo aggiungere che per essere eseguito su un computer, l'NFS necessita (per numeri molto grandi) della capacità di gestire grosse quantità di dati e di una potenza di calcolo enorme. Insomma, implementarlo con successo sul proprio computer di casa non è davvero un'operazione semplice!

Tutte le ultime fattorizzazioni record ottenute portano la firma del crivello del campo numerico. Tra queste, citiamo la fattorizzazione di RSA-160 (risalente al 2003), la fattorizzazione del numero di Cunningham pari a $2^{773} + 1$ (ottenuta nel 2000) e infine la fattorizzazione di F_9, che è il nono numero di Fermat (1990), che tratteremo più nel dettaglio nell'ultimo capitolo della tesi.

Prima del crivello del campo numerico, il miglior algoritmo per la fattorizzazione di un generico numero intero era, come già detto, il crivello quadratico, il cui tempo di esecuzione congetturato, per n che va all'infinito, è $L_n[1/2, 1 + o(1)]$ dove:

$$L_n[u, v] := exp(v\ (log\ n)^u (log\ log\ n)^{1-u})$$

Per l'NFS, invece, il tempo di esecuzione congetturato è:

$$L_n[1/3, (64/9)^{1/3} + o(1)]$$

L'esponente $u = 1/3$ è la principale novità dell'NFS. Difatti, come abbiamo visto sopra, nel caso del crivello quadratico si ha $u = 1/2$; ma non solo, questo vale anche per il metodo delle frazioni continue e per il metodo delle curve ellittiche.

Addirittura, per molto tempo, si è creduto che quest'ultimo valore fosse un limite insuperabile per la complessità degli algoritmi di fattorizzazione.

La struttura della tesi è la seguente.

Nel capitolo 1 descriveremo i principali algoritmi di fattorizzazione esistenti, rinfrescandoci la memoria su alcune definizioni e risultati necessari per la comprensione di tale argomento.

Distingueremo due categorie di algoritmi: quelli di fattorizzazione esponenziale e quelli di fattorizzazione sub-esponenziale; la differenza sta appunto nella loro complessità computazionale.

Per complessità computazionale si intende:

Definizione 0.1. La complessità computazionale di un algoritmo che opera sugli interi è data dal numero di operazioni bit occorrenti per eseguirlo.

Notiamo che la complessità computazionale di un algoritmo *non è un numero*, ma una *funzione*.

L'*operazione bit* è l'unità di misura usata per calcolare la complessità di un algoritmo, la quale, in sostanza, corrisponde ad una operazione elementare costituente l'algoritmo. Per *operazione bit* intendiamo una delle seguenti operazioni elementari:

(1) addizione fra due cifre binarie (es. $0 + 1$);

(2) sottrazione fra due cifre binarie (es. $1 - 0$);

(3) moltiplicazione fra due cifre binarie (es. $1 \cdot 1$);

(4) divisione di un intero a due cifre binarie per una cifra binaria (es. 10 diviso 1);

(5) traslazione a sinistra di un posto, cioè moltiplicazione per 2 e traslazione a destra di un posto, cioè divisione per 2.

E' chiaro che al giorno d'oggi si sottopone un intero N ad uno di questi algoritmi solo dopo aver dimostrato che questo non sia un numero primo, cioè che sia un intero dispari, inoltre si verifica che non abbia fattori primi "piccoli" e che non sia una potenza perfetta. La prima condizione è banalmente verificabile mediante uno dei vari criteri per testare la primalità di un intero, mentre l'altra si può provare calcolando $\lfloor n^{1/k} \rfloor$ (dove con $\lfloor . \rfloor$ si intende la parte intera inferiore di un numero) e inoltre controllando che la sua *k-esima* potenza non sia n, con k che varia tra 2 e $\log n$.

Tra le varie definizioni e teoremi enunciati e discussi all'interno della tesi, i principali sono:

Definizione 0.2. Sia n un intero dispari non primo e $a \in U(\mathbb{Z}_n)$, allora n si dice *pseudoprimo in base a* se:

$$a^{n-1} \equiv 1 \pmod{n}$$

Tale proprietà è detta *pseudoprimalità alla Fermat* e in tal caso a è una *base di Fermat di n.*

La nozione di *numero pseudoprimo in base a* può essere "rafforzata" determinando un tipo più raro di numeri, la cui esistenza dimostra l'impossibilità di invertire il *Piccolo Teorema di Fermat.*

Definizione 0.3. Si chiama *numero di Carmichael* (pseudoprimo assoluto) ogni intero positivo non primo n tale che, per ogni intero a, relativamente primo con n, risulti:

$$a^{n-1} \equiv 1 \pmod{n}.$$

In particolare un intero positivo composto n si dice di *Carmichael* se è pseudoprimo in ogni base.

Verranno poi distinti gli algoritmi di fattorizzazione esponenziale e quelli di fattorizzazione sub-esponenziale, vediamo la loro differenza e descriviamo poi rapidamente i vari algoritmi.

Definizione 0.4. Un algoritmo $\mathcal{A}$ per eseguire un calcolo su numeri interi si dice *di tempo polinomiale*, o semplicemente *polinomiale*, se esiste un intero positivo d, detto *ordine* dell'algoritmo, tale che il numero di operazioni bit necessarie per eseguire l'algoritmo su interi di lunghezza binaria al più k è $\mathcal{O}(k^d)$.

Definizione 0.5. Un algoritmo $\mathcal{A}$ si dice di *tempo esponenziale*, o semplicemente *esponenziale*, se il numero di operazioni bit necessarie per eseguire l'algoritmo su interi di lunghezza binaria al più k è dello stesso ordine di e^{ck}, per una costante $c > 0$.

Un algoritmo $\mathcal{A}$ non esponenziale si dice *subesponenziale* se il numero di operazioni bit necessarie per eseguire l'algoritmo su interi di lunghezza binaria al più k è $\mathcal{O}(e^k)$.

Gli algoritmi descritti sono i seguenti:

- *Divisione per tentativi*, si può dimostrare che un intero $n \geq 2$ è primo verificando direttamente la definizione, cioè verificando che nessuna delle divisioni di n per gli interi $2 \leq m \leq (n-1)$ è esatta.
  Poichè se $n = mr$, allora m e r non possono essere contemporaneamente $m, r > \sqrt{n}$; nel nostro algoritmo potremmo limitarci ad esaminare come divisori di n una lista dei numeri primi $\leq n$ (se si conoscono tali primi, altrimenti si divide per ogni numero dispari).

  La presenza di questo banale algoritmo in questa panoramica è a conferma della difficoltà del problema in oggetto.
  Difatti questo algoritmo è, in alcuni casi, addirittura uno dei migliori che si possa utilizzare (come, per esempio, se bisogna controllare che un numero non abbia fattori primi "piccoli"). Il numero di passi da eseguire nel caso peggiore ($n = pq$ con p e q primi con lo stesso numero di cifre) è dell'ordine di $\sqrt{n}$.

  Per rendersi conto di quanto sia poco efficiente questo algoritmo, basta osservare che se dobbiamo fattorizzare un numero di 100 cifre decimali dobbiamo fare 10^{50} passi e se ogni passo impiega 10^{-10} secondi allora aspetteremo 10^{40} secondi ovvero

10^{32} anni!

- *Differenza di quadrati*, parlando della Divisione per Tentativi abbiamo visto che fattorizzare un numero n è in generale assai dispendioso dal punto di vista della complessità di calcolo. Talvolta è più efficiente il seguente metodo, dovuto al matematico francese Pierre Fermat nel 1600, che viene chiamato sia metodo della *differenza dei quadrati* sia metodo di *fattorizzazione alla Fermat*.
  Esso si basa sui seguenti fatti:

  1. si può ovviamente supporre n dispari;
  2. nel caso in cui n sia dispari, fattorizzare n "*equivale*" a determinare due interi x e y tali che
  $$n = x^2 - y^2.$$
  Infatti se $n = x^2 - y^2$, allora $n = (x + y)(x - y)$ è una fattorizzazione di n. Viceversa se $n = ab$, allora, supposto $a \geq b \geq 1$, si può scrivere
  $$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$
  dove $(a+b)/2$ e $(a-b)/2$ sono interi non negativi. Infatti, essendo n dispari, anche a e b sono dispari e quindi $(a \pm b)$ è pari;
  3. determinare x e y tali che $n = x^2 - y^2$ equivale a determinare x tale che $x^2 - n$ sia un quadrato, cioè $x^2 - n = y^2$.

- *Metodo ρ di Pollard*, tale metodo è basato su un'idea del tutto diversa dalle precedenti.
  E' un metodo probabilistico di fattorizzazione, pubblicato da J.M.Pollard nel 1975. Si suppone di sapere che un numero n è composto e per decomporlo in fattori primi si procede lavorando in $\mathbb{Z}_n$.

- *Metodo delle frazioni continue*, è un'applicazione molto significativa dell'algoritmo euclideo che è data dalle cosiddette *frazioni continue*. Esse forniscono, in sostanza, anche un modo alternativo di rappresentare i numeri e, in particolare, nel 1975 è stato presentato da J.Brillhart e M.A.Morrison l'algoritmo delle frazioni continue. Tale algoritmo fu il primo algoritmo di fattorizzazione di un intero n con tempo di esecuzione sub-esponenziale; esso spostò il limite massimo della grandezza del numero da fattorizzare da 20 a 50 cifre decimali.
  Per fattorizzare n questo algoritmo risolve la congruenza $X^2 \equiv Y^2 \pmod{n}$ e lo fa sfruttando la convergenza del *k-esimo* termine $\frac{p_k}{q_k} \in \mathbb{Q}$ (detto anche *convergente*) dell'espansione di $\sqrt{n}$ in frazione continua. Di seguito definiamo le frazioni continue e alcune loro proprietà che intervengono nel processo di fattorizzazione.

Definizione 0.6. Si dice *frazione continua finita* una frazione della forma:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \quad \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} \tag{1}$$

con $a_0, a_1, ..., a_n$ numeri reali, tutti positivi, ad eccezione al più di a_0. I numeri $a_1, ..., a_n$ si chiamano *denominatori parziali*, o *quozienti parziali*, della frazione.

Una frazione finita continua si dice *semplice* se tutti i suoi quozienti parziali sono interi.

L'interesse principale delle frazioni continue è però legato alla loro applicazione nella rappresentazione dei *numeri irrazionali*. Per far questo ci serviranno le frazioni

continue semplici *infinite*.

Lo studio delle frazioni continue si ritrova nella matematica indiana del sesto e del dodicesimo secolo per risolvere equazioni lineari. I primi studi rigorosi di frazioni continue però compaiono in un libro di L.Bombelli del 1572 inventore, tra l'altro, dei numeri complessi. In particolare, il termine *frazione continua* apparve per la prima volta nell'edizione del 1653 di J.Wallis "Arithmetica infinitorum". Altri grandi matematici si sono occupati di frazioni continue infinite come ad esempio Eulero nel suo *De fractionibus continuis*, Lagrange, Gauss e infine Liouville, che se ne servì nella famosa dimostrazione dell'esistenza di numeri trascendenti.

Definizione 0.7. Sia $[a_0; a_1, ..., a_n]$ una frazione continua semplice finita. La frazione continua che si ottiene *troncando* la frazione continua al k-esimo quoziente parziale si chiama *k-esimo convergente* e si denota nel modo seguente:

$$C_k = [a_0; a_1, ..., a_k], \qquad \text{per ogni } 1 \leq k \leq n.$$

Si noti che C_{k+1} si ottiene da C_k sostituendo a_k con $a_k + 1/a_{k+1}$.
Ovviamente per $k = n$ si ha l'intera frazione continua iniziale $[a_0; a_1, ..., a_n]$.

Proposizione 0.2. Siano $a_0, ..., a_n$ numeri reali positivi (tranne al più a_0, che può essere anche negativo) e siano fatte le successioni $(p_0, ..., p_n)$ e $(q_0, ..., q_n)$ definite ricorsivamente come segue:

$$\begin{aligned} &p_0 = a_0; && q_0 = 1; \\ &p_1 = a_0 a_1 + 1; && q_1 = a_1; \\ &\vdots && \vdots \\ &p_k = a_k p_{k-1} + p_{k-2}; && q_k = a_k q_{k-1} + q_{k-2}; \end{aligned}$$

per $k = 2, 3, .., n$. Allora il k-esimo convergente C_k è dato da:

$$C_k = \frac{p_k}{q_k}$$

con $MCD(p_k, q_k) = 1$.

Teorema 0.3. Ogni numero irrazionale positivo α si può esprimere come frazione continua semplice infinita in modo unico.

Definizione 0.8. Siano n ed a due interi positivi e sia r il resto della divisione di a per n (quindi $0 \leq r < n$). Definiamo *minimo residuo assoluto* di a rispetto ad n, o *modulo* n, l'intero r, se $0 \leq r \leq n/2$, ovvero l'intero $(r-n)$ se $n/2 < r < n$. In quest'ultimo caso, si ha $0 > (r-n) > -n/2$. Denoteremo il minimo residuo assoluto di a rispetto ad n con il simbolo $MRA(a,n)$. In definitiva abbiamo sempre:

$$-\frac{n}{2} < MRA(a,n) \leq \frac{n}{2} \tag{2}$$

e MRA(a,n) è l'unico intero verificante la (2) tale che $a - MRA(a,n)$ sia divisibile per n.

Proposizione 0.4. Sia $n \geq 17$ un intero positivo che non sia un quadrato perfetto e sia $C_k = p_k/q_k$ il k-esimo convergente della frazione continua che esprime $\sqrt{n}$. Allora per ogni $k \geq 1$ si ha

$$|MRA(p_k, n)| < 2\sqrt{n}.$$

La proposizione precedente implica che i minimi residui assoluti dei numeratori dei convergenti della frazione continua di $\sqrt{n}$ siano *ragionevolmente piccoli* rispetto ad n. Dunque, presumibilmente, sapremo fattorizzarli più facilmente di n.

- *Il metodo delle basi di fattorizzazione*, per risolvere l'equazione $X^2 \equiv Y^2 \pmod{n}$ dobbiamo trovare un b tale che $b^2 \pmod{n}$ sia un quadrato.

  L'idea del metodo che ora vogliamo introdurre è la seguente:
  si parte da un intero arbitrario b, si calcola $b^2 \pmod{n}$ e si fattorizza in primi. Se $b^2 \pmod{n}$ è un quadrato, ossia se gli esponenti della sua fattorizzazione in numeri primi sono tutti pari, abbiamo finito, altrimenti si ripete questo procedimento.

Vedremo che, strada facendo, si acquisiscono sufficienti dati che assicurano alla fine il successo del metodo.

Il metodo verrà esposto in maniera sistematica. A tal fine è necessario dare una definizione che giustifica il nome stesso del metodo e un lemma fondamentale per la comprensione di tale procedimento.

Definizione 0.9. Una *base di fattorizzazione* B è una N-upla $(p_1, ..., p_N)$ di numeri primi distinti, che si dicono i *numeri primi* della base.

Un intero m si dice un B-*numero* modulo un intero positivo dispari n, se nella fattorizzazione di $m \pmod n$ appaiono solo i primi $p_1, ..., p_N$, cioè se

$$m \pmod n = p_1^{\alpha_1} \cdots p_N^{\alpha_N}.$$

Il vettore $v(m) = (\alpha_1, ..., \alpha_N) \in \mathbb{N}^N$ è detto il B-*vettore* di $m \pmod n$. Possiamo poi ridurre $v(m)$ modulo 2, cioè considerare il vettore $w(m) = (e_1, ..., e_N) \in \mathbb{Z}_2^N$, tale che $e_i = \alpha_i \pmod 2$ per $i = 1, ...N$. Chiameremo $w(m)$ il B-*vettore ridotto* di $m \pmod n$.

Lemma 0.5. Sia $B \in \mathbb{R}$. Se $m_1, m_2, ..., m_k$ sono interi positivi B-numeri e se $k > \pi(B)$, dove $\pi(B)$ è il numero dei primi nell'intervalllo $[2, B]$, allora esistono $m_{i_1}, m_{i_2}, ..., m_{i_t}$ con $1 \leq i_1 < i_2 < ... < i_t \leq k$ tali che il loro prodotto è un quadrato.

Sia n l'intero da fattorizzare. Fissata una base di fattorizzazione B, il metodo che stiamo esaminando consiste nel cercare un numero K sufficientemente grande di interi $b_1, ..., b_K$ con $b_1^2, ..., b_K^2$ B-numeri $\pmod n$ a partire dai quali si possa determinare un B-numero b che sia un quadrato $\pmod n$, ma in modo *non banale*, cioè si abbia $b^2 \equiv c^2 \pmod n$ ma $b \not\equiv \pm c \pmod n$. Si noti che non chiediamo che il B-numero sia uno dei B-numeri $b_1, ..., b_K$, ma che si possa *determinare a partire da questi.*

Questo metodo, come subito si capisce, non è tanto efficiente: è ben difficile che numeri b scelti a caso si lascino fattorizzare dai *pochi* primi di B. Ci sono tuttavia altri modi di procedere che però non illustreremo.

- *Il crivello quadratico*, tale metodo (in inglese *Quadratic Sieve*) fu ideato da C.Pomerance nel 1981. Lo illustreremo da un punto di vista euristico, senza soffermarci sul perchè funziona. Il suo costo computazionale pur essendo esponenziale, come quello di tutti i metodi di fattorizzazione noti, presenta in qualche caso degli aspetti di convenienza rispetto ad altri metodi. Fino all'avvento di tecniche più recenti come il crivello dei campi numerici, il crivello quadratico, che è una variante del metodo delle basi di fattorizzazione, è stato l'algoritmo di fattorizzazione più efficiente. Tuttora è il sistema più veloce per fattorizzare numeri fino ad un centinaio di cifre.

I primi tre metodi hanno complessità esponenziale, mentre gli ultimi tre hanno complessità sub-esponenziale.

Nel capitolo 2 effettueremo una carrellata sui principali concetti dell'algebra commutativa, soffermandoci maggiormente sulla descrizione di un particolare tipo di anello numerico e sulle sue fondamentali proprietà che, come vedremo, avrà un ruolo determinante nel crivello del campo numerico: tale anello è $\mathbb{Z}[\alpha]$, con $\alpha \in \mathbb{C}$ radice di un polinomio a coefficienti interi, monico e irriducibile. Inoltre in tale capitolo verranno trattati tutti gli argomenti della Teoria Algebrica dei Numeri e della Teoria delle equazioni necessari proprio alla comprensione dell'NFS.
Tra le principali definizioni troveremo:

Definizione 0.10. Sia D un dominio di integrità (cioè un anello commutativo privo di divisori dello zero). Supponiamo che ad ogni elemento $a \neq 0$ si possa associare un intero non negativo $v(a)$ in modo tale che

(a) $v(a) \leq v(ab) \quad \forall a, b \in D, a \neq 0, b \neq 0$;

(b) dati comunque due elementi a e b in D, $b \neq 0$, esistono q ed r in D tali che

$$a = bq + r, \qquad r = 0 \text{ oppure } v(r) < v(b).$$

Allora D si dice *dominio euclideo* (ED) e l'applicazione

$$\begin{aligned} v : D\backslash\{0\} &\longrightarrow \mathbb{N} \\ a &\longmapsto v(a) \end{aligned}$$

prende il nome di *valutazione*.

L'anello degli interi di *Gauss*, che è il sottoanello di $\mathbb{C}$

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

è un dominio euclideo.

Definizione 0.11. Un dominio di integrità con unità in cui ogni ideale è principale, prende il nome di *dominio principale* (PID).

Definizione 0.12. Si dice che un dominio di integrità con unità è un *dominio a fattorizzazione unica* (UFD) se ogni elemento a non nullo e non invertibile si può scrivere come prodotto

$$a = \pi_1 \cdot \pi_2 \cdots \pi_n$$

dove i π_i sono irriducibili. Inoltre, se

$$a = \pi'_1 \cdot \pi'_2 \cdots \pi'_m$$

è un'altra fattorizzazione di a in fattori irriducibili, allora $m = n$ ed esiste una permutazione σ degli indici $1, 2, ..., n$ tale che π_i è associato a $\pi_{\sigma(i)}$ per ogni $i = 1, 2, ..., n$.

Definizione 0.13. Un campo K si dice un *ampliamento* del campo F se esiste un'immersione di F in K. In questo caso, identificando F con la sua immagine isomorfa in K, scriveremo per semplicità di notazione $F \subseteq K$.

Un campo L tale che $F \subseteq L \subseteq K$ si dice un *campo intermedio* dell'ampliamento $F \subseteq K$.

Definizione 0.14. Un polinomio $f(x) \in \mathbb{F}[x]$ si dice *irriducibile* su $\mathbb{F}$ se $deg(f) > 0$ e se $f(x) = g(x)h(x)$ e $deg(g) > 0$, allora $h \in \mathbb{F}$. Altrimenti viene detto *riducibile*.

Corollario 0.6. $\mathbb{F}[X]$ è un UFD, cioè per ogni $f(X) \in \mathbb{F}[X], deg(f) > 0$, esistono $p_1(X), ..., p_r(X) \in \mathbb{F}[X]$ monici irriducibili, $a \in \mathbb{F}$ ed interi $e_i \geq 1$ tali che:

$$f(X) = \prod_{i=1}^{r} p_i^{e_i}(X)$$

e tale scrittura, detta *fattorizzazione canonica* o fattorizzazione in irriducibili, è unica a meno dell'ordine.

Osservazione 1. *Ogni polinomio di grado uno è irriducibile. Se il polinomio ha grado due, esso è riducibile se e soltanto se si spezza in fattori lineari. Analogamente un polinomio di terzo grado è riducibile se e soltanto se si spezza in almeno due fattori, di cui uno necessariamente di grado uno.*

Definizione 0.15. Siano F un campo e $\bar{F}$ una sua fissata chiusura algebrica. Un polinomio $f(x) \in F[x]$ si dice *separabile* su F se le sue radici in F sono tutte distinte ed un elemento $\alpha \in F$ si dice *separabile* su F se il suo polinomio minimo su F è separabile.

Teorema 0.7 (Teorema dell'elemento primitivo)**.** Sia $K := F(\alpha_1, ..., \alpha_n)$ un ampliamento finito di F. Se almeno $(n-1)$ elementi tra gli $\alpha_1, ..., \alpha_n$ sono separabili, allora K è un ampliamento semplice di F.

Definizione 0.16. Un campo K si dice *numerico* se è un'estensione finita di $\mathbb{Q}$.

Osservazione 2. *Ogni anello numerico, essendo sottoanello di un campo, è commutativo e integro. Inoltre, nel seguito della trattazione, supporremo sempre che un anello numerico sia unitario.*
Sia $f \in \mathbb{Z}[X]$ un polinomio monico irriducibile *di grado $d \geq 1$. Sia $\alpha \in \mathbb{C}$ una radice di f. Allora definiamo $\mathbb{Z}[\alpha]$ nel modo seguente:*

$$\mathbb{Z}[\alpha] := \{p(\alpha) : p(X) \in \mathbb{Z}[X]\}.$$

Si verifica facilmente che

$$\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/f\mathbb{Z}[X],$$

e quindi $\mathbb{Z}[\alpha]$ è un anello. Sia $\beta \in \mathbb{Z}[\alpha]$ non nullo. Mostriamo che $\beta = r(\alpha)$ con $deg(r(X)) < d$:

$$\beta \in \mathbb{Z}[\alpha] \Rightarrow \beta = p(\alpha), \qquad \exists\, p(X) \in \mathbb{Z}[X].$$

Dividiamo $p(X)$ per $f(X)$:

$$p(X) = f(X)q(X) + r(X), \qquad r = 0 \text{ oppure } deg(r(X)) < d.$$

Dunque:

$$\beta = p(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$$

dato che $f(\alpha) = 0$. Poichè $\beta \neq 0$ allora $r \neq 0$. Quindi $\beta = r(\alpha)$ con $r(X)$ tale che $deg(r(X)) < d$. Di conseguenza:

$$\mathbb{Z}[\alpha] = \left\{ \sum_{i=0}^{d-1} a_i \alpha^i : a_i \in \mathbb{Z} \right\}.$$

$\mathbb{Z}[\alpha]$ è contenuto in $\mathbb{Q}(\alpha)$ che è un'estensione di grado d di $\mathbb{Q}$ (cioè $\mathbb{Q}(\alpha)$ è un campo numerico), quindi $\mathbb{Z}[\alpha]$ è un anello numerico.

Definizione 0.17. Sia A un anello commutativo unitario. Un *A-modulo* è un gruppo abeliano M su cui A agisce linearmente: più precisamente è una coppia (M, μ), dove M è un gruppo abeliano e μ è un'applicazione $\mu : A \times M \longrightarrow M$ tale che:

1. $\mu(a+s,m) = \mu(a,m) + \mu(s,m)$

2. $\mu(a,m+n) = \mu(a,m) + \mu(a,n)$

3. $\mu(a,\mu(s,m)) = \mu(as,m)$

4. $\mu(1,m) = m$

Definizione 0.18. Sia B un anello, A un sottoanello di B. Un elemento $X \in B$ si dice *intero* su A se X è radice di un polinomio monico a coefficienti in A, ossia se X soddisfa un'equazione della forma

$$X^n + a_1 X^{n-1} + ... + a_n = 0$$

dove gli a_i sono elementi di A. E' chiaro che ogni elemento di A è intero su A.

Definizione 0.19. Sia $A \subset B$ un'estensione di anelli. Allora l'anello degli elementi di B che sono interi su A si dice *chiusura integrale* di A in B e si indica con $\bar{A}^B$.

Definizione 0.20. Sia $A \subset B$ un'estensione di anelli. Allora A si dice *integralmente chiuso* in B se $A = \bar{A}^B$.

Definizione 0.21. Un *sottomodulo* M' di M è un sottogruppo di M che è chiuso rispetto alla moltiplicazione per gli elementi di A.

Proposizione 0.8. Le seguenti condizioni su Σ sono equivalenti:

i) Ogni successione crescente $x_1 \leq x_2 \leq ...$ in Σ è stazionaria (ossia, esiste un intero n tale che $x_n = x_{n+1} = ...$).

ii) Ogni sottoinsieme non vuoto di Σ possiede un elemento massimale.

Se Σ è l'insieme dei sottomoduli di un modulo M, ordinato mediante la relazione $\subseteq$, allora la i) prende il nome di *condizione della catena ascendente* e la ii) prende il nome di *condizione massimale*. Un modulo M che soddisfa l'una o l'altra di tali condizioni

equivalenti si dice *noetheriano*. Se Σ è ordinato mediante la relazione $\supseteq$, allora la i) è la *condizione della catena discendente* e la ii) è la *condizione minimale*. Un modulo M che soddisfa ad esse si dice *artiniano*.

Teorema 0.9 (Teorema della base di Hilbert)**.** Se A è noetheriano, allora l'anello dei polinomi $A[X]$ è noetheriano.

Proposizione 0.10. $\mathbb{Z}[\alpha]$ è noetheriano e ogni suo ideale primo non nullo è massimale.

Definizione 0.22. Sia $K = \mathbb{Q}(\theta)$ un campo numerico di grado d su $\mathbb{Q}$ e sia $\{\alpha_1, ..., \alpha_d\}$ una base di K (come spazio vettoriale su $\mathbb{Q}$). Allora diremo che

$$\Delta[\alpha_1, ..., \alpha_d] := \{det(\sigma_i(\alpha_j))\}^2$$

è il *discriminante* della base $\{\alpha_1, ..., \alpha_d\}$.

Teorema 0.11. Se un dominio D è noetheriano, allora in D esiste una fattorizzazione in elementi irriducibili.

Definizione 0.23. Un anello R si dice *dominio di Dedekind* se è un dominio noetheriano di dimensione 1 e integralmente chiuso.

Teorema 0.12. In un dominio di Dedekind ogni ideale non nullo possiede una fattorizzazione unica come prodotto di ideali primi.

Teorema 0.13. Sia D un dominio di Dedekind. Allora D è UFD se e soltanto se è PID.

Abbiamo già osservato che $\mathbb{Z}[\alpha]$ non è, in generale, l'anello degli interi di $\mathbb{Q}(\alpha)$, quindi non è, in generale, un dominio di Dedekind e quindi in $\mathbb{Z}[\alpha]$ non vale il Teorema 0.12.

Successivamente, nell'ultimo paragrafo del capitolo, verrà definito un omomorfismo di gruppi che permetterà di avere anche in $\mathbb{Z}[\alpha]$ un risultato "simile" e funzionale all'NFS.

Definizione 0.24. Siano a, b interi coprimi, sia p un intero primo e sia r_p una radice di $f \pmod p$. Allora si definisce l'applicazione $e_{p,r_p}(a - b\alpha)$ nel modo seguente:

$$e_{p,r_p}(a - b\alpha) = \begin{cases} ord_p(N(a - b\alpha)) & \text{se } a \equiv br_p \pmod p \\ 0 & \text{altrimenti} \end{cases}$$

E nell'ultimo paragrafo del secondo capitolo vedremo l'estensione di tale applicazione ad un omomorfismo di gruppi su tutto $\mathbb{Q}(\alpha)^*$.

Definizione 0.25. Sia K un campo. Allora $K^* := K \backslash \{0\}$ è il gruppo moltiplicativo di K.

Proposizione 0.14. Sia R un ordine in un campo numerico K. Allora per ogni $\mathbf{p} \in Spec(R)$, esiste, ed è *unico*, un omomorfismo di gruppi $l_{\mathbf{p},R} : K^* \longrightarrow \mathbb{Z}$ tale che:

1) $l_{\mathbf{p},R}(\beta) \geq 0 \qquad \forall \beta \in R, \beta \neq 0$

2) $l_{\mathbf{p},R}(\beta) > 0 \iff \beta \in \mathbf{p} \qquad \forall \beta \in R, \beta \neq 0$

3) $l_{\mathbf{p},R}(\beta) \neq 0$ per un numero finito di primi $\mathbf{p} \qquad \forall \beta \in K^*$

4) $\prod_{\mathbf{p} \subset R} N(\mathbf{p})^{l_{p,R}(\beta)} = |N(\beta)| \qquad \forall \beta \in K^*.$

Quando $R = \mathbb{Z}[\alpha]$ scriveremo semplicemente $l_{\mathbf{p}}$ al posto di $l_{\mathbf{p},\mathbb{Z}[\alpha]}$.

Nel capitolo 3 è analizzato in maniera dettagliata il crivello del campo numerico, tale crivello del campo numerico, in breve NFS (dall'inglese *Number Field Sieve*), è un metodo per la fattorizzazione degli interi. L'idea chiave che sta alla base di questo algoritmo è l'utilizzo di B-numeri (v. Definizione 0.9) all'interno di un opportuno anello numerico diverso da $\mathbb{Z}$. Tale idea è stata proposta da John Pollard nel 1988. Da allora molti matematici hanno contribuito con vari suggerimenti allo sviluppo di questo algoritmo. L'NFS, in origine, era utilizzabile solo per fattorizzare numeri del tipo $r^s \pm e$, con r, s ed e "piccoli" (come, per esempio, i *numeri di Cunningham*, che sono numeri della forma

$b^k \pm 1$ con $b = 2, 3, 5, 6, 7, 10, 12$); qualche anno dopo, però, fu modificato in modo da poter essere applicato a qualsiasi tipo di numero.

Tuttora, a causa della differente velocità di esecuzione, si distingue tra il crivello del campo numerico *speciale*, in breve SNFS, e il crivello del campo numerico *generale*, in breve GNFS o semplicemente NFS, per indicare, rispettivamente, l'algoritmo applicabile ai numeri del tipo sopra descritto ($r^s \pm e$) e l'algoritmo applicabile ad ogni tipo di numero. Nel seguito ci occuperemo, principalmente, della descrizione del caso generale.
Attualmente l'NFS è il miglior algoritmo per fattorizzare numeri molto "grandi" (con più di 110 cifre decimali) privi di fattori primi "piccoli".

Strutturalmente l'NFS è simile al crivello quadratico. Infatti, come quest'ultimo, l'NFS fattorizza n trovando una coppia $(u, v) \in U(\mathbb{Z}_n) \times U(\mathbb{Z}_n)$ tale che:

$$u^2 \equiv v^2 \pmod{n}. \tag{3}$$

Inoltre, allo stesso modo del crivello quadratico, per risolvere (3), l'NFS "setaccia" un ben determinato insieme di numeri alla ricerca dei B-numeri. Ma nell'NFS, a differenza del crivello quadratico, la ricerca di B-numeri viene allargata anche ad anelli numerici diversi da $\mathbb{Z}$ (daremo successivamente la definizione di elemento B-numero in un generico anello numerico) e ciò, come vedremo, introduce nell'algoritmo una serie di difficoltà dovute alla mancanza, negli anelli numerici considerati, di alcune "buone" proprietà di $\mathbb{Z}$ (come ad esempio l'essere Dedekind) e alla necessità di ottimizzare molti dei parametri che intervengono nell'algoritmo.

La strategia è dunque la seguente:

Sia $n \in \mathbb{Z}$ (dispari, diverso dalla potenza di un primo) e sia $\alpha \in \mathbb{C}$ intero su $\mathbb{Z}$. Allora esiste $f \in \mathbb{Z}[X]$ monico e irriducibile tale che $f(\alpha) = 0$. Se esiste $m \in \mathbb{Z}$ tale che $f(m) \equiv 0 \pmod{n}$ allora l'applicazione

$$\begin{aligned} \phi : \mathbb{Z}[\alpha] &\longrightarrow \mathbb{Z}_n \\ \alpha &\longmapsto m \pmod{n} \end{aligned}$$

è un omomorfismo di anelli. Quindi se $p(X) \in \mathbb{Z}[X]$ è tale che:

$$p(\alpha) = \gamma^2 \text{ in } \mathbb{Z}[\alpha] \tag{4}$$

$$p(m) = y^2 \text{ in } \mathbb{Z} \tag{5}$$

allora $(\phi(\gamma), y)$ è una soluzione della (3). Difatti, dato che ϕ è un omomorfismo si ha che:

$$\phi(\gamma)^2 \equiv \phi(\gamma^2) = \phi(p(\alpha)) \equiv p(\phi(\alpha)) = p(m) = y^2 \pmod{n}.$$

Come mostreremo nel paragrafo sulle fattorizzazioni sub-esponenziali, tale soluzione, in più della metà dei casi, è sufficiente per determinare un fattore proprio di n.
Il problema è, quindi, ridotto alla ricerca di un polinomio $p(X) \in \mathbb{Z}[X]$ tale che $p(m)$ è un quadrato in $\mathbb{Z}$ e $p(\alpha)$ è un quadrato in $\mathbb{Z}[\alpha]$.
Utilizzeremo per tale ricerca i seguenti risultati e non solo:

Lemma 0.15. Sia $n, d \in \mathbb{Z}$, con $d > 1$, e sia $m = \lfloor n^{1/d} \rfloor$. Se $n > \frac{2}{(2^{1/d}-1)^d}$ allora $n < 2m^d$.

Dopo di che seguirà il vero e proprio crivello e faremo uso quindi della seguente definizione:

Definizione 0.26. Sia $B \in \mathbb{R}$ e sia $\alpha \in \mathbb{C}$ intero su $\mathbb{Z}$. Si dice che $X \in \mathbb{Z}[\alpha]$ è un B-numero se $N(X)$ è un B-numero.

Alla luce della precedente Definizione, è possibile riassumere il procedimento sopra descritto come segue: la costruzione di $q(X)$ si ottiene *setacciando* "linea per linea" l'insieme

$$T = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 0 < |a| \leq M_2, 0 < b \leq M_1\}$$

alla ricerca di coppie (a, b) tali che $(a - bm)$ e $(a - b\alpha)$ siano B-numeri. Tali coppie sono dette *relazioni*.

Proposizione 0.16. Sia $S \subset \mathbb{Z} \times \mathbb{Z}$ un insieme di coppie di interi coprimi tale che $\prod_{(a,b)\in S} (a - b\alpha) = \gamma^2$ in $\mathbb{Q}(\alpha)$. Allora:

$$\sum_{(a,b)\in S} e_{p,r_p}(a - b\alpha) \equiv 0 \pmod 2 \qquad \forall (p, r_p) \in Spec(\mathbb{Z}[\alpha]).$$

Verranno poi affrontati i punti critici di tale algoritmo, cioè le problematiche connesse con il fatto che $\mathbb{Z}[\alpha]$, in generale, non è l'anello degli interi di $\mathbb{Q}(\alpha)$ e quindi $\mathbb{Z}[\alpha]$ non è un dominio di Dedekind e infine analizzeremo, in maniera euristica, la complessità computazionale dell'NFS dove risulterà che per stimare tale complessità sarà necessario valutare il tempo di esecuzione del passo 2, cioè il crivello, in quanto i restanti passi dell'algoritmo sono notevolmente più veloci e non influenzano in modo sostanziale la sua complessità.
Per quanto riguarda però la complessità del passo 2, è fondamentale il seguente Teorema.

Teorema 0.17. Sia $\{a_n\}_{n\in\mathbb{N}} \subset [1, X]$ una successione di interi scelti in modo casuale e non distribuiti uniformemente, sia N il più piccolo intero tale che esistono $a_{i_1}, ..., a_{i_m} \in \{a_1, ..., a_N\}$ e $a_{i_1} \cdots a_{i_m}$ è un quadrato in $\mathbb{Z}$. Sia, inoltre, $L(X) = e^{\sqrt{log\ X\ loglog\ X}}$ allora il valore atteso per N è $L(X)^{\sqrt{2}+o(1)}$. Se chiediamo che gli a_{i_j} siano B-numeri, con $B = L(X)^{1/\sqrt{2}}$, vale ancora la stessa stima per N.

Nel capitolo 4 sono presenti le fattorizzazioni record ottenute grazie all'NFS già nonimate precedentemente: la fattorizzazione di un RSA di 512 bit, la fattorizzazione di un RSA di 530 bit, la fattorizzazione di F_9 e la fattorizzazione del numero di Cunningham.

Concludendo troveremo vari Appendici che cercano di colmare alcune lacune riguardanti vari argomenti affrontati in maniera del tutto superficiale all'interno della trattazione e cioé:

- il simbolo di Legendre:

Definizione 0.27. Sia p un primo dispari e a un intero tale che $p \nmid a$. Se la congruenza

$$X^2 \equiv (\text{mod } p)$$

è risolubile, allora a si dice *residuo quadratico* di p, altrimenti a si dice *non residuo quadratico* di p.

In altri termini, un residuo quadratico di p è un elemento del gruppo $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$ che è un quadrato.

Definizione 0.28. Sia p un primo dispari e sia a un intero. Si definisce *simbolo di Legendre* il seguente:

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

Il teorema che segue è una pietra miliare della teoria dei numeri, ed è un'informazione cruciale per effettuare in modo efficiente il calcolo dei simboli di Legendre. Il teorema, congetturato nel XVIII secolo da Eulero e Legendre, che non erano però riusciti a fornirne una dimostrazione completa, fu dimostrato da Gauss all'età di 19 anni.

Teorema 0.18 (Legge di reciprocità quadratica)**.** Siano p e q primi dispari distinti. Allora

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{se } p \equiv q \equiv 3 \text{ (mod 4)}, \\ \left(\frac{p}{q}\right) & \text{se } p \equiv 1 \text{ (mod 4) o/e } q \equiv 1 \text{ (mod 4)}. \end{cases}$$

- il simbolo di Jacobi:

  è una generalizzazione del simbolo di Legendre, $\left(\frac{a}{n}\right)$, dove a è un intero qualunque

e n un intero positivo dispari. Se n si fattorizza come $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con $p_1, ..., p_r$ numeri primi dispari distinti, si definisce come

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

La legge di reciprocità quadratica, valida dunque nella sua generalità per il simbolo di Jacobi, e le proprietà formali di quest'ultimo, ne consentono il calcolo *senza dover a priori conoscere la fattorizzazione* dei numeri coinvolti.

- la complessità computazionale di un algoritmo,

- le curve ellittiche,

- il metodo di eliminazione gaussiana.

Bibliografia

[1] Leonard M. Adleman. Factoring number using singular integers. In *Proceeding of the twenty-third annual ACM symposium on Theory of computing*, pages 64-71. ACM Press, 1991.

[2] Cristiano Armellini. *Relazione tra le terne pitagoriche e la fattorizzazione alla Fermat e ulteriori applicazioni: il crivello quadratico.* Relazione.

[3] M.F.Atiyan and I.G.Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[4] M.W.Baldoni, C.Ciliberto, G.M.Piacentini Cattaneo. *Aritmetica, crittografia e codici.* Springer, 2006.

[5] J.P. Buhler, H.W.Lenstra, Jr., and Carl Pomerance. Factoring integers with the number field sieve. In *The development of the number field sieve*, volume 1554 of *Lecture Notes in Math.,* pages 50-94. Springer, Berlin, 1993.

[6] Giulia Cattaneo Piacentini. *Algebra. Un approccio algoritmico.* Zanichelli, 1996.

[7] Stefania Cavallar, Bruce Dodson, Arjen K.Lenstra, Walter M.Lioen, Peter L.Montgomery, Brian Murphy, Herman te Riele, Karen Aardal, Jeff Gilchrist, Gerard Guillerm, Paul C.Leyland, Joel Marchand, Francois Morain, Alec Muffett, Chris Putnam, Craig Putnam and Paul Zimmermann. Factorization of a 512-bit RSA modulus. In *Theory and Application of Cryptographic Techniques*, pages 1-18, 2000.

[8] A.Cerquini. *Il crivello del campo numerico*. Tesi di Laurea, 2003.

[9] Don Coppersmith. Modifications to the number field sieve. *J.Cryptology*, 6(3) : pages 169-180, 1993.

[10] Jean-Marc Couveignes. Computing a square root for the number field sieve. In *The development of the number field sieve*, volume 1554 of *Lecture Notes in Math.*, pages 95-102. Springer, Berlin, 1993.

[11] Richard Crandall and Carl Pomerance. *Prime numbers*. Springer-Verlag, New York, 2001. A computational perspective.

[12] Marco Fontana. Dispense *Teoria dei numeri*.

[13] Stefania Gabelli *Teoria delle equazioni e teoria di Galois*. Springer, 2008.

[14] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A.Clarke, Revised by William C.Waterhouse, Cornelius Greither and A.W.Grootendorst and with a preface by Waterhouse.

[15] Robert W.Gilmer.*Multiplicative ideal theory*. Queen's Papers in Pure and Applied Mathematics, No.12. Queen's University, Kingston, Ont., 1968.

[16] Neal Koblitz. *A course in number theory and cryprography*, volume 114 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[17] Serge Lang. *Algebraic number theory*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970.

[18] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[19] Alessandro Languasco, Alessandro Zaccagnini. *Introduzione alla crittografia*. Ulrico Hoepli Editore, Milano, 2004.

[20] A.K.Lenstra, Jr.M.S.Manasse and J.M.Pollard. The factorization of the ninth Fermat number. Math. Comp., 61(203): pages 319-349, 1993.

[21] H.W.Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2): pages 211-244, 1992.

[22] Peter L.Montgomery. Square roots of products of algebraic numbers. In *Mathematics of Computation 1943-1993: a half-century of computational mathematics (Valcouver, BC, 1993),* volume 48 of *Proc. Sympos. Appl. Math.,* pages 567-571. Amer. Math. Soc., Providence, RI, 1994.

[23] Peter L. Montgomery. A block Lanczos algorithm for finding dependencies over GF(2). In *Advances in cryptology - EUROCRYPT '95 (Siant-Malo, 1995)*, volume 921 of *Lecture Notes in Comput. Sci.,*: pages 106-120. Springer, Berlin, 1995.

[24] B.Murphy. Polynomial selection for the number field sieve integer factorisation algorithm, 1999.

[25] Phong Nguyen. A. Montgomery-like square root for the number field sieve. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.,* pages 151-168. Springer, Berlin, 1998.

[26] Francesco Pappalardi. *Note di crittografia a chiave pubblica*. Dispense, fascicolo 1, maggio 2003.

[27] J.M.Pollard. The lattice sieve. In *The development of the number field sieve*, volume 1554 of *Lecture Notes in Math.,* pages 43-49. Springer, Berlin, 1993.

[28] Carl Pomerance. Smooth numbers and the quadratic sieve. *Algorithmic number theory: lattices, number, fields, curves and cryptography*, pag.83-100. Math.Sci.Res.Inst.Publ,44, Cambridge Univ. Press, Cambridge 2008.

[29] Edoardo Sernesi. *Geometria 1.* Bollati Boringhieri, 1989.

[30] Peter Stevenhagen. The number field sieve. *Algorithmic number theory: lattices, number, fields, curves and cryptography*, pag.69-81. Math.Sci.Res.Inst.Publ,44, Cambridge Univ. Press, Cambridge 2008.

[31] Ian Stewart and David Tall. *Algebraic number theory.* Chapman and Hall Mathematics Series. Chapman & Hall, London, second edition, 1987.

[32] Douglas R.Stinson. *Cryptography.* CRC Press Series on Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, second edition, 2002. Theory and practice.

[33] Edwin Weiss. *Algebraic number theory.* McGraw-Hill Book Co., Inc., New York, 1963.