

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

---

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI  
Corso di Laurea Specialistica in Matematica

**Crittografia e Teoria dei numeri**  
**In aula con Alice e Bob: dalle applicazioni**  
**pratiche alla costruzione di oggetti e teorie**

Tesi di Laurea in Didattica della Matematica

Relatore:  
Chiar.mo Prof.  
Bolondi Giorgio

Presentata da:  
Garulli Marco

Prima Sessione  
Anno Accademico 2009/2010



*Agli studenti  
di oggi e di domani*



# Introduzione

*Se vuoi costruire una nave,  
non radunare uomini per raccogliere il legno,  
distribuire i compiti e suddividere il lavoro,  
ma insegna alla gente la nostalgia del mare infinito.*  
(Antoine De Saint-Exupéry)

Al termine di questi cinque anni di studio universitario della matematica, ho sentito l'esigenza di concludere il mio percorso da studente con un progetto che convogliasse le conoscenze da me acquisite e le esperienze da me vissute verso uno dei possibili sbocchi occupazionali del laureato in matematica: l'insegnamento. Il settore scolastico offre numerosi spunti d'analisi sia sul piano teorico (cosa vuol dire nel ventunesimo secolo dimostrare qualcosa grazie alla matematica?) sia sul piano pratico (a cosa serve oggi conoscere la regola di de l'Hopital?). Personalmente, ho sempre trovato stimolante l'idea di proseguire la mia formazione personale attraverso una carriera da docente, ma quello che mi motiva e stimola è la speranza di insegnare la "nostalgia del mare infinito", il piacere della Matematica, e non formule da imparare a memoria senza la loro comprensione.

Nell'insegnamento della matematica ritengo che si debba tenere in considerazione il fatto che la tendenza è quella di abituare i ragazzi a svolgere esercizi ripetitivi senza che possano mai coglierne appieno l'utilità. Sono semplicemente guidati dalla necessità di avere una sufficienza in una materia ostica a risolvere compiti sempre uguali e per loro completamente privi di interesse, sia pratico che teorico. Chiediamoci invece quanto si potrebbe spronarli e

invogliarli presentando la matematica sotto un'altra veste.

Il punto sta nel riuscire a fornire risposte accattivanti e originali alle domande che vengono poste dagli studenti. Prendiamo ad esempio il caso emblematico della definizione di logaritmo. Tipicamente gli studenti non apprezzano questa funzione, si trovano in difficoltà nel gestirla e spesso la rifiutano. Il motivo di questo comportamento può essere dovuto anche al fatto che non riescono a comprendere per quale ragione si debba introdurre tale definizione. In effetti quando viene chiesto a cosa serve, l'insegnante è posto davanti ad un bivio: fornire una risposta soddisfacente dal punto di vista strettamente matematico o adeguata alle esigenze dell'interlocutore. Nel primo caso la funzione logaritmo è vista come necessaria in quanto inversa dell'esponenziale. Ma siamo sicuri che questo possa avere un reale significato per un quindicenne in cerca di risposte concrete? Il ragazzo potrebbe chiedere allora a che scopo introdurre una funzione inversa, e ancora, a cosa dovrebbe servire l'esponenziale e via di seguito. Nel secondo caso, invece, si potrebbe porre l'interlocutore davanti alle applicazioni di tale funzione: nella scala logaritmica usata in molti ambiti; nell'aritmetica modulare utilizzata per gli algoritmi dei crittosistemi a chiave pubblica. Oppure spiegarne l'origine storica e le motivazioni con le quali fu introdotto dai primi matematici che ne fecero uso.

Spingiamoci oltre, pensiamo ad aprire la mente dei ragazzi, far esplorare loro nuovi orizzonti, diversi oggetti matematici che possano realmente conquistare il loro interesse e la loro attenzione. Questo per far comprendere cosa sia la vera matematica, dove possa condurre con le sue idee a prima vista molto astratte e poco intuitive. Per raggiungere tale scopo è importante contestualizzare tali idee, indicare chi le ha avute, in che periodo, di cosa era in cerca, perché è questo che può indicare come procedere nella ricerca di nuovi risultati. Ritengo che le aspettative sulle conseguenze di un atteggiamento di questo tipo debbano essere elevate.

Inoltre si rende ormai indispensabile tentare un nuovo approccio, in un momento di profonda crisi della matematica in tutta la nostra società. Infatti le

idee esposte finora non devono essere pensate relegate al mondo della scuola; il concetto di una matematica più utile e interessante dovrebbe essere esportato anche nel mondo degli adulti, facendo la sua comparsa nelle mostre, nei musei, in modo da rendere la matematica parte della cultura, e non un mostro da temere ed evitare.

Nel seguente lavoro espongo il progetto che ho deciso di portare in aula e le conclusioni che ne sono derivate: lo studio della crittografia per introdurre concetti fondamentali di teoria dei numeri.

I motivi per cui ho scelto questo argomento di applicazione matematica sono diversi. Innanzitutto non è presente ora nei programmi ministeriali a differenza di altri argomenti (come le applicazioni della matematica in fisica).

Inoltre lo studio di come scambiare dati in sicurezza è un argomento accattivante, nasconde qualcosa di misterioso che può attrarre l'interesse dei ragazzi. Essi si domandano fin da subito che nesso sussista fra crittografia e matematica permettendo di evidenziare come la matematica non sia una disciplina fine a se stessa, ma sia anche uno strumento di grande utilità in molti aspetti della vita di tutti i giorni.

Alcuni degli agganci immediati con argomenti matematici sono:

- i numeri primi;
- l'aritmetica modulare;
- le strutture algebriche (come generalizzazione di quanto visto negli punti precedenti);
- la probabilità e la statistica;
- la complessità computazionale.

Per quanto riguarda il primo punto, i ragazzi conoscono già alcune nozioni di base e possono essere avviati in una direzione tra l'altro attualmente molto importante per la ricerca. Il secondo punto è più critico, dato che gli studenti

non hanno conoscenze preesistenti a riguardo, ma affrontare questo tema non è certo troppo difficile. Per il terzo punto ci si trova ai confini di quello che solitamente è mostrato ai ragazzi delle scuole superiori; infatti le strutture algebriche vengono presentate all'università, dato che sono viste come troppo astratte. Ai ragazzi può essere fornita quindi una finestra per vedere cosa si studia nella matematica universitaria. Naturalmente l'introduzione di questo punto richiederebbe molto tempo, ma potrebbe portare a risultati alquanto interessanti.

Il progetto si è concentrato soprattutto sulla matematica dei numeri primi, sulle congetture e sui teoremi più importanti relativi all'argomento e sull'aritmetica modulare, poiché si è pensato che fossero i concetti più semplici da affrontare, soprattutto tenendo conto del limitato numero di ore a disposizione per il progetto.

La scelta della crittografia permette inoltre di studiare una matematica diversa da quella affrontata usualmente in aula, ossia la matematica discreta, in particolare modo la teoria dei numeri. Questa si distingue parecchio dai concetti dell'analisi, quali il continuo, i limiti ec...

Infine, come già accennato vi sarebbero altri punti di contatto possibili tra la crittografia e la matematica, ad esempio lo studio della complessità computazionale, con l'utilizzo del simbolo  $O$  grande e di conseguenza dei limiti o la probabilità.



# Indice

<b>Introduzione</b>	<b>i</b>
<b>1 Il progetto: costruzione e sviluppo</b>	<b>1</b>
1.1 Presupposti . . . . .	1
1.2 Nascita ed evoluzione del progetto . . . . .	4
1.3 Obiettivi . . . . .	6
1.4 Utilità del progetto . . . . .	7
1.5 Attività in aula . . . . .	8
<b>2 Il progetto: Numeri, Parole e Segreti</b>	<b>11</b>
2.1 Introduzione . . . . .	11
2.2 Indice . . . . .	12
2.3 Cos'è la crittografia . . . . .	12
2.4 Un po' di Storia . . . . .	13
2.5 Macchine per cifrare . . . . .	20
2.6 I Segreti Oggi . . . . .	20
2.7 Crittosistema . . . . .	22
2.8 Sicurezza assoluta? . . . . .	23
2.9 Divisibilità e Numeri Primi . . . . .	26
2.9.1 MCD . . . . .	27
2.9.2 Numeri primi . . . . .	30
2.9.3 Test di primalità e fattorizzazione . . . . .	35
2.10 Aritmetica modulare . . . . .	37
2.11 Esempio di Crittosistema a chiave pubblica: RSA . . . . .	42

---

2.11.1	Generazione delle chiavi . . . . .	43
2.11.2	Cifratura . . . . .	43
2.11.3	Decifrazione . . . . .	43
2.11.4	Sicurezza della chiave segreta . . . . .	44
2.12	Crittografia quantistica . . . . .	45
2.12.1	Esperimento di Young e principio di indeterminazione di Heisenberg . . . . .	45
2.12.2	Computer quantistico . . . . .	49
2.12.3	Fotoni e polarizzazione . . . . .	49
2.12.4	Protocollo BB84 . . . . .	50
2.13	Conclusione . . . . .	55
2.14	Aggiunte . . . . .	55
2.14.1	Cenni sull'ipotesi di Riemann . . . . .	55
2.14.2	Strutture algebriche . . . . .	56
2.14.3	Cifrari a blocchi . . . . .	59
2.15	Esercizio . . . . .	60
2.16	Glossario . . . . .	63
<b>3</b>	<b>Diario di bordo</b>	<b>65</b>
3.1	Prima lezione (due ore) . . . . .	65
3.2	Seconda lezione (un'ora) . . . . .	67
3.3	Terza lezione (un'ora) . . . . .	68
3.4	Quarta lezione (due ore) . . . . .	69
3.5	Quinta lezione (un'ora) . . . . .	70
3.6	Sesta lezione (due ore) . . . . .	71
3.7	Verifica . . . . .	72
<b>4</b>	<b>Analisi e commento</b>	<b>73</b>
4.1	Impressioni generali . . . . .	73
4.2	Analisi didattica . . . . .	74
4.3	Risultato questionario di valutazione . . . . .	77
4.3.1	Materiali e strumenti . . . . .	78

---

4.3.2	Esposizione e metodo . . . . .	79
4.3.3	Considerazioni sul progetto . . . . .	81
4.3.4	Considerazioni sulla matematica . . . . .	83
4.4	Risultati verifica . . . . .	84
<b>5</b>	<b>Analisi Progetto Lauree Scientifiche</b>	<b>87</b>
5.1	Introduzione al Progetto Lauree Scientifiche . . . . .	87
5.2	Considerazioni sul progetto generale . . . . .	88
5.3	Considerazioni sul progetto di crittografia . . . . .	90
<b>A</b>	<b>Slides del corso</b>	<b>97</b>
<b>B</b>	<b>Compiti in classe</b>	<b>107</b>
<b>C</b>	<b>Esercizi per lavoro di gruppo</b>	<b>113</b>
<b>D</b>	<b>Articolo Odifreddi</b>	<b>117</b>
<b>E</b>	<b>Dialogo sull’Orologio</b>	<b>123</b>
<b>F</b>	<b>Questionario di Valutazione</b>	<b>127</b>
	<b>Bibliografia</b>	<b>131</b>



# Capitolo 1

## Il progetto: costruzione e sviluppo

*Le uniche persone che capiscono  
come stanno veramente le cose  
sono quelle che più frequentemente  
vengono incolpate e quasi mai ascoltate:  
gli scolari.*  
(Paul Lockhart)

### 1.1 Presupposti

Per mostrare quali siano le idee che stanno alla base del mio progetto cito Gianfranco Arrigo:

“Da qualche decennio la ricerca didattica [...] mette in primo piano l'apprendimento, o, se si preferisce, l'allievo con le sue peculiarità, il suo vissuto, la sua psicologia e le sue condizioni sociali. Da parecchi anni, in didattica, ci si concentra sulla costruzione del sapere da parte dell'allievo, cercando da un lato le modalità più adatte per ottenere la migliore qualità dell'apprendimento, dall'altro di identificare gli ostacoli che vi si possono frapporre. [...]

Se l'allievo viene convenientemente stimolato e messo in condizione di contribuire in prima persona alla costruzione del proprio sapere, deve poter agire, sentirsi protagonista e riflettere su ciò che ha fatto, che sta facendo, che potrà fare. Deve quindi a poco a poco appropriarsi di una scatola di strumenti personalizzata che gli permetta di apprendere con sempre maggiore autonomia. L'allievo non deve essere lasciato solo in questo fondamentale compito, ma messo nella condizione di collaborare con i propri compagni.” [1]

Quindi l'insegnante si trasforma da semplice trasmettitore di conoscenza a colui che stimola ed organizza attività che rendano partecipi i ragazzi e li responsabilizzino al raggiungimento del loro apprendimento. È qui che si evidenzia il punto centrale dell'atteggiamento didattico odierno: l'attenzione è posta sull'apprendimento, non più sull'insegnamento visto come unico mezzo per il trasferimento dei saperi.

Gli studenti da passivi ascoltatori divengono attivi e coscienti del proprio apprendimento, in modo da acquisire non solo i saperi ma anche il modo di ragionare matematico, conquistando abilità quali l'intuizione e la creatività. È evidente come un atteggiamento di questo tipo contribuisca alla formazione della personalità razionale dei ragazzi ed alla comprensione di come la matematica sia parte della cultura e del pensiero criticamente costruttivo. Riprendendo le parole di Gianfranco Arrigo:

“Per poter agire da protagonista nel processo di apprendimento l'allievo deve acquisire nuove risorse. [...] Oltre ai saperi occorre sviluppare maggiormente alcune capacità procedurali, strategiche e cognitive (i **saper fare**) ed infondere una mentalità matematica che consenta all'allievo di sentirsi responsabile del proprio apprendimento e di vivere la matematica in prima persona (i **saper essere**).” [1]

I *saper fare* possono essere classificati in questo modo:

1. **cognitivi**: anticipare, operare deduzioni, procedere per induzione, de-

- cidere, formulare ipotesi;
2. **procedurali**: eseguire procedimenti, applicare concetti, principi e algoritmi;
  3. **strategici**: stabilire relazioni fra procedimenti, concetti e principi, ideare strategie;
  4. **metacognitivi**: autovalutare ed autoregolare i propri processi, riflettere sull'opportunità di effettuare determinati tentativi risolutivi, prendere coscienza di determinati modi di ragionare in matematica.

Fra i *saper essere* si trova ad esempio la capacità di apprezzare ed interiorizzare aspetti tipici della matematica: precisione del linguaggio, rigore del ragionamento logico, ricchezza del metodo di dimostrazione-confutazione, gusto di porsi ed affrontare problemi. Tali abilità concorrono a migliorare la comprensione della realtà, a guadagnare in sicurezza ed in capacità argomentativa, ad esercitare una critica oggettiva di fronte ad affermazioni proprie ed altrui. I ragazzi che acquisiscono questi *saper essere* saranno gli adulti in grado di perseguire un atteggiamento intellettuale improntato al dubbio ed alla problematizzazione della conoscenza, discutere ed accettare idee altrui, avere il coraggio di proporre e diffondere il proprio pensiero.

La combinazione di queste tre categorie di apprendimenti (sapere, sapere fare e sapere essere) genera competenza, definita da Xavier Roegiers: “mobilitazione di un insieme articolato di risorse allo scopo di risolvere una situazione significativa appartenente ad una famiglia data di situazioni-problema”. Tale competenza si concretizza, durante la risoluzione di un problema, nella capacità di formulare un'idonea congettura. Un problema nuovo ed interessante può produrre una forte motivazione a trovare un percorso risolutivo. Inoltre richiede coraggio, pazienza nel procedere per tentativi e verifiche, avanzando ipotesi che vanno comunicate ad un gruppo lavorativo, il che richiede a sua volta capacità di esprimere con chiarezza le proprie idee e quella di ascoltare le idee degli altri. Solo nella creazione di un percorso risolutivo anche

tortuoso può progredire l'apprendimento. Quello che conta realmente quindi non è il raggiungimento della soluzione del problema, ma l'iter seguito dai ragazzi, che devono imparare anche a gestire l'insuccesso, ripercorrendo il proprio sentiero e tentando nuove congetture. Devono scontrarsi col fatto che non tutti i problemi sono risolubili, e quindi accettare la non riuscita di un loro grande sforzo. Anche in questo modo si evidenzia come l'obiettivo primario non sia il risultato del problema (che può anche non essere trovato) ma la riflessione che il problema ha suscitato nei ragazzi.

In sostanza insegnare non significa fornire informazioni: enunciare dati da memorizzare e procedure da seguire (fornire risposte immediate) elimina il processo creativo. I ragazzi necessitano di tempo per formulare ipotesi e fare scoperte personali. Il compito dell'insegnante dovrebbe essere quello di portarli dove la loro curiosità può condurre, far capire loro come per apprendere veramente sia necessario rispondere a domande e risolvere problemi, il che richiede competenze, ma anche ispirazione, esperienza e fortuna. Devono procedere per tentativi ed errori, essere frustrati, formulare le proprie ipotesi e dimostrazioni. In pratica devono essere protagonisti durante le lezioni.

## 1.2 Nascita ed evoluzione del progetto

Dato quello che si è detto nell'introduzione, ho pensato di portare in aula un progetto che prevedesse due componenti fondamentali: novità di contenuto (**cosa insegnare**) e differente metodologia di insegnamento (**come insegnare**). Per quanto riguarda il primo punto, l'idea è stata quella di introdurre un nuovo argomento, facente parte di un ambito della matematica che difficilmente viene toccato nel corso di studi e che riguarda la teoria dei numeri. Inoltre tale argomento può essere affrontato a seconda dei casi decidendo di sottolineare maggiormente l'aspetto teorico-astratto o quello pratico-applicativo, che trova riscontro nella crittografia.

Sul come insegnare, ho pensato di introdurre alcuni strumenti ed approcci



che favorissero l'apprendimento dei ragazzi:

- **Presentazione tramite slides** (vedi Appendice A) : interessare attraverso immagini, animazioni e video, lasciando alla lavagna gli approfondimenti, le dimostrazioni e gli esercizi che hanno un carattere maggiormente costruttivo;
- **Approccio interattivo**: porre continuamente quesiti e chiedere la loro opinione in modo da mantenerli sempre attenti e reattivi;
- **Lavori di gruppo** (vedi Appendice C): far provare ai ragazzi in prima persona ed in maniera attiva a risolvere problemi e ad applicarsi in quanto spiegato durante le lezioni frontali;
- **Giochi di logica**: porre i ragazzi in situazioni in cui partecipare attivamente e concretamente alla lezione per risolvere problemi di tipo pratico;
- **Letture** (vedi Appendice D): analisi di brani tratti da libri o di articoli di giornale per sottolineare come la matematica sia parte della cultura e come alcuni degli argomenti trattati siano di grande attualità;
- **Decifrazione di parole chiave** (necessaria per aprire i file inviati contenenti le dispense): esercitare i ragazzi fornendo loro un fine che li spingesse ad effettuare realmente il compito. Tali esercizi risultavano anche utili per la comprensione degli argomenti trattati in aula.
- **Inquadramento storico**: presentare gli argomenti seguendo un percorso storico, che sottolinei le vicende e gli sforzi umani per giungere ai risultati ed evidenzi come i problemi siano alla base di ogni scoperta ed innovazione.
- **Materiale aggiuntivo**: fornire ai ragazzi la possibilità di approfondire a casa, distribuendo fotocopie di libri o eventuale materiale che presenti le stesse cose studiate in aula ma con un approccio diverso (ad esempio i dialoghi di Roberto Zanasi, vedi Appendice E).

Un'ultima considerazione: dire che la crittografia viene impiegata in ogni ambito della vita quotidiana potrebbe risultare del tutto insufficiente per raccogliere l'interesse degli studenti. Spesso si pensa che indicare come motivazione di studio di un argomento il fatto che esso sia utile alla comprensione del funzionamento di ciò che ci sta intorno garantisca una buona spinta per i ragazzi. Ma come tutti noi abbiamo appurato nel corso della nostra vita, gli oggetti di uso quotidiano funzionano benissimo anche senza che ne si conosca il meccanismo. Pensiamo a quante cose intorno a noi sono utili ma non abbiamo più idea di come siano state costruite o quale sia il sistema alla base che li rende funzionanti, dagli elettrodomestici fino alle più semplici apparecchiature luminose o di riscaldamento. Si rende dunque essenziale trovare un modo più diretto che riesca a cogliere la curiosità dei ragazzi, affinché si impegnino nell'apprendimento. Nel nostro caso è necessario fare leva sul potenziale che può dare la conoscenza della crittografia per la nostra sicurezza e per la difesa da possibili attacchi. Si può ad esempio porre l'accento sul fatto che lo studio di questi argomenti possa fornire ai ragazzi i mezzi per valutare da soli cosa sia realmente sicuro senza dover dipendere dagli altri.

### 1.3 Obiettivi

Dal punto di vista prettamente didattico, lo scopo di questo progetto è quello di individuare nuovi metodi di gestione delle lezioni frontali adatte alla scuola secondaria superiore ed indagare forme relazionali e motivazionali in grado di aumentare l'interesse e l'impegno dei ragazzi nei confronti della matematica.

Per quanto concerne invece il punto di vista contenutistico, il fine è quello di migliorare la formazione degli allievi nel quadro dell'aritmetica e della teoria dei numeri, nonchè di stimolare la curiosità verso un aspetto della matematica applicata a una situazione del mondo reale. Si spera inoltre di riuscire a presentare agli studenti la matematica come una materia ricca di problemi irrisolti, come un campo aperto a future ricerche (ad esempio

attraverso l'illustrazione delle congetture sui numeri primi).

## 1.4 Utilità del progetto

Al di là dell'evidente positività, in caso di successo, data dal raggiungimento degli obiettivi preposti, il progetto in sé mostra alcuni vantaggi intrinseci. Innanzi tutto, si inserisce nell'attività curricolare relativamente a tre argomenti: numeri primi, aritmetica modulare e strutture algebriche. Il collegamento con il piano didattico può avvenire grazie alla presenza in tale piano dello studio dell'aritmetica in prima liceo: numeri interi, MCD, ecc... Il progetto fornisce inoltre la possibilità per i ragazzi di avere un piccolo spaccato sui metodi e gli argomenti di matematica affrontati a livello universitario (es. teoria dei numeri).

Riporto in dettaglio i punti matematici analizzati ed analizzabili in riferimento al tema presentato:

### 1. Divisibilità:

- Lemma di divisibilità:  $a=bq+r$ ;
- MCD;
- Algoritmo di Euclide;
- Identità di Bezout ed equazioni lineari diofantee;

### 2. Numeri primi:

- Fattorizzazione e teorema fondamentale dell'aritmetica;
- Teorema di Euclide (infinità dei numeri primi) e distribuzione dei numeri primi;
- Crivello di Eratostene;
- Test di primalità: probabilistici e deterministici;
- Fattorizzazione alla Fermat;

**3. Congruenze:**

- Definizione e proprietà;
- $\mathbb{Z}_m$  e le classi di congruenza;
- Operazioni ed inverso;
- Funzione  $\varphi$  di Eulero;
- Piccolo teorema di Fermat e teorema di Eulero;

**4. Strutture algebriche:** generalizzazione a partire dall'anello  $\mathbb{Z}_m$ ;**5. Complessità computazionale** e problema P=NP.

## 1.5 Attività in aula

La possibilità di portare in aula il mio progetto mi è stata accordata dalla professoressa Elettra Battitori e dall'I.S.I.S. Archimede di San Giovanni in Persiceto presso il quale lavora. Sono stato assegnato ad una classe quarta di liceo scientifico PNI. Così come da accordi presi con il docente di riferimento, prof.ssa Battitori, la mia attività in aula è stata concentrata in 9 ore di lezione distribuite nell'arco di una settimana. Ho deciso di suddividere gli argomenti preparati come segue:

1. **Storia:** un'ora e mezza;
2. **Divisibilità e numeri primi:** 2 ore e mezza;
3. **Aritmetica modulare:** 2 ore;
4. **RSA:** un'ora e mezza;
5. **Crittografia quantistica:** un'ora e mezza.

Ho predisposto inoltre una verifica finale, un questionario di gradimento ed una serie di attività, interattive e non solo, da far svolgere ai ragazzi durante

le ore di lezione.

Nel prossimo capitolo, è riportato il progetto completo, così come è stato portato in aula, con aggiunte ed approfondimenti utili nel caso si avessero ore aggiuntive o interessi diversi. Sono inoltre riportate le dimostrazioni di tutte le proposizioni ed i teoremi (anche quelle non effettuate in classe).



## Capitolo 2

# Il progetto: Numeri, Parole e Segreti

*Non con soverchie speranze,  
nè avendo nell'animo illusioni spesso dannose,  
ma nemmeno con indifferenza,  
deve essere accolto ogni nuovo tentativo  
di sottoporre al calcolo fatti di qualsiasi specie.*  
(Vito Volterra)

### 2.1 Introduzione

*“La sicurezza di un crittosistema  
non deve dipendere dal tener celato il crittoalgoritmo.  
La sicurezza dipenderà solo dal tener celata la chiave.”  
(Legge di Kerckhoffs).*

Cos'è un crittosistema? Cos'è un crittoalgoritmo? Chi è Kerckhoffs? Andiamo con ordine: Kerckhoffs è stato un grande teorico della crittografia, autore de *La cryptographie militaire* del 1883, per il resto ... leggiamo qui sotto!

## 2.2 Indice

1. Cos'è la crittografia?
2. Un po' di Storia
3. Macchine per cifrare
4. I Segreti Oggi
5. Crittosistema
6. Sicurezza Assoluta?
7. Divisibilità e Numeri Primi
8. Aritmetica Modulare
9. Esempio di Crittosistema a chiave pubblica: RSA
10. Crittografia quantistica
11. Conclusione

## 2.3 Cos'è la crittografia

La parola crittografia deriva dall'aggettivo greco kryptòs che significa nascosto e dal verbo greco gráphein che significa scrivere. La crittografia è dunque l'arte del rendere un messaggio incomprensibile a chiunque tranne che al destinatario ufficiale. È l'antagonista della crittanalisi, che studia i metodi per decifrare i messaggi che sono stati criptati da altri. L'unione delle due discipline è la crittologia.

La crittografia va distinta dalla steganografia (fusione delle parole greche coperto e scrivere), che si occupa delle tecniche per nascondere un messaggio. La steganografia infatti ha come scopo quello di celare un testo lasciandone il contenuto in chiaro. La crittografia si preoccupa invece di cifrare un messaggio in modo che possa essere *letto* da chiunque, ma *compreso* solo dal vero



destinatario in grado di decifrarlo.

Dalle *Storie* di Erodoto ci giungono due esempi di steganografia. Demarato, un esule greco stabilito a Susa, si accorse che i persiani si stavano preparando ad attaccare Sparta e Atene con una grande flotta. Decise così di inviare un messaggio agli spartani per avvisarli dell'imminente pericolo. Grattò la cera da una tavoletta per la scrittura ed incise il messaggio sul legno sottostante, di modo che non fosse visibile; poi, affinché la tavoletta sembrasse vergine, la ricoprì di nuovo con la cera. Quindi inviò a Sparta un servo che riuscì a consegnare la tavoletta agli spartani, senza insospettire nessuno. Letto il messaggio i greci cominciarono ad armarsi. Quando i persiani attaccarono a Salamina nel 480 a.C. mancò il fattore sorpresa: la sopravvivenza di Atene e Sparta fu così garantita dall'aver saputo in anticipo le mosse dei nemici.

In un altro racconto, Erodoto narra come Istieo, che viveva in Persia presso il re Dario, volesse che la Ionia, antica regione dell'Asia Minore, si ribellasse alla dominazione persiana. Egli non osava però inviare una lettera dato che numerose sentinelle sorvegliavano le strade. Decise perciò di far radere i capelli di un servo fedele e tatuargli sulla testa: "Istieo ad Aristagora: fa ribellare la Ionia". Poi aspettò che gli ricrescessero i capelli. Il portatore del messaggio passò inosservato alle guardie e scese fino al mare, si fece radere la testa, svelando ad Aristagora lo scritto nascosto; letta l'esortazione, Aristagora fece insorgere la Ionia.

Come si evince da queste situazioni esemplari, la protezione offerta dalla steganografia è debole e parziale. Conviene, dunque, tornare alla crittografia.

## 2.4 Un po' di Storia

Fin dall'antichità si è sentita la necessità di nascondere messaggi strategici. Basti pensare che ci sono tracce di cifrari già secoli prima di Cristo, come il codice di atbash usato dagli ebrei, l'origine del quale può essere trovata nella Bibbia. Esso è un semplice cifrario a sostituzione basato sull'alfabeto

ebraico in cui la prima lettera (Aleph) viene cifrata con l'ultima (Taw), la seconda (Beth) viene cifrata con la penultima (Shin) e così via; da queste quattro lettere è derivato il nome di Atbash (A con T, B con SH). Utilizzando l'alfabeto italiano, si avrebbe il seguente schema:

**Alfabeto in chiaro:**    a b c d e f g h i l m n o p q r s t u v z

**Alfabeto cifrato:**     z v u t s r q p o n m l i h g f e d c b a

Un altro famoso esempio è il cifrario di Cesare, chiamato così in nome di Caio Giulio Cesare che probabilmente ne fece uso per primo. Questo è un sistema crittografico elementare, ma molto utile per comprendere le idee basilari della crittografia. È un cifrario a sostituzione monoalfabetica, cioè che fa uso di un singolo alfabeto, in cui ciascuna lettera veniva traslata di  $n$  posizioni. Ad esempio scegliendo  $n = 3$ :

**Alfabeto in chiaro**    a b c d e f g h i l m n o p q r s t u v z

**Alfabeto cifrato**     d e f g h i l m n o p q r s t u v z a b c

La **cifratura** o **cifrario** è la regola che permette di riscrivere un intero messaggio in modo che sia incomprensibile per chi non conosce tale regola.

Per cifrare un messaggio si sostituisce ogni lettera del testo in chiaro con la corrispondente lettera dell'alfabeto cifrato. Ad esempio, utilizzando il cifrario di Cesare con  $n = 3$  avremo:

**Testo in chiaro:**    il modo più veloce di finire una guerra è perderla

**Testo cifrato:**     no prgr sna bhorfh gn inqnuh aqd lahuud h shughuod

L'alfabeto cifrante corrispondente ad un numero intero  $n$ , detto **chiave**, è quello che sposta le lettere dell'alfabeto in chiaro di  $n$  posizioni, cioè quello ottenuto con una **traslazione** di  $n$  posizioni. I possibili cifrari di Cesare nella lingua italiana sono 20, dato che se una lettera si sposta di 21 posizioni

ritorna al punto di partenza, facendo così coincidere il messaggio cifrato con quello in chiaro e rendendo inutile l'operazione.

Cifrare il testo più volte non serve a migliorarne la sicurezza, in quanto una traslazione di  $n$  posizioni seguita da una di  $m$  posizioni equivale ad una di  $n + m$ .

Se si intercetta un messaggio che si pensa possa essere stato cifrato con il cifrario di Cesare, basta tentare di decifrarlo usando le 20 chiavi dei possibili alfabeti cifranti. É quindi molto facile decifrare il crittogramma anche senza essere in possesso della chiave. Se per di più si presta attenzione alla frequenza delle lettere in cifra e nella lingua originale, è facile intuire il valore della chiave: in un testo italiano, le A saranno piuttosto frequenti... le H un po' meno!

Prendendo spunto da cifrari di questo tipo sono state inventate altre tecniche tra cui quella che sfrutta tutte le possibili permutazioni delle 21 lettere dell'alfabeto, anziché le sole traslazioni. In pratica, una qualsiasi permutazione dell'insieme  $\{0, 1, 2, \dots, 20\}$  determina un alfabeto cifrante e viceversa.

Ma come ricordarsi la chiave? Ci si dovrebbe ricordare tutta la sequenza delle lettere riordinate. Un metodo per produrre una permutazione dell'alfabeto facile da memorizzare è quello di usare una chiave che sia determinata a sua volta da una parola chiave o da una frase chiave, cioè da una stringa di lettere che possiamo ricordare. Scegliamo ad esempio come chiave la frase *Mi illumino d'immenso*. Per prima cosa dobbiamo eliminare gli spazi fra le parole e poi le lettere ripetute, ottenendo: *milunodes*.

L'alfabeto cifrante sarà costruito disponendo nell'ordine prima le lettere della parola chiave modificata come sopra, e poi le lettere dell'alfabeto rimaste, secondo il normale ordine alfabetico. Si avrà allora:

**Alfabeto in chiaro**    a b c d e f g h i l m n o p q r s t u v z

**Alfabeto cifrato**     m i l u n o d e s a b c f g h p q r t v z

Se abbandoniamo l'idea di usare una parola chiave e prendiamo qualunque

permutazione dell'alfabeto, il numero di chiavi possibili, e quindi di alfabeti cifranti, passa da 21 (i cifrari di Cesare) a  $21!$  che è il numero di tutte le permutazioni di 21 elementi, cioè circa  $51 \cdot 10^{18}$ . Un intercettatore che sia a conoscenza del metodo di cifratura non può certamente pensare di provare a decifrarlo per tentativi.

Una cifratura che utilizza un solo alfabeto cifrante, come quelle che abbiamo visto fino ad ora, si dice **cifrario monoalfabetico**.

Possiamo però pensare di utilizzare più di un alfabeto cifrante in questo modo: supponiamo di volerne utilizzare  $n \in \mathbb{N}$ . Dividiamo allora il messaggio in blocchi di  $n$  lettere e cifriamo ogni lettera del blocco con uno degli  $n$  alfabeti scelti, seguendo sempre lo stesso ordine. Indicati con  $A_i$ ,  $1 \leq i \leq n$ , gli  $n$  alfabeti, allora tutte le lettere di ciascun blocco che si trovano nella stessa posizione  $i$ -esima verranno cifrate con il medesimo alfabeto  $A_i$ . Ciò significa che ogni lettera viene cifrata usando uno dei metodi precedenti, ma con chiavi diverse. Questo cifrario è chiamato **cifrario polialfabetico periodico**.

Il primo esempio di questo tipo sembra dovuto a Leon Battista Alberti, intorno alla metà del 1400: egli propose l'introduzione di due alfabeti cifranti per ogni messaggio. La sua idea fu poi perfezionata da Vigenère (seconda metà del 1500) che propose di cifrare ogni messaggio utilizzando 26 alfabeti cifranti, cioè tante quante le lettere dell'alfabeto (ora consideriamo l'alfabeto completo, contenente anche le lettere j,k,w,x,y).

Costruiamo la seguente tabella in cui in ogni riga è riportato l'alfabeto di volta in volta traslato di una posizione. Quindi ogni lettera del messaggio viene cifrata attraverso l'alfabeto di una riga della tabella.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Ma ancora una volta, come possiamo ricordare la sequenza degli  $n$  alfabeti da usare per la cifratura? Memorizzandola di nuovo mediante una parola chiave la cui lunghezza  $n$  rappresenta il periodo secondo cui si ripetono gli alfabeti. Ad esempio, scegliendo come parola chiave *vasco*, cifriamo la frase *certe notti*. Come alfabeti cifranti useremo, ripetendoli per ogni blocco di 4 lettere, le righe della tavola di Vigenère corrispondenti rispettivamente alle lettere *v*, *a*, *s*, *c*, *o* della parola chiave:

certenotti  
vascovasco.

La prima lettera del messaggio, *c*, verrà cifrata con la lettera che si trova nella posizione di *c* usando come alfabeto cifrante quello della riga corrispondente alla lettera *v* della parola chiave, fino alla *e* che sarà cifrata con la riga corrispondente alla lettera *o*, per poi ricominciare usando l'alfabeto cor-

rispondente alla lettera  $v$  per la  $n$  del nostro messaggio.

Con questo sistema, quante sono le chiavi possibili? In un certo senso, usando parole chiave prive di significato e di lunghezza arbitraria, le chiavi sono infinite. Dobbiamo però ricordare che il cifrario di Vigenère risale al 1500, quando i corrieri fidati viaggiavano a cavallo ed era essenziale che la chiave fosse breve e facile da ricordare. Per non snaturarlo dunque, la parola chiave dovrebbe essere presente nel vocabolario.

Concentriamoci ora su come il crittanalista possa agire per decifrare i messaggi. Come si è già visto, l'analisi delle frequenze fornisce una stima delle frequenze con cui le lettere compaiono nei testi (peculiare per ogni lingua); ad esempio, dato che nella lingua italiana la maggior parte delle parole termina con una delle vocali  $a$ ,  $e$ ,  $i$ ,  $o$  vorrà dire che la maggior parte delle lettere finali delle parole dovranno essere queste. Entrano poi in gioco considerazioni relative alle doppie: se sono presenti nel messaggio cifrato lettere consecutive identiche deve trattarsi di consonanti. Questo vale però per cifrari in cui si è usato un singolo alfabeto.

I cifrari a sostituzione polialfabetica sono stati a lungo ritenuti inattaccabili data la loro apparente complessità. La stessa lettera può infatti essere cifrata in modi diversi a seconda della sua posizione nel messaggio. In realtà, se il crittanalista riesce a scoprire il periodo  $p$  usato, può decomporre il crittogramma originario in  $p$  "crittogrammi parziali", ognuno dei quali ottenuto da un cifrario a sostituzione monoalfabetica. Forzare il cifrario polialfabetico si riduce quindi a forzare  $p$  cifrari monoalfabetici.

Anche se i cifrari classici sono ormai superati, i principi che stanno alla base della loro costruzione sono validi ancora oggi.

Analizziamo il procedimento effettuato in questi esempi per generalizzare la situazione: il **testo in chiaro** o **messaggio**, viene trasformato secondo certe regole nel **testo cifrato** o **crittogramma**. Questa operazione è chiamata **cifratura**. Per la trasmissione del crittogramma si può utilizzare un canale non sicuro (per esempio la radio). Prima di arrivare a destinazione il messaggio può essere intercettato da una spia. Teoricamente il cifrario

deve essere tale da consentire con facilità le operazioni di decifrazione al legittimo destinatario, mentre per la spia esse dovrebbero rivelarsi proibitive. A determinare la differenza è la conoscenza da parte del destinatario di un'informazione determinante detta chiave del cifrario (ad esempio nel cifrario di Cesare il valore di  $n$ ). Tale chiave deve rimanere inaccessibile alla spia e dunque essere trasmessa attraverso canali assolutamente sicuri (non soggetti ad intercettazioni). Ma se possediamo un canale così sicuro, perchè non trasmettervi direttamente il messaggio in chiaro? La chiave, data la sua ridotta dimensione, ha alcuni vantaggi in fase di trasmissione e può, ad esempio, essere impiegata per smaltire un traffico di messaggi piuttosto intenso. Considerando poi che il canale speciale potrebbe essere disponibile solo per brevi intervalli di tempo, l'invio dell'intero messaggio potrebbe rivelarsi troppo costoso. Insomma, abbiamo capito che il problema della distribuzione delle chiavi è di importanza cruciale per il buon funzionamento di un sistema crittografico. Osserviamo però che il cifrario scelto dipende dall'utilizzo che vogliamo farne; infatti in alcuni casi vogliamo proteggere le informazioni riservate da intercettatori occasionali e per periodi piuttosto brevi. Non ha quindi molta importanza se il crittogramma viene decifrato in un paio d'ore (o di giorni, a seconda dei casi). Diverso è l'obiettivo della crittografia a fini strategici, che mira ad una protezione di durata illimitata, o, più realisticamente, "praticamente" illimitata (non c'è una gran differenza fra milioni di anni e l'eternità).

Un'ultima osservazione: una spia ben preparata con tempo e denaro a disposizione, riuscirà sempre prima o poi a capire qual'è il cifrario utilizzato (ad esempio quello di Cesare). Questa amara considerazione ha portato i crittografi a concentrarsi sul ruolo cruciale e determinante svolto dalla protezione della chiave. Dunque nella crittografia strategica il sistema di cifra non deve essere compromesso se il congegno di cifratura o quello di decifrazione finiscono nelle mani dell'avversario. La sicurezza è quindi affidata esclusivamente alla segretezza della chiave, proprio quello che abbiamo citato nell'introduzione come principio di Kerckhoff, uno degli assiomi indiscussi

della crittologia contemporanea.

## 2.5 Macchine per cifrare

L'epoca delle macchine e dell'industrializzazione non ha risparmiato neppure la crittografia consentendo di realizzare sistemi di cifratura estremamente complessi. Sin dalla fine del '700, congegni meccanici e successivamente elettronici, hanno permesso di automatizzare le operazioni di cifratura dei messaggi e di decifrazione dei crittogrammi. La seconda guerra mondiale rappresenta l'apice di questo sviluppo. I cifrari che vengono costruiti sono solitamente a sostituzione polialfabetica.

L'esempio più famoso è senz'altro la macchina *Enigma*, usata in varie versioni dai tedeschi, proprio durante la seconda guerra mondiale. Essa consiste essenzialmente in un certo numero di rotori, ossia di dischi adiacenti che ruotano su un perno comune. Ogni disco ha 26 contatti su una faccia e 26 sull'altra: i contatti delle due facce sono collegati fra loro in modo che ad uno su una faccia corrisponda uno ed un solo dell'altra. Le lettere in chiaro entrano ad un capo del "banco" dei rotori, viaggiano attraverso i rotori ed escono all'altro capo come lettere in cifra. La chiave è determinata dai collegamenti all'interno dei dischi e dalla posizione iniziale dei rotori. Per forzare l'Enigma gli inglesi ed i loro collaboratori polacchi si avvalsero di macchine elettroniche di calcolo chiamate Colossi, che possono essere considerati i primi calcolatori della storia (1943). Lo sviluppo accelerato della crittografia durante la seconda guerra mondiale è quindi legato profondamente alla nascita dell'informatica.[4]

## 2.6 I Segreti Oggi

Fino a metà Ottocento la crittografia era ancora un'arte, una pratica che si acquisiva con l'esperienza, più che un metodo riproducibile ed analizzabile nelle sue regole. Inoltre si basava sulla fantasia del progettista e richiedeva



intuito nell'analista che voleva infrangere il cifrario.

Secondo il grande crittoanalista Beurling (1921-1948), il lavoro di decrittazione è analogo a quello che precede la dimostrazione di un teorema; si fonda su una massa di dati, di sensazioni e di verifiche empiriche ma non può essere formalizzato. Per i non addetti ai lavori il risultato appare un atto di magia. Quella che oggi è una vera e propria scienza, fu utilizzata per secoli quasi esclusivamente da militari e diplomatici.

Il cambiamento radicale avvenne nel XX secolo. In seguito all'invenzione della radio e poi del computer sono aumentate nel contempo opportunità e necessità di comunicare informazioni in modo riservato: chi fa uso della posta elettronica, della carta di credito per comprare oggetti su internet, del bancomat o della pay-tv si avvale, senza esserne consapevole, di tecniche crittografiche.

Di conseguenza oggi la crittografia ha abbandonato la fase dei sistemi empirici di cifratura, basati sull'intuizione personale e dotati di poche regole, esattamente come nel corso del tempo ha superato altre fasi. Si pensi al periodo "eroico"-monoalfabetico, quando la fantasia costituiva la maggiore sorgente di imprevedibilità per l'intercettatore, o a quello rinascimentale (con i primi cifrari polialfabetici, i primi congegni meccanici e i primi algoritmi) efficacemente contrastabile con metodi statistici.

Come abbiamo visto l'inizio del '900 presenta nuovi concetti e nuovi dispositivi. Ma la vera rivoluzione, riguarda la nascita dell'idea di "chiave pubblica" negli anni '70. Con essa, l'antica arte di trasmettere messaggi segreti diventa scienza, invade diversi campi e discipline scientifiche: teoria dell'informazione, complessità computazionale, calcolo delle probabilità, teoria dei numeri. Investe anche problematiche di grande valore sociale e politico, arrivando persino a coinvolgere la nostra privacy ed il nostro giudizio morale.

Fino agli anni '70 tutti i sistemi crittografici facevano uso di un'unica chiave (o di una coppia di chiavi reciprocamente determinate e quindi determinabili) per cifrare e decifrare il messaggio. Vi ricordate l'adagio di Kerckhoffs? Il problema è riuscire a scambiarsi la chiave senza che venga scoperta... Ma

quanto possono essere affidabili dei corrieri? Quanto sicuro può dirsi un qualunque canale d'informazione? Come si diceva poco fa, la grande novità del secolo scorso fu l'idea di utilizzare chiavi diverse (e non calcolabili vicendevolmente) per cifrare e decifrare un messaggio, eliminando il problema della distribuzione delle chiavi. Infatti non c'è più bisogno di inviarle: la chiave per cifrare può essere vista da chiunque, mentre solo il destinatario ha quella per decifrare. Se Alice vuole ricevere un messaggio segreto da Bob, gli manda una cassaforte vuota con un lucchetto aperto. Bob, dopo aver inserito il messaggio nella cassaforte, chiude il lucchetto, e spedisce tutto ad Alice, che è la sola a possedere le chiavi. La cassaforte può essere intercettata ma non aperta. In questo modo Alice non corre rischi dato che le chiavi rimangono sempre e solo nelle sue mani. Questa viene detta **crittografia asimmetrica**, o **crittografia a chiave pubblica**. Non vi è più un'unica chiave, bensì una coppia:

- la chiave pubblica, conosciuta da tutti, serve a cifrare;
- la chiave privata, segreta, viene utilizzata per decifrare il crittogramma ottenuto con quella particolare chiave pubblica.

Alla fine del nostro percorso vedremo in che modo sia possibile realizzare un sistema di questo tipo, proprio grazie alla matematica.

## 2.7 Crittosistema

Iniziamo a formalizzare quanto visto finora in maniera intuitiva.

Un crittosistema è una  $n$ -upla  $(P, C, K, E, D)$  con le seguenti proprietà:

1.  $P$  è l'insieme dei testi in chiaro e contiene i messaggi da spedire.
2.  $C$  è l'insieme dei testi cifrati e contiene i crittogrammi.
3.  $K$  è l'insieme delle chiavi e contiene tutte le possibili chiavi del cifrario.

4.  $E = \{E_k : k \text{ appartiene a } K\}$  è la famiglia di funzioni di cifratura  $E_k : P \rightarrow C$ .
5.  $D = \{D_k : k \text{ appartiene a } K\}$  è la famiglia di funzioni di decifrazione  $D_k : C \rightarrow P$ .
6. Per ogni  $e$  appartenente a  $K$ , esiste un  $d$  appartenente a  $K$  tale che  $D_d(E_e(p)) = p$  per tutti i  $p$  appartenenti a  $P$ .

Riprendendo quanto già esposto in precedenza, utilizziamo la nuova notazione e facciamo un esempio concreto: Alice può usare un crittosistema per mandare un messaggio segreto  $m$  a Bob. Per farlo usa una chiave di cifratura  $e$ ; Bob usa la corrispondente chiave di decifrazione  $d$ . Alice calcola il testo cifrato  $c = E_e(m)$  e lo manda a Bob il quale può ottenere il testo decifrato come  $m = D_d(c)$ . Ovviamente la chiave di decifrazione deve rimanere segreta.

## 2.8 Sicurezza assoluta?

Esiste un sistema crittografico assolutamente sicuro? Claude Shannon dimostrò nel 1949 che l'unico metodo era quello ideato da Gilbert Vernam nel 1918 che usava chiavi lunghe almeno quanto il messaggio: gli altri sistemi rendevano sicuri i messaggi solo per un breve periodo. La realizzazione di questo metodo pone numerose difficoltà pratiche, che fra poco vedremo. Infatti sembra che questo cifrario sia stato utilizzato solo dai militari o per la protezione di alcune comunicazioni telefoniche tra Washington e Mosca durante la Guerra fredda.

Questo risultato non è solamente una congettura, ma un rigoroso teorema di matematica. Nel paragrafo precedente abbiamo introdotto le notazioni sui crittosistemi proprio perchè i teoremi di matematica si applicano solo a concetti ben definiti ed era quindi indispensabile fornire una cornice adeguata e precisa. Il processo di matematizzazione o formalizzazione della crittografia

è strettamente legato al nome di Claude Shannon ed al suo articolo “Communication theory of secrecy systems” pubblicato nel 1949.

Analizziamo in dettaglio come funziona il cifrario di Vernam: supponiamo che Alice debba trasmettere un messaggio formato da una sequenza ordinata di 0 e 1, cioè in codice binario. Alice sceglie una parola chiave che è una sequenza casuale di 0 e 1 ancora della stessa lunghezza. Allora:

- la cifratura si ottiene sommando il messaggio in chiaro con la chiave, componente per componente;
- la decifrazione è ottenuta nello stesso modo sommando al crittogramma la chiave, sempre componente per componente.

Ad esempio, se il messaggio che vogliamo spedire è

$$x = 1001010110101$$

e la parola chiave scelta è

$$y = 0010101101011$$

allora il crittogramma diventa

$$x' = 1011111011110.$$

Quali sono dunque le difficoltà pratiche a cui si accennava in precedenza?

- la chiave può essere recuperata sommando il messaggio in chiaro e il crittogramma, il che suggerisce di usarla solo una volta;
- il crittosistema prevede che l'insieme delle chiavi coincida con quello dei possibili messaggi: per ogni intero positivo  $l$  ci sono tante chiavi di lunghezza  $l$ , quanti sono i messaggi della stessa lunghezza, cioè  $2^l$ ;
- come al solito il mittente ed il destinatario dovranno concordare per ogni corrispondenza una chiave e trasmettersela; ma questa volta la chiave non è breve, anzi è lunga quanto il messaggio;

- generare una chiave, e cioè una sequenza assolutamente casuale di 0 e 1, è una procedura complicata e costosa: il calcolatore genera numeri in maniera perfettamente deterministica, che possono essere usati come se fossero casuali, ma non lo sono veramente. Nella maggioranza delle applicazioni ciò non ha nessuna importanza, ma in crittografia i normali programmi sono inadeguati. Se infatti qualcuno venisse a conoscenza dell'algoritmo col quale sono stati generati i numeri, allora potrebbe facilmente risalire alla chiave.

Nonostante questi limiti, cerchiamo ora di capire per quale motivo questo sistema sia perfetto. Innanzitutto vediamo cosa si intende per perfetto:

**Definizione 2.1.** Un crittosistema si dice perfetto se e solo se, per ogni  $c_0$  in  $M$ ,  $P_k(c_0 = e_k(m_0))$  è la stessa per tutti gli  $m_0 \in M$ .

Questo equivale a dire che la conoscenza di  $c_0$  non è di aiuto all'intercettatore nell'identificazione di  $m_0$ .

Un altro modo per definire un crittosistema perfetto è il seguente: l'intercettatore, che è a conoscenza del crittogramma, può considerare ogni singolo messaggio  $m_0$  di  $M$ , valutare la probabilità che il messaggio spedito sia proprio  $m_0$ , cioè  $P_m(m = m_0)$  e confrontarla con la probabilità dello stesso evento condizionata alla conoscenza di  $c_0$  e calcolata anche al variare della chiave  $k$ , cioè  $P_{m,k}(m = m_0 | c_0 = e_k(m_0))$ . Vale allora il seguente

**Teorema 2.8.1.** *Un crittosistema è perfetto se e solo se, per ogni scelta di  $m_0, c_0$  in  $M$ ,  $P_m(m = m_0) = P_{m,k}(m = m_0 | c_0 = e_k(m_0))$ .*

Si sta quindi ripetendo il fatto che la conoscenza del crittogramma non fornisce informazioni aggiuntive riguardo al messaggio originario.

Il cifrario di Vernam è perfetto perchè  $M = K = \{0, 1\}^l$  e, per ogni  $k$  in  $K$ , tanto  $e_k$  quanto  $d_k$  agiscono sui messaggi  $m$  di  $M$  come l'addizione modulo 2 per  $k$ . Allora per ogni scelta di  $c_0 \in M$   $P_k(c_0 = e_k(m_0)) = 2^{-l}$  è costante al variare di  $m_0$  in  $M$ .

Vale ancora di più: il cifrario di Vernam è l'unico perfetto. Infatti si può dimostrare che

**Teorema 2.8.2.** *In un crittosistema perfetto ci sono almeno tante chiavi quanti messaggi.*

## 2.9 Divisibilità e Numeri Primi

Andiamo ora a definire e studiare i principali concetti matematici che ci serviranno per formalizzare i crittosistemi precedenti e per costruirne altri più avanzati ed efficienti.

### Definizione 2.2.

Siano  $a$  e  $b$  due interi, si dice che  $a$  divide  $b$ , in simboli  $a|b$ , se esiste un intero  $q$  tale che  $b = qa$ .

Vediamo alcune utili proprietà:

- Se  $a|b$  e  $c$  è un qualsiasi intero allora  $a|bc$ ;
- Se  $a|b$  e  $b|c$  allora  $a|c$ ;
- Se  $a|b$  e  $a|c$  allora  $a|b \pm c$ .

**Dimostrazione 2.9.1** (da far fare ai ragazzi, anche in aula).

- $b = qa \Rightarrow bc = qac$ ;
- $b = qa, c = pb \Rightarrow c = pqa$ ;
- $b = qa, c = pa \Rightarrow b + c = qa + pa = (q + p)a$ .      $\#$

**Proposizione 2.9.2** (in aula solo enunciato).

*Siano  $a$  e  $b$  interi con  $b \neq 0$ . Allora esistono e sono univocamente determinati due interi  $q$  ed  $r$  tali che*

$$a = bq + r, \quad \text{con } 0 \leq r < |b|$$

**Dimostrazione 2.9.3.** Supponiamo inizialmente che  $b$  sia un intero positivo. Consideriamo l'insieme di tutti i multipli interi di  $b$ :

$$\dots, -kb, \dots, -2b, -b, 0, b, 2b, \dots, kb, \dots$$

dove  $k$  è un intero positivo. Esiste un unico  $q \in \mathbb{Z}$  tale che

$$qb \leq a < (q+1)b.$$

Si pone  $r = a - qb$  e ciò determina i due numeri  $q, r$  richiesti. Osserviamo che  $0 \leq r < b$  per costruzione e  $q$  è unico perchè è il minimo intero il cui prodotto per  $b$  non supera  $a$ . Di conseguenza anche  $r$  è unico.

Se  $b$  è negativo, per quanto già dimostrato, si ha in modo unico

$$a = q'(-b) + r$$

con  $0 \leq r < -b = |b|$ . Basta allora porre  $q = -q'$  per trovare  $q$  ed  $r$ .  $\#$

### 2.9.1 MCD

#### Definizione 2.3.

Siano  $a$  e  $b$  due interi non entrambi nulli. Si dice massimo comun divisore di  $a$  e  $b$ , denotato con  $MCD(a, b)$ , il più grande intero positivo che divide sia  $a$  che  $b$ .

#### Proposizione 2.9.4.

*Siano  $a$  e  $b$  due interi non entrambi nulli. Allora  $MCD(a, b)$  è l'unico intero positivo  $d$  tale che:*

- $d|a$  e  $d|b$
- se  $z$  è un intero tale che  $z|a$  e  $z|b$  allora  $z|d$

#### Definizione 2.4.

Si dice che due interi  $a$  e  $b$  sono coprimi o primi fra loro se  $MCD(a, b) = 1$ .

*Osservazione 1.*

L'MCD di due naturali esiste sempre ed è unico; infatti esiste almeno un divisore comune di  $a$  e  $b$ , cioè il numero 1. Poichè i divisori di  $a$  sono tutti minori o uguali ad  $a$  e quelli di  $b$  minori o uguali a  $b$ , l'insieme dei divisori comuni di  $a$  e di  $b$  oltre a non essere vuoto è finito e ha un massimo.

Inoltre si ha:

- Se  $a|b$  allora  $MCD(a, b) = a$ ; infatti se  $a \neq b$  vale  $a < b$  e  $a$  è il massimo divisore di sè stesso;
- se  $a = qb + r$ , con  $0 < r < b$ , allora i divisori comuni alla coppia  $a, b$  coincidono con i divisori comuni alla coppia  $b, r$ . In particolare  $MCD(a, b) = MCD(b, r)$ .

Infatti se  $c$  è un divisore comune alla coppia  $a, b$  allora  $c|b$  e anche  $c|qb$ , e quindi  $c|(a - qb) = r$ , quindi  $c$  è un divisore comune alla coppia  $b, r$ . Viceversa se  $c|b$  e  $c|r$  allora  $c|(qb + r) = a$ , quindi è un divisore comune alla coppia  $a, b$ .

### L'algoritmo di Euclide

Un metodo per trovare  $MCD(a, b)$  è dato dall'algoritmo di Euclide o delle divisioni successive. Esso si fonda sulle due proprietà precedenti. Sia  $a > 1, b > 1, a > b$ . L'algoritmo consiste nel considerare la successione di divisioni:

$$a = bq + r_1$$

con  $r_1 = 0$  oppure  $0 < r_1 < b$ ; nel secondo caso dividiamo  $b$  per  $r_1$ :

$$b = r_1q_1 + r_2$$

con  $r_2 = 0$  oppure  $0 < r_2 < r_1$ ; nel secondo caso dividiamo  $r_1$  per  $r_2$ :

$$r_1 = r_2q_2 + r_3$$

con  $r_3 = 0$  oppure  $0 < r_3 < r_2$ ; nel secondo caso dividiamo  $r_2$  per  $r_3$

...



$$r_i = r_{i+1}q_{i+1} + r_{i+2}$$

con  $r_{i+2} = 0$  oppure  $0 < r_{i+2} < r_{i+1}$ ; nel secondo caso dividiamo  $r_{i+1}$  per  $r_{i+2}$

...

alla fine avremo:

$$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1}$$

con  $r_{n-1} = 0$  oppure  $0 < r_{n-1} < r_{n-2}$

$$r_{n-2} = r_{n-1}q_{n-1}$$

con  $r_n = 0$ .

Se  $n$  è l'indice tale che  $r_n = 0$  allora  $MCD(a, b) = r_{n-1}$ .

### L'identità di Bézout

Dall'algoritmo di Euclide ricaviamo la seguente proprietà:

$$MCD(a, b) = \alpha a + \beta b$$

Infatti, basta osservare che tutti i resti delle divisioni successive si possono scrivere come combinazioni di  $a$  e  $b$  in questo modo:

$$r_1 = a - bq_1$$

$$r_2 = b - r_1q_1$$

⋮

$$r_n = r_{n-2} - r_{n-1}q_n$$

da cui si ricava

$$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = (-q_2)a + (1 + q_1q_2)b,$$

cioè  $r_1$  e  $r_2$  si scrivono come combinazione di  $a$  e  $b$ . Ma allora anche  $r_3$ , che è una combinazione a coefficienti interi di  $r_1$  e  $r_2$ , sarà una combinazione a coefficienti interi di  $a$  e  $b$ . In definitiva,  $MCD(a, b) = r_n$  è una combinazione

a coefficienti interi di  $r_{n-1}$  e  $r_{n-2}$  e quindi di  $a$  e  $b$ .

Un'interessante applicazione di questo risultato si ha nello studio delle equazioni lineari diofantee, cioè del tipo

$$ax + by = c$$

dove però  $a, b, c$  sono in  $\mathbb{Z}$ . Supponiamo dunque di voler vedere se l'equazione possiede soluzioni intere. In un piano cartesiano l'equazione rappresenta una retta, della quale vogliamo sapere se passa per punti interi. Si ha:

**Proposizione 2.9.5.**

*L'equazione  $ax + by = c$ , con  $a, b, c \in \mathbb{Z}$  e  $a, b \neq 0$ , possiede una soluzione intera  $(x, y)$  se e solo se l'MCD( $a, b$ ) divide  $c$ .*

**Dimostrazione 2.9.6.** Sia  $(\bar{x}, \bar{y})$  una soluzione intera dell'equazione, e sia  $d = \text{MCD}(a, b)$ . Allora  $d$  dividendo  $a$  e  $b$ , dividerà il primo membro dell'equazione e di conseguenza anche  $c$ .

Viceversa supponiamo che  $d$  divida  $c$ , quindi  $c = pd$ . Scriviamo  $d = \alpha a + \beta b$  per l'identità di Bézout. Moltiplicando ambo i membri per  $p$  si ha:

$$c = \alpha pa + \beta pb$$

e posto  $\bar{x} = \alpha p$  e  $\bar{y} = \beta p$ , ne segue che  $(\bar{x}, \bar{y})$  è una soluzione dell'equazione.

‡

## 2.9.2 Numeri primi

Passiamo ora allo studio di particolari numeri interi che hanno attratto i matematici di tutti i tempi.

**Definizione 2.5.**

Un naturale  $a \neq 0$  si dice primo o irriducibile quando è diverso da 1 e non ha divisori propri, cioè divisori che non siano né 1 né  $a$  stesso.  $b$  si dice invece composto o riducibile quando è diverso da 1 e non è primo, ossia quando ha divisori propri.

Ecco un'importante caratterizzazione dei numeri primi:

**Proposizione 2.9.7.**

*Un numero intero positivo  $p > 1$  è primo se e solo se vale:*

$$(*) \quad \text{se } p \text{ divide } ab, \text{ allora } p|a \text{ oppure } p|b.$$

**Dimostrazione 2.9.8.** Iniziamo col dimostrare che  $p$  primo implica  $(*)$ . Se  $p$  divide  $a$  non c'è nulla da dimostrare. Supponiamo dunque che  $p$  non divida  $a$ . Dato che  $p$  è primo, non ha altri fattori che  $p$  e  $1$ ; dunque  $p$  e  $a$  non hanno fattori non banali in comune, cioè  $MCD(a, p) = 1$ . Quindi per l'identità di Bézout esistono due interi  $s$  e  $t$  tali che  $1 = sa + tp$ . Se moltiplichiamo per  $b$  entrambi i membri, otteniamo  $b = sab + tpb$ . Dato che  $p|ab$  per ipotesi e  $p|p$  banalmente, si conclude che  $p|b$ .

Viceversa supponiamo che valga  $(*)$ . Se  $p$  non fosse primo, avremmo  $p = hk$  con  $h, k$  interi minori di  $p$ . D'altra parte si ha  $p|hk = p$  e quindi per ipotesi o  $p|h$  o  $p|k$ , il che è assurdo, perchè  $h$  e  $k$  sono minori di  $p$ .

**Teorema 2.9.9** (fondamentale dell'aritmetica).

*Ogni intero  $n$  maggiore di 1 può essere scritto in modo unico (a meno dell'ordine dei fattori) come prodotto di numeri primi. In termini matematici*

$$\forall n \in \mathbb{N} \quad n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

**Dimostrazione 2.9.10** (da fare in aula solo l'esistenza).

- Esistenza della fattorizzazione:

Procediamo per induzione su  $n$ . Se  $n = 2$  non vi è nulla da dimostrare. Supponiamo allora di avere provato l'esistenza di una fattorizzazione per ogni intero positivo  $k$  con  $2 \leq k < n$  e dimostriamo la stessa cosa per  $n$ . Se  $n$  è primo non c'è nulla da dimostrare. Se invece  $n$  è composto possiamo scrivere  $n = ab$  con  $a, b$  positivi, maggiori di 1 e minori di  $n$ . Allora per l'ipotesi induttiva  $a$  e  $b$  sono fattorizzabili in un prodotto di primi in questo modo:

$$a = p_1 \cdots p_r, \quad b = \overline{p}_1 \cdots \overline{p}_s$$

da cui si ricava immediatamente

$$n = ab = p_1 \cdots p_r \cdot \bar{p}_1 \cdots \bar{p}_s.$$

Se raggruppiamo i numeri primi fra loro uguali otteniamo il risultato.

- Unicità della fattorizzazione:

Questa volta l'induzione viene effettuata sul numero  $m$  di fattori irriducibili di una qualche fattorizzazione di  $n$ , cioè su  $m = \alpha_1 + \alpha_2 + \cdots + \alpha_s$ . Se tale  $m$  è 1 significa che  $n$  è un primo  $p$ . Supponiamo ora che  $n = p$  abbia un'altra fattorizzazione

$$p = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}.$$

Essendo  $p$  un primo che divide il secondo membro,  $p$  dividerà uno dei fattori del secondo membro, ad esempio  $p|q_1$ . Per la legge di cancellazione si ottiene:

$$1 = q_1^{k_1-1} q_2^{k_2} \cdots q_t^{k_t}$$

il che implica che tutti gli esponenti a secondo membro sono nulli. Allora, tornando alla fattorizzazione di  $p$ , il secondo membro si riduce a  $q_1$  e quindi  $n = p = q_1$  è l'unica fattorizzazione di  $n$ . Abbiamo così provato la base dell'induzione. Supponiamo ora che l'unicità della fattorizzazione sia stata provata per ogni intero che abbia una fattorizzazione in  $m - 1$  fattori irriducibili. Sia  $n$  un intero che ha una fattorizzazione in  $m$  fattori irriducibili e sia:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s} = q_1^{k_1} \cdot q_2^{k_2} \cdots q_t^{k_t}$$

due fattorizzazioni di  $n$  con  $\alpha_1 + \cdots + \alpha_s = m$ . Ora  $p_1$  è un primo che divide il secondo membro, quindi dividerà ad esempio  $q_1$ . Come prima risulta  $p_1 = q_1$  e quindi di nuovo per la legge di cancellazione si ha

$$p_1^{\alpha_1-1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} = q_1^{k_1-1} q_2^{k_2} \cdots q_t^{k_t}$$

dove al primo membro il numero di fattori irriducibili è sceso a  $m - 1$ . Per l'ipotesi induttiva vale in questo caso l'unicità della fattorizzazione, e dunque i  $q_j$  coincidono con i  $p_i$ , a meno dell'ordine. Ma allora è chiaro che anche la fattorizzazione di  $n$  è unica.  $\#$

Il teorema fondamentale dell'aritmetica fornisce anche un metodo sistematico per trovare tutti i divisori positivi di un intero positivo  $n$ , una volta che esso sia scritto come prodotto di primi. Infatti, se  $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$  allora i divisori  $d$  di  $n$  sono tutti e soli quelli del tipo

$$d = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

con  $0 < \beta_i < \alpha_i$  per ogni  $i = 1 \dots r$ .

Inoltre, se si conosce la fattorizzazione in primi dei due interi  $a$  e  $b$  è facile calcolare il loro massimo comun divisore. Infatti basta prendere il prodotto di tutti i primi che compaiono in entrambe le fattorizzazioni, elevati al minore dei due esponenti con cui compaiono. Tuttavia, nel caso non si conosca la fattorizzazione dei due numeri, questo non è il metodo più efficiente: provate infatti a calcolare il massimo comun divisore di 173927932739274 e 3628462982719372 in questo modo!!!

**Teorema 2.9.11** (di Euclide).

*Esistono infiniti numeri primi.*

**Dimostrazione 2.9.12.** Dimostriamo questo teorema usando il ragionamento per assurdo: se i numeri primi fossero in numero finito il loro insieme sarebbe costituito dai numeri  $p_1, \dots, p_n$  con  $p_1 < p_2 < \dots < p_n$ . Ora consideriamo il numero  $N = p_1 \cdots p_n + 1$ . Per ipotesi questo numero non può essere primo perchè è maggiore di  $p_n$ , il più grande numero primo. Allora  $N$  ha una decomposizione in fattori primi, cioè

$$N = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

con almeno uno degli  $\alpha_i$  positivo. Allora  $p_i | N$  per un qualche  $i$ . Ma vale anche

$$p_i | (N - 1) = p_1 \cdots p_n$$

perchè  $p_i$  è proprio uno di quei primi. Quindi

$$p_i | (N - (N - 1)) = 1$$

il che è assurdo, dato che  $p_i$  deve essere maggiore di 1 per la definizione di numero primo. ‡

### Curiosità

Si hanno molti problemi irrisolti di teoria dei numeri che coinvolgono i numeri primi:

- **Congettura di Goldbach:** ogni numero naturale pari  $n$  maggiore di 2 è somma di due numeri primi.

È stato verificato che tale congettura è vera per tutti i numeri pari  $n$  minori di  $2 \cdot 10^{10}$ . Ciò ovviamente non basta, dato che è sufficiente trovare un pari maggiore di  $2 \cdot 10^{10}$  che non sia somma di due primi per provare che la congettura è falsa. I matematici sono portati a pensare che sia vera perchè sono noti risultati simili a questo, ad esempio:

**Teorema 2.9.13** (di Vinogradov). *Ogni naturale dispari sufficientemente grande è somma di tre numeri primi.*

**Teorema 2.9.14** (di Chen Jing-run). *Ogni naturale pari è somma di due naturali  $p + a$  con  $p$  primo ed  $a$  o primo o prodotto di due primi.*

- Due naturali primi  $p < q$  si dicono gemelli se  $q = p + 2$ .

**Congettura dei primi gemelli:** esistono infiniti primi gemelli.

**Teorema 2.9.15** (di Chen Jing-run). *Esistono infiniti primi  $p$  tali che  $p + 2$  o è primo oppure prodotto di due primi.*

### Crivello di Eratostene

Un buon metodo per generare una lista di numeri primi in ordine crescente minori o uguali ad  $n$  è il crivello di Eratostene, matematico di Cirene

che visse tra il 256 e il 194 A.C. circa. Si procede in questo modo: il primo intero diverso da 1 è 2, che è primo. Sia  $p_1 = 2$ . Il primo passo consiste nell'eliminare tutti i multipli di 2. Il primo numero maggiore di 2 non eliminato è  $p_2 = 3$ , che è primo, e al secondo passo eliminiamo anche tutti i multipli di 3. Ora il primo numero non eliminato maggiore di 3 è  $p_3 = 5$  e si eliminano anche tutti i suoi multipli. In generale, al  $k$ -esimo passo si considera il primo numero  $p_k$  non eliminato maggiore di  $p_{k-1}$ , e si eliminano tutti i suoi multipli. Ad un certo punto il procedimento termina (perché la successione  $p_1 > p_2 > \dots > p_k > \dots$  è strettamente crescente). Scriviamo la lista dei primi 30 numeri maggiori di 1:

2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31.

I numeri sottolineati sono quelli che vengono eliminati dall'algoritmo di Eratostene.

### 2.9.3 Test di primalità e fattorizzazione

Per determinare se un numero intero sia primo o meno si ricorre ai test di primalità. Si noti la differenza tra test di primalità e fattorizzazione di un numero intero: la scomposizione in fattori primi è un'operazione computazionalmente complessa e lenta, tanto da essere sfruttata per la creazione di codici cifrati. Più rapido è invece verificare solamente se un numero sia primo o meno.

Oggigiorno si fa uso di test che danno una risposta certa solo se dicono che il numero è composto; in caso contrario, cioè se affermano che un numero è primo, esiste un certo margine di errore. Questi test, che forniscono una risposta corretta con una probabilità solo vicina a 1, sono chiamati **probabilistici** e hanno il vantaggio di impiegare un tempo molto inferiore rispetto ai test **deterministici**.

Un esempio di test deterministico molto semplice è il tentativo di dividere il numero  $n$  per tutti i numeri  $s < n$ . L'efficienza di questo algoritmo, come si può intuire facilmente, è molto bassa. Proviamo a perfezionarlo un po': dividiamo  $n$  solo per i numeri primi minori di esso. E ancora, è inutile supe-

rare il numero  $\frac{n}{2}$  nei nostri tentativi, dato che nessun numero è divisibile per un numero maggiore della sua metà. Ma non finisce qui: possiamo fermarci prima, osservando che basta dividere per i numeri primi minori di  $\sqrt{n}$ ; infatti vale la seguente

**Proposizione 2.9.16.** *Se un intero positivo  $n$  non è divisibile per nessun primo minore o uguale a  $\sqrt{n}$ , allora  $n$  è primo.*

**Dimostrazione 2.9.17.** Supponiamo che  $n$  sia composto, cioè  $n = ab$  con  $a$  e  $b$  interi tali che  $1 < a, b < n$ . Di sicuro uno dei due fattori,  $a$  o  $b$  è minore o uguale a  $\sqrt{n}$ , altrimenti sarebbe  $n = ab > \sqrt{n} \cdot \sqrt{n} = n$ , il che è assurdo. Dunque  $n$  ha un fattore, ad esempio  $a$ , minore o uguale a  $\sqrt{n}$ . Se esso è primo la proposizione è dimostrata, altrimenti,  $a$  ha comunque un fattore primo  $p$ , che sarà minore di  $a$  che a sua volta abbiamo visto essere minore di  $\sqrt{n}$ .  $\#$

Una volta effettuato un test di primalità, se veniamo a conoscenza del fatto che il numero analizzato non è primo, si può porre il problema di ottenere la sua fattorizzazione in numeri primi. Tale problema è più complesso dal punto di vista computazionale: infatti si tratta quasi esclusivamente di algoritmi di tipo esponenziale, e quindi molto lenti. Vediamo un metodo di fattorizzazione diverso dal semplice tentativo di dividere un numero  $n$  per i numeri primi minori di  $\sqrt{n}$ :

*Fattorizzazione alla Fermat:*

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

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

con  $\frac{a+b}{2}$  e  $\frac{a-b}{2}$  interi non negativi. Infatti, essendo  $n$  dispari, anche  $a$  e  $b$  sono dispari, e quindi  $a \pm b$  è pari. Inoltre determinare  $x$  e  $y$  tali che  $n = x^2 - y^2$  equivale a determinare  $x$  tale che  $x^2 - n$  sia un quadrato, cioè sia uguale ad



$y^2$ . Quindi si procede così: si trova il più piccolo intero positivo  $k$  tale che  $k^2 \geq n$ , poi si calcolano le differenze  $k^2 - n$ ,  $(k+1)^2 - n$ ,  $(k+2)^2 - n$ , ... fino a che si trova un valore  $t \geq k$  tale che  $t^2 - n$  sia un quadrato.

**Esempio 2.1.** Fattorizziamo il numero 29591. Sia  $k = 173$ , si ha:

$$\begin{array}{ll} 173^2 - 29591 = 338 & 177^2 - 29591 = 1738 \\ 174^2 - 29591 = 685 & 178^2 - 29591 = 2093 \\ 175^2 - 29591 = 1034 & 179^2 - 29591 = 2450 \\ 176^2 - 29591 = 1385 & 180^2 - 29591 = 2809 = (53)^2 \end{array}$$

Quindi l'ultima formula dice che

$$29591 = (180 + 53)(180 - 53) = 233 \cdot 127$$

Siccome 233 e 127 sono numeri primi, abbiamo ottenuto la fattorizzazione di 29591.

## 2.10 Aritmetica modulare

Come possiamo formalizzare la lettura delle ore sul quadrante di un orologio? Anche se questa domanda sembra non c'entrare nulla con la crittografia, vedremo che queste idee ci saranno molto utili in seguito.

Per rispondere alla domanda precedente introduciamo quella che è conosciuta come aritmetica modulare o circolare. Iniziamo con la seguente

### Definizione 2.6.

Dati due interi  $a$  e  $b$ , ed un intero positivo  $m$  si dice che  $a$  è congruo a  $b$  modulo  $m$ , in simboli

$$a \equiv b \pmod{m},$$

se  $m|a - b$ .

La relazione definita da  $\equiv_m$  si chiama relazione di congruenza modulo  $m$

In altre parole, la relazione di congruenza modulo un intero positivo  $m$ , identifica tra loro due interi se e solo se la loro differenza è un multiplo di  $m$

e quindi si può pensare come un'uguaglianza a meno di multipli di  $m$ .

Tornando al nostro orologio, se per esempio sono le sei del pomeriggio, cioè 18 ore dopo la mezzanotte, noi leggiamo la cifra 6. Per le ore del giorno quindi, la cifra 18 uguaglia la cifra 6, cioè stiamo lavorando modulo 12.

**Esempio 2.2.**  $-2 \equiv 19 \pmod{21}$ ,  $10 \equiv 0 \pmod{2}$

**Proposizione 2.10.1.**

*Le seguenti affermazioni sono equivalenti:*

1.  $a \equiv b \pmod{m}$
2. esiste  $k$  intero tale che  $a = b + km$
3.  $a$  e  $b$  hanno lo stesso resto quando vengono divisi per  $m$

*Inoltre ogni intero  $a$  è congruo modulo  $m$  ad un unico intero  $b$  tale che  $0 \leq b < m$ .*

**Definizione 2.7.**

La congruenza modulo  $m$  è una relazione di equivalenza (riflessiva, simmetrica e transitiva); data una relazione di equivalenza su un insieme  $A$  (nel nostro caso l'insieme  $\mathbb{Z}$  dei numeri interi) il sottoinsieme che contiene tutti gli elementi equivalenti ad un elemento  $a$  appartenente ad  $A$  è detto classe di equivalenza di  $a$ . La classe di equivalenza di  $a$  è quindi composta da tutti gli interi che sono ottenuti da  $a$  aggiungendo multipli interi di  $m$ , cioè  $\{b : b \equiv a \pmod{m}\}$ . Questa classe di equivalenza è chiamata classe di resto  $a$  modulo  $m$  e si denota con  $a + m\mathbb{Z}$  o  $[a]_m$ .

**Esempio 2.3.**

La classe resto di 1 modulo 4 è l'insieme  $[1] = \{1, 1 \pm 4, 1 \pm 2 \cdot 4, 1 \pm 3 \cdot 4, \dots\}$ .

**Definizione 2.8.**

L'insieme delle classi di resto modulo  $m$  si scrive  $\mathbb{Z}/m$  o  $\mathbb{Z}_m$ ; ha  $m$  elementi dato che  $0, 1, 2, \dots, m - 1$  sono i possibili resti della divisione per  $m$ . Un insieme dei rappresentanti per quelle classi di resto è un insieme di interi

che contiene esattamente un elemento di ogni classe di resto modulo  $m$  come l'insieme  $\{0, 1, \dots, m-1\}$ , cioè  $\mathbb{Z}_m = \{[0], [1], \dots, [m-1]\}$ .

**Esempio 2.4.**

- Un insieme di rappresentanti modulo 3 contiene un elemento di ognuna delle classi di resto  $3\mathbb{Z}$ ,  $1 + 3\mathbb{Z}$ ,  $2 + 3\mathbb{Z}$ , quindi  $\mathbb{Z}_3 = \{0, 1, 2\}$  o  $\{3, -2, 5\}$  o  $\{9, 16, 14\}$ . Il fatto che noi scegliamo come rappresentazione la prima, dipende dal fatto che gli elementi sono in quel caso minori di 3 e ci permettono di visualizzare meglio l'insieme ed i suoi elementi.
- $\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ .

La seguente proposizione ci permette di effettuare le usuali operazioni di  $\mathbb{Z}$  anche in  $\mathbb{Z}_m$ :

**Proposizione 2.10.2.** *Se  $a, b, c, d$  sono interi tali che  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$  allora valgono le seguenti proprietà:*

$$a \pm c \equiv b \pm d \pmod{m}, \quad ac \equiv bd \pmod{m}$$

Ne deriva quindi che le operazioni:  $[a] + [c] = [a + c]$  e  $[a][c] = [ac]$  nell'insieme quoziente  $\mathbb{Z}_m$  delle classi resto modulo  $m$  sono ben definite, cioè non dipendono dai rappresentanti  $a$  e  $c$  scelti. L'elemento neutro per l'addizione è  $[0]$  e quello della moltiplicazione è  $[1]$  ( $\mathbb{Z}_m$  è così un'anello).

Come per le uguaglianze, anche per le congruenze si può porre il problema di risolvere una congruenza rispetto ad una o più incognite, cioè una congruenza lineare nell'incognita  $x$  è un'equazione della forma

$$ax \equiv b \pmod{m}$$

con  $a, b \in \mathbb{Z}$  e  $m > 1$ .

Quando un'equazione di questo tipo ammette soluzioni? La risposta ci viene dalla seguente:

**Proposizione 2.10.3.** *La congruenza  $ax \equiv b \pmod{m}$  ammette soluzioni se e solo se  $d = \text{MCD}(a, m)$  divide  $b$ .*

**Dimostrazione 2.10.4.** Risolvere la congruenza equivale a trovare soluzioni intere dell'equazione lineare diofantea  $ax + my = b$ , che, come abbiamo già dimostrato in precedenza, esistono se e solo se  $\text{MCD}(a, m) | b$ .  $\#$

Quanto visto fino ad ora ci permette di determinare gli elementi invertibili di  $\mathbb{Z}_m$ , cioè

**Definizione 2.9.**

Un elemento  $[a]$  di  $\mathbb{Z}_m$  diverso da  $[0]$  si dice invertibile quando esiste  $[a']$  appartenente a  $\mathbb{Z}_m$  tale che  $[a][a'] = 1$ .

**Proposizione 2.10.5.**

*Una classe resto  $[a]$  in  $\mathbb{Z}_m$  è invertibile se e solo se  $\text{MCD}(a, m) = 1$ , ossia se  $a$  e  $m$  sono coprimi.*

**Dimostrazione 2.10.6.** Determinare gli elementi  $[a] \in \mathbb{Z}_m$  equivale a risolvere la congruenza

$$ax \equiv 1 \pmod{m}.$$

Come abbiamo appena visto tale congruenza ammette soluzione se e solo se  $\text{MCD}(a, m) = 1$ .  $\#$

**Definizione 2.10.**

Il gruppo moltiplicativo dei resti modulo  $m$ , denotato con  $\mathbb{Z}_m^*$ , è l'insieme degli elementi di  $\mathbb{Z}_m$  che sono invertibili.

**Esempio 2.5.**

- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ ,  $\mathbb{Z}_6^* = \{1, 5\}$ ;
- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ ,  $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

Ma a cosa possono servire le congruenze modulo  $m$ ? Vi ricordate la prova del 9? Funzionava così: se per esempio voglio controllare che il mio calcolo

$123 \cdot 456 = 56088$  sia esatto, sommo le cifre dei due fattori:  $1+2+3=6$ ,  $4+5+6=15$ ,  $1+5=6$ . Quindi moltiplico i due risultati ottenuti:  $6 \cdot 6 = 36$ ,  $3+6=9=0$ . Infine sommo le cifre del risultato ottenuto dalla moltiplicazione iniziale:  $5+6+0+8+8=27$ ,  $2+7=9=0$  che coincide col risultato precedente. Il fatto di aver superato il controllo positivamente, non garantisce però che la moltiplicazione sia corretta. Al contrario, se i due risultati ottenuti non fossero stati coincidenti, allora avrei potuto dire che sicuramente era stato commesso un errore.

Questo trucchetto funziona per due semplici motivi:

- se scriviamo 123 in base 10 abbiamo  $1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$ ;
- per ogni  $n > 0$  si ha che  $10^n - 1 = 999 \cdots 9 = 9 \cdot 111 \cdots 1$  e quindi  $10^n \equiv 1 \pmod{9}$ .

Grazie a queste due proprietà possiamo scrivere:

$$123 = 1 \cdot 10^2 + 2 \cdot 10 + 3 \equiv 1 + 2 + 3 \pmod{9}.$$

Più in generale se

$$z = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$$

allora  $z \equiv a_n + a_{n-1} + \cdots + a_0 \pmod{9}$ . Quindi se due numeri sono diversi modulo 9 è chiaro che sono diversi.

Un'altra applicazione delle congruenze consiste nel fornire alcuni criteri di divisibilità, ad esempio il criterio di divisibilità per 3 e per 9:

un numero intero  $z = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$  è divisibile per 3 (rispettivamente per 9) se e solo se la somma delle cifre  $a_0 + a_1 + a_2 + \cdots + a_n$  è divisibile per 3 (rispettivamente per 9). Infatti  $z \equiv a_n + a_{n-1} + \cdots + a_0$  sia modulo 3 che modulo 9 per lo stesso motivo precedente.

Per finire diamo la seguente:

**Definizione 2.11** (Funzione  $\varphi$  di Eulero).

La funzione  $\varphi$  di Eulero è una funzione definita per  $n$  intero positivo nel

modo seguente:  $\varphi(n)$  è il numero di interi non negativi minori o uguali ad  $n$  che sono coprimi con  $n$ . (Si noti che  $\varphi(n)$  è l'ordine del gruppo moltiplicativo degli elementi invertibili dell'anello  $\mathbb{Z}_n$ ).

In particolare osserviamo che  $\varphi(1) = 1$  e se  $p$  è primo, vale banalmente  $\varphi(p) = p - 1$ , dato che  $p$  sarà coprimo con tutti i numeri minori di esso. Inoltre sempre per  $p$  primo vale:  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1)$ .

La funzione  $\varphi$  di Eulero è moltiplicativa, cioè dati due interi  $m$  ed  $n$  maggiori di 1 tali che  $MCD(m, n) = 1$ , si ha che  $\varphi(mn) = \varphi(m)\varphi(n)$ .

## 2.11 Esempio di Crittosistema a chiave pubblica: RSA

Ora che abbiamo acquisito le conoscenze matematiche di base, torniamo alla crittografia.

Tutti i sistemi di cifratura esposti nella prima parte richiedevano che la chiave fosse tenuta rigorosamente segreta. Ora illustriamo un sistema a chiave pubblica per cui basta tenere segreta la chiave di decifrazione. Ricavare infatti la chiave di decifrazione da quella pubblica di cifratura è computazionalmente troppo dispendioso. Questo meccanismo è possibile grazie all'esistenza di funzioni dotate di questa proprietà: sono invertibili, ma, mentre il calcolo della funzione diretta è "facile", quello della funzione inversa è "difficile". Queste funzioni sono dette unidirezionali.

Il sistema che andiamo a studiare si chiama RSA, in nome dei suoi inventori Ron Rivest, Adi Shamir e Len Adleman. Esso fu il primo crittosistema a chiave pubblica ed è ancora il più importante. La sua sicurezza è strettamente legata alla difficoltà di trovare la fattorizzazione di un intero positivo composto che è prodotto di due primi molto grandi. Vediamo come funziona.

### 2.11.1 Generazione delle chiavi

Bob genera in maniera casuale e indipendente due grandi numeri primi  $p$  e  $q$  e ne calcola il prodotto  $n = pq$ . Inoltre sceglie un intero  $e$  tale che:

$$1 < e < \varphi(n) = (p-1)(q-1), \quad MCD(e, (p-1)(q-1)) = 1.$$

Si osservi che  $e$  sarà sempre dispari dato che  $p-1$  è pari. Infine Bob calcola un intero  $d$  tale che

$$1 < d < (p-1)(q-1), \quad de \equiv 1 \pmod{(p-1)(q-1)}.$$

Tale intero esisterà senz'altro dato che  $MCD(e, (p-1)(q-1)) = 1$ . La chiave pubblica è la coppia  $(n, e)$  e la chiave privata è  $d$ . Il numero  $n$  è chiamato modulo RSA,  $e$  è chiamato l'esponente di cifratura, e  $d$  è chiamato l'esponente di decifrazione. Si noti che la chiave segreta  $d$  può essere calcolata da  $e$  se si conoscono i fattori primi  $p$  e  $q$  di  $n$ . Quindi se un crittanalista riesce a trovare la fattorizzazione di  $n$ , può facilmente ricavare la chiave segreta  $d$ .

### 2.11.2 Cifratura

Lo spazio dei testi in chiaro è costituito da tutti gli interi  $m$  tali che  $0 \leq m < n$ . Un testo in chiaro è cifrato calcolando

$$c = m^e \pmod{n}.$$

Il testo cifrato  $c$  può essere ottenuto da chiunque sia a conoscenza della chiave pubblica  $(n, e)$ .

### 2.11.3 Decifrazione

La decifrazione si basa sul seguente:

**Teorema 2.11.1.** *Sia  $(n, e)$  la chiave pubblica di RSA e  $d$  la corrispondente chiave privata. Allora*

$$(m^e)^d \pmod{n} = m$$

per ogni intero  $m$  tale che  $0 \leq m < n$  e  $MCD(m, n) = 1$ .

**Dimostrazione 2.11.2.**

$$(m^e)^d \pmod n = m^{ed} \pmod n$$

Inoltre per ipotesi

$$ed \equiv 1 \pmod{\varphi(n)},$$

cioè  $(ed - 1)$  è un multiplo di  $\varphi(n)$ , quindi possiamo scrivere  $ed = 1 + k\varphi(n)$  per un certo  $k$ . Quindi

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot (m^{\varphi(n)})^k.$$

Dato che  $MCD(m, n) = 1$  per il teorema di Eulero vale

$$m^{\varphi(n)} \equiv 1 \pmod n,$$

da cui

$$(m^e)^d \pmod n = m^{ed} \pmod n \equiv m. \quad \#$$

Quindi il testo in chiaro può essere ricostruito così:  $m = c^d \pmod n$ . Questo mostra anche che RSA è un crittosistema: per ogni funzione di cifratura esiste una funzione di decifrazione.

**2.11.4 Sicurezza della chiave segreta**

Abbiamo affermato che RSA è un sistema a chiave pubblica; ciò è vero solamente se non è possibile calcolare la chiave segreta da quella pubblica. Si dimostra matematicamente che questa operazione è difficile esattamente quanto quella di calcolare i fattori primi  $p$  e  $q$  di  $n$ . Non ci sono prove che questo problema sia computazionalmente difficile, ma in centinaia di anni sono stati effettuati numerosi tentativi che non hanno trovato alcun algoritmo efficiente, o polinomiale, cioè capace di trovare le soluzioni in un tempo che cresca rapidamente come un polinomio  $x^n$  e non un esponenziale  $a^x$ .

Un vantaggio nel basare la sicurezza di un crittosistema su un problema matematico è che molti matematici vi lavorano in tutto il mondo per diversi motivi, anche non correlati alla crittografia, e quindi significativi progressi



nella risoluzione del problema sarebbero difficili da mantenere segreti. Affinché la fattorizzazione di  $n$  sia infattibile  $p$  e  $q$  devono essere circa della stessa lunghezza (oggi si parla di numeri con oltre 150 cifre). La chiave  $e$  viene generalmente scelta piccola, in modo che l'algoritmo di cifratura sia efficiente; non possiamo però utilizzare  $e = 2$  perché  $\varphi(n) = (p-1)(q-1)$  è pari e deve essere  $MCD(e, (p-1)(q-1)) = 1$ . Nemmeno  $e = 3$  è consigliabile, dato che esiste un tipo di attacco che può essere effettuato quando  $e$  assume questo valore.

## 2.12 Crittografia quantistica

La nuova frontiera è la crittografia quantistica, basata su alcune idee della meccanica quantistica. Questa disciplina permette, almeno teoricamente, la creazione di un computer quantistico in grado di effettuare in tempo polinomiale calcoli svolti da un computer classico in tempo esponenziale, rendendo vulnerabile ogni attuale sistema crittografico. Bisogna notare però come le stesse idee su cui poggia il concetto di computer quantistico suggeriscano la via per realizzare sistemi crittografici quantistici assolutamente inattaccabili, persino da un computer quantistico, in grado addirittura di scoprire se eventuali intercettatori hanno anche solo tentato di intromettersi in una comunicazione riservata.

Cerchiamo di capire in dettaglio in cosa consistono queste idee.

### 2.12.1 Esperimento di Young e principio di indeterminazione di Heisenberg

Le leggi della fisica deterministiche valide per la spiegazione dei fenomeni macroscopici non sembrano potersi applicare con successo ai fenomeni microscopici. Proprio per questo i fisici hanno concepito modi completamente nuovi e contrari alla naturale intuizione, di guardare ai fenomeni che riguardano il mondo subatomico, costruendo inoltre modelli matematici spesso

assai raffinati.

Partiamo da questo classico problema: determinare il moto di un punto una volta nota la sua posizione iniziale. Sappiamo che il sistema delle equazioni del moto ha una ed una sola soluzione che verifichi le condizioni iniziali. Ciò significa che il moto di una particella, e dunque in particolare la sua posizione e velocità in ogni istante, sono completamente determinati dalle informazioni che abbiamo sulla particella in un dato istante.

Come si accennava prima, questo modello non funziona per sistemi molto piccoli, ad esempio per le particelle elementari, governate invece da leggi di tipo probabilistico. Questo è l'oggetto della fisica quantistica.

Ma come è nata questa teoria? Quali domande hanno aperto questa nuova strada? Nel XVIII secolo era in corso un dibattito sul fatto che la luce fosse un fenomeno particellare o ondulatorio: alcuni ritenevano fosse composta da particelle, dette fotoni, che viaggiano nello spazio e colpiscono gli oggetti illuminandoli; secondo altri la luce era invece trasportata da onde che si propagano in qualche modo nello spazio.

La moderna teoria quantistica afferma che sono validi entrambi i punti di vista: la luce si compone di singole particelle che hanno però anche un comportamento ondulatorio. Il fatto che noi la percepiamo come un fenomeno ondulatorio o particellare dipende dalle circostanze. Tale ambiguità è detta dualità onda-particella. Non è però l'unica stranezza nel mondo subatomico: infatti per sistemi molto piccoli è valido anche il principio di indeterminazione di Heisenberg, il quale afferma che vi sono coppie di proprietà osservabili di un sistema fisico microscopico, come la posizione e la velocità o l'energia e il tempo, che non si possono determinare o misurare in modo esatto nello stesso istante. Quindi la misurazione di una delle due proprietà altera irrimediabilmente l'altra. Ciò non dipende da scarse capacità dei nostri sistemi di misurazione, ma è un'obiettivo impossibile.

Tornando al dibattito sulla natura della luce, la svolta avvenne nel 1801 quando, attraverso un esperimento, Thomas Young riuscì a dare una convincente evidenza del carattere ondulatorio della luce. L'idea gli venne osservando

due cigni che nuotavano in un laghetto uno affiancato all'altro. Lo scienziato britannico notò che i semicerchi di onde generati dai movimenti dei cigni interferivano: dove si incontravano due creste d'onda, si formava una cresta più alta di ciascuna delle due, dove si incontravano due avvallamenti, si formava un avvallamento più basso, e dove si incontravano una cresta ed un avvallamento, essi si cancellavano a vicenda.

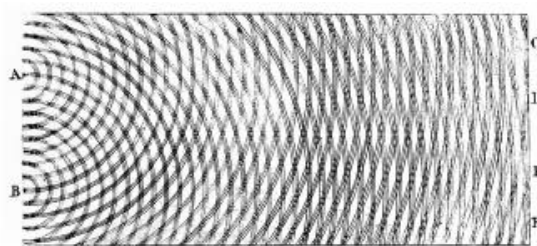


Figura 2.1:

Young scoprì che lo stesso avviene effettuando un esperimento ottico in cui i “raggi” di una sorgente luminosa attraversano due fenditure di una parete e finiscono su uno schermo: il disegno su tale schermo è esattamente quello formato dalle onde lasciate dai cigni sul laghetto. Secondo Young questa era la prova definitiva della natura ondulatoria della luce. Tale fenomeno prende il nome di interferenza, proprio perché le onde luminose interferiscono a vicenda fino a creare la figura sullo schermo di arrivo.

In seguito si scoprì che lo stesso risultato si ottiene sparando singoli fotoni in successione contro una parete con due fenditure come nel caso precedente. Come è possibile? Sembra assurdo, dato che non ci dovrebbero essere onde che interferiscono fra loro, ma fotoni da soli. Come fanno dunque ad interferire?

La meccanica quantistica spiega questo fenomeno attraverso la cosiddetta sovrapposizione di stati. Vediamo cosa si intende con questa espressione. Ogni fotone parte da A e arriva sullo schermo B se passa da una delle due fenditure. Noi non sappiamo cosa accada nell'intervallo tra la partenza del fotone da A ed il suo arrivo su B. Il fotone ha uguale probabilità di passare dalla

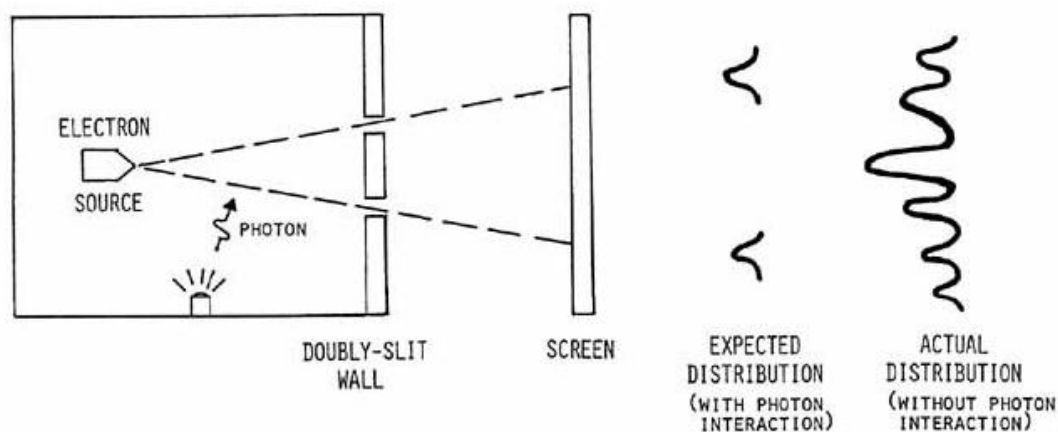


Figura 2.2:

prima o dalla seconda fenditura e possiamo addirittura immaginare che esso passi sia per la prima che per la seconda fenditura, interagendo con se stesso e determinando l'effetto ondulatorio che si presenta nell'esperimento. Ciascuna delle due possibilità (passaggio da una o dall'altra fenditura) si chiama **stato** del fotone. Se supponiamo che, nella fase intermedia del passaggio da A a B, nella quale NON interveniamo con osservazioni, si verificano contemporaneamente i due stati, possiamo parlare di sovrapposizione di stati. Questo risultato può anche essere formalizzato matematicamente. La sovrapposizione di stati è quindi un modo di descrivere un oggetto durante un periodo di ambiguità, nel corso del quale non effettuiamo osservazioni o misure. Se invece decidessimo di effettuare un'osservazione per capire quale sia l'effettivo stato del fotone, allora l'ambiguità cesserebbe e con essa la sovrapposizione degli stati. Questo, in accordo col principio di indeterminazione, modificherebbe irreversibilmente il sistema stesso. Ci aspettiamo pertanto che, modificando l'esperimento di Young in modo tale da misurare per quale delle due fenditure ciascun fotone passa, il risultato dell'esperimento sarebbe diverso. Per quanto possa sembrare sconcertante questo è in effetti ciò che accade.

### 2.12.2 Computer quantistico

Come possiamo sfruttare queste sorprendenti proprietà per inventare un computer quantistico, cioè un calcolatore molto più veloce di quelli classici? Se un computer classico deve esaminare un problema che richiede l'effettuazione di un certo numero di verifiche, esso deve procedere in modo seriale (cioè un'operazione di seguito all'altra). Prendiamo per esempio la fattorizzazione di un numero  $n$ . Il computer procede secondo l'algoritmo del crivello di Eratostene, dividendo  $n$  per tutti i primi minori di  $n$ . Ed è esattamente questa serialità la responsabile della crescita esponenziale del tempo di calcolo. Al contrario un ipotetico computer quantistico può utilizzare il principio di sovrapposizione degli stati per evitare di specificare in modo seriale i numeri da 2 a  $n$ . Esattamente come il fotone dell'esperimento di Young, se non viene osservato, si trova in una situazione di sovrapposizione di stati, l'input del calcolo di questo algoritmo può assumere allo stesso tempo una serie di valori numerici, come fosse una variabile anziché un numero, se non viene disturbato da fattori esterni (cioè se non si controlla che numero è in quel momento effettuando una "misura"). In questo modo il computer quantistico potrebbe riuscire a fattorizzare il numero  $n$  procedendo non in modo seriale, ma effettuando una sola operazione di divisione. Questo evidentemente riduce il tempo di calcolo per il crivello di Eratostene, da esponenziale a polinomiale.

### 2.12.3 Fotoni e polarizzazione

La più piccola unità o quanto di luce è il fotone. Abbiamo visto come in fisica quantistica questo possa essere pensato come una particella o come un ente avente aspetto ondulatorio. In questo caso lo si può immaginare come un minuscolo campo elettromagnetico che si propaga descrivendo una sinusoide contenuta in un piano con un asse di simmetria che si trova sullo stesso piano. La direzione lungo cui il fotone oscilla, ortogonale all'asse di simmetria, prende il nome di polarizzazione del fotone.

La luce è costituita da un enorme numero di fotoni con polarizzazioni diverse; attraverso appositi filtri (polarizzatori) si possono selezionare fotoni con una particolare polarizzazione. Questi filtri non fanno altro che riflettere i fotoni che arrivano con certe polarizzazioni, e quindi con certi angoli di incidenza (direzione) rispetto al filtro, mentre lasciano passare quelli con una determinata polarizzazione.

#### 2.12.4 Protocollo BB84

Riprendendo l'idea dell'esperimento di Young, possiamo supporre che A, la sorgente di fotoni, sia Alice, cioè chi trasmette il messaggio, mentre lo schermo B sia Bob, cioè chi lo riceve. Il messaggio, in assenza di intrusioni consiste in un'immagine descritta dalla seconda curva in figura 1.2. Tuttavia, se vi fosse un intruso che cerca di misurare i fotoni nel loro passaggio attraverso le fenditure, questo altererebbe l'immagine. Il destinatario potrebbe descrivere al mittente una parte dell'immagine ricevuta accorgendosi così dell'intrusione.

La trasmissione delle informazioni avviene attraverso due canali: la prima parte attraverso un canale quantistico, ad esempio una fibra ottica che trasmette fotoni polarizzati, la seconda attraverso un canale non necessariamente sicuro.

##### **Passo 1: comunicare attraverso un canale quantistico.**

Alice, che trasmette, ha a disposizione quattro filtri polarizzatori che le consentono di inviare, attraverso il canale di trasmissione, fotoni aventi le quattro polarizzazioni  $\uparrow$ ,  $\rightarrow$ ,  $\nearrow$ ,  $\searrow$ . Alice e Bob avranno preventivamente concordato di attribuire un valore numerico binario ad ogni fotone polarizzato, ad esempio  $\uparrow=1$ ,  $\rightarrow=0$ ,  $\nearrow=1$ ,  $\searrow=0$ . Alice sceglie un numero  $r$  molto più grande della lunghezza della chiave che vuole spedire a Bob. Inoltre sceglie in modo casuale una stringa di filtri polarizzatori e invia a Bob, conservandone traccia, la corrispondente stringa di fotoni polarizzati. In tal modo Alice ha inviato a Bob una successione di  $r$  cifre binarie che dunque

rappresenta il messaggio. Ad esempio

$$\begin{array}{cccccccc} \uparrow & \uparrow & \nearrow & \searrow & \uparrow & \searrow & \uparrow & \rightarrow \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}$$

Naturalmente se Bob si limitasse a ricevere i fotoni così polarizzati, ricavasse il numero inviato da Alice e lo usasse come chiave, non ci sarebbe alcuna garanzia di sicurezza dato che un intruso potrebbe leggere lo stesso numero. Vediamo come deve comportarsi Bob per ottenere con sicurezza la chiave. Ricordiamo che Bob ha a disposizione due tipi di filtri: quello rettilineo (+) e quello diagonale ( $\times$ ), ma non conosce quali siano le polarizzazioni dei fotoni inviatigli da Alice. Egli allora lascia passare i fotoni attraverso i suoi filtri ed in tal modo ne misura la polarizzazione. Attribuisce poi a ciascun fotone polarizzato il suo equivalente numerico. Ad esempio

$$\begin{array}{l} \text{Alice:} \\ \uparrow \quad \uparrow \quad \nearrow \quad \searrow \quad \uparrow \quad \searrow \quad \uparrow \quad \rightarrow \\ \text{Bob:} \\ + \quad \times \quad \times \quad + \quad + \quad \times \quad \times \quad \times \\ \uparrow \quad \searrow \quad \nearrow \quad \uparrow \quad \uparrow \quad \searrow \quad \nearrow \quad \searrow \\ 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \end{array}$$

Notiamo che in questo procedimento Bob può commettere un certo numero di errori. Infatti, se ad esempio interpone il filtro + ad un fotone con polarizzazione diagonale, di certo questo altera la ricezione del relativo fotone. Poiché sia la polarizzazione dei fotoni trasmessi da Alice sia l'interposizione dei filtri di Bob è casuale, c'è da aspettarsi che vi siano errori con probabilità  $\frac{1}{2}$ . Tuttavia non è detto che ciascuno di questi errori produca di conseguenza un errore nel messaggio ricevuto: per ogni errore fatto nell'interporre ai fotoni inviati da Alice un filtro sbagliato, c'è una probabilità su due che la cifra corrispondente sia quella giusta, pur essendo errata la polarizzazione del relativo fotone. In definitiva abbiamo che la probabilità  $P$  di ricezione esatta del messaggio da parte di Bob è

$$P = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}.$$

Il primo addendo corrisponde al caso in cui Bob non sbaglia nella scelta del filtro, il secondo addendo corrisponde invece al caso in cui la scelta del filtro non sia quella giusta. La percentuale di errore di Bob è quindi del 25 % .

Anche se il messaggio è stato trasmesso, Alice e Bob non possono fermarsi qui, a causa della presenza di errori. Il fatto che essi abbiano luogo è cruciale per scoprire eventuali intromissioni, ma alla fine è necessario eliminarli.

### **Passo 2: eliminare gli errori.**

Alice e Bob vogliono ora procedere all'individuazione ed all'eliminazione degli errori. Ciascuno dei due possiede un pezzo di informazione: Alice conosce la stringa delle polarizzazioni dei fotoni inviati, mentre Bob conosce quali filtri ha interposto. Usando dunque un canale insicuro, Bob comunica ad Alice quale tipo di filtro ha usato e Alice comunica quali di questi filtri erano giusti. Dopo questo scambio di informazioni, Alice e Bob cancellano in entrambi i messaggi, inviato e ricevuto, tutte le cifre corrispondenti agli errori commessi da Bob nell'interposizione dei filtri. Nelle rimanenti posizioni Bob non ha commesso alcun errore e dunque, in assenza di intrusioni sul canale quantistico, la relativa parte del messaggio (chiave grezza), sarà la stessa sia per Alice che per Bob. Nell'esempio precedente Bob comunica la stringa

$$+ \times \times + + \times \times \times$$

e Alice gli comunica che solo nei passi 1, 3, 5, 6 della trasmissione Bob ha interposto il tipo giusto di filtro. I due, cancellando dai messaggi le cifre dei posti 2, 4, 7 e 8, corrispondenti agli errori, ne deducono la chiave grezza

$$1110$$

che rimane segreta. Infatti nello scambio delle informazioni sugli errori commessi Bob e Alice non rivelano ad Eva alcuna informazione sulla chiave grezza. Se Eva non è intervenuta sul canale quantistico la conoscenza dei filtri interposti da Bob non le dà comunque alcuna informazione su quali siano i fotoni effettivamente trasmessi.



**Passo 3: verificare la presenza di Eva.**

Ad Alice e Bob non resta altro che appurare se vi sia stato o meno un'intrusione sul canale quantistico da parte di Eva. Se non vi è stata intrusione i due possono utilizzare la chiave grezza come chiave per un cifrario di Vernam. Se invece vi è stata intrusione sono costretti a gettare via la chiave grezza e ricominciare dall'inizio, utilizzando un canale quantistico più sicuro. L'uso da parte di Alice e Bob di fotoni polarizzati in modo rettilineo e diagonale è proprio motivato dalla necessità di rintracciare un'eventuale intrusione. Polarizzazione rettilinea e diagonale sono infatti osservabili canonicamente coniugate che devono soddisfare il principio di indeterminazione di Heisenberg.

Se Eva si intromette sul canale quantistico e vuole leggere il messaggio di Alice deve misurare la polarizzazione dei fotoni trasmessi. Dato che è nelle stesse condizioni di Bob, non può far altro che procedere come lui, il che la obbliga a commettere degli errori nella lettura dei fotoni. In seguito deve sostituirsi ad Alice e trasmettere a Bob il messaggio, che sarà però diverso da quello originario di Alice poiché sono stati commessi errori in lettura (l'osservazione ha causato una modifica del messaggio). Dunque Alice e Bob possono scoprire se c'è stata intrusione confrontando le loro chiavi grezze. Un'eventuale intrusione da parte di Eva ha un impatto sulla probabilità di errore nella ricezione del messaggio da parte di Bob, che era di  $\frac{1}{4}$ . Supponiamo che Eva interferisca con probabilità  $s$ , ossia  $s$  misura la percentuale di fotoni che Eva intercetta (con  $s = 1$  indichiamo il caso in cui interferisce sempre e con  $s = 0$  mai). Dato che le scelte dei filtri di Bob e Eva sono indipendenti fra loro e indipendenti dalla scelta delle polarizzazioni dei fotoni inviati da Alice, si può avere un errore nel messaggio ricevuto da Bob solo se:

- Bob sbaglia (con probabilità  $\frac{1}{4}$ ) senza che Eva intervenga, ossia con probabilità  $1 - s$ ;
- Bob non sbaglia (con probabilità  $\frac{3}{4}$ ) ma Eva interviene (con probabilità  $s$ ) e determina un errore nell'interposizione del filtro il quale causa a

sua volta un errore nel messaggio ricevuto con probabilità  $\frac{1}{2}$ .

In definitiva, la nuova probabilità di errore  $P'$  nella ricezione del messaggio da parte di Bob è data da:

$$P' = \frac{1}{4} \cdot (1 - s) + \frac{3}{4} \cdot \frac{1}{2} \cdot s = \frac{1}{4} + \frac{s}{8}$$

Se Eva interviene sempre, quindi nel caso  $s = 1$  la probabilità di commettere errori passa da  $\frac{1}{4}$  a  $\frac{3}{8}$ . Dovremmo quindi aver capito che in caso di intrusioni da parte di Eva le chiavi di Alice e Bob potrebbero essere diverse. Tale differenza sussiste solo se Eva interviene (il che accade con probabilità  $s$ ). In tal caso Eva commette un errore con probabilità  $\frac{1}{2}$  nell'interposizione del filtro e viene commesso un errore nel messaggio con probabilità  $\frac{1}{2}$ .

In sostanza la probabilità  $P_k$  di differenza tra le due chiavi è  $P_k = \frac{1}{2} \cdot \frac{1}{2} \cdot s = \frac{s}{4}$ . Dato che ogni differenza tra la chiave grezza di Alice e quella di Bob è dovuta alla presenza di Eva, i primi due saranno sicuri della intromissione di Eva se troveranno anche una sola differenza tra le loro chiavi. Essi scelgono dunque un sottoinsieme casuale di  $m$  cifre delle loro chiavi grezze (che potrebbero essere diverse) e confrontano, comunicando su un canale insicuro, tali cifre. Se è intervenuta Eva troveranno circa  $\frac{ms}{4}$  differenze tra le due chiavi.

Prendendo  $m$  molto grande Alice e Bob troveranno probabilmente una differenza fra le chiavi, il che li porterà a concludere che Eva è intervenuta. Al contrario se non trovano alcuna differenza la probabilità che Eva si sia intromessa, ma la sua intromissione non sia stata avvertita, è  $(\frac{1-s}{4})^m$ . Ovviamente scegliendo  $m$  molto grande tale probabilità è molto bassa.

In conclusione se questo test viene superato, Alice e Bob possono usare come chiave per un cifrario di Vernam quello che rimane dopo l'eliminazione dalla chiave grezza delle  $m$  cifre adoperate per il controllo. Se invece trovano differenze tra le due chiavi grezze, e quindi sanno che Eva si è intromessa, devono ricominciare tutto dall'inizio.

## 2.13 Conclusione

Per concludere, RSA utilizzato singolarmente non può più essere considerato efficace, come d'altronde tutti gli altri algoritmi citati: i furbi corrono veloci col pensiero e con i mezzi!! Noi tutti, che siamo in qualche modo utenti (da oggi spero consapevoli), dei meccanismi di crittografia, dobbiamo augurarci che sempre nuovi metodi ed algoritmi ci vengano in soccorso perché anche se non dobbiamo affrontare i Galli o evitare una guerra atomica, abbiamo tutti i nostri segreti.

## 2.14 Aggiunte

### 2.14.1 Cenni sull'ipotesi di Riemann

I numeri primi erano già conosciuti e studiati dagli antichi Greci: il più grande risultato a riguardo va attribuito ad Euclide, che riuscì a dimostrare che i numeri primi sono infiniti. Per secoli i matematici cercarono di trovare una formula che riproducesse tutti i numeri primi, ma senza ottenere risultati soddisfacenti. La svolta nello studio dei numeri primi avvenne quando Gauss, accortosi dell'impossibilità di determinare una successione di numeri primi, decise di affrontare il problema in modo diverso ossia chiedendosi quanti fossero i numeri primi minori di un certo numero dato. In sostanza lui cercò di dare una stima a questo numero. Si accorse che la probabilità di trovare un numero primo minore di  $n$  diminuiva al crescere di  $n$  e propose questa congettura:

*La densità dei numeri primi in un intervallo di lunghezza  $dx$  centrato su  $x$  è circa*

$$\frac{dx}{\ln x}$$

Di conseguenza secondo Gauss la funzione  $\pi(x)$ , che rappresenta il numero di primi minori di  $x$ , sarebbe dell'ordine di grandezza della primitiva di  $\frac{1}{\ln x}$ , funzione non esprimibile in maniera elementare ed indicata con  $\text{Li}(x)$ .

Anche Adrien Marie Legendre propose una stima per tale funzione presumibilmente nei primi anni dell'800: egli osservò sperimentalmente che

$$\frac{\pi(x)}{x} \approx \frac{1}{\ln x}.$$

In seguito Riemann, sfruttando l'affermazione di Eulero sulla funzione  $\zeta$ , cioè

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ primo}} \frac{1}{1 - p^{-s}}.$$

studiò tale funzione  $\zeta(s)$  per una variabile complessa  $s$ . La sua ipotesi, formulata nel 1859, afferma che gli zeri non banali di tale funzione hanno la parte reale uguale ad  $\frac{1}{2}$ . Nel piano complesso di Gauss questi zeri si disporrebbero dunque sulla retta verticale  $x = \frac{1}{2}$ , detta retta critica. Grazie a questo risultato si potrebbe stabilire esattamente la distribuzione probabilistica dei numeri primi, in un certo senso controllata dagli zeri non banali della funzione  $\zeta(s)$ .

### 2.14.2 Strutture algebriche

**Definizione 2.12.** Un'operazione binaria interna su un insieme  $A$  è una funzione

$$f : A \times A \rightarrow A$$

ossia una funzione che ad ogni coppia di elementi di  $A$  ne associa un terzo ancora appartenente ad  $A$ . In generale viene indicata con

$$* : A \times A \rightarrow A$$

$$(a, b) \rightarrow a * b$$

Sappiamo quindi per la definizione precedente che se  $a, b \in A$  allora  $a * b \in A$ .

**Definizione 2.13.** Una struttura algebrica è un insieme con una o più operazioni interne che possiedono determinate proprietà.

**Esempio 2.6.**  $\mathbb{Z}$  con

$$\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

$$(a, b) \rightarrow a + b$$

$$(a, b) \rightarrow a \cdot b$$

dove  $+$  e  $\cdot$  sono le usuali operazioni di addizione e moltiplicazione sui numeri interi.

**Definizione 2.14.**

L'operazione  $*$  è:

- associativa se  $\forall a, b, c \in A \quad (a * b) * c = a * (b * c)$ ;
- commutativa se  $\forall a, b, c \in A \quad a * b = b * a$ .

**Definizione 2.15.**

Un elemento  $e \in A$  è un elemento neutro (o identità) per  $*$  se

$$a * e = e * a = a \quad \forall a \in A.$$

Se esiste un tale elemento esso è unico.

**Definizione 2.16.**

Sia  $*$  un'operazione su  $A$  con elemento neutro  $e$ . L'elemento  $a \in A$  ha inverso se esiste  $a' \in A$  tale che

$$a * a' = a' * a = e.$$

**Definizione 2.17.**

Un gruppo è un insieme con un'operazione binaria interna  $*$  tale che

- sia associativa;
- abbia un elemento neutro;
- ogni elemento abbia inverso.

Nota: non si richiede che l'operazione sia commutativa.

Notazione standard:

$$G \times G \rightarrow G$$

$$(a, b) \rightarrow a * b$$

Se l'operazione è anche commutativa il gruppo si dice commutativo o abeliano.

**Definizione 2.18.**

Un anello commutativo è un insieme  $A$  con due operazioni (che possono essere denominate addizione e moltiplicazione)

$$(a, b) \rightarrow a + b, \quad (a, b) \rightarrow a \cdot b$$

tali che

- entrambe le operazioni siano associative e commutative;
- esistano due elementi  $0_A, 1_A \in A$  tali che  $x + 0_A = 0_A + x = x$  e  $x \cdot 1_A = 1_A \cdot x = x \quad \forall x \in A$ , cioè sono gli elementi neutri per le due operazioni;
- $\forall x \in A$  esista  $x' \in A$  tale che  $x + x' = x' + x = 0_A$ ;
- valga la proprietà distributiva

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in A$$

**Definizione 2.19.**

L'ordine di un gruppo  $A$ , finito o infinito, è il numero di elementi del gruppo.

Inoltre, dato  $a \in A$  ci sono due possibilità:

- gli  $a^k$  sono tutti distinti, cioè se  $a^k = a^l$  allora  $k = l$ ;
- esistono  $k, l$  con  $k \neq l$  tali che  $a^k = a^l$  o equivalentemente esiste  $n > 0$  tale che  $a^n = 1$ .

Nel secondo caso diciamo che  $a$  ha ordine finito; l'ordine di  $a$  è il minimo naturale  $n$  tale che  $a^n = 1$ .

### 2.14.3 Cifrari a blocchi

#### Alfabeti e parole

**Definizione 2.20.**

Si chiama alfabeto l'insieme finito non vuoto  $\Sigma$ . La lunghezza di  $\Sigma$  è il numero dei suoi elementi. Gli elementi sono chiamati simboli o lettere.

**Esempio 2.7.**

$$\Sigma = \{A, B, C, \dots, Z\}$$

ha lunghezza 26;

$$\Sigma = \{0, 1\}$$

ha lunghezza 2.

**Definizione 2.21.**

Una parola o stringa è una sequenza finita di elementi di  $\Sigma$ . La sua lunghezza è il numero delle sue componenti.

#### Permutazioni

Una permutazione è una funzione biunivoca  $f : X \rightarrow X$  da un insieme in se stesso. Sia  $S(X)$  l'insieme delle permutazioni su  $X$ .

**Esempio 2.8.**

- Sia  $X = \{0, 1, 2, 3, 4, 5\}$ , una possibile permutazione è :

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 & 0 \end{pmatrix}$$

che si può scrivere anche come

$$0 \rightarrow 1 \rightarrow 2 \rightarrow 4 \rightarrow 5 \quad \text{e} \quad 3 \rightarrow 3.$$

- Sia  $X = \{0, 1\}$  e sia  $S_2 = S(X)$  l'insieme delle possibili permutazioni dell'insieme  $X$ ; esso avrà solo i due elementi seguenti:

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Notiamo che  $S(X)$  con l'operazione di composizione è un gruppo ed inoltre che se l'insieme  $X$  ha  $n$  elementi, allora  $S(X)$  ha ordine  $n!$ .

### Cifratura a blocchi

Un crittosistema è chiamato algoritmo di cifratura a blocchi (block-cipher) se lo spazio dei testi in chiaro e quello dei testi cifrati sono l'insieme  $\Sigma^n$  di parole di una certa lunghezza  $n$  su un alfabeto  $\Sigma$ .

Vale il seguente

**Teorema 2.14.1.** *Le funzioni di cifratura di un block-cipher sono delle permutazioni.*

## 2.15 Esercizio

<sup>1</sup> Supponiamo di aver intercettato un messaggio cifrato, che inizia nel modo seguente:

*CCDTVTJI...*

Sappiamo che è stato usato:

- il codice lineare (codice di Hill) con blocchi di lunghezza 2 (digrammi);
- l'alfabeto standard di 26 simboli;
- la lingua italiana.

---

<sup>1</sup>Suggerito dal professore Davide Aliffi



Inoltre sappiamo trattarsi di una pagina tratta da un diario. È probabile che le prime due parole del testo in chiaro siano “Caro diario”. Cerchiamo, utilizzando questa informazione, di ricavare la matrice  $A$  del codice. Abbiamo che  $CC$  deve essere la cifratura di  $CA$  e  $DT$  quella di  $RO$ . Passando alla codifica numerica, abbiamo che

$$\begin{pmatrix} 2 \\ 2 \end{pmatrix} \quad \text{cifra} \quad \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

mentre

$$\begin{pmatrix} 3 \\ 19 \end{pmatrix} \quad \text{corrisponde a} \quad \begin{pmatrix} 17 \\ 14 \end{pmatrix}.$$

Sia

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

la matrice del codice. Allora:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

e

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 17 \\ 14 \end{pmatrix} = \begin{pmatrix} 3 \\ 19 \end{pmatrix}$$

(Ricordare che, naturalmente, tutte le operazioni sono modulo 26, e notare che la matrice  $\begin{pmatrix} 2 & 17 \\ 0 & 14 \end{pmatrix}$  non è invertibile).

Da qui si ricavano le quattro equazioni lineari modulari:

$$\begin{cases} 2a_{11} = 2 \\ 2a_{21} = 2 \\ 17a_{11} + 14a_{12} = 3 \\ 17a_{21} + 14a_{22} = 19 \end{cases}$$

La prima ha un'unica soluzione  $a_{11} \equiv 1 \pmod{13}$  e due soluzioni  $\pmod{26}$  :  $a_{11} = 1, a_{11} = 14$ . Anche la seconda ha due soluzioni  $\pmod{26}$  :  $a_{21} =$

1,  $a_{21} = 14$ . Quindi in tutto abbiamo 4 possibilità per i valori da assegnare ad  $a_{11}$  e  $a_{21}$ . Esaminiamo la prima:

$$a_{11} = a_{21} = 1$$

Sostituendo nella terza e quarta equazione si ha:

$$\begin{cases} 14a_{12} = 12 \\ 14a_{22} = 2 \end{cases}$$

Da queste si ricavano 4 soluzioni mod 26:

$$a_{12} = \begin{cases} 12 \\ -1 \end{cases} \quad a_{22} = \begin{cases} 2 \\ 15 \end{cases}$$

A questo punto abbiamo 4 soluzioni possibili per la matrice  $A$  (con  $a_{11} = a_{21} = 1$ ):

$$\begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 12 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 12 \\ 1 & 15 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 1 & 15 \end{pmatrix}$$

Vediamo come la conoscenza di altre coppie di caratteri che si corrispondono permette di eliminare l'ambiguità. La successiva coppia di caratteri nel testo cifrato è  $VT$ , che dovrebbe corrispondere a  $DI$ . In forma numerica

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 23 \\ 8 \end{pmatrix} = \begin{pmatrix} 21 \\ 19 \end{pmatrix}.$$

Tutte e quattro le matrici soddisfano questa relazione, perciò proviamo ancora con la coppia successiva  $JI$ , che proviene da  $AR$ :

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 0 \\ 17 \end{pmatrix} = \begin{pmatrix} 9 \\ 8 \end{pmatrix}.$$

Questa volta siamo più fortunati: solo la prima matrice  $\begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$  soddisfa questa condizione e quindi è la candidata più attendibile ad essere la condizione cercata. Restano poi da controllare le altre 12 matrici che si ottengono prendendo gli altri valori possibili per  $a_{11}, a_{12}$ .

## 2.16 Glossario

- crittografia = s.f. (pl: crittografie) lo studio delle tecniche per cifrare o codificare un messaggio; scrittura segreta  
inglese: cryptography  
francese: cryptographie  
tedesco: Kryptographie
- crittoanalisi = s.f. (pl: crittanalisi) lo studio delle tecniche per decifrare crittogrammi; la decifrazione di un crittogramma.  
inglese: cryptanalysis  
francese: cryptanalyse  
francese: Kryptoanalyse
- crittogramma = s.m. (pl: crittogrammi) un messaggio cifrato o in codice, preparato per essere letto solo dal destinatario; un gioco enigmistico che richiede di trovare il contenuto di un breve testo, che è stato cifrato, normalmente con la semplice sostituzione di una lettera con un'altra lettera, o con l'uso di numeri ognuno dei quali indica una lettera.  
inglese: cryptogram  
francese: cryptogramme  
tedesco: Kryptogramm
- Algoritmo= s.m. (pl: algoritmi) un elenco finito di istruzioni univocamente interpretabili, ciascuna delle quali deve essere precisamente definita e la cui esecuzione si arresta per fornire i risultati di una classe di problemi per ogni valore dei dati di ingresso. Nel Medioevo con il termine *algorismus* si indicava il complesso di operazioni nel calcolo numerico con numeri arabi. Oggi con il termine algoritmo si indica la sequenza finita di passi effettuabili per risolvere una classe di problemi in un tempo finito;  
un metodo per la soluzione di un problema adatto ad essere implementato sotto forma di programma, procedimento che consente di ottenere

un risultato atteso eseguendo, in un determinato ordine, un insieme di passi semplici corrispondenti ad azioni scelte solitamente da un insieme finito;

sequenza logica di istruzioni elementari (univocamente interpretabili) che, eseguite in un ordine stabilito, permettono la soluzione di un problema in un numero finito di passi

- Altri vocaboli in lingua inglese:

encryption: cifratura

decryption: decifrazione

ciphertext: testo cifrato

plaintext: testo in chiaro

cipher: cifrario

# Capitolo 3

## Diario di bordo

*Non è la conoscenza, ma l'atto di imparare;  
non il possesso ma l'atto di arrivarci,  
che dà la gioia maggiore.*  
(Carl Friedrich Gauss)

Nelle prossime pagine, descriverò il più fedelmente possibile le attività svolte durante le ore in classe, rimandando ogni commento ed analisi al prossimo capitolo. L'intento, ora che i contenuti del progetto sono stati esposti, è quello di rendere chiaro e comprensibile il metodo attraverso il quale le lezioni sono state condotte.

### 3.1 Prima lezione (due ore)

La professoressa mi ha presentato alla classe, dopodichè ho preso la parola, ho spiegato che il progetto era di durata complessiva intorno alle 10 ore e che ci sarebbe stata una verifica finale di cui la professoressa avrebbe tenuto conto. Quindi ho iniziato la lezione con un problema utile ad attirare l'attenzione e a rompere il ghiaccio: nella prima slide compariva scritto in alto  $10^{100000}$ . I ragazzi hanno fatto qualche supposizione su cosa potesse

significare: era semplicemente un numero? o forse era un numero scritto in codice binario? Poco dopo un ragazzo ha detto: “Ma non è il titolo di un libro?”.

Ho dunque fatto notare ai ragazzi che il linguaggio non è altro che una convenzione e che, se ci fossimo messi d'accordo prima sul linguaggio da utilizzare, avrebbero compreso senza problemi anche le altre frasi (apparentemente prive di significato) che vedevano comparire sullo schermo. Ciò che ha colto il loro interesse è stato principalmente l'aspetto ludico della questione, come alcuni giochi di enigmistica quali la crittografia a frase, la crittografia mnemonica od i ditloidi che ho mostrato loro subito dopo.

Dopo questo breve incipit ho iniziato un excursus storico sulla crittografia e, partendo dalle origini di tale disciplina, ho fornito qualche esempio di crittosistema classico, proseguendo con lo sviluppo delle tecniche crittografiche durante la seconda guerra mondiale e arrivando fino ai giorni nostri. Quindi ho generalizzato il concetto di comunicazione “nascosta” in uno schema e l'ho formalizzato secondo la notazione standard della crittografia.

Per illustrare la crittografia a chiave pubblica ed alleggerire un po' la lezione ho proposto ai ragazzi un gioco: ho chiamato due volontari ed ho consegnato a uno di loro una scatola, un lucchetto e la relativa chiave, mentre all'altro alcuni bigliettini che contenevano brevi frasi. Il compito che ho assegnato era quello di fare in modo che un biglietto venisse mandato da un ragazzo all'altro senza che nessuno potesse intercettarlo e leggerlo. In breve tempo i ragazzi hanno capito che bisognava mandare la scatola vuota con il lucchetto aperto a chi possedeva il biglietto. Così facendo si poteva inserire il biglietto nella scatola, chiuderla con il lucchetto e rimandarla indietro, sapendo che chi la riceveva possedeva la chiave ed era così in grado di aprire la scatola e leggere il biglietto.

La seconda sfida consisteva nell'effettuare nuovamente lo scambio di un messaggio, ma avendo a disposizione due lucchetti con chiavi differenti. Questo problema ha richiesto un po' più di tempo e qualche suggerimento, ma alla fine è stato risolto e compreso da tutta la classe. Quindi la scatola e i luc-

chetti sono stati fatti girare in modo che tutti potessero sperimentare quello che i due volontari avevano fatto precedentemente e porre domande su quanto non era risultato chiaro. Approfittando della breve pausa ho fatto girare alcuni libri di crittografia e di matematica divulgativa per dare ai ragazzi dei riferimenti in caso avessero voluto approfondire alcuni aspetti del progetto. Ripresa la lezione ho fatto un breve ripasso di quanto detto fino a quel momento ed ho iniziato la seconda parte del progetto, spiegando in cosa consistesse la divisibilità, esponendo alcune proprietà fondamentali e dando la definizione di MCD. Infine ho introdotto l'algoritmo di Euclide per il calcolo dell'MCD (che già avevano studiato negli anni precedenti) e l'identità di Bézout per scrivere l'MCD come combinazione lineare dei due numeri di partenza.

## 3.2 Seconda lezione (un'ora)

Ho iniziato con ripassi e richiami sulla lezione precedente, poi ho introdotto le equazioni lineari diofantee viste come applicazioni dell'identità di Bézout. Dopo la dimostrazione dell'esistenza di soluzioni intere dell'equazioni diofantee, ho letto il problema della tomba di Diofanto, sottolineando come grazie ai suoi studi abbia avuto inizio il passaggio dalla descrizione di problemi ed equazioni tramite le parole all'utilizzo dei simboli.

Nella seconda parte della lezione ho affrontato l'argomento dei numeri primi, partendo dall'idea dei Greci di dividere un determinato numero di sassi in più file in modo da formare rettangoli. Ho chiesto ai ragazzi se secondo loro fosse sempre possibile effettuare una tale operazione. Ho potuto dare così la definizione di numero primo, fare qualche considerazione ed enunciarne alcuni elementi caratteristici.

In seguito abbiamo letto insieme la prima pagina dell'articolo di Odifreddi (vedi Appendice D) per mostrare come l'argomento sia di grande attualità (pur avendo origini molto antiche) e possa essere considerato alla base di numerose teorie matematiche moderne. Infine ho esposto ai ragazzi i primi

dubbi sui numeri primi: che rapporto sussiste fra un qualunque numero e i numeri primi? (teorema fondamentale dell'aritmetica e sua dimostrazione per induzione); quanti sono i numeri primi? Questa domanda ha provocato un intenso dibattito: era evidente che si diradavano andando avanti a contare, ma non era chiaro se fossero finiti o infiniti. La dimostrazione della loro infinitezza è stata affrontata insieme, per la maggior parte dai ragazzi, che hanno avuto le idee fondamentali per procedere nel ragionamento, dimostrando di possedere una buona logica e creatività matematica. Infine ho esposto la congettura di Goldbach, per mostrare come vi siano enunciati matematici di estrema semplicità ma ancora irrisolti.

### 3.3 Terza lezione (un'ora)

Dopo un breve ripasso della lezione precedente ho continuato ad esporre ai ragazzi dubbi sui numeri primi: esistono infiniti primi gemelli? E quante sono le terne di numeri primi (consecutivi)? Come si può fare a trovare una successione di lunghezza arbitraria di numeri consecutivi non primi? Evidenziando come fosse difficile trovare un metodo per determinare il numero primo successivo ad altri dati, ho illustrato il cambiamento concettuale proposto da Gauss nello studio dei numeri primi. Ho potuto così introdurre l'idea della congettura di Riemann, sottolineando come un problema aperto già da molti anni non sia ancora stato risolto. Rimanendo in tema di problemi irrisolti ho enunciato il teorema di Fermat ed ho spiegato ai ragazzi come in un certo senso anche questo problema sia ancora aperto: sebbene sia stata fornita una dimostrazione, questa non può di certo essere la semplice e bella dimostrazione di cui Fermat parlava nei suoi appunti (sempre ammesso che la possedesse veramente). In questa slide ho anche mostrato come in alcune puntate dei Simpson<sup>1</sup> compaiano finti controesempi al teorema di Fermat ed enunciati di altri problemi irrisolti come  $P = NP$ , che avevo precedente-

---

<sup>1</sup>popolare sitcom animata creata dal fumettista statunitense Matt Groening alla fine degli anni Ottanta per la Fox Broadcasting Company



mente analizzato coi ragazzi nell'ambito della crittografia a chiave pubblica. Tutto questo per mostrare ai ragazzi quanto spesso compaia la matematica intorno a noi, utilizzata anche per far sorridere!

Tornando agli strumenti utili alla crittografia ho spiegato cosa fossero i test di primalità analizzandone uno semplice: a partire dall'idea di dividere un numero dato per tutti quelli inferiori ad esso, diminuire il numero di operazioni notando come fosse sufficiente dividerlo per i numeri primi minori della radice del numero dato. Per quanto riguarda invece gli algoritmi di fattorizzazione, oltre a quello banale da loro già conosciuto, abbiamo studiato la fattorizzazione alla Fermat, dimostrandola e facendo alcuni esempi per chiarirne il funzionamento.

Per terminare la lezione ho letto ad alta voce alcuni brani tratti da "*L'Enigma dei numeri primi*" di Marcus Du Sautoy [2] per tentare di far capire ai ragazzi l'importanza delle dimostrazioni in matematica ed il ruolo chiave dei problemi irrisolti nel motivare la ricerca.

### 3.4 Quarta lezione (due ore)

Dopo qualche breve richiamo alla lezione precedente ho introdotto l'aritmetica modulare a partire dalla lettura dell'orologio, passando così dall'idea alla formalizzazione. Abbiamo poi analizzato orologi con un numero diverso di ore. Dalla definizione matematica di congruenza modulo  $m$  siamo passati al concetto di classi di congruenza, vedendo quali siano le operazioni che si possono eseguire fra questi numeri e le somiglianze o le differenze con i numeri naturali e razionali con cui si è soliti operare.

Come esempio di applicazione di questa "nuova matematica", ho mostrato loro la formula per risalire a quale giorno della settimana corrispondesse una determinata data. Naturalmente questo argomento li ha incuriositi molto: alcuni hanno tentato di ricavare il proprio giorno di nascita.

Infine ho dimostrato, attraverso le congruenze lineari e le equazioni lineari diofantee, che l'inverso di una classe di resto modulo  $m$  esiste solo sotto certe

condizioni.

Nella seconda ora ho diviso i ragazzi in tre gruppi ed ho fatto svolgere una gara di esercizi e problemi (vedi Appendice C), in modo da ripassare le cose già viste a lezione, comprenderle meglio e impararne di nuove attraverso la discussione ed il ragionamento in gruppo. Sembra che i ragazzi abbiano apprezzato e, dato che i risultati sono stati buoni, li ho ricompensati nella lezione successiva, dichiarando il vincitore e dando premi differenti a seconda dei meriti ottenuti.

### 3.5 Quinta lezione (un'ora)

Ho ripreso l'argomento della lezione precedente, aggiungendo qualche dettaglio ed effettuando qualche chiarimento, quindi ho dato la definizione di funzione  $\varphi$  di Eulero, ho fatto qualche esempio e spiegato cosa si intende dicendo che è moltiplicativa, proprietà che ci sarebbe tornata utile in seguito. Con tutti gli strumenti matematici introdotti ho potuto fare ritorno alla crittografia: per dare un esempio di come potessero essere utilizzate le tecniche matematiche studiate, ho formalizzato uno dei cifrari classici affrontato nella prima parte del corso, il cifrario di Cesare.

Dopo questa breve premessa sono passato al punto che sembrava interessare maggiormente i ragazzi: quale fosse il nesso fra la crittografia e la matematica. Questo nesso è rappresentato proprio dal crittosistema RSA. Dopo un veloce ripasso della crittografia a chiave pubblica ho spiegato il funzionamento di RSA: generazione delle chiavi, cifratura e decifrazione. Ho suggerito come il punto cruciale di RSA, cioè la fattorizzazione di numeri molto grandi, o il calcolo della loro  $\varphi$  di Eulero, fosse un esempio di problema *NP*. A fine lezione ho fatto un esempio di cifratura con RSA.

## 3.6 Sesta lezione (due ore)

Dato che RSA rivestiva un ruolo molto importante all'interno del progetto, e che avevo capito che non tutti erano riusciti a seguire la lezione precedente, ho ritenuto fosse il caso di ripeterlo dall'inizio, soffermandomi maggiormente sui passaggi cruciali, fornendo esempi completi e procedendo con maggior lentezza. Infine ho dimostrato il teorema necessario al funzionamento della decifrazione, facendo uso (senza dimostrarlo) del teorema di Eulero e ribadendo il forte legame fra matematica e crittografia.

Nell'ultima ora ho pensato di fornire ai ragazzi alcune conoscenze di crittografia quantistica, in modo che sapessero in che direzione si sta muovendo oggi la crittografia. Per prima cosa ho dato alcune basi di meccanica quantistica, incominciando dalla differenza fra il determinismo del mondo macroscopico e il probabilismo di quello microscopico: ho lasciato cadere un pallone mentre i ragazzi guardavano, poi ho detto a tutti di chiudere gli occhi ed ho ripetuto la stessa azione spiegando come stavo agendo. A questo punto ho chiesto loro cosa fosse accaduto alla palla mentre non vedevano, per far comprendere come l'atto di osservazione non modificasse il comportamento della palla.

Dopo qualche cenno sulla composizione dell'atomo e sul principio di indeterminazione di Heisenberg (entrambi già noti) abbiamo guardato un breve discorso di Odifreddi<sup>2</sup> in cui analizzava il dibattito fra Newton e Huygens sulla natura della luce. Partendo da questo presupposto ho spiegato brevemente in cosa consistesse l'esperimento di Young, per poi mostrare ai ragazzi un video che illustrava in dettaglio tale esperimento e quello della doppia fenditura realizzato con i singoli fotoni (Dr. Quantum Double-slit experiment<sup>3</sup>). Per completezza ho esposto anche il punto di vista di Schroedinger (esperimento mentale del gatto vivo e morto), ribadendo il concetto di sovrapposizione di stati.

---

<sup>2</sup>Piergiorgio Odifreddi racconta *Isaac Newton. La gravità la luce e i colori del mondo* della collana Beautiful Minds

<sup>3</sup>video realizzato da Fred Alan Wolf, fisico teorico e scrittore

A questo punto ho dato un'idea di cosa fosse, in linea teorica, un computer quantistico e di quali sorprendenti capacità potesse avere, ad esempio in relazione al problema della fattorizzazione di un numero.

Come nozioni utili alla comprensione del protocollo di crittografia quantistica, ho ricordato cosa fossero i fotoni, come fosse definita la loro polarizzazione e in che modo si potessero selezionare determinate polarizzazioni scartandone altre attraverso appositi filtri polarizzatori.

Nella parte finale della lezione ho esposto brevemente il protocollo di crittografia quantistica di Bennet-Brassard, dato che il tempo rimanente non permetteva altro che alcuni cenni a tale tema.

### 3.7 Verifica

Esattamente una settimana dopo l'ultima lezione ho fatto svolgere ai ragazzi il compito in classe (vedi Appendice B) strutturato in questo modo:

- 5 domande di crittografia teorica (storia, funzionamento generale, ecc...);
- 8 domande relative alla divisibilità ed ai numeri primi;
- 5 domande riguardanti l'aritmetica modulare;
- 2 domande su RSA;
- 1 domanda facoltativa sulla crittografia quantistica.

Ho consegnato ai ragazzi due verifiche (vedi Appendice B) diverse per poter effettuare più domande, il che mi avrebbe permesso di coprire più argomenti e verificare effettivamente la loro comprensione. Ho dato loro un tempo approssimativo di un'ora e mezza e per tutto il periodo della prova sono rimasto in aula a controllare che non comunicassero fra loro ed a rispondere ai loro quesiti relativi alle domande poste.

# Capitolo 4

## Analisi e commento

*... ch  non fa scienza,  
sanza lo ritenere,  
avere inteso.*  
(Dante Alighieri)

Nello svolgimento del progetto e successivamente nell'analisi dei risultati, si   tenuto conto di alcuni elementi imprescindibili in ogni ambito didattico quali: gli ostacoli epistemologici, il contratto didattico, le situazioni didattiche ed a-didattiche. Con queste premesse, nel seguente capitolo, illustrer  le riflessioni ed i commenti derivati da quest'esperienza, nonch  i risultati del questionario di valutazione delle lezioni consegnato ai ragazzi l'ultimo giorno.

### 4.1 Impressioni generali

Riporto il profilo della classe espresso dalla professoressa:

“La classe   formata da 19 alunni corretti, educati ed abbastanza uniti. Un discreto gruppo partecipa alle lezioni in modo attivo, manifestando interesse per la materia e voglia di apprendere, mentre gli altri seguono con un'attenzione pi  scolastica. Infine c'  sempre qualche studente che necessita di tempi di apprendimento pi  lunghi, talvolta per disimpegno, e deve essere

seguito e guidato nei percorsi logici.”

Durante lo svolgimento del mio progetto mi sono trovato abbastanza d'accordo col parere espresso dalla professoressa. Mi sono sembrati fondamentalmente svegli, vivaci e, anche se non sempre si sono dimostrati partecipi ed interessati (con alcuni cali di attenzione e concentrazione), nel complesso si può affermare che la loro partecipazione attiva durante le lezioni sia stata significativa. Molti ragazzi hanno mostrato un grande interesse nel tentare di dimostrare enunciati posti loro come problemi (ad esempio il fatto che i numeri primi sono infiniti), evidenziando grande propensione al dibattito. Il nesso tra crittografia e matematica, alla base stessa del progetto, ha suscitato in loro grande curiosità spingendoli talvolta a rivalutare alcuni preconcetti verso l'ostica materia solitamente vista come esclusivamente teorica.

L'atmosfera creata in classe sin dal primo giorno era positiva e distesa, tutti potevano esprimersi liberamente, fare ipotesi, domande e interagire in tranquillità durante il corso di tutto il progetto.

La risposta ai lavori di gruppo è stata molto positiva, configurandosi anch'essa come novità rispetto alle attività scolastiche standard.

## 4.2 Analisi didattica

Veniamo ora all'analisi delle componenti prettamente didattiche del progetto da me portato in aula. Il primo e fondamentale tema da trattare è quello del contratto didattico, ovvero:

“In una situazione d'insegnamento, preparata e realizzata da un insegnante, l'allievo ha generalmente come compito di risolvere il problema matematico che gli è presentato, ma l'accesso a questo compito si fa attraverso un'interpretazione delle domande poste, delle informazioni fornite, degli obblighi imposti che sono costanti del modo di insegnare del maestro. Queste abitudini (specifiche) del maestro attese dall'allievo ed i comportamenti dell'allievo

attesi dal docente costituiscono il contratto didattico” [3].

Nel mio caso, non essendo il professore di matematica titolare, ma una persona nuova per gli studenti, ritengo che la questione sia differente. Come spiega D’Amore:

“Quando si parla di contratto didattico, in realtà, si deve parlare anche di una situazione classe, di un particolare argomento matematico, oggetto del contratto; insomma di una interazione tra allievo, insegnante e, appunto, oggetto del sapere. Ma quando un ricercatore fa ricerca in aula, di fatto si ha una sostanziale modifica di tutto l’apparato. Chi assicura che le risposte degli allievi siano ancora da considerarsi il frutto di clausole del contratto didattico? Dato che sono cambiate le condizioni, è indiscutibile che si tratti di una situazione del tutto diversa. Certo, si tende a supporre che lo studente identifichi comunque il ricercatore con un adulto della ... categoria degli insegnanti, ma ciò non basta. Le risposte degli studenti allo sperimentatore, tanto più se l’oggetto tematico non è standard di classe, sembrano più legate a clausole di un *contratto sperimentale* che non di un contratto didattico, anche se sembra ovvio che vi siano fortissimi legami tra le due cose.” [4]

Più in dettaglio, cito le parole di Schbauer-Leoni:

“La differenziazione tra contratto didattico e contratto sperimentale sta essenzialmente nelle intenzioni e nelle finalità tacite attribuite alla situazione da parte dell’attore che si trova in situazione alta (lo sperimentatore o l’insegnante). Quanto all’allievo, questi avrebbe la tendenza a ricondurre il significato alle regole del contratto didattico del quale ha un’esperienza nel quotidiano e ciò anche se l’adulto che ha di fronte ha precedentemente costruito il suo domandare come rilevante in un contratto sperimentale” [5]

Bisogna infatti tener conto delle difficoltà insite nella nascita di un rapporto

nuovo, con una persona giovane ed estranea alla classe che illustra un argomento non presente nel piano didattico. Il nostro caso è forse ancora più complesso, dato che la presenza della professoressa in aula costituiva un ponte tra me ed i ragazzi, agevolando il rispetto delle regole, ma anche limitando la sperimentazione di un rapporto nuovo.

Il mio scopo, per tutta la durata delle lezioni, è stato quello di allontanarmi il più possibile dalle situazioni scolastiche standard caratterizzate da un certo distacco dagli studenti, ed al contrario invogliare continuamente i ragazzi ad una partecipazione attiva attraverso lavori di gruppo ed interazioni per permettere loro di apprendere attraverso nuove stimolanti relazioni docente-studente. Ritengo che la mia giovane età ed il mio approccio amichevole abbiano agevolato il raggiungimento di tale obiettivo.

Gli unici momenti che si sono configurati come situazioni a-didattiche, mostrandone tutte le positività, sono stati i lavori di gruppo. Infatti, in una situazione a-didattica devono entrare in gioco gli studenti e l'oggetto della conoscenza, ma non l'insegnante. Notoriamente lavorare in gruppo presenta vantaggi e svantaggi peculiari per ogni situazione. Nel nostro caso, dedicare alcuni momenti alla risoluzione di problemi e domande in gruppi da 6/7 ragazzi ha permesso loro di unire conoscenze ed intuizioni in modo produttivo e stimolante.

Mostrare sin dal primo giorno ai ragazzi come sia possibile giocare (ed anche ridere) con la matematica e con le parole è servito sul piano didattico ad illustrare le potenzialità delle convenzioni linguistiche e logiche, e sul piano relazionale all'instaurarsi di un rapporto il più possibile paritetico e disteso. Per quanto riguarda la parte matematica del progetto ci si trova davanti ad alcuni ostacoli epistemologici importanti. L'aritmetica modulare risulta completamente nuova per i ragazzi, potrebbe confonderli e richiedere un lungo periodo affinché avvenga l'interiorizzazione. Diventano dunque necessari ulteriori accorgimenti per rendere questo argomento più interessante e comprensibile. A tale scopo ho pensato di introdurla attraverso gli orologi (prima standard, poi con differenti numeri di ore), fornendo numerosi esempi e mo-



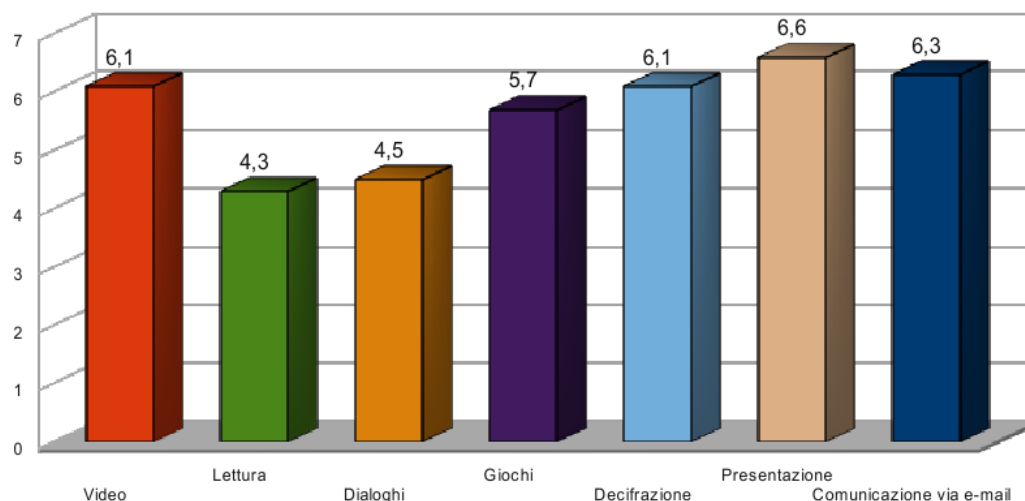
strandando varie rappresentazioni della stessa definizione. Anche in questo caso ritengo sia opportuno far sperimentare loro tali concetti in prima persona. Vorrei inoltre far notare come non solo le conoscenze che gli studenti già possiedono rivestono un ruolo importante nella presentazione delle nuove idee proposte, ma anche il loro modo di ragionare, acquisito nei precedenti anni, li può porre in modi differenti di fronte al progetto che assume per loro un aspetto nuovo.

Infine, tra gli elementi didattici e relazionali che si configurano come novità in questo progetto, vi è la scelta di comunicare con i ragazzi via mail. Si è dimostrata una strategia vincente: sapevano di poter contare su di una risposta veloce e precisa ad ogni dubbio emerso durante i compiti a casa e nessuno ha utilizzato i miei contatti per ragioni che esulassero dal rapporto didattico instauratosi (es. no spam, no domande non inerenti il progetto).

### 4.3 Risultato questionario di valutazione

Al termine di tutte le attività svolte in classe (verifica compresa) ho consegnato ai ragazzi un questionario da me predisposto alla valutazione del mio operato, dei metodi da me scelti e degli argomenti trattati nel corso del progetto. L'idea era quella di permettere ai ragazzi di esprimere un sincero parere su quanto avevano vissuto in quelle poche ore. L'opinione degli studenti è, dal mio punto di vista, fondamentale per comprendere se e cosa si è sbagliato e come eventualmente aggiustare la rotta in futuro. Il questionario, completamente anonimo, era composto da tre sezioni (materiali e strumenti, esposizione e metodo, argomento e prospettiva) che contenevano alcune domande aperte, atte a permettere una libera espressione da parte degli alunni, ed alcune domande chiuse (classiche scale likert da 1 a 7, dove 1=per nulla e 7=del tutto). Per ogni dettaglio vedi Appendice F.

### 4.3.1 Materiali e strumenti



Dai grafici possiamo in primo luogo osservare come tutti gli strumenti utilizzati abbiano ottenuto un punteggio più che positivo, questo a sottolineare come gli studenti apprezzino le novità introdotte nell'insegnamento cogliendone spesso anche l'utilità per il loro apprendimento (tutti i punteggi medi sono superiori a 4 su 7). Inoltre si nota come gli strumenti che prevedono una maggior partecipazione attiva da parte degli studenti siano privilegiati rispetto a quelli che li rendono passivi: ad esempio la lettura dell'articolo riceve il gradimento medio più basso con 4,3 punti su 7. Caso a parte il video (media 6,1 su 7) che come sempre attrae molto i ragazzi.

Particolarmente apprezzato (6,6 su 7 di media) è l'utilizzo combinato di presentazione tramite slides e lavagna per approfondire gli argomenti matematici, sviluppare dimostrazioni, risolvere esercizi e analizzare esempi: la funzionalità incontra l'intrattenimento.

Una tecnica che ha riscosso particolare successo (6,1 su 7 come punteggio medio) è stata quella di non fornire direttamente le dispense cartacee ai ragazzi, ma inviare file contenenti le singole lezioni tramite mail. In aggiunta,

tali file erano stati protetti da password che dovevano essere ricavate dai ragazzi effettuando semplici operazioni crittografiche per risalire al messaggio in chiaro od a quello cifrato conoscendo il crittosistema e la chiave utilizzati. Questo espediente è risultato vincente proprio perchè ha permesso ai ragazzi di esercitarsi su quanto visto in maniera teorica avendo in mente un fine, ossia quello di accedere ad un file che sarebbe stato utile per lo studio successivo. In pratica un buon trucco per incitarli a fare quei semplici esercizi che aiutano la comprensione e che spesso non hanno voglia di eseguire.

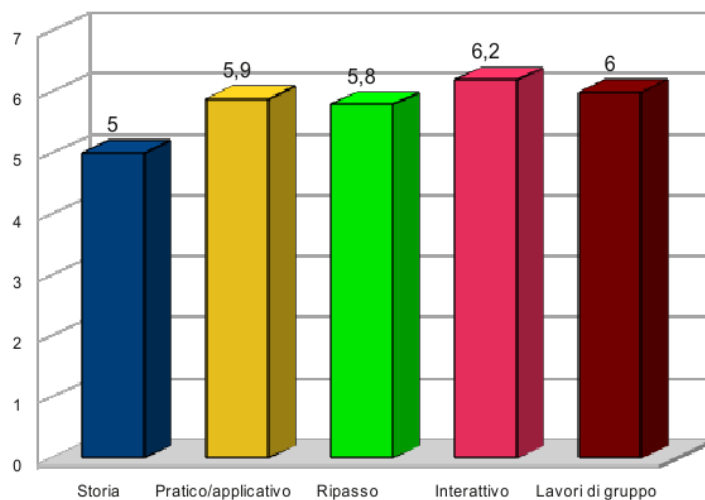
La comunicazione tramite e-mail è risultata molto utile per dialogare in ogni istante, permettendo un rapporto diretto fra studente e docente, diminuendo le distanze relazionali. Tale utilità è stata apprezzata e riconosciuta dai ragazzi che le hanno conferito un punteggio medio di gradimento di 6,3 su 7. Per quanto riguarda i dati ricavati dalle domande cui i ragazzi potevano rispondere liberamente, emerge come quasi tutti (15 su 19) abbiano ritenuto utile per approfondire lo studio il materiale didattico aggiuntivo distribuito a lezione (escluse le dispense), ossia le fotocopie su argomenti specifici ed i dialoghi<sup>1</sup>. Due ragazzi hanno criticato una certa carenza di esemplificazioni pratiche reputando dunque il materiale fornito troppo teorico. Ad ogni modo, le dispense sono state valutate positivamente da tutti gli studenti. Vengono descritte come esaurienti, utili, chiare precise, facili da comprendere, ben strutturate e complete. Anche in questo caso un paio di studenti lamentano la scarsità di esempi.

### 4.3.2 Esposizione e metodo

Per quanto riguarda gli approcci ed i metodi di esposizione l'approccio applicativo (media 5,9 su 7) è risultato più utile ed interessante di quello storico (media 5 su 7), dato probabilmente prevedibile vista la connotazione stessa del progetto: l'attenzione era posta principalmente sulle applicazioni della matematica nella sicurezza della comunicazione, ponendo in secondo piano il punto di vista storico. Ciò nonostante diversi studenti hanno apprezzato vi

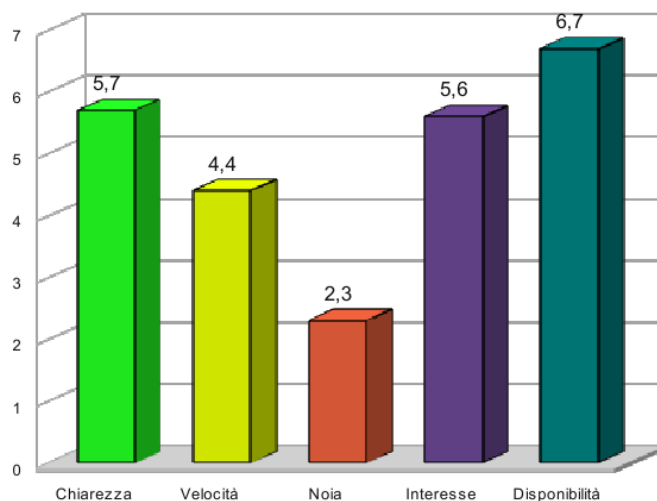
---

<sup>1</sup>Dialoghi scritti da Roberto Zanasi, professore di matematica all'ITI Fermi di Modena



fosse un percorso storico che contestualizzasse i risultati presentati. La storia della matematica permette infatti di affrontare lo studio di determinati argomenti in modo interessante, mostrando agli allievi come la matematica sia una scienza sviluppata dagli esseri umani ed in continua evoluzione.

Alto gradimento hanno avuto i ripassi ad inizio lezione e i lavori di gruppo (media 5,8 su 7), ma va sottolineato come l'approccio interattivo sia quello in assoluto maggiormente gradito da tutti i ragazzi (media 6,2 su 7).

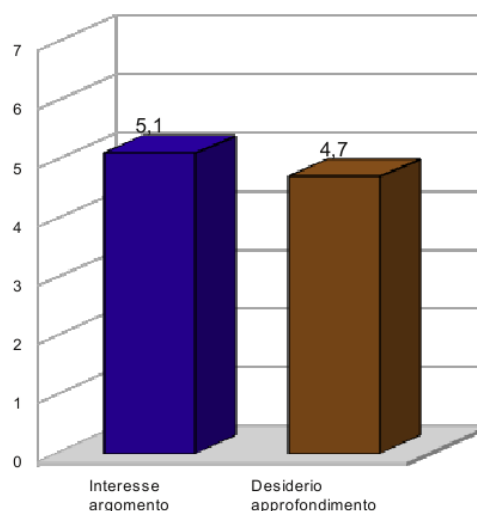


Per quanto riguarda i metodi di esposizione c'è da notare come le lezioni non

siano risultate assolutamente noiose (media 2,3 su 7), ma talvolta eccessivamente veloci (media 4,4 su 7, ma con deviazione standard 1,82). A mio avviso si tratta di trovare un migliore compromesso fra questi due aspetti, dato che rallentare il ritmo non provoca necessariamente un aumento della noia. La rapidità delle lezioni può ovviamente essere regolata a seconda del numero di ore a disposizione, al limite tralasciando alcuni argomenti marginali e non necessari. A tal riguardo cinque ragazzi hanno indicato “*rallentare il ritmo*” come suggerimento per l’esposizione.

Nel complesso le lezioni sono state giudicate chiare (media 5,7 su 7) ed interessanti (media 5,6 su 7). Il mio operato è apparso particolarmente disponibile (media 6,7 su 7).

### 4.3.3 Considerazioni sul progetto



Si può affermare che l’argomento scelto sia riuscito a catturare l’interesse dei ragazzi. Inoltre si può notare come l’interesse dimostrato nei confronti dell’argomento (punteggio medio di 5,1 su 7) sia superiore al desiderio di approfondirlo (4,7 su 7 come punteggio medio)

Gli aspetti più apprezzati sono stati: la cifratura e la decifrazione in generale

(7 studenti), quindi i vari codici e crittosistemi incontrati nella prima parte (5 studenti), la storia della crittografia (2 studenti) e RSA (2 studenti).

Le parti segnalate come meno interessanti e coinvolgenti sono state quelle di matematica teorica (6 studenti), anche se sono state viste come indispensabili in vista delle applicazioni studiate. Bisogna notare come uno studente abbia risposto: *“Mi è piaciuto meno l’aspetto legato alla matematica perchè non sono troppo bravo”*, il che evidenzia ancora una volta come il clima di sfiducia dei ragazzi possa influire notevolmente sulle loro opinioni a riguardo della cultura e della matematica. In relazione a tale questione riporto una frase scritta da un altro ragazzo: *“Le dimostrazioni non sono il mio forte e non sono di mio interesse”*.

Infine, gli studenti hanno indicato i seguenti suggerimenti per un’eventuale evoluzione futura del progetto:

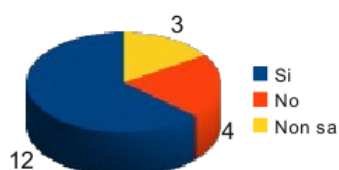
- più spazio alla crittografia ed alla crittanalisi (crittosistemi, esempi, ecc...);
- maggior numero di ore dedicate al progetto, così da avere tempi meno ristretti per ogni argomento;
- meno attenzione alla matematica pura;
- più esercizi da svolgere singolarmente e/o in gruppo;
- più esempi pratici;
- più spazio alla crittografia quantistica.

Se ne evince una preferenza per un approccio concreto e tangibile con più esempi ed applicazioni e meno teoria, anche se questo non è valido per tutti i ragazzi: cinque di loro hanno intuito l’importanza delle dimostrazioni nella comprensione della materia e sono stati fortemente interessati ai ragionamenti logici effettuati durante il progetto nonchè alla, per loro, nuova matematica introdotta.

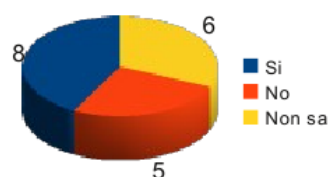
#### 4.3.4 Considerazioni sulla matematica

In queste domande conclusive del questionario, agli studenti veniva chiesto di dire se ed in che modo l'esperienza appena conclusa aveva modificato la loro visione ed il loro approccio alla matematica.

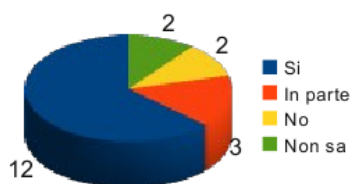
Modifica visione della matematica



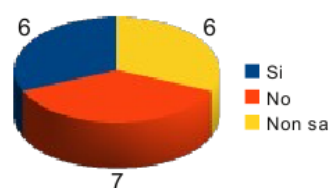
Stimolo riflessione su matematica e cultura



Matematica differente



Opinione sulle dimostrazioni immutata

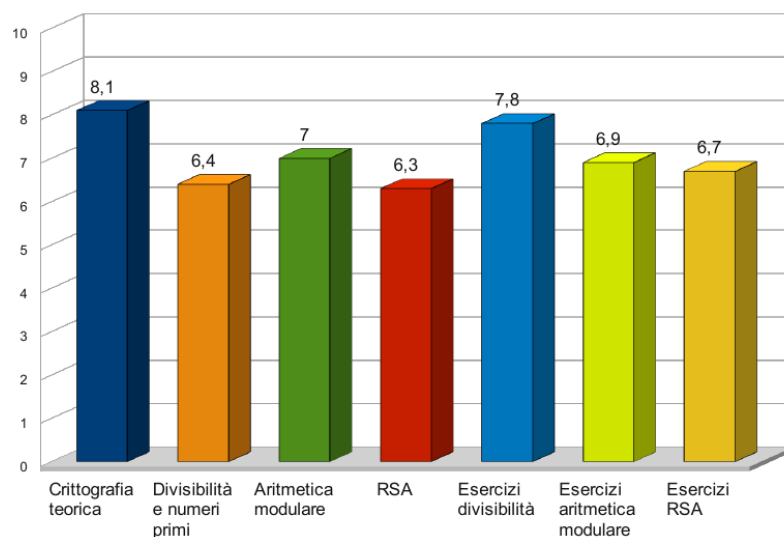


Molti ragazzi (12 su 19) hanno percepito la matematica presente nel percorso come diversa dall'usuale materia presentata in aula (più interessante e stimolante, utile alla società ed applicabile alla vita quotidiana) il che ha portato ad una forte modifica della loro visione della stessa (sempre 12 ragazzi su 19). Per quanto riguarda lo stimolo dato dal progetto alla riflessione su matematica e cultura, la percentuale scende (8 ragazzi su 19). Infine per quanto concerne le impressioni degli studenti sulle dimostrazioni, benchè 1/3 di loro non trovi che il progetto abbia influito sulla propria opinione delle stesse, emerge come quest'approccio abbia condotto ad alcune modifiche importanti: i ragazzi colgono maggiormente l'importanza dell'intuizione, il peso delle dimostrazioni per la comprensione finale di un fenomeno e finiscono per rilevarle più interessanti di quanto non facessero precedentemente. In particolare tre di loro le hanno considerate più semplici ed utili alla comprensione e altri due le descrivono come maggiormente intuitive e che necessitano di

più logica che apprendimento mnemonico.

Per concludere cito alcune delle affermazioni dei ragazzi: “*La matematica non è solo quella materia noiosa ma è anche interessante*”; “*Ho potuto vedere un’applicazione della matematica che, per me, era quasi completamente teorica*”; “*Mi è venuta un po’ più voglia di studiare la matematica*”.

#### 4.4 Risultati verifica



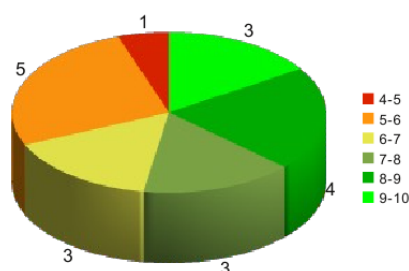
Come si può osservare dai grafici<sup>2</sup> tutte le componenti della verifica sono state risolte dalla maggioranza degli studenti, anche se con percentuali diverse: mentre la crittografia teorica ha dato ottimi risultati (81 % di risposte corrette), RSA (63 %) e la divisibilità (64 %) sono risultati più ostici per i ragazzi.

Inoltre si può notare come gli esercizi forniscano sempre esiti migliori nei confronti delle rispettive domande teoriche. Si può supporre che questo sia

<sup>2</sup>percentuale di risposte corrette; es. il 70 % dei quesiti sull’aritmetica modulare è stato risolto correttamente



dovuto alla concezione che hanno i ragazzi della matematica: essi ritengono spesso che la teoria e gli esercizi non siano necessariamente correlati, prediligendo i secondi che hanno un carattere spesso meno astratto e più chiaro. Riporto infine un grafico che rappresenta il risultato della verifica da parte di tutta la classe:



Se ne evince come circa i tre quarti degli alunni abbiano superato la prova con un risultato più che sufficiente, mentre vi sia stata un'unica insufficienza "grave". I voti fra il 5 ed il 6 sono in maggioranza spostati verso il 6. Analizzando tali dati, la professoressa ed io abbiamo notato come i voti rientrino nella norma per la maggioranza dei ragazzi, mentre per quattro di loro il risultato sia stato sensibilmente migliore rispetto all'andamento scolastico. È possibile che questi studenti abbiano trovato l'argomento di loro interesse e si siano applicati maggiormente nello studio dello stesso.



# Capitolo 5

## Analisi Progetto Lauree Scientifiche

*Lo scienziato non è l'uomo  
che fornisce le vere risposte:  
è quello che pone le vere domande.*  
(Claude Lévi-Strauss)

### 5.1 Introduzione al Progetto Lauree Scientifiche

Il mio progetto aveva come scopo, tra gli altri, anche quello di cambiare la visione della Matematica da parte dei ragazzi, mostrando argomenti diversi atti a cogliere il loro interesse. Questo ha un duplice vantaggio: da una parte permette agli studenti di conoscere meglio alcuni aspetti della materia, dall'altra può indirizzarli al suo studio (anche in vista della scelta universitaria). Per questo motivo mi soffermerò ora ad illustrare ed analizzare un importante progetto a livello nazionale che si prefigge scopi simili.

Tale iniziativa, Progetto Lauree Scientifiche (PLS), è nato nel 2004 con i seguenti obiettivi ([6]):

- incrementare il numero di immatricolati ai Corsi di Laurea afferenti alle classi 21, 25 e 32 (Chimica, Fisica e Matematica), mantenendo un alto standard di qualità degli studenti;
- incrementare il numero di laureati delle Classi 21, 25 e 32 e potenziare il loro inserimento nel mercato del lavoro.

Tale necessità è stata determinata dal sensibile calo di iscritti a questi corsi di laurea negli ultimi anni. Per lo sviluppo dell'Italia è richiesto il rilancio della scienza ed il potenziamento degli investimenti di alta tecnologia. Ottenere questo risultato è possibile grazie ad alcune azioni strategiche quali: stimolare l'interesse dei giovani verso lo studio di queste materie, fornire una preparazione migliore nelle materie scientifiche di base (già a livelli scolastici inferiori), favorire l'inserimento degli studenti migliori nel mercato, potenziando l'interazione fra Università ed Impresa.

Per sviluppare questi punti, in seguito ad un accordo fra MIUR, Confindustria e Conferenza Nazionale dei Presidi delle Facoltà di Scienze e Tecnologie, una commissione nazionale ha selezionato, per il triennio 2005-2007, nove progetti: quattro relativi a "*Orientamento preuniversitario e formazione degli insegnanti (OFI)*", tre relativi a "*Stage in azienda*", uno per "*Borse di studio*" (per neoimmatricolati nelle tre Classi di Laurea precedentemente citate) ed un progetto per la "*Produzione di materiale informativo*" e la realizzazione di un sito web dedicato al PLS (<http://www.progettolaureescientifiche.it>). È stato inoltre ripreso il progetto per il quadriennio 2009-2012 [7].

## 5.2 Considerazioni sul progetto generale

Per quanto riguarda la sezione Matematica, gli obiettivi generali posti dal Progetto Lauree Scientifiche erano di estrema importanza: contribuire a diffondere tra gli studenti una più corretta percezione del ruolo e del valore della matematica e dell'informatica. Più in dettaglio, il progetto *Orientamento preuniversitario e formazione degli insegnanti* aveva come scopi principali ([8],[9]):

1. mostrare agli studenti della scuola secondaria problemi e temi rilevanti della matematica, collegati con altre discipline e con il mondo del lavoro; offrire quindi occasioni efficaci di apprezzare la matematica e di valutarla come scelta di studio e di lavoro, utilizzando soprattutto modalità di laboratorio;
2. alzare in generale il livello delle conoscenze matematiche degli studenti nella scuola, ampliando in particolare la fascia degli studenti con buone capacità e motivazioni, già a cominciare dai primi anni di scuola, anche con azioni mirate a rimuovere atteggiamenti negativi e concezioni errate tra studenti ed insegnanti;
3. fornire agli studenti l'opportunità di valutare la propria formazione (in relazione agli studi universitari);
4. perfezionare le conoscenze disciplinari ed interdisciplinari degli insegnanti, nonché la loro capacità di interessare e motivare gli studenti (anche per favorire lo sviluppo delle vocazioni per la matematica).

Alcune forti motivazioni alla realizzazione del progetto (oltre all'ingente calo di iscritti al Corso di Laurea in Matematica) erano le seguenti ([9]):

- l'immagine della matematica che i ragazzi parevano acquisire dalla scuola superiore sembrava assai negativa: una materia astrusa, arida, lontana dalla vita, poco utile, e poco remunerativa;
- gli insegnanti della scuola superiore non sembravano spesso in grado (né sufficientemente consapevoli della necessità) di dare ai loro studenti adeguate opportunità di conoscere la natura della matematica e che cosa la matematica potesse essere per loro;
- il mancato sviluppo, in molti studenti, di un buon livello di conoscenza della matematica riduceva in generale la propensione verso le discipline scientifiche e tecnologiche.

Il principio alla base del progetto era quello di realizzare azioni nelle quali gli studenti fossero attivamente coinvolti (laboratori di matematica) e si impegnassero in lavori individuali e di gruppo su problemi significativi. Tali attività erano progettate congiuntamente da docenti della scuola superiore e dell'università.

Un valido strumento per l'attuazione del progetto è stato il coinvolgimento di docenti di grandissima esperienza e specializzati proprio in didattica della matematica. In molti dipartimenti questo ha creato un collegamento nuovo, prima assente, fra i matematici esperti in didattica e gli altri matematici.

Come in ogni progetto anche in questo vi sono stati alcuni punti critici che hanno generato disagi. Ad esempio vi erano argomenti sui quali gli insegnanti non si sentivano sufficientemente preparati (come probabilità o crittografia). Tale difficoltà è stata risolta grazie alla realizzazione di attività formative rivolte agli insegnanti. Un altro problema erano le numerose attività pomeridiane degli studenti, che rendevano complicato trovare date ed orari per i laboratori extracurricolari ed ostacolavano la presenza costante da parte di alcuni ragazzi. Anche per questo motivo si ritiene preferibile realizzare attività rivolte a classi intere durante l'orario curricolare.

Per ogni informazione aggiuntiva sul Progetto Lauree Scientifiche e sui sottoprogetti rimando a:

<http://laureescientifiche.science.unitn.it>.

### 5.3 Considerazioni sul progetto di crittografia

Il Progetto Lauree Scientifiche-Orientamento e Formazione Insegnanti-Matematica si è articolato in 33 sottoprogetti locali territoriali ed in un sottoprogetto trasversale-nazionale. I progetti locali hanno organizzato le attività, per la maggior parte laboratori (cioè con coinvolgimento attivo degli studenti), sul territorio in collaborazione con gli Istituti scolastici.

Uno dei temi considerati nei progetti locali è stata proprio la Crittografia. Alla base di questo progetto vi era l'intenzione di interessare gli studenti verso la matematica e le sue applicazioni a partire da un problema concreto come la crittografia, analizzando passo passo gli strumenti matematici necessari alla comprensione dell'argomento.

L'espedito utilizzato per raggiungere la comprensione degli argomenti trattati era quello di rendere lo studente parte attiva nel processo di apprendimento, coinvolgendolo direttamente nella ricerca di soluzioni al problema posto. Come nel mio caso i destinatari del progetto erano classi IV.

Mi soffermo dunque ad analizzare alcune peculiarità di questo percorso che ritengo essere molto interessanti, valide e che mi hanno aiutato nella preparazione del mio progetto:

- utilizzo di un approccio storico per presentare problemi matematici visti come processi "in fieri", in particolare alcune congetture aperte sui numeri primi;
- illustrazione di alcune semplici tecniche crittografiche (come il cifrario di Cesare) utile a stimolare l'interesse degli studenti su strumenti matematici come l'aritmetica modulare;
- utilizzo del laboratorio, in cui lo studente è reso attore del processo di apprendimento mediante:
  - utilizzo di strumenti informatici, grazie ai quali egli stesso è posto nella condizione di costruire esempi e di formulare proprie congetture;
  - gare di decifrazione di crittogrammi, nelle quali può testare la propria comprensione;
- incontri con rappresentanti di aziende informatiche per la presentazione di applicazioni crittografiche (come RSA);

- suddivisione della valutazione in tre momenti, che permette di analizzare la progressione nell'apprendimento e nella percezione della matematica da parte degli studenti:
  - valutazione iniziale (tramite questionario) della visione degli alunni nei confronti della matematica;
  - valutazione progressiva, effettuata nel corso delle lezioni, tramite gare di crittanalisi per testare il livello di apprendimento degli studenti;
  - valutazione finale tramite test dell'apprendimento dei contenuti e della percezione della matematica;
- valutazione dell'efficacia del progetto tramite questionari nazionali proposti sia agli alunni che ai docenti.



# Conclusioni

*Non cercate di soddisfare la vostra vanità,  
insegnando loro troppe cose.  
Risvegliate la loro curiosità.  
É sufficiente aprire la mente,  
non sovraccaricarla.  
Mettetevi soltanto una scintilla.  
Se vi è della buona materia infiammabile,  
prenderà fuoco.  
(Anatole France)*

Giunto al termine di questo lavoro, posso affermare che il progetto da me ideato e realizzato ha portato a risultati più che soddisfacenti, corrispondendo appieno alle mie aspettative. I ragazzi hanno vissuto questa esperienza in maniera molto positiva, hanno dimostrato di avere acquisito delle buone competenze in relazione all'argomento trattato ed hanno almeno in parte modificato la propria visione della matematica. Cosa non meno importante, si sono divertiti imparando.

Ritengo che, in future riedizioni di questo progetto, si potrebbe lasciare maggiore spazio ai lavori di gruppo ed alla risoluzione di situazioni pratiche con ragionamenti di logica. Inoltre in alcuni casi risulterebbe più produttivo non avere un programma rigido, tale da non permettere cambiamenti in corso d'opera, ma essere liberi di modificarlo a seconda di quello che interessa di più i ragazzi, seguendo quello che loro stessi propongono.

Un obiettivo futuro molto importante, a livello ministeriale, potrebbe essere

quello di tentare l'inserimento della crittografia nella programmazione curricolare, nonchè introdurre nella prassi didattica nuove metodologie ed attività di tipo laboratoriale. Il primo punto condurrebbe a presentare un esempio di applicazione matematica disponibile a tutti gli studenti e non solo ad alcune classi, mentre il secondo punto permetterebbe di avvicinare i ragazzi alla matematica, rendendoli più partecipi ed attivi, in modo da predisporli favorevolmente all'apprendimento della materia. A tal proposito desidero citare:

“Nulla egli sappia per averlo udito da voi, ma solo per averlo compreso da sè: non impari la scienza, la scopra.” (Jean-Jacques Rousseau).

Del resto, chiediamoci quale altra materia venga insegnata senza alcun riferimento alla sua utilità, alle sue applicazioni pratiche, alla sua storia, alla sua filosofia, ai suoi criteri estetici, ed al suo stato attuale. La tecnica matematica che ora insegnamo andrebbe imparata nello scenario dei grandi problemi, della loro motivazione e del loro processo creativo.

Ritengo che la crittografia sia un semplice ed utile esempio di matematica applicata. Il vantaggio principale che offre è quello di poter essere portata in qualunque tipo di scuola, non esclusivamente in un liceo scientifico. È vero che in quest'ultimo si può porre l'accento sulla teoria dei numeri, sulle dimostrazioni, sulla problematicità dei numeri primi, come da me attuato, ma in altri indirizzi è possibile procedere con approcci diversi, ad esempio concentrandosi su aspetti informatici ed algoritmici. Si tratta solo di stabilire il taglio che si vuole dare al lavoro e gli obiettivi che ci si propone.

Ad esempio un approccio molto interessante è stato utilizzato da Christian Ferrari<sup>1</sup> in un progetto simile portato in una classe di prima liceo [10]. Egli ha diviso il percorso in due fasi: scoperta e messa a punto. Nella prima fase ha illustrato ai ragazzi il funzionamento generale di RSA, permettendo loro di sperimentarlo e vederlo in azione. Quindi, è passato all'insegnamento dei concetti matematici necessari alla crittografia RSA, riprendendo infine il pro-

---

<sup>1</sup>Docente di Fisica e Matematica presso il Liceo Cantonale di Locarno

tocollo precedentemente abbozzato ed evidenziando come i dettagli appresi si rivelino essenziali. Infine ha preparato un'attività di gioco che utilizza il protocollo RSA per scambiare messaggi.

L'idea che considero più interessante (oltre ad avere scelto di incuriosire i ragazzi mostrando loro prima RSA e poi la matematica) è l'introduzione dell'utilizzo di software informatici per far visualizzare in maniera concreta le limitazioni dei calcolatori (velocità di calcolo e costo computazionale) ed i concetti che stanno alla base di RSA: in dettaglio ha affidato ai ragazzi il compito di indagare con Maple ed Excel sul problema della difficoltà di fattorizzare i numeri al crescere del numero di cifre. Inoltre, dal punto di vista pedagogico-didattico, l'interrogativo alla base del suo lavoro era molto simile al mio: "Può un'attività di matematica applicata fungere da catalizzatore per l'apprendimento di alcuni concetti elementari della teoria dei numeri?" [10].

Nel suo lavoro egli sottolinea come tra i campi di studio liceali figurino anche la voce *Elementi di statistica*, il che permette di pensare ad un'attività simile per la crittanalisi e la statistica (analisi statistica delle frequenze per i cifrari a sostituzione mono e polialfabetica). Effettuando insieme le due attività (crittografia e teoria dei numeri, crittanalisi e statistica) si potrebbero mostrare agli studenti le due facce della crittologia.

Infine, proseguendo sulla strada dei collegamenti, si può affrontare un tema più vasto e generale come *Informazione e matematica*, aggiungendo la teoria dei codici correttori, con possibili aperture sulla probabilità ed analizzando casi elementari della teoria di Shannon. Ed ancora, grazie al protocollo di crittografia quantistica, è possibile legare anche matematica, crittografia e fisica, come è stato fatto in parte nella fase conclusiva del mio progetto.

Come si vede da queste considerazioni, la teoria dei numeri e la crittografia offrono molte altre attività realizzabili in classe (con prerequisiti di prima liceo!), sempre legati ad aspetti della matematica che fanno parte della nostra vita quotidiana ogni giorno più tecnologica.



# Appendice A

## Slides del corso

## Numeri parole e segreti

Basi matematiche (e non solo...) della crittografia

a cura di **Marco Garulli**,

mail to: [marco.garulli@studio.unibo.it](mailto:marco.garulli@studio.unibo.it) [garu86@msn.com](mailto:garu86@msn.com)

Università degli Studi di Bologna, Alma Mater Studiorum,  
Dipartimento di Matematica

ubuntu

1 0 100000

**Crittografia a frase**  
(4 7 = 6 5)  
GLI SCONTI

u p o l i l u i m b z d d s u z t s  
h t q n f s i w t j g j x y n f q j

**Dittoiidi:**  
1 4 C dell'A  
5 D in una M  
24 O in un G

[http://www.weddomus.it/iao/test\\_intelligenza\\_mensa.html](http://www.weddomus.it/iao/test_intelligenza_mensa.html)

**Crittografia mnemonica:**  
(5 6 2 13)  
CUCCHIAINO

(5 1 8)  
SCONTRO DI TARTARUGHE

(6 11)  
FOSSI SULLA LUNA

<http://0.xmau.com/>


ubuntu

## Crittografia vs Steganografia

**Crittografia:** nascondere il significato o il contenuto di un messaggio

**Steganografia:** nascondere il messaggio stesso.

kryptòs - gráphein



"La steganografia da Erodoto a Bin Laden. Viaggio attraverso le tecniche elusive della comunicazione" di Amato Nicola


ubuntu

## Un po' di Storia

- Cifrario Atbash:** invertire l'ordine delle lettere dell'alfabeto

Alfabeto in chiaro: *abcdefghijklmnopqrstuvwxyz*  
Alfabeto cifrato: *zvu tsrqponmlihgfedcba*

- Cifrario di Cesare:** traslare di alcune posizioni le lettere



Giulio Cesare (100-44 a.C.)

Alfabeto in chiaro: *abcdefghijklmnopqrstuvwxyz*  
Alfabeto cifrato: *defghilmnopqrstuvzabc*

ubuntu

## Esercizi

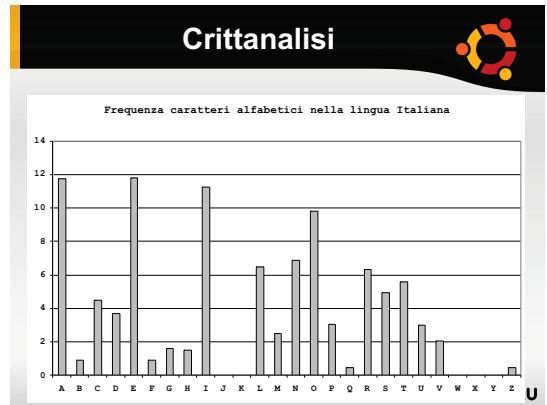
Testo cifrato: *u p o l i l u i m b z d d s u z t s*  
**Testo in chiaro:** *ch i n o n c o m b a t t e c a d e*

Testo cifrato: *h t q n f s i w t j g j x y n f q j*  
**Testo in chiaro:** *co l i a n d r o è b e s t i a l e*

*Quanti sono i possibili cifrari a traslazione di Cesare?*

*È utile cifrare lo stesso testo più volte col cifrario di Cesare?*

ubuntu




## Evoluzioni

- Cifrario delle permutazioni:** permutare in ogni modo possibile l'alfabeto

Alfabeto in chiaro: *abcdefghijklmnopqrstuvwxyz*  
Alfabeto cifrato: *ultimos aerbcdfghnpqzv*

- Cifrario di Vigenère:** usare più alfabeti, ossia uno per ogni lettera. Come si può fare?



Blaise de Vigenère (1523-1596)

ubuntu

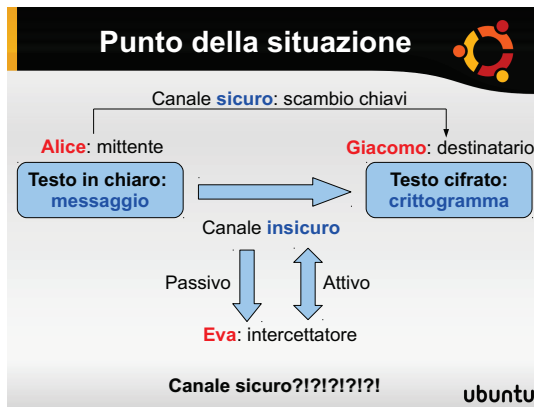
## Tavola di Vigenère

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Se voglio cifrare il messaggio "certe notti" con la parola chiave "vasco", procedo in questo modo:

*c e r t e n o t t i*  
*v a s c o v a s c o*  
*x e j v s i o l v i*

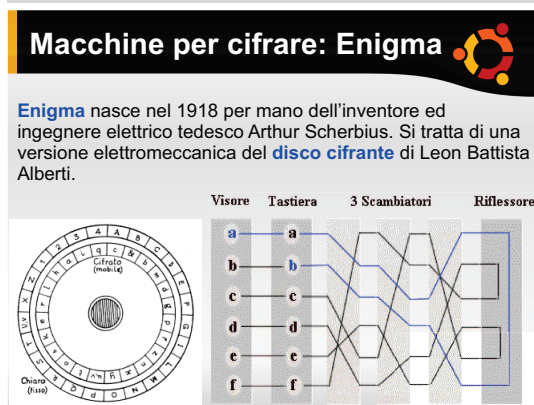
ubuntu



### Legge di Kerckhoffs

"La sicurezza di un crittosistema non deve dipendere dal tener celato il crittoalgoritmo. La sicurezza dipenderà solo dal tener celata la **chiave**."

ubuntu



### Crittografia a chiave pubblica

Da arte a scienza

Whitfield Diffie

*New Directions in Cryptography* (1976)

Martin Edward Hellman

Si basa sul problema **P=NP**

ubuntu

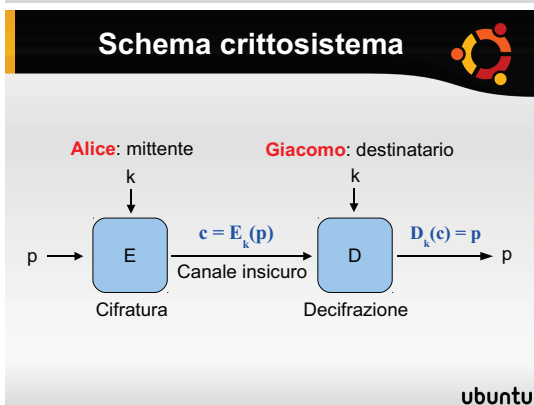
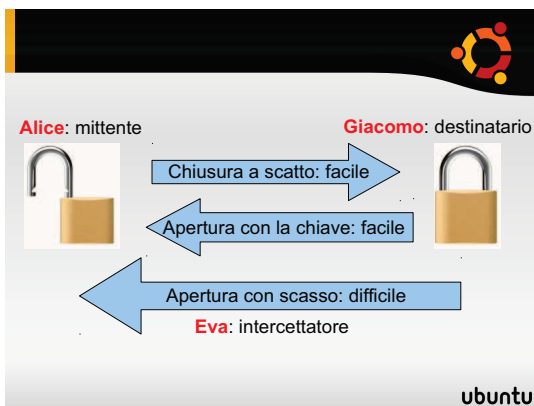
### Complessità computazionale

È la teoria che studia le risorse di calcolo richieste per risolvere un dato problema. Ci sono due possibilità:

- **problemi semplici** (detti della classe **P**): esiste un algoritmo che richiede un tempo polinomiale rispetto alla dimensione dei dati del problema (il numero di cifre nella fattorizzazione);
- **problemi difficili** (detti della classe **NP**), ossia problemi per i quali, data una possibile soluzione, la sua verifica avviene con un algoritmo in tempo polinomiale.

Per la classe NP esistono algoritmi esponenziali... ma non si sa se esistono algoritmi polinomiali → **P=NP?**

ubuntu



### Cifrario di Vernam

La chiave è lunga quanto il messaggio.

Ad esempio, se il messaggio che vogliamo spedire è

$$x = 1001010110101$$

e la parola chiave scelta è

$$y = 0010101101011$$

allora il crittogramma diventa

$$x' = 101111011110.$$

Gilbert Vernam (1890-1960)      Claude Shannon (1916-2001)

ubuntu

### Lavoriamo un po' con gli interi

12 : 2 = 6	}	12 = 2 · 6
12 : 3 = 4		12 = 3 · 4
12 : 4 = 3		12 = 4 · 3
12 : 6 = 2		12 = 6 · 2
12 : 5 = ?!?		12 = 5 · ?!?

Manca un numero che moltiplicato per 5 dia 12, quindi a differenza di prima non possiamo più scrivere 12 come prodotto di 5 per qualcosa...

ubuntu

### Crittosistema

( $P, C, K, E, D$ ) con le seguenti proprietà:

- $P$  è l'insieme dei testi in chiaro e contiene i messaggi da spedire
- $C$  è l'insieme dei testi cifrati e contiene i crittogrammi
- $K$  è l'insieme delle chiavi e contiene tutte le possibili chiavi
- $E = \{E_k : k \text{ appartiene a } K\}$  è la famiglia di funzioni di cifratura
- $D = \{D_k : k \text{ appartiene a } K\}$  è la famiglia di funzioni di decifrazione

Per ogni  $e$  appartenente a  $K$ , esiste un  $d$  appartenente a  $K$  tale che  $D_d(E_e(p)) = p$  per tutti i  $p$  appartenenti a  $P$ .

ubuntu

### Sicurezza assoluta...

Chiavi diverse danno luogo a numerose decifrazioni leggibili ma incoerenti come significato. Nemmeno tentare tutte le chiavi possibili permette di scoprire il significato del messaggio.

**Questo crittosistema è perfetto.**

ubuntu

### Crittosistema perfetto

Per ogni  $c_o$  in  $M$ ,  $P_k(c_o = e_k(m_o))$  è la stessa per tutti gli  $m_o \in M$

$\leftrightarrow$  per ogni scelta di  $m_o, c_o$  in  $M$ ,

$$P_m(m = m_o) = P_{m_k}(m = m_o | c_o = e_k(m_o)).$$

**Difetti:**

- la chiave può essere recuperata sommando il messaggio in chiaro e il crittogramma, il che suggerisce di usarla una sola volta
- il mittente ed il destinatario dovranno concordare una chiave lunga quanto il messaggio e trasmettersela
- generare una chiave, cioè una sequenza assolutamente casuale di 0 e 1, è una procedura complicata e costosa.

ubuntu

### Divisibilità

- $a$  divide  $b$ ,  $a|b$ , se e solo se esiste  $q$  tale che  $b = q a$
- Proprietà:**  $a|b$  e  $a|c$  allora  $a|b \pm c$
- $a = b q + r$  con  $0 \leq r < |b|$
- $MCD(a,b)$ : i divisori comuni della coppia  $(a,b)$  sono gli stessi della coppia  $(b,r) \rightarrow$  **algoritmo euclideo.**
- Dato l'algoritmo precedente, cosa possiamo dire dell' $MCD(a,b)$ ? Ha qualche correlazione con  $a$  e  $b$  stessi?

Euclide (300 a.C.)

ubuntu



### Algoritmo euclideo

$$a = bq + r_1$$

$$b = r_1q_1 + r_2$$

$$r_1 = r_2q_2 + r_3$$

$$\dots$$

$$r_i = r_{i+1}q_{i+1} + r_{i+2}$$

$$\dots$$

$$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1}$$

$$r_{n-2} = r_{n-1}q_{n-1}$$

con  $r_1 = 0$  oppure  $0 < r_1 < b$

con  $r_2 = 0$  oppure  $0 < r_2 < r_1$

con  $r_3 = 0$  oppure  $0 < r_3 < r_2$

con  $r_{i+2} = 0$  oppure  $0 < r_{i+2} < r_{i+1}$

con  $r_{n-1} = 0$  oppure  $0 < r_{n-1} < r_{n-2}$

e quindi  $r_n = 0$ .

alla fine avremo:

**L'ultimo resto non nullo, cioè  $r_{n-1}$  è l' $MCD(a,b)$ .**

ubuntu

### Identità di Bézout


$$r_1 = a - bq_1$$

$$r_2 = b - r_1q_1$$

$$\dots$$

$$\dots$$

$$r_n = r_{n-2} - r_{n-1}q_n$$



Étienne Bézout  
(1730-1783)

da cui si ricava:

$$r_2 = b - r_1q_1 = b - (a - bq_1)q_1 = (-q_1)a + (1 + q_1q_2)b$$

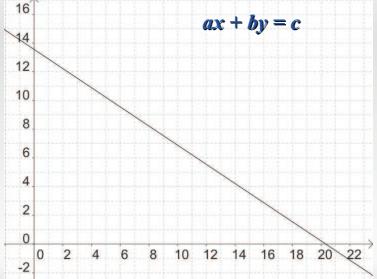
**$MCD(a, b) = \alpha a + \beta b$**

ubuntu

### Equazioni lineari diofantee...



Diophanto  
di Alessandria  
200-284



ubuntu

### ... e loro soluzione

L'equazione  $ax + by = c$ , con  $a, b, c \in \mathbb{Z}$  e  $a, b \neq 0$ , possiede una soluzione intera  $(x, y)$  se e solo se l' $MCD(a, b)$  divide  $c$ .

↓

- $d = MCD(a, b)$  divide  $a$  e  $b \rightarrow$  dividerà il primo membro dell'equazione e quindi anche  $c$ .
- $d$  divide  $c$ , quindi  $c = pd$ . Inoltre per l'identità di Bézout  $d = \alpha a + \beta b$ . Moltiplico ambo i membri per  $p \rightarrow c = \alpha pa + \beta pb$ . Posto  $x = \alpha p$  e  $y = \beta p$ ,  $(x, y)$  è una soluzione dell'equazione.

ubuntu

### Numeri primi

○○ ○○○ ○○○○

Si riescono a formare  
sempre dei rettangoli!  
**Oppure no?**

○○ ○○○ ○○○○

Un naturale  $a \neq 0$  si dice **primo** o **irriducibile** quando è diverso da 1 e non ha divisori propri, cioè divisori che non siano né 1 né  $a$  stesso. Ad esempio

3, 5, 7, 11, 13, 17, 19 .....

Un numero intero positivo  $p > 1$  è primo se e solo se vale:  
se  $p$  divide  $ab$ , allora  $p|a$  oppure  $p|b$ .

ubuntu

### Numeri primi e attualità

NUMERI PRIMI: LA SOLUZIONE DEI LORO ENIGMI VALE UN MILIONE DI DOLLARI

ubuntu

### Un po' di dubbi

- Teorema fondamentale dell'aritmetica:** si può dire qualcosa sul rapporto fra un qualsiasi numero e i numeri primi?
- Quanti sono i numeri primi?
- Osserviamo questi due fatti:
 
$$4=2+2, 6=3+3, 8=5+3, 10=7+3, 12=7+5, 14=11+3 \dots$$

$$15=7+3+5, 17=7+5+5, 19=11+5+3, 21=13+5+3 \dots$$

Cosa possiamo dire a riguardo?

ubuntu

### ...

- Numeri **primi gemelli** sono della forma:  $p, p+2$ , come 5 e 7 o 11 e 13. Quanti sono?
- E le **terne** di numeri primi consecutivi (come 3, 5 e 7)?
- Si può trovare una successione di lunghezza arbitraria di numeri consecutivi non primi?

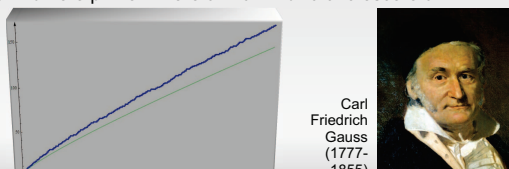
Ad esempio, se voglio trovarne 100 posso fare così:

$101! + 2, 101! + 3, \dots, 101! + 101$

ubuntu

### È possibile conoscere i numeri primi?

**Gauss** si accorse dell'impossibilità di determinare una successione di numeri primi, quindi decise di affrontare il problema in modo diverso: quanti sono i numeri primi fra 1 e 10? E fra 1 e 100? E fra 1 e 1000? In sostanza lui stava cercando una stima del numero di numeri primi minori o uguali ad un numero dato  $n$ . Si accorse che la probabilità di trovare un numero primo minore di  $n$  diminuiva al crescere di  $n$ ...



Carl Friedrich Gauss (1777-1855)

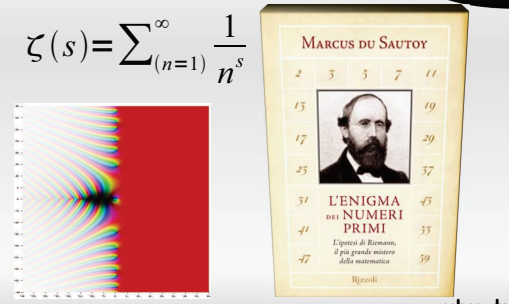
### Frequenza dei numeri primi

N	$\pi(N)$	Intervallo medio fra 2 primi
10	4	2,5
100	25	4,0
1.000	168	6,0
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,3
1.000.000.000	50.847.534	19,8

$$\frac{N}{\ln N} \xrightarrow{N \rightarrow \infty} \pi(N)$$

ubuntu

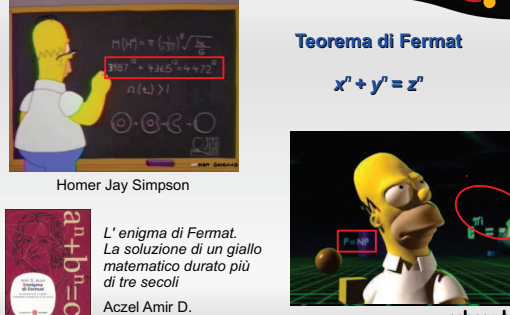
### La funzione Z di Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$


ubuntu

### Altra questione aperta sui numeri

**Teorema di Fermat**

$$x^n + y^n = z^n$$


Homer Jay Simpson

L'enigma di Fermat. La soluzione di un giallo matematico durato più di tre secoli. Aczel Amir D.

ubuntu


### Test di primalità e fattorizzazione

Due grandi problemi sono:

- dato un numero  $n$  capire **se è primo**
- se non lo è, trovare la sua **fattorizzazione**

Partiamo dal primo: qual'è la prima cosa che ci viene in mente per verificare se un numero è primo o meno? Sviluppando tale idea, come possiamo diminuire il numero di operazioni da effettuare?

Per quanto riguarda il secondo punto si può utilizzare questo trucchetto: invece di trovare i fattori di  $n$  cerchiamo due numeri  $x$  e  $y$  tali che  $n = x^2 - y^2$ . Perché dovrebbe interessarci?



Pierre de Fermat (1601-1665)

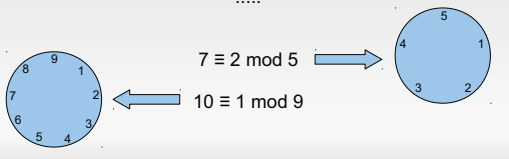
### L'aritmetica dell'orologio



ubuntu

### Formalizzazione

$17 \equiv 5 \pmod{12}$   
 $22 \equiv 10 \pmod{12}$   
 ....  
 $7 \equiv 2 \pmod{5}$   
 $10 \equiv 1 \pmod{9}$



ubuntu

$19 \equiv 1 \pmod{9}$  .....

Che rapporto intercorre tra i tre numeri precedenti?

19 è divisibile per 9?

Se non lo è, cosa può renderlo divisibile per 9?

ubuntu

### Classi di resto modulo $m$

$$a \equiv b \pmod{m} \leftrightarrow m \mid a - b \leftrightarrow$$

$$\leftrightarrow a - b = qm \leftrightarrow a = b + qm$$

Quindi  $b$  rappresenta il **resto** della divisione di  $a$  per  $m$ .

Chiamiamo  $[a]_m = \{b, b \equiv a \pmod{m}\}$   
 classe di resto  $a$  modulo  $m$ .

ubuntu

### $Z_m$

L'insieme delle classi di resto modulo  $m$  si scrive  $Z/m$  o  $Z_m$ .  
 Ha  $m$  elementi dato che  $0, 1, 2, \dots, m-1$  sono i possibili **resti** della divisione per  $m$ .

Un insieme dei rappresentanti per quelle classi di resto è un insieme di interi che contiene esattamente un elemento di ogni classe di resto modulo  $m$ , cioè

$$Z_m = \{[0], [1], \dots, [m-1]\}.$$

ubuntu

"Sei lento a imparare, Winston" disse O'Brien, con dolcezza.

"Ma come posso fare a meno..." borbottò Winston "come posso fare a meno di vedere quel che ho dinanzi agli occhi? Due e due fanno quattro."

"Qualche volta, Winston. Qualche volta fanno cinque. Qualche volta fanno tre. Qualche volta fanno quattro e cinque e tre nello stesso tempo. Devi sforzarti di più. Non è facile recuperare il senno."

ubuntu

### Somme e moltiplicazioni

$$a \pm c \equiv b \pm d \pmod{m}, \quad ac \equiv bd \pmod{m}$$

$$\downarrow \qquad \qquad \qquad \downarrow$$

$$[a] + [c] = [a + c] \qquad [a][c] = [ac]$$

Esiste un elemento  $[a']$  tale che

$$[a] + [a'] = [a'] + [a] = [0] \rightarrow [-a]$$

un elemento  $[e]$  tale che

$$[a] + [e] = [e] + [a] = [a] \rightarrow [0]$$

ed un elemento  $[i]$  tale che

$$[a][i] = [i][a] = [a] \rightarrow [1]$$

ubuntu

### Che giorno della settimana era?

$$x = g + \left[ \frac{(m+1)26}{10} \right] + a + \left[ \frac{a}{4} \right] + \left[ \frac{s}{4} \right] - 2s \pmod{7}$$

$g$  = giorno del mese,  $m$  = mese,  $a$  = anno (solo le due ultime cifre),  $s$  = secolo (solo le prime due cifre)  
 1 = Domenica, 2 = Lunedì, 3 = Martedì,  
 4 = Mercoledì, 5 = Giovedì, 6 = Venerdì, 0 = Sabato

**Eccezioni:** gennaio viene indicato con 13, febbraio con 14 e i rispettivi anni vengono diminuiti di 1.

ubuntu

### Inverso

Un elemento  $[a]$  di  $Z_m$  diverso da  $[0]$  si dice **invertibile** quando esiste  $[a']$  appartenente a  $Z_m$  tale che  $[a][a'] = 1$ .

Una classe resto  $[a]$  in  $Z_m$  è invertibile se e solo se  $MCD(a, m) = 1$ , ossia se  $a$  e  $m$  sono coprimi.

ubuntu

### Funzione $\phi$ di Eulero

La **funzione  $\phi$  di Eulero** è una funzione definita per  $n$  intero positivo nel modo seguente:

$\phi(n)$  è il numero di interi non negativi minori o uguali ad  $n$  che sono coprimi con  $n$ .



Leonhard Euler (1707-1783)

In particolare osserviamo che  $\phi(1) = 1$ .

Se  $p$  è primo quanto vale  $\phi(p)$ ?

La funzione  $\phi$  di Eulero è **moltiplicativa**, cioè dati due interi  $m$  ed  $n$  maggiori di 1 tali che  $MCD(m, n) = 1$ , si ha che  $\phi(mn) = \phi(m)\phi(n)$ .

ubuntu

### Prova del nove

$$123 \cdot 456 = 56088$$

sommo le cifre dei due fattori:  $1+2+3=6, 4+5+6=15, 1+5=6$ .

Quindi moltiplico i due risultati ottenuti:  $6 \cdot 6 = 36, 3+6=9=0$ .

Infine sommo le cifre del risultato ottenuto dalla moltiplicazione iniziale:  $5+6+0+8+8=27, 2+7=9=0$

$$123 = 1 \cdot 10^2 + 2 \cdot 10 + 3 \equiv 1 + 2 + 3 \pmod{9}$$

$$456 = 4 \cdot 10^2 + 5 \cdot 10 + 6 \equiv 4 + 5 + 6 \pmod{9}$$

$$56088 = 5 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10 + 8 \equiv 4 + 5 + 6 \pmod{9}$$

ubuntu

## Formalizzazione cifrari classici

### Cifrario di Cesare:

iniziamo con l'associare ad ogni lettera un numero intero:  
 $a \rightarrow 0, b \rightarrow 1, c \rightarrow 2 \dots$

se scegliamo come chiave il numero 3, dobbiamo spostare ogni lettera di 3 posti, cioè sommare 3 al valore di ogni lettera. Per esempio per la b si avrà:

$$1 + 3 \pmod{26}$$

che corrisponde alla e. In generale si avrà

$$c \equiv p + k \pmod{26}$$



ubuntu

## Generazione chiavi

Giacomo genera due primi  $p$  e  $q$  e ne calcola il prodotto  $n = p \cdot q$ ; quindi sceglie un numero  $e$  tale che

$$1 < e < \varphi(n) = (p-1)(q-1), \quad \text{MCD}(e, (p-1)(q-1)) = 1$$

Infine calcola l'intero  $d$  tale che

$$1 < d < (p-1)(q-1), \quad de \equiv 1 \pmod{(p-1)(q-1)}$$

Tale intero esisterà senz'altro dato che  $\text{MCD}(e, (p-1)(q-1)) = 1$ .

La chiave pubblica è la coppia  $(n, e)$  e la chiave privata è  $d$ .

ubuntu

## Cifratura e decifrazione

Lo spazio dei testi in chiaro è costituito da tutti gli interi  $m$  tali che  $0 \leq m < n$ . Il crittogramma è ottenuto in questo modo

$$c = m^e \pmod{n}$$

Per riottenere il testo in chiaro è sufficiente calcolare

$$m = c^d \pmod{n}$$

Questo risultato può essere dimostrato attraverso il **teorema di Eulero**, cioè:

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

ubuntu

## Crittografia quantistica

Si basa su alcune idee della **meccanica quantistica**.

- Principio di indeterminazione di **Heisenberg**
- Esperimento di **Young**
- Il computer quantistico
- Polarizzazione di fotoni

ubuntu

## RSA

La sua sicurezza è strettamente legata alla difficoltà di trovare la **fattorizzazione** di un intero positivo composto che è prodotto di due primi molto grandi.



1978

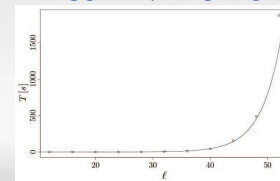
Adi Shamir, Ronald Rivest, Leonard Adleman

ubuntu

• Se  $n$  è un numero "grande" è praticamente impossibile calcolare  $\varphi(n)$ , cioè è un problema della classe **NP**.

• Se  $n$  è il prodotto di due numeri primi noti si può facilmente calcolare  $\varphi(n)$ :

$$n = pq \rightarrow \varphi(n) = (p-1)(q-1)$$



ubuntu

## Piccolo teorema di Fermat

Il teorema di Eulero è la generalizzazione del piccolo teorema di Fermat:

se  $p$  è un numero primo, allora, per ogni  $x \in \mathbb{Z}_p$  con  $x \neq 0$ ,

$$x^{p-1} \equiv 1 \pmod{p}$$

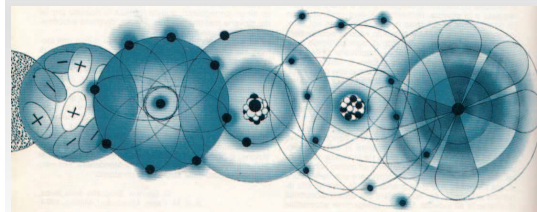
I multipli di  $x$ , vale a dire  $0, x, 2x, 3x, \dots, (p-1)x$ , sono tutti distinti. In particolare l'insieme  $\{x, 2x, 3x, \dots, (p-1)x\}$  deve coincidere con  $\{1, 2, \dots, p-1\}$

$$x^{p-1} (1 \cdot 2 \cdot \dots \cdot (p-1)) \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$$

Semplificando  $1 \cdot 2 \cdot \dots \cdot (p-1)$ , otteniamo il risultato.

ubuntu

## L'atomo



ubuntu





### Protocollo BB84 (Bennet-Brassard)

1. Comunicazione mediante trasmissione di fotoni attraverso un canale quantistico
2. Comunicazione su un canale non protetto per l'eliminazione degli errori e l'estrazione della chiave grezza
3. Comunicazione su un canale non protetto per verificare la presenza di Eva

ubuntu

Sequenza di bit di Alice:	0	0	1	0	1	0	1	1	1
Schema di filtraggio di Alice:	+	+	+	+	+	+	+	+	+
Schema di filtraggio di Bob:	+	+	+	+	+	+	+	+	+
Misurazione dei bit di Bob:	1	0	1	0	1	0	0	1	1
Sequenza ottenuta (chiave):	-	0	-	0	1	-	-	1	1

ubuntu

Bit Sequence	1	1	0	0	1	0	1	0	1	0
Photon Sequence	↑	↑	↓	↓	↘	↘	↙	↙	↘	↘
Bases Sequence	+	+	+	+	+	+	+	+	+	+
Detection Results	0	1	1	0	0	1	1	0	1	0
Compatibility	x	x	✓	✓	✓	✓	x	x	✓	✓
Key	-	1	-	0	0	1	-	-	1	0

ubuntu

untu

Alice and Bob now use quantum cryptography.

But now, Eve has a PhD in string theory.

ubuntu

### Indice

- Crittografia vs Steganografia
- Un po' di Storia
- Evoluzioni
- Tavola di Vigenere
- Macchine per cifrare: Enigma
- Colossus
- Punto della situazione
- Crittografia a chiave pubblica
- Crittosistema
- Sicurezza assoluta...
- Divisibilità
- Algoritmo euclideo
- Identità di Bézout
- Equazioni lineari diofantee...
- ... e loro soluzione
- Numeri primi e attualità
- Un po' di dubbi

- È possibile conoscere i numeri primi?
- La funzione Z di Riemann
- Altra questione aperta sui numeri
- Test di primalità e fattorizzazione
- L'aritmetica dell'orologio
- Formalizzazione
- Classi di resto modulo  $m$
- $Z_m$
- Somme e moltiplicazioni
- Inverso
- Funzione  $\phi$  di Eulero
- Prova del nove
- Formalizzazione cifrari classici
- RSA
- Generazione chiavi
- Cifratura e decifrazione
- Crittografia quantistica

ubuntu

# Appendice B

## Compiti in classe

### Verifica di Crittografia (A)

Nome e cognome: \_\_\_\_\_

Voto: \_\_\_\_\_

#### Domande

**Domanda B.1.** Che differenza c'è fra crittografia e steganografia?

**Domanda B.2.** Come funziona il cifrario di Vigenere? In cosa differisce dal cifrario di Cesare o da quello delle permutazioni?

**Domanda B.3.** Cosa ha portato l'invenzione e l'utilizzo della radio e poi dei computer nel campo della crittografia?

**Domanda B.4.** Qual'è la novità introdotta dalla crittografia a chiave pubblica? Chi sono stati i personaggi più importanti di questa svolta?

**Domanda B.5.** Come funziona il cifrario di Vernam? Come mai non è molto utilizzato? (descrivi qualche difetto).

**Domanda B.6.** Spiega in cosa consistono la divisibilità fra due numeri e la divisione euclidea, poi fai un esempio.

**Domanda B.7.** Se  $a|b$ ,  $a|c$  cosa possiamo dire e perchè?

**Domanda B.8.** Perchè funziona l'algoritmo euclideo per trovare l'MCD fra due numeri, cioè quale proprietà permette di ricavare l'MCD grazie a questo algoritmo?

**Domanda B.9.** Che cosa studiò Diofanto e a che conclusioni giunse?

**Domanda B.10.** Che cosa afferma il teorema fondamentale dell'aritmetica? Qual'è l'idea alla base della dimostrazione?

**Domanda B.11.**  $4=2+2$ ,  $6=3+3$ ,  $8=5+3$ ,  $10=7+3$ ,  $12=7+5$  ... cosa rappresenta? È sempre vero?

**Domanda B.12.** Sapresti indicare uno dei problemi da un milione di dollari che abbiamo incontrato?

**Domanda B.13.** Qual'è stato il cambio di prospettiva proposto da Gauss per quanto riguarda i numeri primi?

**Domanda B.14.** Fai un'esempio di congruenza e spiegalo.

**Domanda B.15.** Cosa rappresenta il numero  $b$  nella scrittura  $a \equiv b \pmod{n}$ ? Perchè?

**Domanda B.16.** Scrivi una classe di congruenza modulo 11. Quanti elementi ha  $\mathbb{Z}_{11}$ ? Come sono fatti? Scegli tu come rappresentarli.

**Domanda B.17.** Come funziona la somma sull'orologio (con un qualsiasi numero di ore)? Fai un esempio.

**Domanda B.18.** Cos'è la  $\varphi$  di Eulero? Quale proprietà fondamentale ha?

**Domanda B.19.** Sapresti spiegare come mai trovare la fattorizzazione di un numero e calcolarne la  $\varphi$  di Eulero siano due operazioni collegate? E tutto questo cosa ha a che fare con RSA?



**Domanda B.20.** Descrivi brevemente cos'è e come funziona RSA. Ricordi come funziona la decifrazione e perchè?

**Domanda B.21.** Su cosa si basa la crittografia quantistica? Cosa ti ricordi di questo tipo di crittografia?

### Esercizi

**Esercizio B.1.** Usa l'algoritmo euclideo per trovare l'MCD(71,53). Era necessario procedere in questo modo per determinare l'MCD?

**Esercizio B.2.** 299 è primo? (anche se di solito si usa per la fattorizzazione, prova con l'idea di Fermat).

**Esercizio B.3.** Quale numero è congruo a  $15 \pmod{9}$ ?

**Esercizio B.4.** Qual'è l'opposto di  $[2]_5$  (cioè in un orologio con 5 ore) rispetto alla somma?

**Esercizio B.5.** Qual'è l'inverso di  $[7]_{21}$  (rispetto alla moltiplicazione)?

**Esercizio B.6.** Se i due numeri primi scelti per generare le chiavi per RSA sono 5 e 7 e la chiave pubblica  $e$  è 5, quanto vale la chiave privata  $d$ ?

**Esercizio B.7.** Se la chiave pubblica di RSA è  $(n, e) = (15, 7)$  come si cifra il messaggio  $m = 4$ ?

## Verifica di Crittografia (B)

Nome e cognome: \_\_\_\_\_

Voto: \_\_\_\_\_

### Domande

**Domanda B.22.** Quante chiavi possibili ha il cifrario di Cesare? E quello delle permutazioni?

**Domanda B.23.** Spiega cos'è la crittanalisi e quali metodi utilizza.

**Domanda B.24.** Descrivi brevemente come funziona in generale la comunicazione di un messaggio attraverso la cifratura. Che cos'è un crittosistema?

**Domanda B.25.** Come funziona il cifrario di Vernam? Quale proprietà fondamentale possiede? Cosa significa questa proprietà a parole?

**Domanda B.26.** Ti ricordi quali macchine elettromeccaniche sono state inventate per cifrare e decifrare? In che periodo storico?

**Domanda B.27.** Perché funziona l'algoritmo euclideo per trovare l'MCD fra due numeri, cioè quale proprietà permette di ricavare l'MCD grazie a questo algoritmo?

**Domanda B.28.** Spiega in cosa consistono la divisibilità fra due numeri e la divisione euclidea, poi fai un esempio.

**Domanda B.29.** Da cosa deriva l'identità di Bézout? Come?

**Domanda B.30.** La scomposizione di un numero in fattori primi (fattorizzazione in primi) esiste sempre? Qual'è l'idea alla base della dimostrazione? Tale fattorizzazione è unica?

**Domanda B.31.** Cosa si può dire di un numero  $c$  se divide  $a \cdot b$ , cioè se  $c|(a \cdot b)$ ? Ad esempio, cosa deve succedere affinché  $c$  sia primo?

**Domanda B.32.** Sapresti indicare uno dei problemi da un milione di dollari che abbiamo incontrato?

**Domanda B.33.** Ci sono terne di numeri primi consecutivi oltre a 3,5,7?

**Domanda B.34.** Sapresti trovare 50 numeri composti, cioè non primi, consecutivi?

**Domanda B.35.** Come si può "matematizzare" il funzionamento del trascorrere delle ore sull'orologio?

**Domanda B.36.** Cosa rappresenta il numero  $b$  nella scrittura  $a \equiv b \pmod{n}$ ? Perché?

**Domanda B.37.** Scrivi una classe di congruenza modulo 6. Quanti elementi ha  $\mathbb{Z}_6$ ? Come sono fatti? Scegli tu come rappresentarli.

**Domanda B.38.** Che particolarità ha la moltiplicazione nell'aritmetica dell'orologio? Fai un esempio.

**Domanda B.39.** Esiste sempre l'opposto (rispetto alla somma) di un elemento di  $\mathbb{Z}_n$ ? Puoi fare un esempio.

**Domanda B.40.** Descrivi brevemente cos'è e come funziona RSA. Ricordi come funziona la decifrazione e perché?

**Domanda B.41.** Sapresti spiegare come mai trovare la fattorizzazione di un numero e calcolarne la  $\varphi$  di Eulero siano due operazioni collegate? E tutto questo cosa ha a che fare con RSA?

**Domanda B.42.** Ricordi cos'è la meccanica quantistica? E un computer quantistico? Che cosa lo differenzia da un computer classico?

## Esercizi

**Esercizio B.8.** Usa l'algoritmo euclideo per trovare l'MCD(88,40). Era necessario procedere in questo modo per determinare l'MCD?

**Esercizio B.9.** Fattorizza il numero 527 (prova con l'idea di Fermat).

**Esercizio B.10.** È vero che  $17 \equiv 7 \pmod{9}$ ?

**Esercizio B.11.** Qual'è l'opposto di  $[3]_5$  (cioè in un orologio con 5 ore)?

**Esercizio B.12.** Quanto vale  $\varphi(6)$ ? E  $\varphi(19)$ ?

**Esercizio B.13.** Se la chiave privata di RSA è  $(n, d) = (15, 7)$  come si decifra il messaggio  $c = 7$ ?

**Esercizio B.14.** Se i due numeri primi scelti per generare le chiavi per RSA sono 5 e 7 e la chiave pubblica  $e$  è 5, quanto vale la chiave privata  $d$ ?

# Appendice C

## Esercizi per lavoro di gruppo

### Problemi

#### Problema C.1.

Dimostrare che dati  $a, b \in \mathbb{Z}$  esistono  $q, r$  tali che  $a = bq + r$ .

#### Suggerimento:

Si può utilizzare il principio del minimo che dice che

*ogni insieme di numeri naturali non vuoto contiene un numero che è più piccolo di tutti gli altri*

In altre parole, un qualsiasi sottoinsieme non vuoto dei numeri naturali ammette minimo.

Provate ad applicare tale principio a questo insieme:  $S = \{n | (n + 1)b < a\}$ .

#### Problema C.2.

Vogliamo trovare resto e quoziente della divisione:  $123456 : 365$ , cioè vogliamo  $q, r$  tali che  $123456 = q \cdot 365 + r$  con  $0 \leq r < 365$ . Non abbiamo per voglia di fare la divisione a mano, quindi usiamo la calcolatrice, ottenendo... Come facciamo dato questo valore a sapere quanto valgono  $q$  e  $r$ ?

#### Problema C.3.

Se  $(\bar{x}, \bar{y})$  è soluzione di  $ax + by = c$ , tutte le altre soluzioni si ottengono aggiungendo ad  $(\bar{x}, \bar{y})$  una soluzione intera  $(x_0, y_0)$  dell'equazione omogenea

associata  $ax + by = 0$ . Sapreste spiegare il perchè?

**Suggerimento:**

Provate proprio a scrivere la somma indicata nel problema... cosa potete dedurne?

**Problema C.4.**

Dimostrare che la relazione di congruenza modulo  $n$  ( $\equiv_n$ ) è una relazione di equivalenza.

**Suggerimento:**

Una relazione di equivalenza è una relazione riflessiva, cioè tale che  $a \equiv a \pmod n$ , simmetrica, cioè tale che se  $a \equiv b \pmod n$  allora  $b \equiv a \pmod n$ , e transitiva, cioè tale che se  $a \equiv b \pmod n$  e  $b \equiv c \pmod n$  allora  $a \equiv c \pmod n$ . Utilizzate semplicemente la definizione di congruenza.

## Esercizi

**Esercizio C.1.** Fate un esempio di divisibilità e uno di non divisibilità fra due numeri e nel secondo caso scrivete la divisione euclidea dei due numeri.

**Esercizio C.2.** Di che periodo storico sono Euclide, Diffie ed Hellman, Vernam e Gauss?

**Esempio C.1.** Di che periodo storico sono Vigenere, Shannon, Diofanto e Fermat?

**Esercizio C.3.** Cosa hanno proposto Diffie ed Hellman di così innovativo?

**Esempio C.2.** Che particolarità ha il cifrario di Vernam? Vi ricordate chi ha contribuito a chiarire questa proprietà?

**Esempio C.3.** A parole, cosa significa che un crittosistema è perfetto o assolutamente sicuro?

**Esercizio C.4.** Cos' è la crittanalisi e che metodi o tecniche utilizza?

**Esempio C.4.** Come funziona in generale la comunicazione di un messaggio attraverso la cifratura? Potete descriverlo sia a parole che con uno schema formalizzato.

**Esercizio C.5.** Se  $a|b$  e  $a|c$ , cosa possiamo dire e perchè?

**Esempio C.5.** Quando  $ax + by = c$  ha soluzioni? Ricordate per quale motivo?

**Esempio C.6.** Come facciamo a dire che i numeri primi sono infiniti?

**Esercizio C.6.** Qual'è il massimo comun divisore di 491 e 245?

**Esercizio C.7.** Quali sono rispettivamente i coefficienti di 491 e 245 nell'identità di Bézout per l'MCD(491,245)?

**Esempio C.7.** Qual'è il massimo comun divisore di 28762 e 1515?

**Esempio C.8.** Quali sono rispettivamente i coefficienti di 28762 e 1515 nell'identità di Bézout per l'MCD(28762,1515)?

**Esercizio C.8.** L'equazione  $92x + 28y = 180$  ha soluzioni intere?

**Esercizio C.9.** Come si scrive il numero 10 in base 2?

**Esercizio C.10.** Quanto valgono rispettivamente la somma e il prodotto di 10010111 e 11101 in base 2?

**Esercizio C.11.** 91 è primo? Se non lo è come potete fattorizzarlo?

**Esempio C.9.** La coppia (59,61) è formata da primi gemelli? E la coppia (61,63)?

**Esercizio C.12.** A quale parola corrisponde la sequenza di numeri 02 14 18 04 00 02 00 18 14?

**Esempio C.10.** Come potete scrivere in numeri la parola *esercizio*?





# Appendice D

## Articolo Odifreddi

### NUMERI PRIMI: LA SOLUZIONE DEI LORO ENIGMI VALE UN MILIONE DI DOLLARI

*Repubblica — 03 febbraio 2010 pagina 55 sezione: CULTURA*

La complessità del reale rende difficile, se non addirittura impossibile, una sua conoscenza esaustiva e ostensiva. Da sempre, dunque, si è cercato di ridurlo e classificarlo, all'insegna del Divide et impera dei conquistatori: ad esempio, Platone insegnava nel Fedro che «l'uomo deve necessariamente comprendere in funzione delle idee, procedendo da una molteplicità sensibile a un'unità intellettuale». In un progressivo percorso di semplificazione e astrazione, la rappresentazione della realtà è dunque stata ridotta dapprima a concetti, poi a ideogrammi, e così via, fino alle lettere dell'alfabeto che costituiscono un armamentario atto a rappresentare l'intera complessità del linguaggio, se non del pensiero. Naturalmente, il fatto che i simboli alfabetici siano ristretti a poche decine non impedisce loro di essere potenzialmente in grado di generare, combinandosi, una quantità illimitata di parole finite. Sembra comunque che non solo la sua rappresentazione, ma la stessa realtà fisica sia riconducibile a un armamentario finito da cui essa può essere ricostruita, a vari livelli: due esempi ormai entrati a far parte della cassetta degli attrezzi

scientifici a disposizione di qualunque studente delle superiori sono, da un lato, il centinaio di elementi atomici che formano la tavola di Mendeleev, le cui combinazioni permettono di ricostruire tutte le molecole della chimica, e dall'altro lato, le decine di particelle elementari come gli elettroni o i quark, alle quali è stata ridotta l'intera fisica subatomica. La situazione non è diversa in matematica, dove anche i numeri interi possono essere ricondotti a una serie di mattoni fondamentali che permettono di ricostruirli tutti. Se l'operazione di ricostruzione è l'addizione, allora c'è addirittura un unico mattone, l'unità: ogni numero intero, infatti, si può ottenere partendo dallo zero e aggiungendo un'unità, esattamente quel numero di volte (benché la cosa possa sembrare circolare, questa è in realtà una vera e propria definizione di «numero intero», proposta per la prima volta nel 1921 da Ludwig Wittgenstein nel suo famoso Trattato logico filosofico). Se invece l'operazione di ricostruzione è la moltiplicazione, le cose si fanno più complicate, ma anche più interessanti. Anzitutto, non ci vuol molto a capire che anche qui ci devono essere dei mattoni fondamentali, che sono semplicemente i numeri che non possono essere divisi per altri numeri, se non in maniera banale: cioè, dividendoli per l'unità o per se stessi, cosa che ovviamente si può sempre fare, con qualunque numero. Questi mattoni fondamentali si chiamano numeri primi, e ne sono esempi non banali (cioè, diversi da 1) i numeri 2, 3, 5, 7, 11, 13, ... Di nuovo, non ci vuol molto a convincersi che ogni numero si può scomporre in un prodotto di numeri primi. Infatti, può succedere che quel numero non sia divisibile per altri numeri: allora è primo esso stesso, e la cosa finisce lì. Se così non è, quel numero deve essere divisibile per altri numeri, ed è dunque il prodotto di due fattori, ciascuno dei quali sarà o primo, o divisibile: nel primo caso si è raggiunto un mattone fondamentale che compone il numero di partenza, e nel secondo caso si può ripetere la cosa e dividere a sua volta quel fattore in altri due fattori, e così via, fino a quando rimangono soltanto mattoni fondamentali (cosa che deve succedere, prima o poi, perché a ogni divisione i fattori diventano più piccoli, e prima o poi il procedimento si esaurisce). Senza quasi accorgercene, abbiamo dimostrato un teorema importante del-

l'aritmetica: che ogni numero intero si può scomporre nel prodotto di un numero finito di numeri primi. Ma negli Elementi di Euclide, la summa della matematica greca, si dimostra ingegnosamente qualcosa di più, che viene addirittura chiamato teorema fondamentale dell'aritmetica: precisamente, che la scomposizione in fattori primi di un numero è unica, nel senso che comunque si proceda si arriva sempre agli stessi fattori primi, a parte l'ordine. I numeri primi sono dunque veramente i mattoni dell'aritmetica, e la domanda più ovvia che ci si può fare, dato un numero, è se esso sia appunto primo, oppure no. La risposta si può sempre trovare, se si ha pazienza, perché basta provare a dividerlo per tutti i numeri minori, uno dietro l'altro, fino a che o si trova che uno di essi divide il numero, che allora non è primo, oppure nessuno di essi lo divide, e allora esso è primo. La cosa è facile da dire ma lunga da fare: per numeri con poche centinaia di cifre diventa impossibile in un tempo inferiore alla durata dell'universo! Secoli, anzi, millenni di tentativi per rendere il procedimento meno lungo e laborioso, sono culminati nel 2002 in un metodo veloce e sicuro per determinare se un numero è primo o no, trovato dai tre matematici indiani Manindra Agrawal, Neeraj Kayal e Nitin Saxena. Purtroppo, però, il loro risultato non fornisce un metodo altrettanto veloce e sicuro per scomporre in fattori un numero che non è primo. Lo farebbe, invece, una soluzione positiva al cosiddetto problema  $P=NP$ , il più importante dell'informatica teorica, che costituisce anche uno dei sette problemi del millennio, per la soluzione di ciascuno dei quali il miliardario americano Landon Clay ha offerto un premio di un milione di dollari, e ai quali Keith Devlin ha dedicato un omonimo libro (Longanesi, 2004). Il motivo per cui l'informatica si interessa ai numeri primi, è che la crittografia ha recentemente incominciato a usarli per produrre metodi di codifica delle informazioni a prova di bomba. O quasi, visto che questi metodi si basano tutti sull'assunzione che sia appunto impossibile trovare un metodo veloce e sicuro per determinare i fattori primi di un numero. E dopo il risultato dei tre matematici indiani le banche, le industrie, i politici e le spie di tutto il mondo hanno incominciato a tremare, perché se qualcuno riuscisse a fare il passo successivo, salterebbe-

ro i sistemi crittografici del mondo intero, usati dai bancomat alle carte di credito, dai telefoni alle e-mail. Nel 1994 un metodo del genere è già stato trovato da Peter Shor per i computer quantistici: dunque, un altro modo di risolvere il problema sarebbe di riuscire a costruirli, questi computer, che per ora esistono ancora soltanto sulla carta. Se il problema della fattorizzazione è tipicamente pratico e informatico, quello di capire come sono distribuiti i numeri primi è altrettanto tipicamente teorico e matematico. Il primo grande passo lo fecero, o almeno lo riportano, ancora una volta gli Elementi di Euclide, nei quali si trova la risposta alla domanda se i numeri primi siano finiti, oppure no: una domanda alla quale si potrebbe pensare di rispondere «ovviamente sì», visto che i numeri interi sono infiniti, ma che l'esempio delle infinite parole generate da un numero finito di lettere dimostra non essere così banale. La risposta di Euclide è «sì, ma non ovviamente». Anzi, la sua dimostrazione è uno dei gioielli della matematica, e consiste nel notare che, comunque si prenda un insieme di numeri primi, ce n'è sempre un altro che non sta fra loro. L'idea di Euclide è di moltiplicare tutti quei primi fra loro, e aggiungere uno: si ottiene così un numero, che o è primo, o non lo è. Se lo è, abbiamo costruito un nuovo numero primo. Se non lo è, deve avere un fattore primo, che non può essere nessuno di quelli di partenza: altrimenti, dividerebbe sia il loro prodotto, che il loro prodotto più uno, e dunque la loro differenza, mentre invece nessun numero non banale può dividere uno! Benché infiniti, i numeri primi non sono distribuiti uniformemente, e si diradano sempre più: ce ne sono 25 fra i primi 100 numeri, 168 fino a 1000, 1.229 fino a 10.000, 9.592 fino a 100.000, eccetera. Determinare esattamente la loro distribuzione, costruendo un analogo della tavola di Mendeleev per gli elementi chimici, costituisce un altro dei problemi del millennio da un milione di dollari, la cosiddetta ipotesi di Riemann. E, insieme al problema  $P=NP$ , essa dimostra come i due problemi più importanti e difficili della matematica e dell'informatica moderna riguardino in realtà oggetti e concetti già introdotti e affrontati dai Greci, facili da capire ma difficili da dominare, sui quali il pensiero si arrovella da millenni senza posa, a dimostrazione della

sua insuperabile limitatezza, ma anche della sua indomita audacia.

*PIERGIORGIO ODIFREDDI*



# Appendice E

## Dialogo sull'Orologio

giovedì 15 aprile 2010

Alice, Bob e Eva — L'orologio

“Che ore saranno tra 314 ore?”.

“Eh? Boh, devo fare il conto, non so”.

“Fai il conto, allora”.

“Uhm, 314 ore, ci sono 24 ore in un giorno, 314 diviso 24 fa 13.08(3)”.

“E quindi?”.

“E quindi 314 ore sono un po' più di 13 giorni”.

“Vabbé, ma se vuoi sapere che ore saranno con precisione?”.

“Uhm, allora, rimane un resto di zero virgola zero otto tre periodico...”.

“Che non è propriamente un resto”.

“Eh?”.

“Eh, no. Non è il resto della divisione che hai fatto. Hai presente la regola per la divisione che hai imparato alle elementari?”.

“Uh, quella! Da quanto tempo non ne faccio una. Eccola qua:”.

$$\begin{array}{r|l} \widehat{314} & 24 \\ 74 & 13 \\ \hline \textcircled{2} & \end{array}$$

“Oh, bene. Quindi vedi che 314 diviso 24 ti dà come quoziente 13 e come resto 2. Quello che ti interessa, ai fini della risposta alla mia domanda, è proprio il resto”.

“Ah, ho capito: 314 ore corrispondono a 13 giorni e 2 ore, quindi per sapere che ore saranno devo guardare l’orologio adesso e aggiungere 2 ore. Facile”.

“Benissimo. Il calcolo che hai fatto potrebbe essere scritto anche in questo modo:  $314 = 13 \cdot 24 + 2$ ”.

“Vero”.

“I Veri Matematici lo scrivono anche così:  $314 \equiv 2 \pmod{24}$ ”.

“Eh?”.

“Significa che 314 e 2 danno lo stesso resto nella divisione per 24; il resto è naturalmente 2, che è minore di 24. Si legge in questo modo: 314 è congruente (o congruo) a 2 modulo 24”.

“Manca però il 13, il quoziente della divisione”.

“Quello non ci interessa molto. Quando siamo interessati di più ai resti che ai quozienti, utilizziamo questo tipo di scrittura. Ed entriamo nel cosiddetto campo dell’aritmetica modulare”.

“Che non è altro che un modo pomposo per definire l’aritmetica dell’orologio, a quanto vedo”.

“Bè, sì, l’aritmetica dell’orologio è l’aritmetica modulo 24, ma naturalmente possiamo scegliere qualunque numero come base per i nostri moduli”.

“E questo è interessante?”.

“Certo”.

“Voglio dire, serve a qualcosa?”.



“Stranamente, sì. Non che ai Veri Matematici questo fatto interessi molto, però l'aritmetica modulare ha una effettiva applicazione pratica. Praticamente quotidiana”.

*ROBERTO ZANASI*



# Appendice F

## Questionario di Valutazione

### Questionario di valutazione del Progetto di Crittografia

Rispondi alle seguenti domande dopo averle lette attentamente. Esprimi il tuo parere con sincerità e ricordandoti che i questionari sono anonimi e servono esclusivamente alla valutazione dell'operato del docente e del progetto da lui presentato... per una volta sta a te giudicare!

#### Materiali e Strumenti

In una scala da 1 a 7, indica quanto ritieni che i seguenti materiali e strumenti utilizzati durante le lezioni siano risultati utili e funzionali.

1. Video ..... 1 2 3 4 5 6 7
2. Lettura articolo/libro ..... 1 2 3 4 5 6 7
3. Dialoghi stampati ..... 1 2 3 4 5 6 7
4. Giochi di logica (lucchetti) ..... 1 2 3 4 5 6 7
5. Decifrazione dei file inviati ..... 1 2 3 4 5 6 7

6. Presentazione tramite slides e lavagna ..... 1 2 3 4 5 6 7
7. Comunicazione via e-mail ..... 1 2 3 4 5 6 7
8. Quale di questi approcci o strumenti ti ha colpito di più e perché? Puoi indicarne più d'uno.
9. Il materiale didattico fornito (escluse le dispense) ti è stato utile?
10. Come hai trovato le dispense fornite? Commentale brevemente.

### Esposizione e Metodo

In una scala da 1 a 7, indica quanto ritieni che le seguenti peculiarità del metodo espositivo e didattico utilizzato durante le lezioni siano risultate utili ed interessanti.

1. Inquadramento storico del tema ..... 1 2 3 4 5 6 7
2. Approccio pratico e applicativo alla materia ..... 1 2 3 4 5 6 7
3. Ripassi e richiami a inizio lezione ..... 1 2 3 4 5 6 7
4. Approccio interattivo (domande del docente, risoluzione di problemi, costruzione di dimostrazioni) ..... 1 2 3 4 5 6 7
5. Lavori di gruppo ..... 1 2 3 4 5 6 7

Di seguito ti viene richiesto di esprimere una sincera opinione sull'operato del docente e le lezioni da lui tenute: 1 equivale a completamente falso, 7 a completamente vero.

6. Le lezioni sono state chiare e comprensibili ..... 1 2 3 4 5 6 7
7. Le spiegazioni sono state eccessivamente veloci ..... 1 2 3 4 5 6 7
8. Le lezioni sono state molto noiose ..... 1 2 3 4 5 6 7

9. Il docente stimolava l'interesse per la materia ..... 1 2 3 4 5 6 7
10. Il docente era effettivamente reperibile  
e disponibile ..... 1 2 3 4 5 6 7
11. Eventuali suggerimenti

### Argomento e Prospettiva

Di seguito 1 equivale a "per nulla" mentre 7 a "molto".

1. L'argomento trattato è di tuo interesse? ..... 1 2 3 4 5 6 7
2. Desidereresti approfondirlo? ..... 1 2 3 4 5 6 7
3. Quale aspetto ti è interessato maggiormente? Perché?
4. Quale invece non ti è interessato o non ti è piaciuto? Perché?
5. Questa esperienza ha modificato la tua visione della matematica? Se  
sì in che modo?
6. Ti ha fatto riflettere su qualche aspetto in particolare della matematica  
o in generale della cultura? Se sì in che modo?
7. Ti è sembrata diversa la matematica introdotta in questo progetto  
rispetto a quella che vedi di solito?
8. Che idea ti sei fatto delle dimostrazioni matematiche? Rispecchia  
quello che già pensavi prima?
9. Cosa cambieresti del progetto nel suo insieme?

Grazie per la tua collaborazione!

Le tue risposte serviranno ad un futuro insegnante nel suo percorso di preparazione all'insegnamento. Le tue opinioni (sincere speriamo!) gli serviranno a farsi un'idea sul modo migliore per impostare lezioni di matematica che

siano al contempo utili ai fini didattici (svolgimento del programma ministeriale), divertenti e coinvolgenti dal punto di vista umano e, ultimo ma non meno importante, intellettualmente stimolanti.

Per qualsiasi dubbio, curiosità, chiarimento e, ovviamente, critica, non esitare a contattare: Marco Garulli.

# Bibliografia

- [1] Arrigo, G., (2003) *Matematica e formazione del pensiero, Atti del Convegno "Incontri con la matematica"*, Castel San Pietro Terme, n. 17;
- [2] Du Sautoy, M., (2004) *L'enigma dei numeri primi. L'ipotesi di Riemann, il più grande mistero della matematica*, Milano, Rizzoli;
- [3] Brousseau, G., (1980) "Les échecs électifs dans l'enseignement des mathématiques à l'école élémentaire", *Revue de laryngologie, otologie, rhinologie*, 101, 3-4, 107-131;
- [4] D'Amore, B., (1999) *Elementi di Didattica della Matematica*, Bologna, Pitagora Editrice;
- [5] Schubauer-Leoni, M.L., Ntamakiliro, L., (1994) "La construction de réponses à des problèmes impossibles", *Revue des sciences de l'éducation*, XX, 1, 87-113;
- [6] MIUR-Confindustria-Con.Sienze, (17 Giugno 2004) *Progetto Lauree Scientifiche*;
- [7] Ministero dell'Istruzione, dell'Università e della Ricerca, (29 Aprile 2010) *Il Piano Lauree Scientifiche. Linee Guida*, Roma;
- [8] Mezzetti, E., (2008) (a cura di), *Relazione sull'attività svolta nel biennio accademico 2005-2007, Progetto lauree scientifiche*, Università degli Studi di Trieste;

- 
- [9] Anzelotti, G., Mazzini, F., (2007) Il progetto di orientamento e di formazione degli insegnanti - Area matematica (PLS-OFI-MAT), *Annali della pubblica istruzione*, n. 2/3, P. 59-105;
- [10] Ferrari, C., (2009) Un approccio alla teoria dei numeri in prima liceo basato sulla crittografia per stimolare la curiosità dell'allievo e migliorare la qualità dell'apprendimento, unpublished, Liceo di Locarno;
- [11] Lockhart, P., (2010) *Contro l'ora di matematica. Un manifesto per la liberazione di professori e studenti*, Milano, Rizzoli;
- [12] Bolondi, G., D'amore, B., (2010) *La matematica non serve a nulla. Provocazioni e risposte per capire di più*, Bologna, Editrice Compositori;
- [13] Rizzi, A., (2008) *Crittografia: dai cifrari classici alla sicurezza web*, Roma, Cisu;
- [14] Baldoni, M.W., Ciliberto, C., Piacentini Cattaneo, G.M., (2006) *Aritmetica, crittografia e codici*, Milano, Springer-Verlag;
- [15] Sgarro, A., (1986) *Crittografia: tecniche di protezione dei dati riservati*, Padova, Muzzio;
- [16] Leonesi, S., Toffalori, C., (2006) *Numeri e crittografia*, Springer Verlag;
- [17] Beckman, B., (2005) *Codici cifrati: Arne Beurling e la crittografia nella II guerra mondiale*, Milano, Springer;
- [18] Buchman, J., (2001) *Introduction to Cryptography*, New York, Springer-Verlag.



# Ringraziamenti

Questa tesi, così come questo percorso di cinque anni all'interno del mondo della matematica universitaria, non sarebbero stati possibili senza il prezioso aiuto di molte persone. Spero che ognuno di Voi sappia quanto e come è stato importante per me.

Tra le persone che non posso non ringraziare, i primi sono sicuramente il Chiar.mo Prof. Giorgio Bolondi per avermi aiutato e consigliato nella stesura del presente lavoro e la Prof.ssa Elettra Battitori per avermi concesso la possibilità di svolgere il progetto nella sua classe e per avermi assistito durante tutto il percorso.

Desidero inoltre porgere i miei ringraziamenti a coloro che mi hanno sostenuto costantemente e che hanno creduto in me: i miei genitori Francesca ed Alberto e la mia ragazza Valentina, che mi ha suggerito numerose idee affiancandomi come una vera musa.

Un grande supporto mi è stato fornito anche dai miei compagni di corso, che ringrazio per la loro presenza ed amicizia: Marco M., Marco S., Elisa, Chiara, Cristina, Armijo, Giacomo e Jacopo.

Grazie davvero, non si raggiunge mai alcun obiettivo se si è soli. . .