Sorprendenti applicazioni di Algebra e Geometria

Ciro Ciliberto, Università di Roma Tor Vergata

PISTOIA, SETTEMBRE 2013

Vorrei parlare ...

... di matematica solitamente ritenuta, dagli stessi matematici di professione, molto astratta: cioè ALGEBRA e GEOMETRIA.

Il termine ALGEBRA deriva dal titolo del libro del matematico arabo persiano Muhammad ibn Musa al–Kwarizmi (780–850), intitolato Al-Kitab al-Jabr wa-l-Muqabala, cioè Compendio sul Calcolo per Completamento e Bilanciamento, che tratta la risoluzione delle equazioni di primo e di secondo grado in vista di applicazioni a problemi molto concreti.

L'algebra ...

... e in particolare l'aritmetica o teoria dei numeri, fu importata in occidente nel secolo XIII per motivi assai pratici, cioè per far di conto negli affari, principalmente da Leonardo Fibonacci (1170–1250), autore del Liber Abaci e Practica Geometriae.

Il primo a usare il termine algebra nel mondo occidentale fu il maestro d'abaco fiorentino Raffaello di Giovanni Canacci, autore dei Ragionamenti di Algebra (1490).

Geometria ...

... viene dal greco

$$\gamma\epsilon\omega\mu\epsilon\tau\rho\iota\alpha$$

che significa misura della terra. Dunque le sue origini molto concrete sono fuori di ogni dubbio.

Nel 1940, G. H. Hardy scrive in “A mathematician’s apology” ...

... Gauss e altri matematici possono essere giustificati nel rallegrarsi del fatto che vi sia soprattutto una scienza, la teoria dei numeri, quella che loro hanno coltivato, la cui lontananza dalle ordinarie attività umane ne preservi la dolcezza e purezza.

Ma Hardy si sbagliava: già durante la seconda guerra mondiale Alan Turing, inventore dell’informatica teorica, che era stato collega di Hardy a Cambridge, lavorava come crittografo per i servizi segreti britannici per decifrare, usando tecniche algebriche, in particolare teoria dei numeri, i messaggi in codice dei tedeschi trasmessi con la macchina Enigma.

Crittografia

La crittografia si occupa del seguente:

Problema

Come si fa a comunicare in modo segreto e sicuro?

Come si fa a inviare messaggi cifrati che possano essere facilmente decifrati dai destinatari ma non da chi non sia autorizzato?

Questo problema è estremamente attuale ai giorni nostri, in cui le comunicazioni sono essenziali, frequenti, facili e molto rapide, e richiedono riservatezza, ma sono anche molto vulnerabili.

Applicazioni

Sono ubique, in ambito militare, industriale, privato ...

La crittografia nell'antichità

- Erodoto (Alicarnasso, V sec. a.C.), *Le Storie*, Libro V e Libro VII: steganografia (procedura che consiste nel nascondere i messaggi).
- Svetonio (II sec. d.C.), *Vite dei Cesari*: Giulio Cesare, per scopi militari, usava semplici modelli matematici per la crittografia (che consiste nel nascondere non il messaggio ma il suo significato).
- Il tipico esempio consiste nello spostare di tre lettere, rispetto alla posizione nell'alfabeto, ogni lettera del messaggio da inviare.

Equivalenti numerici delle 26 lettere

a $\longrightarrow$ 0	h $\longrightarrow$ 7	o $\longrightarrow$ 14	u $\longrightarrow$ 20
b $\longrightarrow$ 1	i $\longrightarrow$ 8	p $\longrightarrow$ 15	v $\longrightarrow$ 21
c $\longrightarrow$ 2	j $\longrightarrow$ 9	q $\longrightarrow$ 16	w $\longrightarrow$ 22
d $\longrightarrow$ 3	k $\longrightarrow$ 10	r $\longrightarrow$ 17	x $\longrightarrow$ 23
e $\longrightarrow$ 4	l $\longrightarrow$ 11	s $\longrightarrow$ 18	y $\longrightarrow$ 24
f $\longrightarrow$ 5	m $\longrightarrow$ 12	t $\longrightarrow$ 19	z $\longrightarrow$ 25
g $\longrightarrow$ 6	n $\longrightarrow$ 13		

Aritmetica modulare (I)

Scegliamo un numero naturale

$$n \in \mathbb{N} = \{1, 2, ...\}$$

Ad ogni numero intero

$$x \in \mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$$

possiamo associare

$$x \bmod n \in \mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$$

che è il resto della divisione di x per n.

Esempi

$$3 \bmod 2 = 1, \quad 3 \bmod 4 = 3, \quad 100 \mod 9 = 1$$

$$7 \bmod 5 = 2, \quad 11 \bmod 3 = 2, \quad 137 \mod 6 = 5$$

Aritmetica modulare (II)

- Con i numeri di $\mathbb{Z}_n$ possiamo operare sommandoli, sottraendoli e moltiplicandoli e poi prendendo il resto della divisione per n;
- il cifrario di Cesare consiste nel sommare ad ogni numero di $\mathbb{Z}_{26}$ un fissato numero C, che è la chiave per cifrare. La chiave per decifrare è $C' = -C = n - C$;
- questo sistema di cifratura si può raffinare in vari modi, rendendolo più complicato (L. B. Alberti XVI sec., B. de Vigenère XVII sec.);
- complesse macchine prima meccaniche, poi elettro–meccaniche, per cifrare e decifrare con sistemi consimili sono state usate nel corso della storia fino a tempi recenti, ad es. la macchina Enigma.

Crittoanalisi

- La crittoanalisi consiste nello sviluppare tecniche atte a decifrare messaggi cifrati, di cui non conosciamo la chiave.
- Ad esempio, come si fa a decifrare un messaggio in codice inviato col cifrario di Cesare, se non conosciamo la chiave?
- Si usa l'analisi delle frequenze.

Lettera	%	Lettera	%	Lettera	%
a	11,74	h	1,54	q	0,51
b	0,92	i	11,28	r	6,38
c	4,50	l	6,51	s	4,98
d	3,73	m	2,52	t	5,63
e	11,79	n	6,88	u	3,02
f	0,95	o	9,83	v	2,10
g	1,65	p	3,05	z	0,49

Un esempio di crittoanalisi (I)

Vogliamo decifrare il messaggio:

```
IN DNHHN OFZHHRIRGN ON A DNHHATA LAZLCA
```

Frequenza delle lettere nel messaggio:

Lettera	Occorrenze	Lettera	Occorrenze	Lettera	Occorrenze
A	5	H	6	Q	0
B	0	I	2	R	2
C	1	L	2	S	0
D	2	M	0	T	1
E	0	N	6	U	0
F	1	O	2	V	0
G	1	P	0	Z	2

Un esempio di crittoanalisi (II)

- L'analisi delle frequenze suggerisce che:

A=i, N=a, I=l, Z=o, R=u, H=t

- Otteniamo:

`la Datta OFottuluGa Oa i DattiTi LioLCi`

.

- Con un po' di buonsenso perveniamo alla soluzione:

`la gatta frettolosa fa i gattini ciechi`

- Metodo analogo per la interpretazione di lingue sconosciute: es. lineare B cretese (A. Evans, 1900).

Quanto costano crittografia e crittoanalisi?

- I numeri si rappresentano con scrittura posizionale in una data base b, che è numero intero maggiore di 1.
- Di solito usiamo $b = 10$:

$$1.498.742 = \mathbf{1}\cdot 10^6 + \mathbf{4}\cdot 10^5 + \mathbf{9}\cdot 10^4 + \mathbf{8}\cdot 10^3 + \mathbf{7}\cdot 10^2 + \mathbf{4}\cdot 10^1 + \mathbf{2}\cdot 10^0.$$

- I computer usano la base $b = 2$:

$$(1111110110000)_2 = \mathbf{1}\cdot 2^{12} + \mathbf{1}\cdot 2^{11} + \mathbf{1}\cdot 2^{10} + \mathbf{1}\cdot 2^9 + \mathbf{1}\cdot 2^8 + \\ + \mathbf{1}\cdot 2^7 + \mathbf{0}\cdot 2^6 + \mathbf{1}\cdot 2^5 + \mathbf{1}\cdot 2^4 + \mathbf{0}\cdot 2^3 + \mathbf{0}\cdot 2^2 + \mathbf{0}\cdot 2^1 + \mathbf{0}\cdot 2^0$$

che in base 10 si scrive 8.112.

La lunghezza dei numeri

- La lunghezza $L(n)$ di un numero n è il numero di cifre che occorrono per scriverlo in base 2. La lunghezza è una misura della grandezza di un numero.
- Notiamo che $L(n)$ è in generale molto minore di n. Precisamente, si ha

$$\boxed{L(n) \sim \log_2 n}$$

- Ad esempio

$$L(8.112) = 12.$$

Come si fanno le operazioni?

Riporti

$$\begin{array}{cccccccccc} & & 1 & 1 & 1 & 1 & 1 & 1 & & \\ & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & + \\ & & & & & 1 & 0 & 1 & 1 & = \\ \hline & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & \end{array}$$

$$\begin{array}{cccccccccc} & & & & & 1 & 1 & 1 & 0 & 1 & \times \\ & & & & & & 1 & 1 & 0 & 1 & = \\ \hline & & & & & 1 & 1 & 1 & 0 & 1 & \\ & & & 1 & 1 & 1 & 0 & 1 & - & - & \\ & & 1 & 1 & 1 & 0 & 1 & - & - & - & \\ \hline & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & \end{array}$$

Algoritmi e loro complessità

Il termine Algoritmo ha origine dal nome di Muhammad ibn Musa al–Kwarizmi.

- Un algoritmo (deterministico) $\mathcal{A}$ è una procedura di calcolo con numeri interi, consistente in una successione finita di operazioni elementari, volta a risolvere con certezza un problema di calcolo;
- la complessità di $\mathcal{A}$ è il numero di operazioni elementari che occorre effettuare per eseguire $\mathcal{A}$;
- il tempo $T(\mathcal{A})$ per eseguire $\mathcal{A}$ è proporzionale alla sua complessità;
- $\mathcal{A}$ è polinomiale se la sua complessità per eseguire calcoli con numeri di lunghezza k è approssimativamente k^d, con d numero intero positivo;
- $\mathcal{A}$ è esponenziale se la sua complessità per eseguire calcoli su numeri di lunghezza k è approssimativamente 2^k (cioè praticamente pari al numero stesso).

Algoritmi polinomiali

- In generale costa poco effettuare algoritmi polinomiali.
- Ad esempio

$$T(a+b) = \text{costante} \cdot \max\{L(a), L(b)\}$$
$$T(a \cdot b) = \text{costante} \cdot (L(a) + L(b))$$

  e la costante dipende dallo strumento di calcolo.
- Quindi, effettuare somme e prodotti costa poco.
- Vi sono algoritmi polinomiali per effettuare sottrazioni, divisioni e per il calcolo di MCD e MCM.
- La crittografia classica, che è basata su questi algoritmi, costa poco.
- Ma allora costa poco anche la crittonalisi: dunque la crittografia classica è molto vulnerabile.

Ad esempio...

... ecco 200 numeri tra 1 e 1.000.000, generati a caso dal computer:

651789,106737,549047,590588,189111,334832,664168,81364,624419,737973,873545,559792,643004,820024,461744,
865331,510367, 675227,353689,256245,953389,924572,525925,986892,395998, 802914,453642,57974,
755766,257215,977252,943634,960154,62604, 112900, 711544,962059,865516,624106,390715,479251,956418,
494787,427643,237209,195559,712266,936699, 741422,180394,270653,636106,34453,268619,
154640,215232,694682,997579, 160255, 603540,685489,311714,503197,543597,925731, 130972,81364,980960,
246087,757874, 113785,251885,310348,911910, 14202,507086,958763, 521543,
747215,825884,247586,31167,87149,896038,696722, 128184, 500851,960796,
747612,309093,530278,548056,929428,579874, 407458,976429,856543,527658,31403,442276,
726631495074,65420,869822,38929,855607,761661,46068,253922,333916,364426,94574,104329,864189,829905,
975230,543589,228939,119623,414781,180070,31044,751512,916063,119692,586026,964607,262675,927807,678508,
866942,239677,889715,44069,400565,403182,20896,897446,79287,325602,698195,760643,4533,375022,
70172,278585,434374,439845,361287,227234,42067,716457,284318,920152,342427,
219109,489634,566960,190650,625899,586313,851322,349578,
458325,513274,458413,54285,155256,264543,935403,771700,795635,86881,623206,692723,817266,412336,147342,
691355,438272,323100, 262429,204178,824438,964016,265764,865808,655728,569467,
577996,574447,382042,929291,479344,980752,386127,689869, 988139,511037,139324

In un attimo ...

... il computer dà la loro somma:

102443688

... il loro prodotto

38176139217436633964610237281480709501284608489074045347750594869957807602946646860209475037663795771908685823155493346260882729242879539830745705498194911160817877935949924083066474283125702767433007364012013794524930131805924827946323237421626104847383405418284097300664285736754864813013388261791801741342161168031484852447369462680550003611080185542210518044866284543542896328337969412992584022030447104848065168772901232705058027459473384011727537172971706970882752739514240358734496443859866446039027264539271637090881719306189103372824349021200116770425634383659079648206673424421904259487691530535472950755612406251413388764190630548014686685717147074196079956133388870136958788526032949314266960122379565318227301818656547112073879298774308545219003004977116357523805010767407159035258314501957578725052997561822774762171064489922918411299587791706723541946504646921611084580009593027136284619288564003946365140024827909052139268468602068036891757128813455379087629166945162177723475555855068177161715790159570311630195541229502136442597487291213399976309517090553856000000000000000000000000000000000000000000000000000000000000
... e il loro minimo comune multiplo...

77541156234563311888401182527972780904194704826340663337182708885466648049120062315739994813426347150844238387827678448732097224203202628416074605764433327518946090201841990314837366648347323754423487958549146783406677446261861958729596734835420459653208469181692602894610044782886750162031643029315735009183564028776433718916181036909411554961087385219988961778179175453343103102930420397909805111491496976267873779846965639944631538092736904360691453295561868427868889149871789543098171582898856898030823605905938673133291508218838803751821218979892739106520639396870149779289825794237542836591707574297713571086273497417517323960102453489279607930643795330770260660125247766610410262407179353364463 1065344794530197318391006434719532335691345612800

Quali algoritmi costano molto?

Esempio

Decomporre un numero nel prodotto dei suoi fattori primi.

- Ogni numero si può fattorizzare, in modo unico nel prodotto di numeri primi.
- Essenzialmente c'è un unico algoritmo per ottenere questa fattorizzazione: il crivello di Eratostene.
- Esso consiste nel provare a dividere un numero n per tutti i numeri da 2 a $\sqrt{n}$.
- La complessità di esecuzione del crivello di Eratostene su un numero n è

$$\boxed{n \log_2 n}$$

dunque (più che) esponenziale, cioè molto più grande di quel che occorre per sommare o moltiplicare numeri della lunghezza di n.

Nella prima riga della tabella compare la complessità dell'algoritmo a fronte della lunghezza n dell'input. Nelle righe successive la durata a fronte di vari valori di n, supponendo che il tempo occorrente per eseguire ogni operazione elementare sia di 10^{-9} secondi.

n	$\log_2 n$	$n \log_2 n$	n^2	2^n	$n!$
10	$3 \cdot 10^{-9}$ s	$3 \cdot 10^{-8}$ s	10^{-7} s	10^{-6} s	$3 \cdot 10^{-3}$ s
10^2	$7 \cdot 10^{-9}$ s	$7 \cdot 10^{-7}$ s	10^{-5} s	$4 \cdot 10^{13}$ a	$> 10^{100} a$
10^3	10^{-8} s	10^{-5} s	10^{-3}	$> 10^{100} a$	$> 10^{100} a$
10^4	$1.3 \cdot 10^{-8}$ s	10^{-4} s	10^{-1} s	$> 10^{100} a$	$> 10^{100} a$
10^5	$1.7 \cdot 10^{-8}$ s	$2 \cdot 10^{-3}$ s	10 s	$> 10^{100} a$	$> 10^{100} a$
10^6	$2 \cdot 10^{-8}$ s	$2 \cdot 10^{-2}$ s	17 m	$> 10^{100} a$	$> 10^{100} a$

Osservazione

Il numero di protoni nell'universo è $\sim 10^{79}$.

Un commento sul crivello di Eratostene

- la complessità $n \log_2 n$ non è poi male se operiamo su numeri non troppo grandi. Ad esempio, se usiamo un buon PC:
- **Input**: fattorizzare il numero di Mersenne $2^{67} - 1$.
- **Output**: dopo una frazione di secondo otteniamo

$$2^{67} - 1 = 193707721 \cdot 761838257287$$

- Lo stesso risultato fu ottenuto da Frank Cole, 1903, Meeting of the American Mathematical Society in San Francisco: “Three years of Sundays”.

L'importanza di essere primo

- Inumeri primi sono infiniti (Euclide, III sec. AC) e sono i mattoni costitutivi dei numeri, perché da loro si ottengono, per moltiplicazione, tutti gli altri numeri.
- L'individuazione e la distribuzione dei numeri primi sono problemi basilari della matematica: il primo è risolto, il secondo presenta ancora vaste zone d'ombra.
- Uno dei sette Problemi del Millennio, posti all'attenzione dei matematici dal Clay Mathematics Institute il 24 maggio 2000 con un premio di un milione di dollari per la soluzione di ciascuno di essi, riguarda la cosiddetta Ipotesi di Riemann, una congettura formulata da Bernard Riemann nel 1859, la cui soluzione getterebbe piena luce sulla distribuzione dei numeri primi.

Secondo K. F. Gauss (Disquisitiones Aithmeticae, 1801) ...

[...] Il problema di distinguere i numeri primi dai numeri composti e di decomporre questi ultimi nei loro fattori primi è ben noto essere uno dei più importanti ed utili in matematica.

[...] La dignità della scienza stessa sembra richiedere che sia esplorata ogni via possibile per la soluzione di un problema così celebre ed elegante.

[...] Le tecniche finora note richiederebbero una fatica intollerabile perfino per il calcolatore più infaticabile.

K. F. Gauss (1777–1855)

B. Riemann (1826–1866)

I numeri di Mersenne

- Anticamente si riteneva che, se p è primo, lo è anche
$$M_p = 2^p - 1$$
- Questo è vero per $p = 2, 3, 5, 7, 17, 19$, ma non per
$$M_{11} = 23 \cdot 89$$
- M. Mersenne (1588–1648) in *Cogitata Physico–Mathematica* (1644): M_{31} è primo, più alcune congetture sbagliate, come M_{67} è primo.
- Per i numeri di Mersenne M_p esiste l'efficace test di primalità di Lucas–Lehmer: Lehmer prova negli anni '30 che $M_{127} \sim 10^{39}$ è primo.

M. Mersenne (1588–1648)

Numeri da record!

- Il più grande numero primo noto è il numero di Mersenne

$$2^{57.885.161} - 1, \quad \text{ha } 17.425.170 \text{ cifre decimali}$$

  Trovato da Curtis Cooper, University of Central Missouri, il 25 gennaio 2013 dopo 39 giorni di calcolo ininterrotto nell'ambito del progetto Great Internet Mersenne Prime Search (GIMPS) che è un progetto di calcolo condiviso su Internet su larga scala.
- I primi dieci più grandi numeri primi noti sono numeri di Mersenne.
- Per informazioni, cfr. i siti

  http://primes.utm.edu/
  http://www.mersenne.org/

M. Agrawal, N. Kayal, N. Saxena, Primes is in P, Annals of Mathematics, 160 (2004), 781–793: algoritmo AKS

- È un algoritmo polinomiale che determina se n è primo in un tempo polinomiale $\sim \log_2^{11} n$.
- Dato un numero, AKS ci informa se ne esiste un divisore non banale. Se sì, sappiamo che esiste un fattore primo, ma non ne sappiamo calcolare nessuno! Dunque AKS non risolve del tutto il problema posto da Gauss perchè non dà la fattorizzazione.
- Ad esempio, dato il numero di 700 cifre decimali

$$
\begin{aligned}
&260783078086802291630898489158398374001918523623118809818074881183730174756775297234360159843071544592612061134688545949381918633952227696873251782511679728083146853148841350191425592418691900448569721209805524889482723239193470418630024145705141510215908950847034964857801938033370437862988355489743074622758085072132585346254113277829934672391731598156402883831557775410394925101802244529638774275753641388000789851431439455183474732311869931221824074970424099882433532151343127434641524327098918152279835078277614311792378450164328137706610236628327542724765609332704733232053534386942833969092082010370617236614698065633264586518280542850931392543736288869497283325586500087279040192598219394393519580337547286758545808695284570599 3
$$

- In pochi passi di calcolo l'algoritmo AKS ci informa che ne esiste un divisore non banale. Però l' algoritmo AKS non ci dice come trovare un tale divisore.

Nuove esigenze in crittografia

- Nei cifrari classici la decifratura è simmetrica rispetto alla cifratura sia da un punto di vista logico, sia da un punto di vista computazionale.
- In particolare i sistemi crittografici classici riguardano lo scambio di messaggi tra due soli utenti e sono basati sullo scambio di una chiave che consente cifratura e decifratura.
- Oggi invece c'è l'esigenza che possano comunicare fra loro più soggetti che non si conoscono tra loro e che quindi non hanno avuto, in linea di principio, la possibilità di scambiarsi chiavi private di cifratura.
- È pertanto indispensabile trovare nuovi, e più sicuri, metodi per crittare i messaggi. Questo è l'obiettivo della crittografia a chiave pubblica.
- Paradossalmente, essa è basata proprio sulla difficoltà di determinare i fattori primi di numeri grandi.

Crittografia a chiave pubblica

- Un cifrario a chiave pubblica permette di divulgare il metodo ed anche la chiave di cifratura, senza per questo rivelare il modo di decifrare.
- Infatti, per decifrare, è necessario essere in possesso di informazioni aggiuntive oltre a quelle rese pubbliche.
- Tali informazioni sono tenute segrete. Senza di loro la complessità di calcolo della decifratura è presumibilmente tale da renderne implausibile l'esecuzione.
- L'idea su cui ciò si basa è semplice: il sapere fare facilmente una certa operazione non implica che sappiamo fare altrettanto facilmente anche l'operazione inversa.

Un paio di esempi

- Si pensi all'elenco telefonico di una grande città.
- È facile trovare il numero di una persona se ne conosciamo il cognome, ma è in pratica impossibile risalire dal numero al cognome della persona.
- Si pensi ora di avere a disposizione due numeri primi p e q molto grandi, e pressocchè di eguale grandezza: $p \sim q$.
- Il loro prodotto

$$\boxed{n = pq \sim p^2 \sim q^2}$$

  è facile da calcolare, ed è ancora più grande.
- D'altra parte, se conosciamo n, senza sapere che è il prodotto di p e q, e ne cerchiamo i fattori primi con il crivello di Eratostene, saremo costretti ad effettuare circa $p \sim q$ prove, il che richiede un tempo enorme, ed è in pratica impossibile da effettuare con gli attuali sistemi di calcolo.

Il sistema RSA

- È basato sulla difficoltà di fattorizzare numeri con fattori primi grandi.
- Ideato da W. Diffie e M. E. Hellman (1976).
- Realizzato da L. M. Adleman, R. L. Rivest, A. Shamir del **Massachusetts Institute of Technology** (1978).

Applicazioni:

- spedizione di messaggi cifrati tra innumerevoli utenti;
- autentica elettronica della firma;
- accesso ad archivi segreti o sistemi di sicurezza;
- accesso a servizi come carte di credito, programmi televisivi a pagamento, telefonia cellulare, ecc.

Sensi unici e trappole

- Da un punto di vista matematico, la realizzazione dei crittosistemi a chiave pubblica è basata sul concetto di funzione a senso unico.
- Si tratta in sostanza di una funzione biettiva definita mediante un calcolo facile da fare, ma tale che il calcolo della sua inversa risulta in pratica impossibile da effettuare perchè la sua complessità è troppo grande.
- Si parla invece di funzione trappola se con qualche informazione aggiuntiva diventa computazionalmente fattibile effettuare anche il calcolo della inversa.
- Queste funzioni si usano per la cifratura in un sistema a chiave pubblica.

Iscrizione al sistema RSA

- Ci iscriviamo fornendo la nostra chiave pubblica di cifratura.
- La chiave è una coppia di numeri interi positivi (n, e), dove:
- n è prodotto di due numeri primi grandi p e q che conosciamo solo noi;
- e non ha fattori primi in comune con $p - 1$ e con $q - 1$.
- Per ogni utente U, la chiave (n_U, e_U) viene pubblicata in un elenco di dominio pubblico.
- Non viene però resa pubblica la fattorizzazione $n = p \cdot q$ che è il dato indispensabile per ottenere la chiave di decifratura.

Come funziona

- Vogliamo inviare un messaggio a Beatrice, la cui chiave è $(n_B, e_B) = (1003, 3)$. Si ha

$$\boxed{1003 = n_B = p_B \cdot q_B = 17 \cdot 59}$$

- Supponiamo il messaggio consista del numero

$$\boxed{P = 11}$$

- Cifriamo P mandando a Beatrice

$$\boxed{C = P^{e_B} \bmod n_B = \text{resto della div. di } \quad P^{e_B} \text{ per } \quad n_B}$$

cioè

$$\boxed{C = 328}$$

Come fa Beatrice a decrittare?

- Sfruttando la sua conoscenza della fattorizzazione di $n_B = 1003$, Beatrice determina, e tiene segreta, la chiave per decrittare che è un numero d_B tale che

$$(P^{e_B})^{d_B} \bmod n_B = P, \text{per ogni numero } P$$

- **Osservazione cruciale**: determinare d_B sostanzialmente equivale a trovare la fattorizzazione di n_B.
- In questo caso

$$\boxed{d_B = 619}$$

e quindi

$$C^{d_B} = 328^{619} \bmod 1003 = 11$$

Sicurezza del sistema RSA (I)

- Nel 1977 Rivest, Shamir e Adleman sfidarono i lettori della rivista Scientific American a decifrare un messaggio, il che corrispondeva a fattorizzare il numero a 129 cifre decimali:

  114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

  Ciò secondo loro avrebbe richiesto un tempo enorme.
- Nel 1994 Arjen K. Lenstra riesce a trovare la soluzione (due fattori, uno con 64 e uno con 65 cifre decimali), con la tecnica del crivello quadratico polinomiale multiplo.
- Per organizzare il lavoro, Lenstra ebbe bisogno di centinaia di collaborazioni, impegnando per circa 48 ore molti calcolatori coordinati via Internet.
- Il messagio di Rivest, Shamir e Adleman non aveva senso compiuto!

Sicurezza del sistema RSA (II)

- **Pertanto**: algoritmi di fattorizzazione più efficienti o computer più veloci (ad esempio il computer quantistico), possono mettere in pericolo i nostri sistemi di sicurezza. Un sistema ritenuto sicuro oggi può non esserlo domani!
- **In particolare**: se esistessero algoritmi polinomiali (tipo l'AKS) per la fattorizzazione dei numeri, tutti i nostri sistemi di sicurezza sarebbero eludibili: la nostra organizzazione sociale sarebbe a rischio!
- **Quindi**: c'è la necessità di nuove idee matematiche per creare sistemi crittografici più sicuri. La ricerca in merito è molto attiva e usa strumenti algebrici e geometrici assai raffinati, come quelli usati da A. Wiles per dimostrare l'Ultimo Teorema di Fermat, ovvero idee della fisica quantistica (crittografia quantistica).

L'Ultimo Teorema di Fermat

- L'Ultimo Teorema di Fermat afferma che non esistono soluzioni intere positive all'equazione:

$$x^n + y^n = z^n \quad \text{se} \quad n > 2.$$

- L'ipotesi fu formulata da Pierre de Fermat (1601–1665) nel 1637.
- Egli non fornì una dimostrazione, ma scrisse, ai margini di una copia dell'Arithmetica di Diofanto (III–IV sec. d.C.):

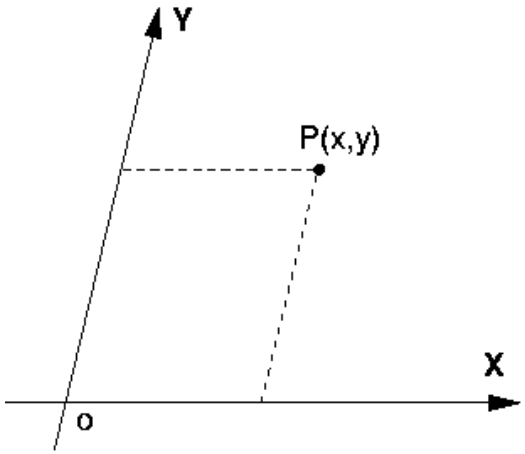
> *Dispongo di una meravigliosa dimostrazione di questo teorema, che non può essere contenuta nel margine troppo stretto della pagina.*

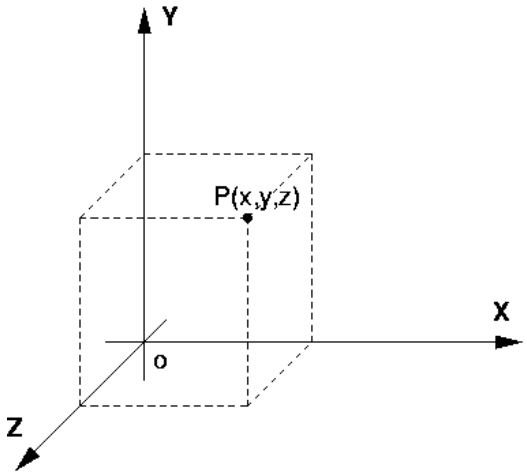
La dimostrazione di A. Wiles

- Una dimostrazione fu cercata da molti matematici per più di 350 anni.
- Solo nel 1994 Andrew Wiles riuscì a trovarne una, che utilizza idee algebrico–geometriche e raffinate tecniche moderne certamente fuori della portata di Fermat.
- La dimostrazione di Wiles mette in luci sorprendenti relazioni dell'Ultimo Teorema di Fermat con la Ipotesi di Riemann e quindi con la distribuzione dei numeri primi.

La Geometria Algebrica ...

... può pensarsi come la naturale prosecuzione del cammino intrapreso da R. Descartes (1596–1650) con l'introduzione delle coordinate cartesiane.





Essa riguarda lo studio di curve, superficie, etc. descritte da equazioni algebriche.

Curve ellittiche

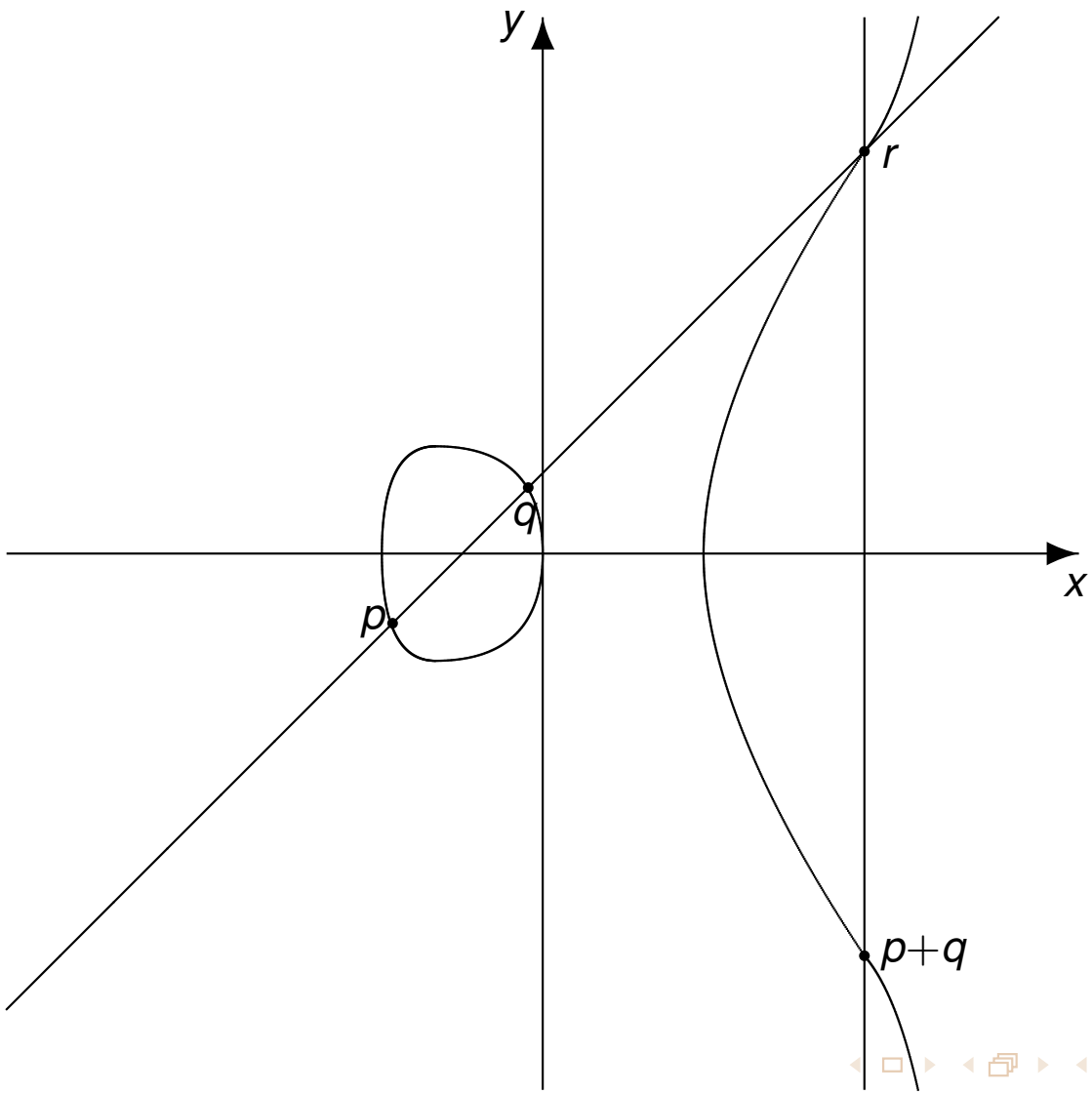
- Sono le curve del piano i cui punti hanno coordinate cartesiane (x, y) che sono soluzioni di una equazione del tipo

$$\boxed{y^2 = x^3 + ax + b}$$

con $x^3 + ax + b = 0$ avente tre soluzioni distinte.

- Le curve ellittiche giocano un ruolo fondamentale nella dimostrazione di Wiles del Teorema di Fermat.
- Si può lavorare prendendo le coordinate in $\mathbb{Z}_p$, con p primo.
- In tal caso la curva ha un numero finito di punti: ci sono algoritmi (deterministici) per calcolarne il numero (cfr. R. Schoof) e algoritmi (probabilistici) per trovarne.

Le curve ellittiche posseggono una operazione di addizione che le rende dei gruppi:



Curve ellittiche e crittografia

- Nel fare crittografia a chiave pubblica si sostituisce $\mathbb{Z}$ o $\mathbb{Z}_n$ con una curva ellittica, sulla quale si può operare addizionando i punti, moltiplicandoli per numeri interi, etc.
- Il vantaggio è che si hanno molte curve ellittiche a disposizione, e se ne possono, ad esempio, utilizzare varie, cambiando così chiave di crittaggio. Ciò rende la crittoanalisi molto più problematica.
- Le curve ellittiche, e più in generale curve algebriche, definite da equazioni del tipo

$$\boxed{f(x,y)=0}$$

con $f(x,y)$ polinomio in x e y, vengono usate anche in teoria dei codici, la disciplina che si occupa di correggere gli errori di trasmissione di dati su canali con disturbi di trasmissione.

Cifrari di Vernam (one time pad)

Un cifrario inattaccabile:

- $p = p_1 p_2 \dots p_r$ messaggio binario in chiaro;
- $k = k_1 k_2 \dots k_r$ la chiave, stringa binaria della stessa lunghezza del messaggio, costituita da cifre casuali da non utilizare MAI DUE VOLTE;
- la cifratura consiste nel sostituire il messaggio p col messaggio $c = c_1 c_2 \dots c_r$ dove:

$$c_i = p_i + k_i \bmod 2, \qquad i = 1, \dots r.$$

Esempio:

$$p = 01001, \quad k = 11010, \quad c = 10011.$$

Il pregio della casualità

La casualità della chiave rende:

- enorme la complessità della crittoanalisi;
- impossibile rintracciare il messaggio giusto p a partire da c.

  Esempio: A partire da $c = 10011$ tutti i messaggi in chiaro

  $$00000, \quad 00001, \quad 00011, \quad 00111, \quad \text{ecc.},$$

  sono ugualmente probabili!

  C. E. Shannon (1949) ha provato che ogni cifrario inattaccabile è di questo tipo.

Il punto debole

Il tallone d'Achille di Vernam:

- generazione delle chiavi;
- trasmissione della chiave: è un serpente che si mangia la coda!
- la fisica quantistica supera quest'ultimo ostacolo e consente tale trasmissione (protocollo di C. H. Bennett-G. Brassard, 1984): questo è il campo della crittografia quantistica di recente sviluppo.

  M. W. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo, Aritmetica, crittografia e codici, Springer–Verlag Italia, 2006.

  M. W. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo, Uno sguardo alla crittografia quantistica, Lettera Matematica PRISTEM, 59 (2006), 22–34.

Conclusione

- All'atto dell'unità d'Italia, Luigi Cremona (1830–1903), nominato professore di Geometria Superiore nell'Università di Bologna esorta nella sua prolusione:

  Respingete da voi, o giovani, le malevole parole di coloro che a conforto della propria ignoranza o a sfogo d'irosi pregiudizi vi chiederanno con ironico sorriso a che giovino questi ad altri studi, e vi parleranno dell'impotenza pratica di quegli uomini che si consacrano al progresso di una scienza prediletta.

- Le molteplici e utilissime applicazioni della matematica teorica mostrano che oltre che ignoranza e pregiudizi, occorre combattere la scarsa lungimiranza dei detrattori della cultura e della scienza pura.
- Solo chi ha una solida cultura di base ed è padrone di raffinate teorie può aspirare a sfruttare a fondo, in modo consapevole e umano, i benefici della tecnologia.

Il Premio Turing 2013 a Silvio Micali

Silvio Micali (Palermo, 1954)
Professore presso il MIT di Boston

- Laureato nel 1978 all'Università di Roma, dove è stato allievo del prof. Corrado Böhm. Ha ottenuto il Ph.D. in Informatica presso l'Università della California (UCLA) di Berkeley nel 1983.
- Le sue ricerche sono indirizzate all'uso di tecniche algebriche e combinatoriche per la crittografia e la sicurezza informatica. Nel 2013 ha ricevuto il Premio Turing (il più importante riconoscimento internazionale per l'informatica), insieme a Shafi Goldwasser.