UNIVERSITÀ CATTOLICA DEL SACRO CUORE
Facoltà di Scienze Matematiche, Fisiche e Naturali

TEORIA DEI NUMERI

(INTRODUZIONE ALLA CRITTOGRAFIA)

Corso di eccellenza in Matematica

Brescia, 19–23 Giugno 2023

Docente: prof. Marco Antonio Pellegrini
marcoantonio.pellegrini@unicatt.it

Indice

CAPITOLO 1

Introduzione

Ci sono situazioni in cui è importante poter comunicare in modo sicuro. Questo avviene non solo in ambito militare, quando si vuole inviare al proprio esercito un messaggio che il nemico non deve poter leggere, ma anche nella nostra vita quotidiana. Infatti, ogni volta che comunichiamo i dati della nostra carta di credito ad un venditore online, vogliamo che tali dati rimangano segreti, in modo che nessuno possa appropriarsene e utilizzarli in seguito al posto nostro (facendo così acquisti a nostre spese). Inoltre, vorremmo che questa comunicazione sicura possa avvenire in tempi rapidi e in modo che chi riceve il messaggio possa essere davvero certo dell'identità del mittente.

Un sistema crittografico, per potersi ritenere valido, dovrebbe soddisfare le seguenti richieste:

- La cifratura del messaggio dovrebbe essere un'operazione semplice da effettuare. La cifratura è il processo di conversione del messaggio originale in un nuovo messaggio, che dovrebbe essere leggibile solo al destinatario di tale messaggio (attenzione: non è richiesto che il mittente sia in grado di poter leggere il messaggio cifrato).
- La trasmissione del messaggio cifrato dovrebbe essere un processo facile. Il messaggio infatti deve arrivar in modo veloce e corretto dal mittente al destinatario.
- La decifrazione del messaggio dovrebbe essere un'operazione facile da effettuare da parte del destinatario.
- Per chi eventualmente intercettasse il messaggio, la decifrazione dovrebbe essere un processo estremamente difficile.

La crittologia si occupa proprio di come creare messaggi segreti (crittografia) e di come decifrare tali messaggi (crittoanalisi). Non è certo una disciplina giovane! Già nell'antico Egitto o nel mondo greco-romano si utilizzavano vari metodi per poter inviare in sicurezza messaggi ai propri eserciti. Nel nostro mondo, più che trasmettere messaggi composti di parole, è fondamentale poter inviare numeri: la Matematica fornisce proprio gli strumenti adatti a tale scopo. Grande importanza rivestono le proprietà dei numeri interi e, in particolare, dei numeri primi, che sono l'oggetto di studio della Teoria dei Numeri.

Questo ramo della Matematica Pura storicamente ha attratto l'interesse più per l'eleganza e la difficoltà dei suoi problemi che per le sue applicazioni pratiche. Vista spesso come esempio di qualcosa di "bello ma inutile" (un semplice gioco), è proprio nel nostro mondo digitale, dove le informazioni devono viaggiare in modo sempre più sicuro, che la Teoria dei Numeri si è invece rivelata una preziosa fonte di applicazioni concrete. Vediamo quindi qualche classico problema di Teoria dei Numeri.

ESEMPIO 1.1. Un intero positivo $n > 1$ è detto *perfetto* se n è la somma dei sui divisori d tali che $1 \leq d < n$. I primi tre numeri perfetti sono:

$$6 = 1 + 2 + 3, \qquad 28 = 1 + 2 + 4 + 7 + 14,$$

$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248.$$

Già Euclide aveva trovato una formula che fornisce numeri perfetti. Eulero (Leonhard Euler, 1707–1783) poi provò che tutti i numeri perfetti pari si possono trovare tramite questa formula. Abbiamo così il seguente teorema.

> *Sia n un numero perfetto pari. Allora esiste un primo p tale che $2^p - 1$ è primo e $n = 2^{p-1}(2^p - 1)$. Viceversa ogni n di questa forma, con p e $2^p - 1$ entrambi primi, è perfetto.*

Vale la pena osservare che non sono noti numeri perfetti dispari: ne esistono? Non abbiamo ancora un risposta, ma è stato provato che, se esiste un numero perfetto dispari, allora questo deve essere maggiore di 10^{1500}.

ESEMPIO 1.2. Un famoso esempio di congettura rimasta irrisolta per secoli è quello che viene chiamato Ultimo Teorema di Fermat:

> *Fissato un intero $n > 2$, non esistono tre interi positivi a, b, c tali che $a^n + b^n = c^n$.*

Questa congettura fu posta nel 1637 da Pierre de Fermat (1601–1665), il quale affermò di possederne una dimostrazione, ma questa era troppo lunga per poter essere scritta sul margine del libro che stava leggendo (l'*Arithmetica* di Diofanto). Per lungo tempo, i matematici hanno cercato di provare tale risultato, finché il matematico inglese Andrew Wiles ci riuscì nel 1995.

ESEMPIO 1.3. Altrettanto famosa è la congettura di Goldbach, posta nel 1742:

> *Ogni intero pari maggiore di 2 può essere scritto come somma di due primi.*

Tale congettura è ancora aperta (cioè non se ne possiede una dimostrazione), sebbene sia stata provata per tutti gli interi pari $n < 4 \cdot 10^{18}$. Esiste anche una versione "debole" di tale congettura, riguardante i numeri dispari:

> *Ogni intero dispari $n > 5$ può essere scritto come somma di tre primi.*

ESEMPIO 1.4. Un po' meno famosa, ma altrettanto interessante è la Congettura di Catalan, posta nel 1844 e provata nel 2002 dal matematico romeno Preda Mihăilescu:

> *Gli unici interi a, b, x, y, con $a, b > 1$ e $x, y > 0$, tali che $x^a - y^b = 1$ sono $x = 3$, $a = 2$, $y = 2$ e $b = 3$.*

CAPITOLO 2

Sistemi crittografici a chiave privata

Bob vuole mandare un messaggio (che chiameremo *plaintext*) ad Alice in modo che Alice, e solo Alice, possa leggerlo. Per mantenerlo segreto, Bob lo cifra rendendolo illeggibile. Il nuovo messaggio così ottenuto viene detto *ciphertext*: Alice, una volta decifrato il ciphertext, è in grado di leggere il messaggio mandatogli da Bob.

Uno dei metodi più elementari è quello *permutazionale*, nel quale le lettere vengono permutate tra loro. Un permutazione è una funzione biettiva da un insieme in se stesso: in altre, parole stiamo disponendo le lettere in un ordine differente. Giusto per fare un facile esempio, supponiamo che Bob voglia fissare un appuntamento con Alice, e quindi decide di spedirle il messaggio (plaintext) DOMANI. Bob sceglie allora una delle $26!$ possibili permutazioni (usiamo alfabeto di 26 lettere), ad esempio quella descritta nella Figura 1. Alice riceve così il ciphertext RGAEXI. Per poter decifrare tale messaggio, Alice deve conoscere la chiave utilizzata da Bob, cioè la permutazione di Figura 1, che Alice applicherà al contrario:

$$\mathsf{R} \to \mathsf{D}, \quad \mathsf{G} \to \mathsf{O}, \quad \mathsf{A} \to \mathsf{M}, \quad \mathsf{E} \to \mathsf{A}, \quad \mathsf{X} \to \mathsf{N}, \quad \mathsf{I} \to \mathsf{I}.$$

Si tratta quindi di un sistema crittografico simmetrico, nel senso che Alice e Bob dispongono delle stesse informazioni, la chiave, per cifrare e decifrare il messaggio. Ovviamente tale chiave deve essere mantenuta segreta. Infatti, un eventuale rivale (solitamente chiamato Eve, da *eavesdrop*, intercettare) che possedesse la permutazione di Figura 1 non avrebbe nessun problema a decifrare il messaggio di Bob.

A	→	E	B	→	Z	C	→	W
D	→	R	E	→	S	F	→	V
G	→	Q	H	→	B	I	→	I
J	→	T	K	→	H	L	→	U
M	→	A	N	→	X	O	→	G
P	→	P	Q	→	O	R	→	F
S	→	D	T	→	C	U	→	L
V	→	K	W	→	M	X	→	N
Y	→	J	Z	→	Y			

FIGURA 1. Un esempio di permutazione.

Al di là della poca sicurezza garantita da questo metodo, il problema principale consiste nel fatto che Bob deve in qualche modo comunicare ad Alice la permutazione scelta (cioè 1 delle $26! = 403291461126605635584000000$ possibili chiavi). Anzi, sarebbe meglio che ogni volta che Alice e Bob comunicano tra loro, essi scegliessero una chiave diversa, per aumentare la sicurezza.

Ad esempio, Bob può decidere di cifrare il proprio messaggio applicando uno *shift* di tre posizioni

$$\mathsf{D} \to \mathsf{G}, \quad \mathsf{O} \to \mathsf{R}, \quad \mathsf{M} \to \mathsf{P}, \quad \mathsf{A} \to \mathsf{D}, \quad \mathsf{N} \to \mathsf{Q}, \quad \mathsf{I} \to \mathsf{L}.$$

In questo caso, Alice quindi riceve il messaggio GRPDQL. Conoscendo la chiave, cioè sapendo quale metodo ha utilizzato Bob (uno shift di 3 posizioni), Alice può facilmente recuperare il messaggio originale, applicando l'operazione inversa (uno shift di -3 posizioni). Il vantaggio dello shift è che Bob deve comunicare ad Alice molte meno informazioni riguardo alla chiave. Certo, ora Bob ha a disposizioni solo 26 possibili chiavi. Sistemi crittografici moderni come DES e AES sono anch'essi simmetrici, ma ovviamente ammettono un numero ben superiore di chiavi (siamo nell'ordine di 10^{30} possibili chiavi). Nel prossimo capitolo vedremo altri sistemi crittografici, come RSA, che invece sono asimmetrici.

Ovviamente, non tutti i metodi crittografici sono basati sulla matematica: ad esempio, i soldati americani durante la seconda guerra mondiale utilizzavano il linguaggio degli indiani Navajo per codificare i propri messaggi; papa Giovanni XXIII, quando era nunzio apostolico in Bulgaria, utilizzava il dialetto bergamasco. Questi metodi sono sicuri finché il nemico non si procura un interprete, magari catturando un soldato nemico.

Secondo lo storico romano Svetonio, Giulio Cesare comunicava proprio adoperando il metodo che abbiamo visto usare da Alice e Bob (uno shift di tre posizioni), mentre Cesare Augusto utilizzava uno shift di una sola posizione, ma usando $\mathsf{Z} \to \mathsf{AA}$. Risulta invece più "naturale" usare solo le 26 lettere dell'alfabeto, disponendole in cerchio. Nel cifrario di Cesare, quindi usiamo

$$\mathsf{A} \to \mathsf{D}, \quad \ldots, \quad \mathsf{W} \to \mathsf{Z}, \quad \mathsf{X} \to \mathsf{A}, \quad \mathsf{Y} \to \mathsf{B}, \quad \mathsf{Z} \to \mathsf{C}.$$

In termini numerici, identifichiamo ogni lettera con un numero, partendo da $\mathsf{A} = 0$:

$$\mathsf{A} = 0, \quad \mathsf{B} = 1, \quad \ldots, \quad \mathsf{Z} = 25.$$

Il messaggio di Bob diventa quindi la sequenza numerica

$$3\ 14\ 12\ 0\ 13\ 8.$$

Bob cifra questo messaggio sommando $+3$ ad ogni numero e quindi invia ad Alice il messaggio

$$6\ 17\ 15\ 3\ 16\ 11.$$

Alice deve semplicemente sommare -3 per scoprire che Bob vuole incontrarla domani. Cosa succede alle ultime lettere dell'alfabeto? Quello che facciamo è lavorare modulo 26, cioè lavoriamo come se possedessimo un orologio con 26 ore, da 0 a 25. Abbiamo così $23 + 3 = 0$, $24 + 3 = 1$ e $25 + 3 = 2$. Stiamo utilizzando una nuova aritmetica detta *aritmetica modulare*.

2.1. Anelli commutativi

Iniziamo richiamando alcune proprietà dell'insieme dei numeri interi

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

Tale insieme è un esempio (forse l'esempio principale) di anello commutativo.

DEFINIZIONE 2.1. Sia A un insieme non vuoto su cui siano definite due operazioni binarie

$$\begin{array}{rcl} +: A\times A & \to & A \\ (x,y) & \mapsto & x+y \end{array} \qquad \begin{array}{rcl} \cdot: A\times A & \to & A \\ (x,y) & \mapsto & x\cdot y \end{array}$$

Diremo che $(A,+,\cdot)$ è un *anello commutativo* se valgono le seguenti proprietà:

(1) l'operazione $+$ è associativa: $(a+b)+c=a+(b+c)$ per ogni $a,b,c\in A$;
(2) l'operazione $+$ è commutativa: $a+b=b+a$ per ogni $a,b\in A$;
(3) l'operazione $+$ ammette elemento neutro, denotato con 0: $a+0=0+a=a$ per ogni $a\in A$;
(4) ogni elemento ammette opposto: per ogni a in A, esiste un elemento $b\in A$ tale che $a+b=b+a=0$ (tale b viene indicato con $-a$);
(5) l'operazione $\cdot$ è associativa: $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ per ogni $a,b,c\in A$;
(6) l'operazione $\cdot$ è commutativa: $a\cdot b=b\cdot a$ per ogni $a,b\in A$;
(7) l'operazione $\cdot$ ammette elemento neutro, denotato con 1: $a\cdot 1=1\cdot a=a$ per ogni $a\in A$;
(8) valgono le leggi distributive: $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$ e $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ per ogni $a,b,c\in A$.

Anelli commutativi sono anche l'insieme dei numeri razionali $(\mathbb{Q},+,\cdot)$, quello dei numeri reali $(\mathbb{R},+,\cdot)$ e quello dei numeri complessi $(\mathbb{C},+,\cdot)$. Un altro esempio è l'anello dei polinomi in x a coefficienti reali: $\mathbb{R}[x]$. Dall'altro lato, l'insieme dei numeri naturali $\mathbb{N}$ non lo è, in quanto, ad esempio, l'opposto di 2 (cioè -2) non è un numero naturale.

Dato un anello commutativo A, diremo che un elemento $a\in A$ è unitario (o invertibile) se esiste un elemento b tale che $ab=ba=1$. In tal caso, scriveremo $b=a^{-1}$ (si può provare che se l'inverso di un elemento di un anello esiste, allora esso è unico).

ESEMPIO 2.2. Gli unici elementi unitari di $\mathbb{Z}$ sono 1 e -1. Infatti, abbiamo $1^{-1}=1$ e $(-1)^{-1}=-1$.

Vediamo ora il concetto di divisibilità.

DEFINIZIONE 2.3. Sia A un anello commutativo. Dati due elementi x e y in A, diremo che x divide y e scriveremo $x\mid y$ se esiste un elemento $c\in A$ tale che

$$y=cx.$$

ESEMPIO 2.4. Prendiamo $A=\mathbb{Z}$. Allora 2 divide 4, 6 divide 18 ma 15 non divide 10. Se invece prendiamo $A=\mathbb{Q}$ allora 15 divide 10. Infatti si ha

$$15=10\cdot\frac{3}{2}.$$

Attenzione però: non stiamo calcolando quoziente e resto (né affermando che essi esistono). Infatti, possiamo dire che $0\mid 0$, avendo $0=0\cdot 0$. Più in generale, $a\mid 0$ per ogni $a\in A$, in quanto $0=a\cdot 0$. Viceversa, $0\mid a$ se e solo se $a=0$ (Esercizio 2.2).

DEFINIZIONE 2.5. Dati due elementi a e b, non entrambi nulli, di un anello commutativo A, chiamiamo massimo comun divisore tra a e b ogni $d\in A$ tale che

(1) $d\mid a$ e $d\mid b$;
(2) se $c\in A$ è tale che $c\mid a$ e $c\mid b$, allora $c\mid d$.

Il massimo comun divisore non è unico. Però, supponiamo che d_1 e d_2 siano due massimi comun divisori di due interi a, b non entrambi nulli. Per definizione, si ottiene che $d_1 \mid d_2$ e $d_2 \mid d_1$, implicando $d_1 = \pm d_2$. Infatti, abbiamo $d_2 = d_1 x$ e $d_1 = d_2 y$ per opportuni $x, y \in \mathbb{Z}$. Otteniamo così $d_2 = d_2 xy$, da cui $d_2(xy - 1) = 0$. Ora, in $\mathbb{Z}$ il prodotto tra due interi è uguale a zero se e solo se almeno uno dei due fattori è zero. Se fosse $d_2 = 0$, allora avremmo $a = b = 0$, una contraddizione. Pertanto dobbiamo avere $xy = 1$, da cui $x = \pm 1$ e $d_2 = \pm d_1$.

In altre parole, in $\mathbb{Z}$ il massimo comun divisore tra due interi non entrambi nulli è definito a meno del segno. Indicheremo con M.C.D.(a, b) il massimo comun divisore positivo. Diremo che a, b sono coprimi, se M.C.D.$(a, b) = 1$.

PROPOSIZIONE 2.6. *Siano $a, b \in \mathbb{Z}$ con $b \neq 0$. Esistono e sono unici due interi q, r tali che*

$$a = q \cdot b + r \quad \text{con } 0 \leq r < |b|.$$

L'intero q viene chiamato quoziente e l'intero non negativo r viene detto resto della divisione. Possiamo calcolare il massimo comun divisore tra due interi utilizzando l'*algoritmo euclideo delle divisioni successive*.

TEOREMA 2.7. *Siano a e b due interi non negativi, tali che $b \neq 0$. Consideriamo la seguente sequenza di divisioni:*

$$\begin{aligned}
a &= q_1 b + r_1 && \text{con } 0 \leq r_1 < b,\\
b &= q_2 r_1 + r_2 && \text{con } 0 \leq r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3 && \text{con } 0 < r_3 < r_2,\\
&\vdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} && \text{con } 0 < r_{n-1} < r_{n-2},\\
r_{n-2} &= q_n r_{n-1} + 0.
\end{aligned}$$

L'ultimo resto non nullo r_{n-1} coincide con M.C.D.(a, b). *Inoltre, esistono allora due interi x, y tali che* M.C.D.$(a, b) = ax + by$.

ESEMPIO 2.8. Calcoliamo M.C.D.$(456, 123)$:

$$\begin{aligned}
456 &= 3 \cdot 123 + 87,\\
123 &= 1 \cdot 87 + 36,\\
87 &= 2 \cdot 36 + 15,\\
36 &= 2 \cdot 15 + 6,\\
15 &= 2 \cdot 6 + 3,\\
6 &= 2 \cdot 3 + 0.
\end{aligned}$$

Ne segue che M.C.D.$(456, 123) = 3$. Ora, risaliamo le precedenti divisioni:

$$\begin{aligned}
3 &= 15 - 2 \cdot 6,\\
3 &= 15 - 2 \cdot (36 - 2 \cdot 15) = 5 \cdot 15 - 2 \cdot 36,\\
3 &= 5 \cdot (87 - 2 \cdot 36) - 2 \cdot 36 = 5 \cdot 87 - 12 \cdot 36,\\
3 &= 5 \cdot 87 - 12(123 - 1 \cdot 87) = 17 \cdot 87 - 12 \cdot 123,\\
3 &= 17(456 - 3 \cdot 123) - 12 \cdot 123 = 17 \cdot 456 - 63 \cdot 123.
\end{aligned}$$

Otteniamo così che M.C.D.$(456, 123) = 17 \cdot 456 + (-63) \cdot 123$.

Sfruttando il concetto di divisibilità in $\mathbb{Z}$ possiamo definire la seguente relazione.

DEFINIZIONE 2.9. Fissato un intero $n \geq 2$, diremo che due interi $a, b \in \mathbb{Z}$ sono *congrui modulo* n se n divide $a - b$; in altre parole, se esiste $z \in \mathbb{Z}$ tale che

$$a - b = nz.$$

In tal caso scriveremo

$$a \equiv b \pmod{n}, \quad \text{oppure} \quad a \equiv_n b.$$

Ad esempio, abbiamo

$$5 \equiv 2 \pmod{3}, \quad -3 \equiv 5 \pmod{4} \quad \text{e} \quad 12 \equiv 2 \pmod{5}.$$

Utilizzare il cifrario di Cesare equivale quindi a lavorare modulo 26.

TEOREMA 2.10. *Sia $n > 1$. La relazione modulo n è una relazione di equivalenza.*

DIMOSTRAZIONE. Dobbiamo provare che la relazione modulo n è riflessiva, simmetrica e transitiva.
(Riflessività) Per ogni $a \in \mathbb{Z}$ si ha $a \equiv_n a$, poiché $a - a = 0 = 0 \cdot n$.
(Simmetricità) Dobbiamo provare che, dati $a, b \in \mathbb{Z}$, se $a \equiv_n b$ allora $b \equiv_n a$. Partiamo da $a \equiv_n b$: questo significa che possiamo scrivere $a - b = zn$ per un certo $z \in \mathbb{Z}$. Moltiplicando per -1, otteniamo $-a + b = -zn$ che possiamo riscrivere come $b - a = (-z)n$. Poiché $-z$ è ancora un elemento di $\mathbb{Z}$, abbiamo ottenuto che $b \equiv_n a$.
(Transitività) Dobbiamo provare che, dati $a, b, c \in \mathbb{Z}$ tali che $a \equiv_n b$ e $b \equiv_n c$ si ha $a \equiv_n c$. Poiché $a \equiv_n b$, esiste $z \in \mathbb{Z}$ tale che $a - b = zn$; poiché $b \equiv_n c$, esiste $w \in \mathbb{Z}$ tale che $b - c = wn$. Sommando queste due espressioni si ottiene $(a-b)+(b-c) = zn+wn$, da cui $a - c = (z + w)n$. Poiché $z + w \in \mathbb{Z}$, abbiamo provato che $a \equiv_n c$. □

Avendo provato che la relazione $\equiv_n$ è di equivalenza, possiamo considerarne le classi di equivalenza. Dati $a, n \in \mathbb{Z}$ con $n > 1$ poniamo

$$[a]_n = \{b \in \mathbb{Z} : b \equiv_n a\} = \{a + kn : k \in \mathbb{Z}\}.$$

LEMMA 2.11. *Sia $n > 1$ e $a, b \in \mathbb{Z}$. Allora*

(1) $[a]_n = [b]_n$ *se e solo se* $a \equiv_n b$;
(2) *se* $a \not\equiv_n b$, *allora* $[a]_n \cap [b]_n = \emptyset$.

Fissato $n > 1$, denotiamo con $\mathbb{Z}_n$ l'insieme delle classi di equivalenza modulo n:

$$\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\}.$$

Sfruttando il concetto di quoziente e resto in $\mathbb{Z}$ possiamo vedere che, fissato $n > 1$, due elementi $a, b \in \mathbb{Z}$ sono congrui modulo n se e solo se i resti delle divisioni di a e b per n coincidono. Possiamo così utilizzare gli n possibili resti come rappresentanti delle classi di equivalenza modulo n.

ESEMPIO 2.12. Prendiamo $n = 8$. Allora

$$\begin{aligned}
[0]_8 &= \{0, 8, 16, \ldots, -8, -16, -24, \ldots\};\\
[1]_8 &= \{1, 9, 17, \ldots, -7, -15, -23, \ldots\};\\
[2]_8 &= \{2, 10, 18, \ldots, -6, -14, -22, \ldots\};\\
[3]_8 &= \{3, 11, 19, \ldots, -5, -13, -21, \ldots\};\\
[4]_8 &= \{4, 12, 20, \ldots, -4, -12, -20, \ldots\};\\
[5]_8 &= \{5, 13, 21, \ldots, -3, -11, -19, \ldots\};\\
[6]_8 &= \{6, 14, 22, \ldots, -2, -10, -18, \ldots\};\\
[7]_8 &= \{7, 15, 23, \ldots, -1, -9, -17, \ldots\}.
\end{aligned}$$

Osserviamo che, per esempio, $[1]_8 = [9]_8$ e $[5]_8 = [-3]_8$. Abbiamo così

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}.$$

ESEMPIO 2.13. Vogliamo determinare la classe di equivalenza di 105 modulo 8. Dividiamo allora 105 per 8, determinando quoziente e resto:

$$105 = 8 \cdot 13 + 1.$$

Ne segue che $[105]_8 = [1]_8$.

Possiamo definire sull'insieme $\mathbb{Z}_n$ un'operazione di somma e una di prodotto, ereditate dall'anello $\mathbb{Z}$. Dati $a, b, n \in \mathbb{Z}$ con $n > 1$, poniamo

$$[a]_n + [b]_n = [a + b]_n \quad \text{e} \quad [a]_n \cdot [b]_n = [ab]_n.$$

Queste operazioni sono ben definite (non dipendono dalla scelta del rappresentante della classe di equivalenza $[a]_n$) e rendono $(\mathbb{Z}_n, +, \cdot)$ un anello commutativo.

ESEMPIO 2.14. Si ha

$$\begin{gathered}
[2]_8 + [5]_8 = [7]_8, \quad [5]_8 + [7]_8 = [4]_8, \quad [-3]_8 + [-2]_8 = [3]_8,\\
[8]_8 + [2]_8 = [2]_8, \quad [3]_8 + [5]_8 = [0]_8, \quad [4]_8 + [4]_8 = [0]_8,\\
[2]_8 \cdot [3]_8 = [6]_8, \quad [3]_8 \cdot [3]_8 = [1]_8, \quad [5]_8 \cdot [3] = [7]_8,\\
[4]_8 \cdot [4]_8 = [0]_8, \quad [6]_8 \cdot [2]_8 = [4]_8, \quad [10]_8 \cdot [12]_8 = [0]_8.
\end{gathered}$$

In particolare, lo zero di $\mathbb{Z}_n$ è la classe $[0]_n$ e l'uno è la classe $[1]_n$. Inoltre $-[a]_n = [-a]_n$. Come si è visto nell'esempio precedente, in $\mathbb{Z}_n$ può succedere che $[a]_n \cdot [b]_n = [0]_n$ anche se $[a]_n, [b]_n \neq [0]_n$ (cioè il prodotto di due numeri non nulli può essere uguale a zero). Possiamo determinare quali elementi di $\mathbb{Z}_n$ sono invertibili grazie alla seguente.

PROPOSIZIONE 2.15. *Sia $n > 1$. L'elemento $[a]_n \in \mathbb{Z}_n$ è invertibile in $\mathbb{Z}_n$ se e solo se* M.C.D.$(a, n) = 1$.

ESEMPIO 2.16. Vogliamo determinare, qualora esista, l'inverso di $[5]_9$. Questo problema può essere risolto attraverso il metodo delle divisioni successive: iniziamo calcolando M.C.D.$(5, 9)$.

$$\begin{aligned}
9 &= 1 \cdot 5 + 4,\\
5 &= 1 \cdot 4 + 1,\\
4 &= 4 \cdot 1 + 0.
\end{aligned}$$

Abbiamo così che M.C.D.$(5, 9) = 1$: per la proposizione precedente, questo significa che esiste $[5]_9^{-1}$. Risaliamo ora la sequenza delle divisioni:

$$1 = 5 - 4 = 5 - (9 - 5) = 2 \cdot 5 - 9.$$

Abbiamo così ottenuto $[1]_9 = [2]_9 \cdot [5]_9 - [9]_9$, cioè $[2]_9 \cdot [5]_9 = [1]_9$ da cui $[5]_9^{-1} = [2]_9$.

2.2. Cifrari affini

Il cifrario di Cesare con chiave c è quindi la funzione $\psi_c : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ data da

$$\psi_c([x]_{26}) = [x + c]_{26}.$$

È chiaramente una funzione invertibile: $(\psi_c)^{-1} = \psi_{-c}$. Questo è un esempio di sistema crittografico affine. Infatti, presi due interi $a, b \in \mathbb{Z}$, consideriamo la funzione

$$\begin{aligned} \psi_{a,b} : \ \mathbb{Z}_{26} &\to \mathbb{Z}_{26} \\ [x]_{26} &\mapsto [ax + b]_{26}. \end{aligned} \tag{2.1}$$

Questa funzione non è sempre invertibile e questo è ovviamente un problema! Torniamo ai nostri amici Alice e Bob. Bob, folle d'amore, vuol mandare ad Alice il messaggio LOVE. Per mantenere però il loro amore segreto, decide di cifrarlo utilizzando la funzione $\psi_{13,5}$:

$$\begin{array}{lllllllllll} \mathsf{L} & = & [11]_{26} & \mapsto & [13 \cdot 11 + 5]_{26} & = & [148]_{26} & = & [18]_{26} & = & \mathsf{S} \\ \mathsf{O} & = & [14]_{26} & \mapsto & [13 \cdot 14 + 5]_{26} & = & [187]_{26} & = & [5]_{26} & = & \mathsf{F} \\ \mathsf{V} & = & [21]_{26} & \mapsto & [13 \cdot 21 + 5]_{26} & = & [278]_{26} & = & [18]_{26} & = & \mathsf{S} \\ \mathsf{E} & = & [4]_{26} & \mapsto & [13 \cdot 4 + 5]_{26} & = & [57]_{26} & = & [5]_{26} & = & \mathsf{F} \end{array}$$

Alice, ricevendo SFSF non riesce a recuperare il messaggio originale. Infatti:

$$\begin{array}{lllllllllll} \mathsf{H} & = & [7]_{26} & \mapsto & [13 \cdot 7 + 5]_{26} & = & [96]_{26} & = & [18]_{26} & = & \mathsf{S} \\ \mathsf{A} & = & [0]_{26} & \mapsto & [13 \cdot 0 + 5]_{26} & = & [5]_{26} & = & [5]_{26} & = & \mathsf{F} \\ \mathsf{T} & = & [19]_{26} & \mapsto & [13 \cdot 19 + 5]_{26} & = & [252]_{26} & = & [18]_{26} & = & \mathsf{S} \\ \mathsf{E} & = & [4]_{26} & \mapsto & [13 \cdot 4 + 5]_{26} & = & [57]_{26} & = & [5]_{26} & = & \mathsf{F} \end{array}$$

L'errore fatto da Bob è stato quello di prendere un valore di a tale che M.C.D.$(a, 26) \neq 1$. Abbiamo infatti il seguente risultato.

LEMMA 2.17. *Siano a, b due interi con $a \neq 0$. La funzione $\psi_{a,b}$ è invertibile se e solo se* M.C.D.$(a, 26) = 1$. *Più in generale, se $n > 1$, la funzione $\psi : \mathbb{Z}_n \to \mathbb{Z}_n$ data da $[x]_n \mapsto [ax + b]_n$ è invertibile se e solo se* M.C.D.$(a, n) = 1$.

Utilizzando $\psi_{7,5}$, Bob riesce a inviare il suo messaggio ad Alice:

$$\begin{array}{lllllllllll} \mathsf{L} & = & [11]_{26} & \mapsto & [7 \cdot 11 + 5]_{26} & = & [82]_{26} & = & [4]_{26} & = & \mathsf{E} \\ \mathsf{O} & = & [14]_{26} & \mapsto & [7 \cdot 14 + 5]_{26} & = & [103]_{26} & = & [25]_{26} & = & \mathsf{Z} \\ \mathsf{V} & = & [21]_{26} & \mapsto & [7 \cdot 21 + 5]_{26} & = & [152]_{26} & = & [22]_{26} & = & \mathsf{W} \\ \mathsf{E} & = & [4]_{26} & \mapsto & [7 \cdot 4 + 5]_{26} & = & [33]_{26} & = & [7]_{26} & = & \mathsf{H} \end{array}$$

Alice, ricevendo il messaggio EZWH, vuole recuperare il messaggio originale. Ma come deve fare? Ricordiamo che Alice possiede la chiave, cioè sa che Bob ha applicato

la funzione $\psi_{7,5}$: deve determinare $c, d \in \mathbb{Z}$ tali che $\psi_{c,d}(\psi_{7,5}(z)) = z$ per ogni $z \in \mathbb{Z}_{26}$. Abbiamo quindi

$$[x]_{26} \mapsto [7x+5]_{26} \mapsto [c(7x+5)+d]_{26} = [7cx+5c+d]_{26}.$$

Determiniamo prima di tutto l'elemento $[c]_{26}$ tale che $[c]_{26} = [7]_{26}^{-1}$: determiniamo cioè l'inverso di $[7]_{26}$. Calcoliamo quindi M.C.D.$(7, 26)$:

$$\begin{aligned} 26 &= 3 \cdot 7 + 5, \\ 7 &= 1 \cdot 5 + 2, \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$

Risalendo:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2, \\ &= 5 - 2(7-5) = 3 \cdot 5 - 2 \cdot 7, \\ &= 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7 = 3 \cdot 26 - 11 \cdot 7. \end{aligned}$$

Abbiamo così ottenuto $[(-11) \cdot 7]_{26} = [1]_{26}$, cioè $[-11]_{26} \cdot [7]_{26} = [1]_{27}$. Concludiamo che $[7]_{26}^{-1} = [-11]_{26} = [15]_{26}$, da cui $c = 15$. Abbiamo così

$$[x]_{26} \mapsto [7x+5]_{26} \mapsto [15(7x+5)+d]_{26} = [7 \cdot 15x + 5 \cdot 15 + d]_{26} = [x + 23 + d]_{26}.$$

Ora, dobbiamo solo prendere $d = 3$, ottenendo

$$(\psi_{7,5})^{-1} = \psi_{15,3}.$$

Alice applica quindi la funzione $\psi_{15,3}$ al messaggio ricevuto, ottenendo:

$$\begin{array}{ccccccccccc} \mathsf{E} & = & [4]_{26} & \mapsto & [15 \cdot 4 + 3]_{26} & = & [63]_{26} & = & [11]_{26} & = & \mathsf{L} \\ \mathsf{Z} & = & [25]_{26} & \mapsto & [15 \cdot 25 + 3]_{26} & = & [378]_{26} & = & [14]_{26} & = & \mathsf{O} \\ \mathsf{W} & = & [22]_{26} & \mapsto & [15 \cdot 22 + 3]_{26} & = & [333]_{26} & = & [21]_{26} & = & \mathsf{V} \\ \mathsf{H} & = & [7]_{26} & \mapsto & [15 \cdot 7 + 3]_{26} & = & [108]_{26} & = & [4]_{26} & = & \mathsf{E} \end{array}$$

I cifrari permutazionali (e in particolare quelli affini) non sono molto sicuri. Infatti è possibile decifrare un messaggio codificato mediante la funzione $\psi_{a,b}$ attraverso l'analisi delle frequenze. Ogni lingua infatti utilizza certe lettere con frequenza maggiore e certe altre con frequenza minore. Un testo italiano, se abbastanza lungo, conterrà molte più lettere A rispetto alle lettere H o Q.

Osservando la Figura 2, è facile vedere che le lettere A, E, I sono quelle che, in un testo scritto in lingua italiana, compaiono con la frequenza maggiore (circa 11%), mentre le lettere Q e Z sono le più rare (circa 0.5%). Nonostante il testo italiano, manteniamo ancora l'alfabeto a 26 lettere. Chiaramente, maggiore è la lunghezza del testo, più l'analisi delle frequenze rispecchierà la tabella della Figura 2.

Supponiamo di aver intercettato il seguente ciphertext, che sappiamo essere stato prodotto applicando un cifrario affine:

AMQLDEOUNQLLEWUNCKUOUKZQPULWQEOQBBUWCUDRUJDENMQK
EJQRQRURCRJQDDUJJQNCOURJCJMJJUEGQRCQEWULTCEGQKUR
NENQLLUGXUDWQDQQNQLDCQRJDEDQNCAMQLLCPCQRAMEGCEMR
JDEJJUEDCGJDCRWQDGCQEXDQRNQDKUDGUQTCWMDENCTCMOQJ
DEMRXDUOURJUDCUENQGJDEQMREOXCEKUGJCQDENELLELJDEXEDJQ.

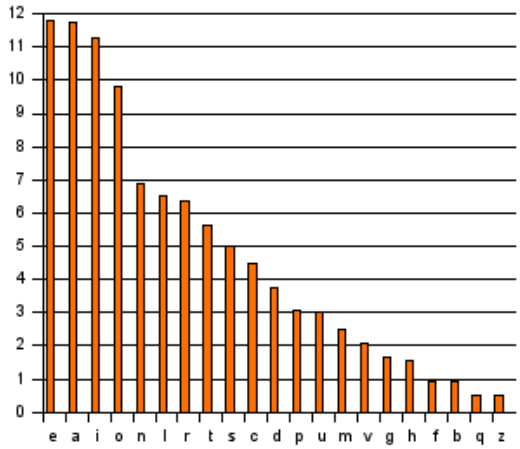

FIGURA 2. Frequenze delle 21 lettere nell'alfabeto italiano (fonte https://it.wikipedia.org/wiki/Analisi_delle_frequenze).

Contiamo quante volte appare una data lettera:

A	B	C	D	E	F	G	H	I	J	K	L	M
3	2	21	25	26	0	9	0	0	20	6	13	10
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	7	2	32	16	0	3	24	0	7	5	0	1

La lettera che compare più volte è quindi la Q, seguita dalla E. Guardando la Figura 2, è plausibile supporre (ovviamente si possono fare vari tentativi) che E $\mapsto$ Q e A $\mapsto$ E, cioè che $\psi_{a,b}([4]_{26}) = [16]_{26}$ e $\psi_{a,b}([0]_{26}) = [4]_{26}$. Otteniamo così le condizioni

$$4a + b \equiv 16 \pmod{26} \quad \text{e} \quad 0a + b \equiv 4 \pmod{26}.$$

Ricaviamo $b = 4$ e quindi $a = 3$: in altre parole, stiamo ipotizzando che il ciphertext sia stato ottenuto applicando la funzione $\psi_{3,4}$. Per averne conferma, applichiamo al ciphertext la funzione $\psi_{3,4}^{-1} = \psi_{9,16}$. Iniziamo con le prime lettere:

$$\begin{aligned} \text{A} &= [0]_{26} \mapsto [16]_{26} = \text{Q} \\ \text{M} &= [12]_{26} \mapsto [20]_{26} = \text{U} \\ \text{Q} &= [16]_{26} \mapsto [4]_{26} = \text{E} \\ \text{L} &= [11]_{26} \mapsto [11]_{26} = \text{L} \end{aligned}$$

Sembra promettere bene! Applicando allora all'intero ciphertext otteniamo il plaintext:

QUELRAMODELLAGODICOMOCHEVOLGEAMEZZOGIORNOTRADUECATENE
NONINTERROTTEDIMONTITUTTOASENIEAGOLFIASECONDADELLOSPORGERE
EDALRIENTRAREDIQUELLIVIENQUASIAUNTRATTOARISTRINGERSIEA
PRENDERCORSOEFIGURADIFIUMETRAUNPROMONTORIOADESTRAEUNAMPIA
COSTRIERADALLALTRAPARTE.

2.3. Cifrario di Hill e Cifrario di Vigenère

Con lo scoppiare della prima guerra mondiale, le analisi delle frequenze si fecero sempre più sofisticate. Il cifrario di Hill, inventato da Lester Hill nel 1929 per evitare questo tipo di attacco, sfrutta le matrici. In questo modo, la cifratura di una lettera dipenderà anche dalle lettere ad essa vicina. In realtà, nemmeno questo metodo è davvero sicuro.

ESEMPIO 2.18. Bob vuol mandare ad Alice il messaggio

DOMANI ALLE ORE OTTO E TRENTA.

Decide di dividere il messaggio in blocchetti da 3 lettere:

$$\begin{pmatrix}\mathsf{D}\\ \mathsf{O}\\ \mathsf{M}\end{pmatrix}, \begin{pmatrix}\mathsf{A}\\ \mathsf{N}\\ \mathsf{I}\end{pmatrix}, \begin{pmatrix}\mathsf{A}\\ \mathsf{L}\\ \mathsf{L}\end{pmatrix}, \begin{pmatrix}\mathsf{E}\\ \mathsf{O}\\ \mathsf{R}\end{pmatrix}, \begin{pmatrix}\mathsf{E}\\ \mathsf{O}\\ \mathsf{T}\end{pmatrix}, \begin{pmatrix}\mathsf{T}\\ \mathsf{O}\\ \mathsf{E}\end{pmatrix}, \begin{pmatrix}\mathsf{T}\\ \mathsf{R}\\ \mathsf{E}\end{pmatrix}, \begin{pmatrix}\mathsf{N}\\ \mathsf{T}\\ \mathsf{A}\end{pmatrix}.$$

Il plaintext è dato quindi da una sequenza $(v_1, v_2 \ldots, v_8)$ di vettori colonna di lunghezza 3 a valori in $\mathbb{Z}_{26}$ (per brevità, qui scriviamo x al posto di $[x]_{26}$):

$$\begin{pmatrix}3\\14\\12\end{pmatrix}, \begin{pmatrix}0\\13\\8\end{pmatrix}, \begin{pmatrix}0\\11\\11\end{pmatrix}, \begin{pmatrix}4\\14\\17\end{pmatrix}, \begin{pmatrix}4\\14\\19\end{pmatrix}, \begin{pmatrix}19\\14\\4\end{pmatrix}, \begin{pmatrix}19\\17\\4\end{pmatrix}, \begin{pmatrix}13\\19\\0\end{pmatrix}.$$

Bob sceglie quindi una matrice invertibile 3×3 a valori in $\mathbb{Z}_{26}$. In altre parole, sceglie una matrice $A \in \mathrm{GL}_3(\mathbb{Z}_{26})$:

$$A = \begin{pmatrix}1 & 2 & 1\\ 1 & 11 & 1\\ 0 & 1 & 1\end{pmatrix}$$

di determinante $[9]_{26}$. Ricordiamo che una matrice $A \in \mathrm{Mat}_m(\mathbb{Z}_n)$ è invertibile se e solo se M.C.D.$(\det(A), n) = 1$. Il ciphertext è $(w_1, w_2, \ldots, w_8)$, dove $w_i = Av_i$ per ogni $i = 1, \ldots, 8$:

$$\begin{pmatrix}17\\13\\0\end{pmatrix}, \begin{pmatrix}8\\21\\21\end{pmatrix}, \begin{pmatrix}7\\2\\22\end{pmatrix}, \begin{pmatrix}23\\19\\5\end{pmatrix}, \begin{pmatrix}25\\21\\7\end{pmatrix}, \begin{pmatrix}25\\21\\18\end{pmatrix}, \begin{pmatrix}5\\2\\21\end{pmatrix}, \begin{pmatrix}25\\14\\19\end{pmatrix}.$$

In lettere:

$$\begin{pmatrix}\mathsf{R}\\ \mathsf{N}\\ \mathsf{A}\end{pmatrix}, \begin{pmatrix}\mathsf{I}\\ \mathsf{V}\\ \mathsf{V}\end{pmatrix}, \begin{pmatrix}\mathsf{H}\\ \mathsf{C}\\ \mathsf{W}\end{pmatrix}, \begin{pmatrix}\mathsf{X}\\ \mathsf{T}\\ \mathsf{F}\end{pmatrix}, \begin{pmatrix}\mathsf{Z}\\ \mathsf{V}\\ \mathsf{H}\end{pmatrix}, \begin{pmatrix}\mathsf{Z}\\ \mathsf{V}\\ \mathsf{S}\end{pmatrix}, \begin{pmatrix}\mathsf{F}\\ \mathsf{C}\\ \mathsf{V}\end{pmatrix}, \begin{pmatrix}\mathsf{Z}\\ \mathsf{O}\\ \mathsf{T}\end{pmatrix}.$$

Osserviamo che la lettera O è stata sostituita con le lettere N, T, V e V. Per decifrare il messaggio, Alice deve moltiplicare per

$$A^{-1} = \begin{pmatrix}4 & 23 & 25\\ 23 & 3 & 0\\ 3 & 23 & 1\end{pmatrix}.$$

Formalizzando, per applicare il cifrario di Hill, fissiamo una matrice $A \in \mathrm{GL}_m(\mathbb{Z}_{26})$ e dividiamo il plaintext in sequenze di m lettere (se la lunghezza del testo non è un multiplo di m, aggiungiamo in coda delle lettere extra, tipo una sequenza ZZZ...). Convertendo le lettere in elementi di $\mathbb{Z}_{26}$, otteniamo una sequenza di vettori colonna $v_1, v_2, \ldots, v_k$ di lunghezza m a valori in $\mathbb{Z}_{26}$. Applichiamo ora la funzione $\psi_A : v_i \mapsto Av_i$ e riconvertiamo gli elementi di $\mathbb{Z}_{26}$ in lettere, ottenendo così il ciphertext.

Anche il cifrario di Vigenère è un tentativo per evitare l'attacco tramite l'analisi delle frequenze. Questo crittosistema sembra essere stato inventato intorno al 1553 da Giovan Battista Bellaso, ma nel XIX secolo fu erroneamente attribuito a Blaise de Vigenère (1523–1596), un altro crittografo. Tale metodo fu comunemente utilizzato durante la prima guerra mondiale e ritenuto inattaccabile, anche se il crittografo prussiano Friedrich Wilhelm Kasiski aveva già pubblicato nel 1863 un metodo per la sua decifratura.

Nel cifrario di Vigenère la chiave è una sequenza (adeguatamente lunga) di shift. Scegliamo, ad esempio, 2, 5, 4, 7 e applichiamo questi shift ciclicamente:

2	5	4	7	2	5	4	7	2	5
A	R	R	I	V	O	O	G	G	I
C	W	V	P	X	T	S	M	I	N

L'ultima linea è il ciphertext. Per decifrare il messaggio, bisogna conoscere la chiave e applicare gli shift opposti. Notiamo come lettere uguali (le due O, per esempio) vengano cifrate in modo diverso: il metodo di Vigenère resiste quindi all'attacco tramite l'analisi delle frequenze, o almeno così sembrerebbe...

Ancora più comodo risulta l'utilizzo di una parola ripetuta (facile da memorizzare o comunicare), che viene letta come una serie di shift, come illustrato nella Figura 3.

A $\leftrightarrow$ ψ_0	B $\leftrightarrow$ ψ_1	C $\leftrightarrow$ ψ_2
D $\leftrightarrow$ ψ_3	E $\leftrightarrow$ ψ_4	F $\leftrightarrow$ ψ_5
G $\leftrightarrow$ ψ_6	H $\leftrightarrow$ ψ_7	I $\leftrightarrow$ ψ_8
J $\leftrightarrow$ ψ_9	K $\leftrightarrow$ ψ_{10}	L $\leftrightarrow$ ψ_{11}
M $\leftrightarrow$ ψ_{12}	N $\leftrightarrow$ ψ_{13}	O $\leftrightarrow$ ψ_{14}
P $\leftrightarrow$ ψ_{15}	Q $\leftrightarrow$ ψ_{16}	R $\leftrightarrow$ ψ_{17}
S $\leftrightarrow$ ψ_{18}	T $\leftrightarrow$ ψ_{19}	U $\leftrightarrow$ ψ_{20}
V $\leftrightarrow$ ψ_{21}	W $\leftrightarrow$ ψ_{22}	X $\leftrightarrow$ ψ_{23}
Y $\leftrightarrow$ ψ_{24}	Z $\leftrightarrow$ ψ_{25}	

FIGURA 3. Identificazione lettera-shift.

Prendiamo ad esempio la parola ROMA.

R	O	M	A	R	O	M	A	R	O
A	R	R	I	V	O	O	G	G	I
R	F	D	I	M	C	A	G	X	W

In altre parole, abbiamo calcolato

$$\begin{array}{rcccl} \mathsf{R}+\mathsf{A} & = & \psi_{17}([0]_{26}) = [17]_{26} & = & \mathsf{R} \\ \mathsf{O}+\mathsf{R} & = & \psi_{14}([17]_{26}) = [5]_{26} & = & \mathsf{F} \\ \vdots & & & & \vdots \end{array}$$

2.4. Esercizi

ESERCIZIO 2.1. Sia A un anello commutativo. Provare, usando gli assiomi della Definizione 2.1, che ogni elemento di A ammette un unico opposto e che ogni elemento invertibile di A ammette un unico inverso (rispetto al prodotto).

ESERCIZIO 2.2. Sia A un anello commutativo. Provare, usando gli assiomi della Definizione 2.1, che per ogni $a \in A$ si ha $a \cdot 0 = 0$, $-(-a) = a$ e $(-1) \cdot a = -a$.

ESERCIZIO 2.3. Determinare gli elementi unitari di $\mathbb{Q}$.

ESERCIZIO 2.4. Determinare gli elementi unitari di $\mathbb{Z}_5$ e di $\mathbb{Z}_8$. Determinare per ciascuno di essi l'inverso.

ESERCIZIO 2.5. Per ognuna delle seguenti coppie (a, b), determinare $d = \mathrm{M.C.D.}(a, b)$ e determinare due interi x, y tali che $d = ax + by$:

$$(15, 20), \quad (13, 21), \quad (153, 222), \quad (195, 208), \quad (255, 323), \quad (3215, 7073).$$

ESERCIZIO 2.6. Calcolare l'inverso dei seguenti elementi (se esistono):

$$[13]_{15}, \quad [7]_{21}, \quad [100]_7, \quad [111]_{212}.$$

ESERCIZIO 2.7. Avete ricevuto da Giulio Cesare il seguente messaggio:

$$\mathsf{YHQL} \quad \mathsf{YLGL} \quad \mathsf{YLFL}.$$

Cosa vi ha comunicato?

ESERCIZIO 2.8. Considerate la funzione $\psi_{a,b}$ descritta in (2.1) e determinatene l'inversa (quando esiste) per ognuna delle seguenti coppie (a, b):

$$(11, 13), \quad (20, 5), \quad (9, 5), \quad (7, 19), \quad (15, 15), \quad (8, 8).$$

ESERCIZIO 2.9. Data una matrice $A = \begin{pmatrix} [a]_n & [b]_n \\ [c]_n & [d]_n \end{pmatrix}$ a valori in $\mathbb{Z}_n$ tale che $\mathrm{M.C.D.}(ad - bc, n) = 1$, provare che

$$A^{-1} = [ad - bc]_n^{-1} \begin{pmatrix} [d]_n & [-b]_n \\ [-c]_n & [a]_n \end{pmatrix}.$$

ESERCIZIO 2.10. Calcolare la matrice inversa A^{-1}, se esiste, nei seguenti casi:

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_6), \quad \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_5), \quad \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_7),$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_4), \quad \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_5), \quad \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_8).$$

ESERCIZIO 2.11. Bob vuol mandare ad Alice il seguente messaggio

ATTENTA IL NEMICO CI SPIA.

Applica quindi il cifrario di Hill utilizzando la matrice $A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$. Qual è il ciphertext che Bob invia ad Alice?

ESERCIZIO 2.12. Alice riceve il seguente messaggio di Bob:

JX NNWYYQVJ EP BFUITH UIFYK VU R.

Sapendo che Bob ha utilizzato il cifrario di Hill con la matrice $A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, cosa ha comunicato Bob?

ESERCIZIO 2.13. Applicate il cifrario di Vigenère al messaggio

GASTON DE FOIX E ENTRATO NEL CASTELLO,

utilizzando la chiave BRESCIA.

ESERCIZIO 2.14. Decifrate il seguente messaggio, sapendo che è stato applicato il cifrario di Vigenère con chiave TARTAGLIA:

B SFEDGEQ FKAEVEYT AOGO VGTXLBI GEC WUUXW.

ESERCIZIO 2.15. Alice ha inviato a Bob il seguente messaggio:
TWJJSEMW SROWRVLELOS TWMERS.

Decifrate tale messaggio, sapendo che Alice ha utilizzato un cifrario affine basato sulla funzione $\psi_{5,4}$. Bob risponde così, utilizzando un cifrario permutazionale:
POZO OTVPF,
VLPYLIZVOEYPV O JZFCPVO VL WVO UFTTO DOZQFIIO HSOZOLIYIIY.
HSFCIY EFIYUY LYL F CVPSZY: AFZ V AZYCCVEV EFCCODDV SCO
VT PVGZOZVY UV WVDFLFZF. TFDDFZOV TO PMVOWF OTT'VLDZFCCY.

Bob invia poi il seguente messaggio:
MNZJ EC HZBMQ PBTBZ KQRSS DMD CCZG IFV HIQQXM V LZXNVA.

Cosa ha comunicato Bob ad Alice?

CAPITOLO 3

Sistemi crittografici a chiave pubblica

Per poter vedere il funzionamento di un sistema crittografico *asimmetrico*, abbiamo bisogno di qualche altro risultato algebrico.

3.1. Funzione di Eulero

DEFINIZIONE 3.1. Sia $\mathbb{N}^+ = \{a \in \mathbb{Z} : a \geq 1\}$. Si chiama *funzione di Eulero* la funzione $\phi : \mathbb{N}^+ \to \mathbb{N}^+$ definita nel seguente modo. Per ogni $n \in \mathbb{N}^+$,

$$\phi(n) = |\{k \in \mathbb{N}^+ : 1 \leq k \leq n \text{ e } \mathrm{M.C.D.}(k, n) = 1\}|.$$

Per esempio, si ha

$$\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \quad \phi(4) = 2, \quad \phi(5) = 4, \quad \phi(6) = 2.$$

PROPOSIZIONE 3.2. *Valgono le seguenti proprietà:*

(1) *se* $a, b \in \mathbb{N}^+$ *sono tali che* $\mathrm{M.C.D.}(a, b) = 1$*, allora* $\phi(ab) = \phi(a)\phi(b)$*;*
(2) *se* $p \in \mathbb{N}^+$ *è un primo e* $n \geq 1$*, allora* $\phi(p^n) = p^n - p^{n-1}$.

ESEMPIO 3.3. Calcoliamo $\phi(540)$. Fattorizziamo $540 = 2^2 \cdot 3^3 \cdot 5$ da cui

$$\phi(540) = \phi(2^2) \cdot \phi(3^3) \cdot \phi(5) = (4 - 2) \cdot (27 - 9) \cdot (5 - 1) = 144.$$

TEOREMA 3.4 (Eulero). *Siano* $a, n > 1$ *tali che* $\mathrm{M.C.D.}(a, n) = 1$*. Allora*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

ESEMPIO 3.5. Prendiamo $a = 77$ e $n = 540$. Allora

$$77^{144} \equiv 1 \pmod{540}.$$

Infatti, $77^{144} = 1 + 540 \cdot (836123952768667103644516911262982045490694183082125901$
$717589320938869965600927727214075210027503015579963213922373454727317355442$
$897246859296598878003914478592496429766090864084032619451302577058714849101$
$960932931128787219681045647702987691938196256533634816762077227 36).$

COROLLARIO 3.6 (Piccolo Teorema di Fermat). *Sia* $p \in \mathbb{N}^+$ *un primo e sia* $a \in \mathbb{N}^+$ *tale che* $\mathrm{M.C.D.}(a, p) = 1$*. Allora*

$$a^p \equiv a \pmod{p}.$$

DIMOSTRAZIONE. Segue dal fatto che, se p è un primo, allora $\phi(p) = p - 1$. Applicando il Teorema 3.4 si ottiene $a^{p-1} \equiv 1 \pmod{p}$, cioè che $[a^{p-1}]_p = [1]_p$. Moltiplicando per $[a]_p$ otteniamo $[a^p]_p = [a]_p$, cioè $a^p \equiv a \pmod{p}$. □

ESEMPIO 3.7. Prendiamo $p = 11$ e $a = 19$. Allora

$$19^{11} \equiv 19 \pmod{11}.$$

Infatti abbiamo $19^{11} = 116490258898219 = 19 + 11 \cdot 10590023536200$.

CONGETTURA 3.8 (Carmichael, 1907). *Per ogni* $n \in \mathbb{N}^+$*, esiste* $m \in \mathbb{N}^+$ *con* $m \neq n$ *tale che* $\phi(m) = \phi(n)$.

ESEMPIO 3.9. Ecco alcune prove a supporto di questa congettura:

$$\phi(1) = \phi(2) = 1, \quad \phi(3) = \phi(4) = \phi(6) = 2,$$

$$\phi(5) = \phi(8) = \phi(10) = \phi(12) = 4, \quad \phi(7) = \phi(9) = \phi(14) = \phi(18) = 6.$$

3.2. Un sistema crittografico asimmetrico

I sistemi crittografici simmetrici funzionano bene se Alice e Bob riescono a scambiarsi in sicurezza la chiave (incontrandosi, ad esempio, lontano dagli occhi di Eve). Questo però non è sempre possibile: ad esempio, Alice effettua un acquisto online e vuole inviare del denaro a Bob che si trova in un altro continente. Essi non possono incontrarsi né scambiarsi la chiave tramite telefono o e-mail, per timore di essere intercettati da Eve. Per risolvere questo problema, utilizzano un sistema crittografico a chiave *pubblica*. Alice genera due chiavi, una pubblica che manda a Bob e una privata, che tiene per sé. Bob, utilizzando la chiave pubblica, può cifrare il messaggio da mandare ad Alice utilizzando un canale pubblico. Alice, e solo lei, può decifrare il messaggio, conoscendo la chiave privata. Alice e Bob dispongono di informazioni diverse: Alice possiede le due chiavi, Bob solo quella pubblica. Per tale motivo questo sistema crittografico è asimmetrico.

Uno dei sistemi crittografici asimmetrici più utilizzati ai giorni nostri è il metodo RSA (dagli inventori, Rivest, Shamir e Adleman). La sua sicurezza si basa sulla difficoltà computazionale del fattorizzare un intero con un grande numero di cifre. Dall'altro lato, tale sistema richiede molta potenza di calcolo, per cui risulta poco pratico per inviare lunghi messaggi. Solitamente, si utilizza il metodo RSA per inviare in modo sicuro la chiave privata di un sistema simmetrico (da utilizzare poi per inviare il messaggio).

(1) Alice sceglie due numeri primi distinti p e q, e calcola
$$n = pq \quad \text{e} \quad \phi(n) = (p-1)(q-1).$$
(2) Alice sceglie la chiave di cifratura e in modo che M.C.D.$(e, \phi(n)) = 1$.
(3) Alice calcola la chiave di decifratura d in modo che $ed \equiv 1 \pmod{\phi(n)}$.
(4) Alice rende pubblici e e n, mantenendo segreti p, q, d.

Ora Bob vuole mandare un messaggio ad Alice:

(1) Bob chiede ad Alice la chiave pubblica (e, n).
(2) Bob scrive il proprio messaggio $m \pmod{n}$.
(3) Bob calcola
$$c \equiv m^e \pmod{n}.$$
(4) Bob manda ad Alice il messaggio c.

Alice, per decifrare il messaggio di Bob, calcola

$$m \equiv c^d \pmod{n}.$$

ESEMPIO 3.10. Alice sceglie i primi (nella realtà saranno molto più grandi, più di 100 cifre)

$$p = 3598279, \quad q = 7815629.$$

Può facilmente calcolare

$$n = pq = 28122813702491, \quad \phi(n) = 28122802288584.$$

Ora, Alice deve scegliere un esponente e per la cifratura (ne basta uno piccolo, molto usato è 65537), in modo che M.C.D.$(e, \phi(n)) = 1$. Alice prende

$$e = 233,$$

e quindi calcola (tramite l'algoritmo euclideo)

$$d = 27519308677241.$$

La chiave pubblica che viene divulgata è quindi $(e, n) = (233, 28122813702491)$.

Bob vuole comunicare ad Alice che si incontreranno in auto. Decide quindi di inviarle il messaggio CAR, cioè l'intero

$$m = 03\ 01\ 18 = 30118.$$

Qui Bob usa l'identificazione A $= 01, \ldots,$ Z $= 26$. Prende allora la chiave pubblica di Alice e calcola (come?):

$$c \equiv m^e \equiv 30118^{233} \equiv 21666077416496 \pmod{28122813702491}.$$

Alice riceve quindi il testo $c = 21666077416496$, che decifra nel modo seguente (come?):

$$m \equiv c^d \equiv 21666077416496^{2751930867724} \equiv 30118 \pmod{28122813702491}.$$

Ora, da $m = 30118$ ricava il messaggio originale CAR.

Vediamo prima di tutto perché Alice riesce a decifrare il messaggio di Bob.

PROPOSIZIONE 3.11. *Siano p, q due primi distinti e si ponga $n = pq$. Siano d, e due interi positivi tali che $ed \equiv 1 \pmod{\phi(n)}$. Allora, per ogni intero m tale che* M.C.D.$(m, n) = 1$*, si ha*

$$m^{ed} \equiv m \pmod{n}.$$

Quindi, se $c \equiv m^e \pmod{n}$, allora $m \equiv c^d \pmod{n}$.

DIMOSTRAZIONE. Poiché $ed \equiv 1 \pmod{\phi(n)}$, possiamo scrivere

$$ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$$

per un opportuno $k \in \mathbb{Z}$. Per il Teorema 3.4 (Eulero), abbiamo

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

da cui

$$m^{ed} \equiv m^{1+k\phi(n)} \equiv m(m^{\phi(n)})^k \equiv m \cdot 1^k \equiv m \pmod{n}.$$

□

Il caso M.C.D.$(m, n) \neq 1$ è molto improbabile, visto che p e q sono due primi molto grandi. Può comunque sempre essere evitato dividendo il messaggio m in più parti.

Vediamo ora come sono stati ottenuti d, m^e, c^d. Alice deve calcolare la chiave di decifratura d in modo che $ed \equiv 1 \pmod{\phi(n)}$. In altre parole, deve determinare

$[d]_{\phi(n)} = ([e]_{\phi(n)})^{-1}$. Alice quindi calcola:

$$\begin{aligned} 28122802288584 &= 233 \cdot 120698722268 + 140 \\ 233 &= 140 \cdot 1 + 93 \\ 140 &= 93 \cdot 1 + 47 \\ 93 &= 47 \cdot 1 + 46 \\ 47 &= 46 \cdot 1 + 1 \\ 46 &= 1 \cdot 46 + 0 \end{aligned}$$

e risalendo

$$\begin{aligned} 1 &= 47 \cdot 1 - 46 \cdot 1 \\ &= 47 \cdot 2 - 93 \cdot 1 \\ &= 140 \cdot 2 - 93 \cdot 3 \\ &= 140 \cdot 5 - 233 \cdot 3 \\ &= 28122802288584 \cdot 5 - 233 \cdot 603493611343. \end{aligned}$$

Ottiene così $[d]_{\phi(n)} = [-603493611343]_{28122802288584} = [27519308677241]_{\phi(n)}$, cioè $d = 27519308677241$.

Bob invece deve calcolare $m^e \pmod n$: attenzione, non calcola m^e e poi riduce modulo n, ma direttamente $[m^e]_n$. Anche qui, iniziamo con un esempio più facile: calcoliamo $3^{385} \pmod{479}$. Iniziamo con le seguenti potenze, ottenute quadrando la precedente:

$$\begin{aligned} 3^2 &\equiv 9 \pmod{479}, \\ 3^4 &\equiv 9^2 \equiv 81 \pmod{479}, \\ 3^8 &\equiv 81^2 \equiv 334 \pmod{479}, \\ 3^{16} &\equiv 334^2 \equiv 428 \pmod{479}, \\ 3^{32} &\equiv 428^2 \equiv 206 \pmod{479}, \\ 3^{64} &\equiv 206^2 \equiv 284 \pmod{479}, \\ 3^{128} &\equiv 284^2 \equiv 184 \pmod{479}, \\ 3^{256} &\equiv 184^2 \equiv 326 \pmod{479}. \end{aligned}$$

Ora, scriviamo $385 = 256 + 128 + 1$, ottenendo

$$3^{385} \equiv 3^{256} \cdot 3^{128} \cdot 1 \equiv 236 \cdot 184 \cdot 3 \equiv 237 \pmod{479}.$$

Per calcolare $30118^{233} \pmod{28122813702491}$ abbiamo:

$$\begin{aligned} 30118^2 &\equiv 907093924 \pmod{28122813702491}, \\ 30118^4 &\equiv 2103650236098 \pmod{28122813702491}, \\ 30118^8 &\equiv 24824004621578 \pmod{28122813702491}, \\ 30118^{16} &\equiv 27269132180366 \pmod{28122813702491}, \\ 30118^{32} &\equiv 28098731400573 \pmod{28122813702491}, \\ 30118^{64} &\equiv 24038757816969 \pmod{28122813702491}, \\ 30118^{128} &\equiv 14769900920905 \pmod{28122813702491}. \end{aligned}$$

Scrivendo $233 = 128 + 64 + 32 + 8 + 1$, otteniamo

$$\begin{aligned} 30118^{233} &\equiv 14769900920905 \cdot 24038757816969 \cdot 28098731400573 \cdot \\ &\quad 24824004621578 \cdot 30118 \\ &\equiv 21666077416496 \pmod{28122813702491}. \end{aligned}$$

Infine, Alice deve calcolare $c^d \pmod n$. Prima di vedere come, chiediamoci perché Eve non riesce a decifrare il messaggio che eventualmente ha intercettato? Non conoscendo p, q, Eve ha bisogno di una grossa potenza di calcolo e di molto tempo per calcolare $d \pmod{\phi(n)}$ e ancor di più per calcolare $c^d \pmod n$. Alice invece, può utilizzare il piccolo Teorema di Fermat e sfruttare il Teorema Cinese dei Resti.

Alice ha ricevuto il messaggio $c = 21666077416496$ e deve calcolare $c^d \pmod n$. Poiché $n = pq$, inizia calcolando $c^d \pmod p$ e $c^d \pmod q$:

$$\begin{aligned} c^d &\equiv 21666077416496^{27519308677241} \equiv 1158489^{27519308677241} \\ &\equiv (1158489^{(p-1)})^{7647910} \cdot 1158489^{2378261} \\ &\equiv 1158489^{2378261} \equiv 30118 \pmod{3598279}. \end{aligned}$$

$$\begin{aligned} c^d &\equiv 21666077416496^{27519308677241} \equiv 4931033^{27519308677241} \\ &\equiv (4931033^{(q-1)})^{3521061} \cdot 4931033^{5735933} \\ &\equiv 4931033^{5735933} \\ &\equiv 30118 \pmod{7815629}. \end{aligned}$$

Si tratta di risolvere ora il seguente sistema di congruenze lineari:

$$\begin{cases} c^d \equiv 30118 \pmod{3598279}, \\ c^d \equiv 30118 \pmod{7815629}. \end{cases}$$

Qui, viene facilmente

$$m \equiv c^d \equiv 30118 \pmod{3598279 \cdot 7815629}.$$

Più in generale, lo si può fare sempre utilizzando il metodo delle divisioni successive. Per esempio, vogliamo risolvere il sistema

$$\begin{cases} z \equiv 12 \pmod{15} \\ z \equiv 6 \pmod{21} \end{cases}$$

Lavorando in $\mathbb{Z}$ abbiamo $z = 12 + 15 \cdot x = 6 + 21 \cdot y$, da cui

$$15 \cdot x - 21 \cdot y = -6.$$

Ora dividiamo 21 per 15:

$$\begin{aligned} 21 &= 15 \cdot 1 + 6 \\ 15 &= 6 \cdot 2 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

Ricaviamo così che M.C.D.$(21, 15) = 3$ e $3 = 15 \cdot 3 - 21 \cdot 2$; moltiplicando per $-2 = \frac{-6}{3}$ otteniamo

$$15 \cdot (-6) - 21 \cdot (-4) = -6$$

cioè $x = -6$ e $y = -4$. Finalmente,

$$z \equiv 12 + 15(-6) \equiv -78 \equiv 27 \pmod{105}.$$

Qui, dobbiamo lavorare modulo 105, il minimo comun multiplo di 15 e 21.

3.3. Firma digitale

Alice vuole stipulare una polizza assicurativa e si rivolge a Bob, il suo agente assicurativo. Invece di stampare il contratto e inviarlo ad Alice per essere firmato, Bob sceglie di inviare il contratto via mail, in modo che Alice lo approvi. Bob non si preoccupa della sicurezza del contratto, è una polizza standard, ma vuole essere sicuro che Alice ha davvero firmato il contratto (e non Eve che magari ha avuto accesso alla casella di posta elettronica di Alice). Come possono fare?

Sia m il documento da firmare, che Bob ha proposto ad Alice, Come nel metodo RSA, Alice sceglie due primi grandi p, q, li moltiplica ottenendo $n = pq$, sceglie un intero e tale che M.C.D.$(e, \phi(n)) = 1$ e $1 < e < \phi(n)$. Calcola poi d tale che $ed \equiv 1 \pmod{\phi(n)}$, pubblica (e, n), mentre tiene segreti p, q, d.

Alice crea la sua firma s calcolando

$$s \equiv m^d \pmod{n},$$

e quindi invia (s, m) a Bob. Ora, come può Bob essere sicuro che Alice ha davvero firmato il contratto? Calcola

$$s^e \equiv (m^d)^e \equiv m^{ed} \equiv m \pmod{n}.$$

Lo schema è ancora quello dell'RSA, applicato in ordine inverso:

(1) Alice pubblica (e, n) e tiene segreti p, q, d;
(2) Alice firma $s \equiv m^d \pmod{n}$;
(3) Il documento firmato è (s, m);
(4) Bob verifica se $s^e \equiv m \pmod{n}$.

Supponiamo che Eve falsifichi la firma di Alice. Per ingannare Bob, deve trovare una firma s_1 tale che $s_1^e \equiv m \pmod{n}$, e questo è computazionalmente molto improbabile. Allo stesso modo, anche partendo da s_1 e computando $m_1 \equiv s_1^e \pmod{n}$, è molto improbabile che m_1 risulti un messaggio sensato.

3.4. Esercizi

ESERCIZIO 3.1. Bob vuole comunicare con Alice usando il metodo RSA. Alice sceglie quindi la coppia di primi $p = 1117$ e $q = 1217$ e la chiave di cifratura $e = 113$. Bob, ricevuta la chiave pubblica, invia ad Alice la password del suo conto bancario. Alice riceve il messaggio $c = 1015894$. Qual è la password di Bob?

ESERCIZIO 3.2. Alice e Bob decidono di comunicare in modo sicuro, sfruttando sia il metodo RSA sia un cifrario affine. Alice prende $p = 251$, $q = 277$ ed invia a Bob la chiave pubblica $(49, 69527)$ del sistema RSA. Usando tale chiave, Bob invia ad Alice prima il messaggio $(52063, 13175)$ e in seguito il messaggio KZXOL IBTBOGL.

Alice, decodificando il primo messaggio, ricava la coppia $(100a, 100b)$ e quindi, applicando l'inverso della funzione $\psi_{a,b}$ al secondo messaggio, ricava il testo della comunicazione di Bob. Quale era il messaggio di Bob?