Capitolo 3

# Teoria dei numeri

Nei moderni sistemi di crittanalisi, i messaggi sono rappresentati da valori numerici prima di essere cifrati e trasmessi. I processi di cifratura sono operazioni matematiche che trasformano i valori numerici di input in valori numerici di output. Per costruire, analizzare e attaccare questi crittosistemi servono strumenti matematici. Il più importante di questi è la teoria dei numeri e in modo particolare la teoria delle congruenze. In questo capitolo si presentano gli strumenti fondamentali che saranno usati nel resto del libro. Argomenti più avanzati, come la fattorizzazione, il logaritmo discreto e le curve ellittiche, verranno trattati in capitoli successivi (più precisamente, nei Capitoli 6, 7, 16).

## 3.1 Nozioni di base

### 3.1.1 Divisibilità

La teoria dei numeri si occupa delle proprietà dei numeri interi. Una delle proprietà più importanti è la divisibilità.

**Definizione.** *Dati due interi $a$ e $b$, con $a \neq 0$, si dice che $a$* **divide** *$b$, e si scrive $a|b$, quando esiste un intero $k$ tale che $b = ak$. Equivalentemente, si dice che $b$ è un multiplo di $a$.*

**Esempi.** $3|15$, $-15|60$, $7 \nmid 18$ (non divide). ■

**Proposizione.** *Siano $a, b, c$ tre numeri interi.*

1. *Per ogni $a \neq 0$, si ha che $a|0$ e $a|a$. Inoltre, $1|b$ per ogni $b$.*

2. *Se $a|b$ e $b|c$, allora $a|c$.*

3. *Se $a|b$ e $a|c$, allora $a|(sb+tc)$ per ogni intero $s$ e $t$.*

*Dimostrazione.* (1) Poiché $0 = a \cdot 0$, la condizione che compare nella definizione è verificata per $k = 0$ e quindi $a|0$. Poiché $a = a \cdot 1$, si ha $k = 1$ e quindi $a|a$. Poichè $b = b \cdot 1$, si ha $1|b$. (2) Se esistono due numeri $k$ e $\ell$ per cui $b = ak$ e $c = b\ell$, allora $c = (k\ell)a$, ossia $a|c$. (3) Se $b = ak_1$ e $c = ak_2$, allora $sb + tc = a(sk_1 + tk_2)$ e quindi $a|sb + tc$. □

Per esempio, se $a = 2$ nel punto (2), allora $2|b$ significa semplicemente che $b$ è pari. La proposizione dice che $c$, che è un multiplo del numero pari $b$, deve essere anch'esso pari (cioé un multiplo di $a = 2$).

### 3.1.2 Numeri primi

Un **numero primo** è numero intero $p > 1$ divisibile solo per 1 e per se stesso. I valori iniziali dei numeri primi sono $2, 3, 5, 7, 11, 13, 17, \ldots$ Un **numero composto** è un numero intero $n > 1$ non primo, ossia un numero $n$ esprimibile come il prodotto $ab$ di due interi con $1 < a, b < n$. Come era già noto a Euclide, esistono infiniti primi. Più precisamente, si ha la seguente proprietà dimostrata nel 1896 (della quale non si dà la dimostrazione che esula dagli scopi di questo libro).

**Teorema dei numeri primi.** *Se $\pi(x)$ è il numero dei primi minori di $x$, allora*

$$\pi(x) \sim \frac{x}{\ln x},$$

*ossia il rapporto $\pi(x)/(x/\ln x) \to 1$ per $x \to +\infty$.*

In varie applicazioni si utilizzano numeri primi grandi, con circa 100 cifre. Il numero dei primi con 100 cifre può essere stimato nel modo seguente:

$$\pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 3.9 \times 10^{97}.$$

Più avanti si discuterà come determinare questi primi.
I numeri primi sono i mattoni con cui si costruiscono gli interi. Infatti ogni intero positivo ha un'unica rappresentazione come prodotto di numeri primi distinti elevati a un'opportuna potenza. Per esempio, 504 e 1125 hanno le seguenti fattorizzazioni

$$504 = 2^3\,3^2\,7, \qquad 1125 = 3^2\,5^3.$$

Inoltre queste fattorizzazioni sono uniche, a meno dell'ordine dei fattori. Per esempio, se si fattorizza 504 in primi, allora si troveranno sempre tre fattori uguali a 2, due fattori uguali a 3 e un fattore uguale a 7.

**Teorema.** *Ogni intero positivo è prodotto di primi. Questa fattorizzazione è unica, a meno dell'ordine dei fattori.*



*Dimostrazione.* Come prima cosa osserviamo che il prodotto vuoto è convenzionalmente posto uguale a 1 (analogamente alla proprietà che $x^0 = 1$). Pertanto l'intero positivo 1 è il prodotto di zero primi. Inoltre ogni primo è il prodotto di un solo primo. Si supponga che esista almeno un intero positivo che non sia prodotto di primi. Sia $n$ il più piccolo di questi interi. Allora $n$, non potendo essere uguale a 1 (che è il prodotto vuoto) né a un primo (che è il prodotto di un solo primo), deve essere composto, ossia $n = ab$ con $1 < a, b < n$. Poiché $n$ è il più piccolo intero positivo che non è prodotto di primi, sia $a$ che $b$ sono prodotti di primi. Ma un prodotto di primi per un prodotto di primi è un prodotto di primi, ossia $n = ab$ è un prodotto di primi. Si ha quindi una contraddizione che mostra che l'insieme degli interi positivi che non sono prodotto di primi è l'insieme vuoto. Di conseguenza ogni intero positivo è un prodotto di primi.
L'unicità della fattorizzazione è più difficile da dimostrare e si basa sul seguente lemma (che verrà dimostrato alla fine di questo paragrafo, dopo aver discusso l'algoritmo euclideo).

**Lemma.** *Se un primo $p$ divide un prodotto di interi $ab$, allora $p|a$ oppure $p|b$. Più in generale, se un primo $p$ divide un prodotto $ab\cdots z$, allora $p$ divide uno dei fattori $a, b, \ldots, z$.*

Per esempio, per $p = 2$, se un prodotto di due interi è pari allora uno dei due interi deve essere pari.
Continuando con la dimostrazione del teorema, si supponga che un intero $n$ possa essere scritto come prodotto di primi in due modi diversi:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t},$$

dove $p_1, \ldots, p_s$ e $q_1, \ldots, q_t$ sono primi e gli esponenti $a_i$ e $b_j$ sono non nulli. Se un primo compare in entrambe le fattorizzazioni, basta dividere entrambi i membri per ottenere un'identità più corta. Continuando in questo modo, si può assumere che nessuno dei primi $p_1, \ldots, p_s$ compaia tra i $q_j$. Poiché $p_1$ divide $n$, che è uguale a $q_1 q_1 \cdots q_1 q_2 \cdots q_t$, per il lemma $p_1$ deve dividere uno dei fattori $q_j$. Poiché $q_j$ è primo, si ha $p_1 = q_j$ e questo è contro l'ipotesi che $p_1$ non compaia tra i $q_j$. Quindi un intero non può avere due fattorizzazioni diverse. □

### 3.1.3 Massimo comune divisore

Il **massimo comune divisore** di due numeri interi $a$ e $b$ è il più grande intero positivo che divide sia $a$ che $b$ e viene indicato con MCD($a$,$b$), oppure con $(a,b)$. In questo libro si userà la prima notazione.

**Esempi.** $\mathrm{MCD}(6,4) = 2$, $\mathrm{MCD}(5,7) = 1$, $\mathrm{MCD}(24,60) = 12$. ■

Due numeri interi $a$ e $b$ sono **primi tra loro** se MCD($a$,$b$) $= 1$. Ci sono due modi standard per determinare il massimo comune divisore di due numeri.

1. **Se si conosce la fattorizzazione di $a$ e $b$ in primi, allora il loro massimo comune divisore è dato dal prodotto dei primi che compaiono in entrambe le fattorizzazioni di $a$ e $b$, ognuno scelto con l'esponente minore.** Per esempio

$$576 = 2^6 3^2, \quad 135 = 3^3 5, \quad \text{MCD}(576,135) = 3^2 = 9$$

$$\text{MCD}(2^5 3^4 7^2, 2^2 5^3 7) = 2^2 3^0 5^0 7^1 = 2^2 7 = 28.$$

Si osservi che se un primo non compare in una fattorizzazione, allora esso non può apparire nel massimo comune divisore.

2. Se $a$ e $b$ sono numeri grandi, allora può non essere facile fattorizzarli. Il massimo comune divisore può essere calcolato con l'**algoritmo euclideo**. Si tratta di utilizzare la divisione con il resto, come si vede dai seguenti esempi preliminari.

**Esempio.** Calcolare MCD(482, 1180).

*Soluzione.* Dividendo 1180 per 482, il quoziente è 2 e il resto è 216. Ora dividendo 482 per il resto 216, il quoziente è 2 e il resto è 50. Dividendo il vecchio resto 216 per il nuovo resto 50, il quoziente è 4 e il resto è 16. Continuando in questo modo, dividendo il vecchio resto per il nuovo resto, alla fine si ottiene il massimo comune divisore. Nel caso presente si ottiene 2:

$$\begin{aligned} 1180 &= 2 \cdot 482 + 216 \\ 482 &= 2 \cdot 216 + 50 \\ 216 &= 4 \cdot 50 + 16 \\ 50 &= 3 \cdot 16 + 2 \\ 16 &= 8 \cdot 2 + 0. \end{aligned}$$

Si noti come i numeri si trasformano:

$$\text{resto} \to \text{divisore} \to \text{dividendo} \to \text{ignora}.$$

Ecco un secondo esempio:

$$\begin{aligned} 12345 &= 1 \cdot 11111 + 1234 \\ 11111 &= 9 \cdot 1234 + 5 \\ 1234 &= 246 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Quindi MCD(12345,11111) = 1. ■

Usando questi esempi come linea guida, è ora possibile dare una descrizione più formale dell'**algoritmo euclideo**. Si può sempre supporre che $a$ sia maggiore di $b$ (in caso contrario basta scambiare $a$ con $b$). Il primo passo consiste nel dividere $a$ per $b$, ossia nello scrivere $a$ nella forma

$$a = q_1 b + r_1.$$



Se $r_1 = 0$, allora $b$ divide $a$ e il massimo comune divisore è $b$. Se $r_1 \neq 0$, allora si continua scrivendo $b$ nella forma

$$b = q_2 r_1 + r_2.$$

Si continua in questo modo finché il resto non è zero:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k. \end{aligned}$$

Alla fine si ha

$$\text{MCD}(a,b) = r_k.$$

Ci sono due aspetti importanti di questo algoritmo.

1. Non richiede la fattorizzazione dei numeri.
2. È veloce.

Per la dimostrazione del fatto che in questo modo si ottiene effettivamente il massimo comune divisore, si veda l'Esercizio 28.
L'algoritmo euclideo permette di dimostrare il seguente fondamentale risultato.

**Teorema.** *Siano $a$ e $b$ due interi, non entrambi nulli, e sia $d = \text{MCD}(a,b)$. Allora esistono due interi $x$ e $y$ tali che $ax + by = d$. In particolare, se $a$ e $b$ sono primi tra loro, allora esistono due interi $x$ e $y$ tali che $ax + by = 1$.*

*Dimostrazione.* Più in generale, si dimostrerà che se $r_j$ è un resto ottenuto applicando l'algoritmo euclideo, allora esistono due interi $x_j$ e $y_j$ tali che $r_j = ax_j + by_j$. Per $j = 1$, si ha $r_1 = ax_1 + by_1$ con $x_1 = 1$ e $y_1 = -q_1$. Analogamente, $r_2 = a(-q_2) + b(1 + q_1 q_2)$. Si supponga ora di avere $r_i = ax_i + by_i$ per ogni $i < j$. Allora

$$r_j = r_{j-2} - q_j r_{j-1} = ax_{j-2} + by_{j-2} - q_j(ax_{j-1} + by_{j-1}).$$

ossia

$$r_j = a(x_{j-2} - q_j x_{j-1}) + b(y_{j-2} - q_j y_{j-1}).$$

Continuando in questo modo, la proprietà risulta valida per ogni $j$ e in particolare per $j = k$. Poiché $r_k = \text{MCD}(a,b)$, la dimostrazione è conclusa. □

Come corollario si ha il lemma utilizzato nella dimostrazione dell'unicità della fattorizzazione in primi.

**Corollario.** *Se un primo $p$ divide un prodotto di interi $ab$, allora $p|a$ oppure $p|b$. Più in generale, se un primo $p$ divide un prodotto $ab\cdots z$, allora $p$ deve dividere uno dei fattori $a, b, \ldots, z$.*

*Dimostrazione.* Nel caso in cui $p|ab$, se $p$ divide $a$ allora non c'è più nulla da dimostrare. Si può così assumere che $p \nmid a$. In questo caso $p|b$. Infatti, poiché $p$ è primo, $\text{MCD}(a,p) = 1$ o $\text{MCD}(a,p) = p$. Poiché $p \nmid a$, deve essere $\text{MCD}(a,p) = 1$. Quindi esistono due interi $x$ e $y$ tali che $ax + py = 1$. Moltiplicando per $b$ si ha $abx + pby = b$. Poiché $p|ab$ e $p|p$, si ha $p|abx + pby$, ossia $p|b$.
Se $p|ab\cdots z$, allora $p|a$ o $p|b\cdots z$. Se $p|a$, la dimostrazione è conclusa. Altrimenti, $p|b\cdots z$. Si ha così un prodotto più corto. O $p|b$, nel qual caso si è a posto, o $p$ divide il prodotto dei rimanenti fattori. Continuando in questo modo, alla fine si trova che $p$ divide uno dei fattori del prodotto. □

La proprietà enunciata nel corollario vale solo per i numeri primi. Per esempio, se un prodotto $ab$ è divisibile per 6, non si può concludere che $a$ o $b$ è un multiplo di 6. Il problema è che $6 = 2 \cdot 3$ e il 2 può essere in $a$, mentre il 3 può essere in $b$, come nell'esempio $60 = 4 \cdot 15$. Più in generale, se $n = ab$ è un numero composto, allora $n|ab$ ma $n \nmid a$ e $n \nmid b$. Quindi, i primi e 1 sono gli unici interi che possiedono la proprietà enunciata nel corollario.

## 3.2 L'equazione $ax + by = d$

Un fatto molto importante, che verrà dimostrato più avanti, è che per ogni intero $a$ e $b$ esistono due interi $x$ e $y$ tali che

$$ax + by = \text{MCD}(a,b).$$

Per trovare $x$ e $y$, si inizia a dividere $b$ per $a$, cosicché $b = q_1 a + r_1$, e poi si procede come nell'algoritmo euclideo. Sia $q_1, q_2, \ldots, q_n$ la successione dei quozienti. Nel primo esempio del Paragrafo 3.1, si ha $q_1 = 2$, $q_2 = 2$, $q_3 = 4$, $q_4 = 3$, $q_5 = 8$. Formando le successioni

$$x_0 = 0, \quad x_1 = 1, \quad x_j = -q_{j-1}x_{j-1} + x_{j-2}$$
$$y_0 = 1, \quad y_1 = 0, \quad y_j = -q_{j-1}y_{j-1} + y_{j-2}$$

si ha

$$ax_n + by_n = \text{MCD}(a,b).$$

Nel primo esempio, si ha

$$\begin{aligned} x_0 &= 0, \quad x_1 = 1 \\ x_2 &= -2x_1 + x_0 = -2 \\ x_3 &= -2x_2 + x_1 = 5 \\ x_4 &= -4x_3 + x_2 = -22 \\ x_5 &= -3x_4 + x_3 = 71. \end{aligned}$$



Analogamente si ottiene $y_5 = -29$. Un facile calcolo mostra che

$$482 \cdot 71 + 1180 \cdot (-29) = 2 = \text{MCD}(482, 1180).$$

Si noti che non si è usato l'ultimo quoziente. Se lo si fosse usato, si sarebbe ottenuto $x_{n+1} = 590$, che è il numero 1180 di partenza diviso per il massimo comune divisore, ossia 2. Analogamente $y_{n+1} = 241$ è $482/2$.
Il metodo precedente è spesso chiamato **algoritmo euclideo esteso**. Esso sarà usato nel prossimo paragrafo per risolvere alcune congruenze.
Per numeri piccoli, $x$ e $y$ possono essere trovati in un altro modo che non richiede di tener traccia di tanti indici. Si consideri l'esempio $\text{MCD}(12345, 11111) = 1$ del paragrafo precedente. Si useranno i numeri provenienti da quel calcolo. L'idea è quella di tornare indietro utilizzando i resti 1, 4, 5, 1234, e i numeri 11111 e 12345 di partenza, e ottenere alla fine il massimo comune divisore 1 come una combinazione di 12345 e 11111. Dalla riga che dà il massimo comune divisore, si ottiene

$$1 = 5 - 1 \cdot 4,$$

ossia si ottiene 1 come combinazione dei due resti precedenti. Salendo di una riga, si ottiene 4 come combinazione di 1234 e 5 e quindi, andando a sostituire nell'equazione precedente, si ha

$$4 = 1234 - 246 \cdot 5,$$

ossia

$$1 = 5 - 1 \cdot 4 = 5 - 1 \cdot (1234 - 246 \cdot 5) = 247 \cdot 5 - 1 \cdot 1234.$$

Per ora si sono utilizzati gli ultimi due resti provenienti dal calcolo del massimo comune divisore. Il resto non ancora utilizzato, cioè 5, può essere scritto come combinazione di 11111 e 1234 e quindi sostituito nell'ultima equazione:

$$1 = 247 \cdot (11111 - 9 \cdot 1234) - 1 \cdot 1234 = 247 \cdot 11111 - 2224 \cdot 1234.$$

Infine, sostituendo 1234, si ottiene

$$1 = 247 \cdot 11111 - 2224 \cdot (12345 - 1 \cdot 11111) = 2471 \cdot 11111 - 2224 \cdot 12345.$$

Questo dà il massimo comune divisore 1 come combinazione di 12345 e 11111. Se il calcolo del massimo comune divisore non richiede troppi passaggi, questa procedura è piuttosto semplice da eseguire a mano. In generale, tuttavia, il metodo precedente è migliore e adatto al computer.

## 3.3 Congruenze

Uno degli strumenti più importanti e di maggiore utilità della teoria dei numeri è dato dall'aritmetica modulare, ossia dalle congruenze.

**Definizione.** *Siano $a$, $b$, $n$ tre numeri interi con $n \neq 0$. Si dice che $a$ è* **congruente** *$a$ $b$ modulo $n$, ossia*

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

*quando $a - b$ è un multiplo (positivo o negativo) di $n$.*

CEFRIEL

## Algoritmo di Euclide

$MCD(a,n) = n$

$MCD(m,n) = MCD(n \bmod m, m) \qquad m < n$

## Algoritmo di Euclide esteso per calcolare $MCD(a,b)$ $a < b$

$a^{-1} \bmod b$ se $a \perp b$

$MCD(a,b) = 1$

$x_0 = 0 \quad x_1 = 1$

$b = q_1 \cdot a + r_1$

$a = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

$r_2 = q_4 r_3 + r_4$

$\vdots$

$r_{k-2} = q_k \cdot r_{k-1} + r_k$

$r_{k-1} = q_{k+1} \cdot r_k + 0$

$t_{max}$

$MCD(a,b)$

$x_2 = -q_1 x_1 + x_0$

$x_3 = -q_2 x_2 + x_1$

$x_4 = -q_3 x_3 + x_2$

$x_5 = -q_4 x_4 + x_3$

$\vdots$

$x_{k+1} = -q_k x_k + x_{k-1}$

$t_{max}$

$x_{k+1} = a^{-1} \bmod b$

$(se\ MCD(a,b) = 1)$

$(non\ mai\ q_{max} = q_{k+1}!)$

Equivalentemente, si ha che $a \equiv b \pmod{n}$ se $a$ e $b$ differiscono per un multiplo di $n$, ossia se $a = b + nk$ per qualche intero $k$ (positivo o negativo).

**Esempi.** $32 \equiv 7 \pmod{5}$, $-12 \equiv 37 \pmod{7}$, $17 \equiv 17 \pmod{13}$.

Le congruenze si comportano in modo analogo alle uguaglianze. Per questo motivo la notazione per le congruenze è stata scelta in modo da ricordare quella delle uguaglianze.

**Proposizione.** *Siano $a$, $b$, $c$, $n$ quattro numeri interi con $n \neq 0$.*

1. *$a \equiv 0 \pmod{n}$ se e solo se $n|a$.*
2. *$a \equiv a \pmod{n}$.*
3. *$a \equiv b \pmod{n}$ se e solo se $b \equiv a \pmod{n}$.*
4. *Se $a \equiv b$ e $b \equiv c \pmod{n}$, allora $a \equiv c \pmod{n}$.*

*Dimostrazione.* (1) $a \equiv 0 \pmod{n}$ significa che $a = a - 0$ è un multiplo di $n$, ossia che $n|a$. (2) Poiché $a - a = 0 \cdot n$, si ha $a \equiv a \pmod{n}$. (3) Se $a \equiv b \pmod{n}$, si ha $a - b = nk$. Quindi $b - a = n(-k)$, cioé $b \equiv a \pmod{n}$. Ribaltando i ruoli di $a$ e di $b$ si ottiene l'implicazione inversa. (4) Poiché $a = b + nk$ e $c = b + n\ell$, si ha $a - c = n(k - \ell)$, ossia $a \equiv c \pmod{n}$. □

Si lavorerà spesso con gli interi modulo $n$. L'insieme di questi interi è indicato con $\mathbb{Z}_n$ e può essere pensato come l'insieme $\{0, 1, 2, \ldots, n-1\}$ munito dell'addizione, della sottrazione e della moltiplicazione modulo $n$. Se $a$ è un intero, allora dividendo $a$ per $n$ si ottiene un resto in questo insieme:

$$a = nq + r \qquad \text{con} \quad 0 \leq r < n$$

(si tratta semplicemente della divisione con resto, dove $q$ è il quoziente e $r$ è il resto). Di conseguenza $a \equiv r \pmod{n}$ e pertanto ogni numero $a$ è congruente modulo $n$ a qualche intero $r$ con $0 \leq r < n$.

**Proposizione.** *Siano $a$, $b$, $c$, $d$, $n$ degli interi con $n \neq 0$, tali che $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Allora*

$$a + c \equiv b + d, \quad a - c \equiv b - d, \quad ac \equiv bd \pmod{n}.$$

*Dimostrazione.* Si ha $a = b + nk$ e $c = d + n\ell$, per opportuni interi $k$ e $\ell$. Di conseguenza $a + c = b + d + n(k + \ell)$, ossia $a + c \equiv b + d \pmod{n}$. Analogamente si dimostra che $a - c \equiv b - d$. Per la moltiplicazione, si ha $ac = bd + n(dk + b\ell + nk\ell)$, ossia $ac \equiv bd$. □

La proposizione dice che per le congruenze valgono le usuali operazioni di addizione, sottrazione e moltiplicazione. Per moltiplicare due numeri modulo $n$ si può procedere nel modo seguente. Se il prodotto è minore di $n$, ci si ferma. Se invece il prodotto è maggiore di $n - 1$, lo si divide per $n$ e si prende il resto. L'addizione e la sottrazione si eseguono in modo analogo. Per esempio, per i numeri modulo 6 si hanno le seguenti tavole di addizione e di moltiplicazione:



| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| × | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

**Esempio.** Risolvere l'equazione $x + 7 \equiv 3 \pmod{17}$.

*Soluzione.* $x \equiv 3 - 7 \equiv -4 \equiv 13 \pmod{17}$. ■

Non c'è nulla di sbagliato nella soluzione negativa ma, quando si lavora modulo $n$, il risultato finale viene scelto tra 0 e $n - 1$.

### 3.3.1 Divisione

La divisione modulo $n$ è molto più delicata di quella tra numeri razionali. La regola generale è che si può dividere per $a$ modulo $n$ quando $\text{MCD}(a,n) = 1$.

**Proposizione.** *Siano $a$, $b$, $c$, $n$ quattro numeri interi con $n \neq 0$ e con $\text{MCD}(a,n) = 1$. Se $ab \equiv ac \pmod{n}$, allora $b \equiv c \pmod{n}$. In altre parole, se $a$ e $n$ sono primi tra loro, entrambi i membri della congruenza possono essere semplificati dividendo per $a$.*

*Dimostrazione.* Poiché $\text{MCD}(a,n) = 1$, esistono due interi $x$ e $y$ tali che $ax + ny = 1$. Moltiplicando per $b - c$ si ottiene

$$(ab - ac)x + n(b - c)y = b - c.$$

Poiché $ab - ac$ è, per ipotesi, un multiplo di $n$ e poiché $n(b - c)y$ è ovviamente un multiplo di $n$, si ha che anche $b - c$ è un multiplo di $n$. Quindi $b \equiv c \pmod{n}$. □

**Esempio.** Risolvere l'equazione $2x + 7 \equiv 3 \pmod{17}$.

*Soluzione.* Si ha $2x \equiv 3 - 7 \equiv -4$ e quindi $x \equiv -2 \equiv 15 \pmod{17}$. La divisione per 2 è lecita essendo $\text{MCD}(2,17) = 1$. ■

**Esempio.** Risolvere l'equazione $5x + 6 \equiv 13 \pmod{11}$.

*Soluzione.* Si ha $5x \equiv 7 \pmod{11}$. E ora? Si dovrebbe dividere per 5, ma cosa significa $7/5$ modulo 11? Si noti che $7 \equiv 18 \equiv 29 \equiv 40 \equiv \cdots \pmod{11}$. Pertanto $5x \equiv 7$ è uguale a $5x \equiv 40$. Ora si può dividere per 5 e ottenere come risposta $x \equiv 8 \pmod{11}$. Si noti che, essendo $7 \equiv 8 \cdot 5 \pmod{11}$, il numero 8 si comporta come $7/5$. ■

L'ultimo esempio può essere risolto anche in un altro modo. Poiché $5 \cdot 9 \equiv 1 \pmod{11}$, si ha che 9 è l'inverso moltiplicativo di 5 (mod 11). Di conseguenza dividere per 5 è equivalente a moltiplicare per 9. Se si vuole risolvere $5x \equiv 7 \pmod{11}$, basta moltiplicare entrambi i membri per 9, ottenendo

$$x \equiv 45x \equiv 63 \equiv 8 \pmod{11}.$$

**Proposizione.** *Sia* $\mathrm{MCD}(a,n) = 1$ *e siano* $s$ *e* $t$ *due interi tali che* $as + nt = 1$ *(essi possono essere trovati usando l'algoritmo euclideo esteso). Allora* $as \equiv 1 \pmod{n}$, *ossia* $s$ *è l'inverso moltiplicativo di* $a \pmod{n}$.

*Dimostrazione.* Poiché $as - 1 = -nt$, si ha che $as - 1$ è un multiplo di $n$. □

L'algoritmo euclideo esteso è abbastanza efficiente per il calcolo dell'inverso moltiplicativo di $a$ mediante il metodo descritto nella proposizione.

**Esempio.** Risolvere l'equazione $11111x \equiv 4 \pmod{12345}$.

*Soluzione.* Utilizzando il calcolo di $\mathrm{MCD}(12345, 11111)$ fatto in precedenza, si hanno i quozienti $q_1 = 1$, $q_2 = 9$, $q_3 = 246$, $q_4 = 1$, $q_5 = 4$. Pertanto, nell'algoritmo euclideo esteso, si ha $x_0 = 0$, $x_1 = 1$, $x_2 = -1$, $x_3 = 10$, $x_4 = -2461$, $x_5 = 2471$, da cui $11111 \cdot 2471 + 12345 \cdot y_5 = 1$. Quindi

$$11111 \cdot 2471 \equiv 1 \pmod{12345}.$$

Moltiplicando entrambi i membri della congruenza originale per 2471 si ottiene

$$x \equiv 9884 \pmod{12345}.$$

In pratica, questo significa che se stiamo lavorando mod 12345 e incontriamo la frazione 4/11111, è possibile sostituirla con 9884. Anche se questo può sembrare un po' strano, basta pensare al significato di 4/11111. È semplicemente un simbolo che rappresenta una quantità che moltiplicata per 11111 dà 4. Quando si lavora modulo 12345, anche il numero 9884 ha questa proprietà poiché $11111 \cdot 9884 \equiv 4 \pmod{12345}$. ■

Possiamo riassumere quanto visto nel modo seguente.

**Calcolo di** $a^{-1} \pmod{n}$.

1. Mediante l'algoritmo euclideo esteso si trovano gli interi $s$ e $t$ tali che $as + nt = 1$.
2. $a^{-1} \equiv s \pmod{n}$.

**Risoluzione dell'equazione** $ax \equiv c \pmod{n}$ **con** $\mathrm{MCD}(a,n) = 1$. *(Questo equivale a considerare una frazione* $c/a$ *con* $\mathrm{MCD}(a,n) = 1$, *quando si lavora modulo* $n$.*)*

1. Mediante l'algoritmo euclideo esteso si trovano gli interi $s$ e $t$ tali che $as + nt = 1$.
2. La soluzione è $x \equiv cs \pmod{n}$ (equivalentemente, si sostituisce la frazione $c/a$ con $cs \pmod{n}$).



**Cosa accade se** $\mathrm{MCD}(a,n) > 1$? Per risolvere una congruenza della forma $ax \equiv b \pmod{n}$ quando $\mathrm{MCD}(a,n) = d > 1$ si procede nel modo seguente.

1. Se $d$ non divide $b$, allora non ci sono soluzioni.
2. Se $d|b$, si considera la nuova congruenza

   $$(a/d)x \equiv b/d \pmod{n/d}$$

   dove $a/d$, $b/d$, $n/d$ sono interi e $\mathrm{MCD}(a/d, n/d) = 1$. Si risolve quindi questa congruenza mediante la procedura precedente ottenendo una soluzione $x_0$.
3. Le soluzioni della congruenza originale $ax \equiv b \pmod{n}$ sono

   $$x_0, \quad x_0 + (n/d), \quad x_0 + 2(n/d), \ldots, \quad x_0 + (d-1)(n/d) \qquad \pmod{n}.$$

**Esempio.** Risolvere la congruenza $12x \equiv 21 \pmod{39}$.

*Soluzione.* Si ha che $\mathrm{MCD}(12, 39) = 3$ e che 3 divide 21. Dividendo per 3 si ottiene la nuova congruenza $4x \equiv 7 \pmod{13}$. Provando a sostituire direttamente qualche numero o utilizzando l'algoritmo euclideo esteso, si trova la soluzione $x_0 = 5$. Di conseguenza, le soluzioni della congruenza originale sono $x \equiv 5, 18, 31 \pmod{39}$. ■

Nella congruenza precedente $x$ compare solo al primo grado. Tuttavia, anche le congruenze non lineari sono utili. Spesso si incontrano equazioni della forma

$$x^2 \equiv a \pmod{n}.$$

Per esempio, le soluzioni di $x^2 \equiv 1 \pmod{7}$ sono $x \equiv 1, 6 \pmod{7}$, come si può vedere facilmente sostituendo direttamente a $x$ i valori $0, 1, 2, \ldots, 6$. In generale, quando $p$ è un primo dispari, $x^2 \equiv 1 \pmod{p}$ ha esattamente due soluzioni $x \equiv \pm 1 \pmod{p}$ (si veda l'Esercizio 8).
Tuttavia, per l'equazione $x^2 \equiv 1 \pmod{15}$, sostituendo a $x$ i numeri 0, 1, 2, ..., 14, si trovano le soluzioni $x = 1, 4, 11, 14$. Per esempio, $11^2 \equiv 121 \equiv 1 \pmod{15}$. Quindi una congruenza quadratica per un modulo composto può avere più di due soluzioni, a differenza di quanto accade con le equazioni di secondo grado sul campo dei numeri reali, che possiedono al massimo due soluzioni. Questo fenomeno verrà studiato nel Paragrafo 3.4, mentre nei Paragrafi 6.4 (fattorizzazione), 13.1 (lancio di monete) e 14.2 (schemi di identificazione) si incontreranno alcune sue applicazioni.

### 3.3.2 Frazioni

In molte situazioni conviene lavorare con le frazioni modulo $n$. Per esempio, $1/2 \pmod{12345}$ è più semplice da scrivere che $6173 \pmod{12345}$ (si noti che $2 \cdot 6173 \equiv 1 \pmod{12345}$). La regola generale è che la frazione $b/a$ può essere usata modulo $n$ se $\mathrm{MCD}(a,n) = 1$. Naturalmente bisogna ricordare che $b/a \pmod{n}$ in realtà

significa $a^{-1}b \pmod n$, dove $a^{-1}$ è l'intero modulo $n$ che soddisfa l'equazione $a^{-1}a \equiv 1 \pmod n$.
Equivalentemente, il simbolo "1/2" può essere pensato come il simbolo che possiede la proprietà seguente: se si moltiplica 1/2 per 2 si ottiene 1. In ogni calcolo che coinvolga 1/2, questa è l'unica proprietà che si usa. Lavorando modulo 12345, anche il numero 6173 possiede questa proprietà, poiché $6173 \cdot 2 \equiv 1 \pmod{12345}$. Di conseguenza 1/2 (mod 12345) e 6713 (mod 12345) sono intercambiabili.
Si tenga presente che non è possibile lavorare con frazioni aventi denominatore arbitrario. Naturalmente non si può usare 1/6 (mod 6), perché si dovrebbe dividere per 0 (mod 6). Ma non si può utilizzare nemmeno 1/2 (mod 6). Per esempio, moltiplicando entrambi i membri di $2 \equiv 8 \pmod 6$ per 1/2 si otterrebbe $1 \equiv 4 \pmod 6$ e questo è falso. Il problema è che $\mathrm{MCD}(2,6) = 2 \neq 1$. Poiché 2 è un fattore di 6, si può pensare la divisione per 2 come una "divisione parziale per 0", che non è ammessa.

## 3.4 Teorema cinese del resto

In molti casi è utile spezzare una congruenza modulo $n$ in un sistema di congruenze modulo i fattori di $n$. Si supponga, per esempio, che un numero $x$ soddisfi l'equazione $x \equiv 25 \pmod{42}$. Questo significa che $x = 25 + 42k$ per un opportuno intero $k$. Riscrivendo 42 come $7 \cdot 6$, si ha $x = 25 + 7(6k)$, da cui $x \equiv 25 \equiv 4 \pmod 7$. Analogamente, poiché $x = 25 + 6(7k)$, si ha $x \equiv 25 \equiv 1 \pmod 6$. Quindi

$$x \equiv 25 \pmod{42} \quad \Longrightarrow \quad \begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 1 \pmod 6. \end{cases}$$

Il Teorema cinese del resto mostra che questa implicazione può essere invertita, ossia che sotto opportune condizioni un sistema di congruenze può essere sostituito da un'unica congruenza.

**Teorema cinese del resto.** *Siano $m$ e $n$ due interi positivi tali che* $\mathrm{MCD}(m,n) = 1$. *Dati due interi $a$ e $b$, esiste esattamente una soluzione $x \pmod{mn}$ del sistema di congruenze*

$$x \equiv a \pmod m, \qquad x \equiv b \pmod n.$$

*Dimostrazione.* Poiché $m$ e $n$ sono primi tra loro, esistono due interi $s$ e $t$ tali che $ms + nt = 1$. Quindi $ms \equiv 1 \pmod n$ e $nt \equiv 1 \pmod m$. Posto $x = bms + ant$, si ha $x \equiv ant \equiv a \pmod m$ e $x \equiv bms \equiv b \pmod n$. Quindi esiste almeno una soluzione $x$. Se $x_1$ è un'altra soluzione, allora $x \equiv x_1 \pmod m$ e $x \equiv x_1 \pmod n$ e quindi $x - x_1$ è un multiplo sia di $m$ sia di $n$.

**Lemma.** *Siano $m$ e $n$ due interi tali che* $\mathrm{MCD}(m,n) = 1$. *Se un intero $c$ è multiplo sia di $m$ sia di $n$, allora $c$ è un multiplo di $mn$.*

*Dimostrazione.* Si ha $c = mk = n\ell$, per due interi $k$ e $\ell$, e $ms + nt = 1$, per altri due interi $s$ e $t$. Pertanto si ha $c = cms + cnt = mn\ell s + mnkt = mn(\ell s + kt)$. □

Per concludere la dimostrazione, posto $c = x - x_1$ nel lemma, si ha che $x - x_1$ è un multiplo di $mn$. Quindi $x \equiv x_1 \pmod{mn}$, ossia due soluzioni del sistema di congruenze sono congruenti modulo $mn$. □



**Esempio.** Risolvere $x \equiv 3 \pmod 7$, $x \equiv 5 \pmod{15}$.

*Soluzione.* Si ha $x \equiv 80 \pmod{105}$ (si noti che $105 = 7 \cdot 15$). Poiché $80 \equiv 3 \pmod 7$ e $80 \equiv 5 \pmod{15}$, 80 è una soluzione. Il teorema garantisce che tale soluzione esiste e che è univocamente determinata modulo il prodotto $mn$, che nel presente esempio è 105. ■

Un modo per trovare la soluzione quando i numeri $m$ e $n$ sono piccoli, consiste nell'elencare i numeri congruenti a $b$ modulo $n$ finché si trova quello congruente ad $a$ modulo $m$. Per esempio, i numeri congruenti a 5 (mod 15) sono $5, 20, 35, 50, 65, 80, 95, \ldots$. Modulo 7, diventano $5, 6, 0, 1, 2, 3, 4, \ldots$. Poiché si vuole 3 (mod 7), si ha 80.

Quando i numeri $m$ e $n$ sono più grandi, questo metodo può diventare inefficiente. Tuttavia si può utilizzare un procedimento analogo. Poiché i numeri congruenti a $b \pmod n$ sono della forma $b + nk$, con $k$ intero, si tratta di risolvere $b + nk \equiv a \pmod m$, ossia

$$nk \equiv a - b \pmod m.$$

Poiché per ipotesi $\mathrm{MCD}(m,n) = 1$, esiste un inverso moltiplicativo $i$ per $n \pmod m$. Moltiplicando per $i$ si ha

$$k \equiv (a - b)i \pmod m.$$

Sostituendo in $x = b + nk$ e riducendo modulo $mn$, si ottiene la risposta.
Naturalmente per numeri grandi la dimostrazione del teorema dà un metodo efficiente per trovare $x$ che è quasi uguale a quello appena descritto.

**Esempio.** Risolvere $x \equiv 7 \pmod{12345}$, $x \equiv 3 \pmod{11111}$.

*Soluzione.* Per i calcoli fatti nel Paragrafo 3.3, l'inverso di 11111 (mod 12345) è $i = 2471$. Di conseguenza $k \equiv 2471(7 - 3) \equiv 9884 \pmod{12345}$ e quindi $x = 3 + 11111 \cdot 9884 \equiv 109821127 \pmod{(11111 \cdot 12345)}$. ■

Come si usa il teorema cinese del resto? L'idea è che se si parte con una congruenza modulo un numero composto $n$, tale congruenza può essere spezzata in congruenze simultanee modulo ognuna delle potenze di primi che fattorizzano $n$, in modo da ottenere il risultato modulo $n$ ricombinando i vari risultati parziali. Il vantaggio è che spesso è più facile analizzare congruenze modulo un primo o modulo una potenza di primo che lavorare modulo un numero composto.
Si supponga di voler risolvere $x^2 \equiv 1 \pmod{35}$. Poiché $35 = 5 \cdot 7$, si ha

$$x^2 \equiv 1 \pmod{35} \quad \Longleftrightarrow \quad \begin{cases} x^2 \equiv 1 \pmod 7 \\ x^2 \equiv 1 \pmod 5. \end{cases}$$

Ora, $x^2 \equiv 1 \pmod 5$ ha due soluzioni: $x \equiv \pm 1 \pmod 5$. Anche $x^2 \equiv 1 \pmod 7$ ha due soluzioni: $x \equiv \pm 1 \pmod 7$. Esse possono essere messe insieme in quattro modi:

$$x \equiv 1 \pmod 5, \quad x \equiv 1 \pmod 7 \quad \longrightarrow \quad x \equiv 1 \pmod{35},$$

$$x \equiv 1 \pmod 5, \quad x \equiv -1 \pmod 7 \quad \longrightarrow \quad x \equiv 6 \pmod{35},$$
$$x \equiv -1 \pmod 5, \quad x \equiv 1 \pmod 7 \quad \longrightarrow \quad x \equiv 29 \pmod{35},$$
$$x \equiv -1 \pmod 5, \quad x \equiv -1 \pmod 7 \quad \longrightarrow \quad x \equiv 34 \pmod{35}.$$

Pertanto le soluzioni di $x^2 \equiv 1 \pmod{35}$ sono $x \equiv 1, 6, 29, 34 \pmod{35}$.
In generale, se $n = p_1 p_2 \cdots p_r$ è il prodotto di $r$ primi dispari distinti, allora $x^2 \equiv 1 \pmod n$ ha $2^r$ soluzioni. Questo è una conseguenza del seguente

**Teorema cinese del resto (forma generale).** *Siano $m_1, \ldots, m_k$ degli interi tali che $\mathrm{MCD}(m_i, m_j) = 1$ per ogni $i \neq j$. Dati gli interi $a_1, \ldots, a_k$, esiste esattamente una soluzione $x \pmod{m_1 \cdots m_k}$ delle seguenti congruenze simultanee*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_k \pmod{m_k}.$$

Per esempio, il teorema garantisce che esiste una soluzione delle congruenze simultanee

$$x \equiv 1 \pmod{11}, \quad x \equiv -1 \pmod{13}, \quad x \equiv 1 \pmod{17}.$$

Infatti la soluzione è $x \equiv 1871 \pmod{11 \cdot 13 \cdot 17}$. L'Esercizio 24 fornisce un metodo per calcolare il numero $x$ che compare nell'enunciato del teorema.

## 3.5 Elevamento a potenza mod $n$

In questo e nei prossimi due paragrafi, verranno discusse alcune proprietà dei numeri del tipo

$$x^a \pmod n.$$

Si supponga di dover calcolare $2^{1234} \pmod{789}$. Se prima si calcola $2^{1234}$ e poi lo si riduce modulo 789, si è portati a lavorare con numeri molto grandi, anche se il risultato finale è un numero di sole tre cifre. Si dovrebbero svolgere tutte le moltiplicazioni e poi calcolare il resto. Calcolare le potenze consecutive di 2 porterebbe a eseguire il prodotto 1233 volte. Questo metodo è troppo lento per essere pratico, specialmente quando l'esponente è molto grande. Si può procedere più efficientemente nel modo seguente (dove tutte le congruenze sono modulo 789). Si parte da $2^2 \equiv 4 \pmod{789}$ e si procede elevando al quadrato entrambi i membri delle congruenze che di volta in volta si ottengono:

$$\begin{aligned}
2^4 &\equiv 4^2 \equiv 16 \\
2^8 &\equiv 16^2 \equiv 256 \\
2^{16} &\equiv 256^2 \equiv 49 \\
2^{32} &\equiv 34 \\
2^{64} &\equiv 367 \\
2^{128} &\equiv 559 \\
2^{256} &\equiv 37 \\
2^{512} &\equiv 580 \\
2^{1024} &\equiv 286.
\end{aligned}$$

Square & Multiply
resti, MA



Poiché $1234 = 1024 + 128 + 64 + 16 + 2$ (questo significa semplicemente che 1234 è uguale a 10011010010 in binario), si ha

$$2^{1234} \equiv 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 \equiv 481 \pmod{789}.$$

Si noti che in questo modo non si ha mai la necessità di lavorare con numeri più grandi di $788^2$.
Questo metodo funziona anche in generale. Il calcolo di $a^b \pmod n$ può sempre essere effettuato con al più $2\log_2(b)$ moltiplicazioni modulo $n$ e non si ha mai la necessità di lavorare con numeri più grandi di $n^2$. Questo significa che l'elevamento a potenza può essere fatto in modo molto rapido e senza utilizzare molta memoria.
Questo metodo è particolarmente utile se $a$, $b$ e $n$ sono numeri con 100 cifre. Se si calcola semplicemente $a^b$ e poi si riduce modulo $n$, la memoria del calcolatore va in overflow: il numero $a^b$ ha più di $10^{100}$ cifre, ossia ha un numero di cifre maggiore del numero delle particelle presenti nell'universo. Tuttavia, con il metodo considerato, il calcolo di $a^b \pmod n$ può essere effettuato in meno di 700 passi, senza mai usare numeri con più di 200 cifre. Nell'Esercizio 23 verrà data una versione algoritmica di questa procedura.

## 3.6 Fermat ed Eulero

Il teorema di Fermat[1] e il teorema di Eulero sono due risultati fondamentali della teoria dei numeri. Originariamente ammirati per il loro valore teorico, essi hanno oggi importanti applicazioni nella crittografia e sono ripetutamente usati in tutto il libro.

**Teorema di Fermat.** *Se $p$ è un numero primo che non divide $a$, allora*

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

*Dimostrazione.* Posto $S = \{1,2,3,\ldots,p-1\}$, si consideri la funzione $\psi : S \to S$ definita da $\psi(x) = ax \pmod p$. Per esempio, se $p = 7$ e $a = 2$, la funzione $\psi$ prende un numero $x$, lo moltiplica per 2 e riduce il risultato modulo 7.
Bisogna verificare che se $x \in S$, allora $\psi(x)$ è effettivamente in $S$, ossia che $\psi(x) \neq 0$. Se $\psi(x) = 0$, allora $ax \equiv 0 \pmod p$. Poiché $\mathrm{MCD}(a,p) = 1$, si può dividere questa congruenza per $a$ ottenendo $x \equiv 0 \pmod p$, ossia $x \notin S$. Questa contraddizione significa che $\psi(x)$ non può essere 0 e quindi che $\psi(x) \in S$.
Si supponga ora che esistano due elementi $x, y \in S$ tali che $\psi(x) = \psi(y)$, ossia tali che $ax \equiv ay \pmod p$. Poiché $\mathrm{MCD}(a,p) = 1$, si può dividere questa congruenza per $a$ e ottenere $x \equiv y \pmod p$. Pertanto, se $x$ e $y$ sono elementi distinti di $S$, allora anche $\psi(x)$ e $\psi(y)$ sono distinti. Di conseguenza $\psi(1), \psi(2), \psi(3), \ldots, \psi(p-1)$ sono tutti elementi distinti di $S$. Poiché $S$ ha solo $p-1$ elementi, questi sono esattamente gli elementi di $S$ scritti in un qualche ordine. Pertanto

$$\begin{aligned}
1 \cdot 2 \cdot 3 \cdots (p-1) &\equiv \psi(1) \cdot \psi(2) \cdot \psi(3) \cdots \psi(p-1) \\
&\equiv (a \cdot 1)(a \cdot 2)(a \cdot 3) \cdots (a \cdot (p-1)) \\
&\equiv a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \pmod p.
\end{aligned}$$

[1] Il teorema di Fermat usato in questo libro è anche noto come "piccolo teorema di Fermat", per distinguerlo dal più famoso "ultimo teorema di Fermat" che, tuttavia, il matematico francese non dimostrò. (*N.d.Rev.*)

Poiché $\text{MCD}(j,p) = 1$ per ogni $j \in S$, si può dividere questa congruenza per $1, 2, 3, \ldots, p-1$. Ciò che rimane è $1 \equiv a^{p-1} \pmod{p}$. □

**Esempio.** Dalla semplice congruenza $2^{10} = 1024 \equiv 1 \pmod{11}$ si può valutare $2^{53} \pmod{11}$. Basta scrivere $2^{53} = (2^{10})^5 2^3 \equiv 1^5 2^3 \equiv 8 \pmod{11}$. Si noti che quando si lavora modulo 11, sugli esponenti si lavora essenzialmente modulo 10 e non modulo 11. In altre parole, da $53 \equiv 3 \pmod{10}$ si deduce che $2^{53} \equiv 2^3 \pmod{11}$. ■

Di solito, se $2^{n-1} \equiv 1 \pmod{n}$, il numero $n$ è primo. Tuttavia, ci sono delle eccezioni: $561 = 3 \cdot 11 \cdot 17$ è composto ma $2^{560} \equiv 1 \pmod{561}$. Questo può essere spiegato nel modo seguente. Poiché $560 \equiv 0 \pmod{2}$, si ha $2^{560} \equiv 2^0 \equiv 1 \pmod{3}$. Analogamente, poiché $560 \equiv 0 \pmod{10}$ e $560 \equiv 0 \pmod{16}$, si ha che $2^{560} \equiv 1 \pmod{11}$ e $2^{560} \equiv 1 \pmod{17}$. Mettendo insieme questi due risultati mediante il teorema cinese del resto, si trova che $2^{560} \equiv 1 \pmod{561}$.
Un'altra di queste eccezioni è $1729 = 7 \cdot 13 \cdot 19$. Tuttavia, queste eccezioni sono piuttosto rare in pratica. Quindi, se $2^{n-1} \equiv 1 \pmod{n}$, è molto probabile che $n$ sia primo. Naturalmente, se $2^{n-1} \not\equiv 1 \pmod{n}$, allora $n$ non può essere primo. Poiché $2^{n-1} \pmod{n}$ può essere valutato molto rapidamente (si veda il Paragrafo 3.5), si ha così un metodo di ricerca dei numeri primi. Più precisamente, si sceglie un punto di partenza $n_0$ e successivamente si ripete il test per ogni numero dispari $n \geq n_0$ per vedere se $2^{n-1} \equiv 1 \pmod{n}$. Se $n$ fallisce il test, lo si scarta e si passa al successivo $n$. Quando $n$ supera il test, si usano tecniche più sofisticate per valutarne la primalità (si veda il Paragrafo 6.3). Il vantaggio è che questa procedura è molto più veloce che provare a fattorizzare ogni $n$, soprattutto poiché essa elimina molti $n$ rapidamente. Naturalmente, ci sono metodi per rendere più veloce la ricerca. Per esempio, si possono eliminare inizialmente tutti gli $n$ con fattori primi piccoli.
Esiste un teorema analogo a quello di Fermat anche quando il modulo $n$ è composto. Sia $\varphi(n)$ il numero di interi $1 \leq a \leq n$ tali che $\text{MCD}(a,n) = 1$. Per esempio, se $n = 10$ allora ci sono quattro di questi interi, ossia 1,3,7,9, e quindi $\varphi(10) = 4$. Spesso $\varphi$ è chiamata **funzione $\varphi$ di Eulero.**
Se $p$ è primo e $n = p^r$, allora basta eliminare tutti i multipli di $p$ per ottenere esattamente tutti gli $a$ con $\text{MCD}(a,n) = 1$. Quindi

$$\varphi(p^r) = \left(1 - \frac{1}{p}\right) p^r.$$

In particolare

$$\varphi(p) = p - 1.$$

Più in generale, dal teorema cinese del resto si può dedurre che per ogni intero $n$ si ha

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

dove il prodotto è esteso a tutti i primi $p$ che dividono $n$. Quando $n$ è il prodotto di due primi distinti, $n = pq$, si ha

$$\varphi(pq) = (p-1)(q-1).$$



**Esempi.**

$$\varphi(10) = (2-1)(5-1) = 4$$

$$\varphi(120) = 120\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 32.$$

■

**Teorema di Eulero.** *Se* $\text{MCD}(a,n) = 1$, *allora* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

*Dimostrazione.* La dimostrazione di questo teorema è simile a quella del teorema di Fermat. Sia $S$ l'insieme degli interi $1 \leq x \leq n$ con $\text{MCD}(x,n) = 1$. Sia $\psi : S \to S$ definita da $\psi(x) \equiv ax \pmod{n}$. Come nella dimostrazione del teorema di Fermat, i numeri $\psi(x)$ con $x \in S$ sono i numeri in $S$ scritti in un qualche ordine. Quindi

$$\prod_{x \in S} x \equiv \prod_{x \in S} \psi(x) \equiv a^{\varphi(n)} \prod_{x \in S} x.$$

Dividendo per i fattori $x \in S$, si resta con $1 \equiv a^{\varphi(n)} \pmod{n}$. □

Si noti che quando $n = p$ è primo, il teorema di Eulero si riduce al teorema di Fermat.

**Esempio.** Quali sono le ultime tre cifre di $7^{803}$?

*Soluzione.* Per determinare le ultime tre cifre basta lavorare modulo 1000. Poiché $\varphi(1000) = 1000(1 - \frac{1}{2})(1 - \frac{1}{5}) = 400$, si ha $7^{803} = (7^{400})^2 7^3 \equiv 7^3 \equiv 343 \pmod{1000}$. Quindi le ultime tre cifre sono 343. In questo esempio si può cambiare l'esponente 803 in 3 perché $803 \equiv 3 \pmod{\varphi(1000)}$. ■

**Esempio.** Calcolare $2^{43210} \pmod{101}$.

*Soluzione.* Si noti che 101 è primo. Dal teorema di Fermat si ha che $2^{100} \equiv 1 \pmod{101}$. Quindi

$$2^{43210} \equiv (2^{100})^{432} 2^{10} \equiv 1^{432} 2^{10} \equiv 1024 \equiv 14 \pmod{101}.$$

In questo caso si può cambiare l'esponente 43210 in 10, perché $43210 \equiv 10 \pmod{100}$. ■

Quanto appena visto può essere riassunto nel seguente

**Principio fondamentale.** *Siano $a$, $n$, $x$ e $y$ dei numeri interi con $n \geq 1$ e $\text{MCD}(a,n) = 1$. Se $x \equiv y \pmod{\varphi(n)}$, allora $a^x \equiv a^y \pmod{n}$. In altre parole, se si vuole lavorare modulo $n$, bisogna lavorare modulo $\varphi(n)$ sugli esponenti.*

*Dimostrazione.* Scritto $x = y + \varphi(n)k$, si ha

$$a^x = a^{y+\varphi(n)k} = a^y (a^{\varphi(n)})^k \equiv a^y 1^k \equiv a^y \pmod{n}.$$

□

Questa proprietà è molto importante e verrà utilizzata ripetutamente nel resto del libro. Pertanto, si riguardino gli esempi precedenti fino a quando non si sia persuasi che ciò che conta sono gli esponenti modulo $400 = \varphi(1000)$ e modulo 100 (e non gli esponenti modulo 1000 e modulo 101).

### 3.6.1 Protocollo a tre vie

Alice vuole mandare a Bob una chiave segreta $K$ (o un qualsiasi breve messaggio) mediante una comunicazione su un canale pubblico. Il Principio Fondamentale può essere utilizzato per risolvere questo problema.
Un modo non matematico per farlo è il seguente. Alice mette $K$ in una scatola, la chiude con il proprio lucchetto e la invia a Bob. Quando la riceve, Bob appone alla scatola il proprio lucchetto e la rimanda ad Alice. Quando riceve la scatola, Alice toglie il proprio lucchetto e la rimanda a Bob. Infine, Bob toglie il proprio lucchetto, apre la scatola e trova $K$.
Ecco ora una realizzazione matematica di questo metodo. Inizialmente, Alice sceglie un numero primo $p$ sufficientemente grande per rappresentare la chiave $K$. Per esempio, se Alice stesse cercando di inviare una chiave a 56 bit, avrebbe bisogno di un numero primo lungo almeno 56 bit. Tuttavia, per una questione di sicurezza, dovrebbe scegliere un primo significativamente più lungo di 56 bit (in modo che il problema del logaritmo discreto sia intrattabile). Alice pubblica $p$ in modo che Bob (o chiunque altro) possa scaricarlo. Bob scarica $p$. A questo punto Alice e Bob procederanno nel modo seguente.

1. Alice sceglie a caso un numero $a$ con $\text{MCD}(a, p-1) = 1$ e Bob sceglie a caso un numero $b$ con $\text{MCD}(b, p-1) = 1$. Gli inversi di $a$ e $b$ modulo $p-1$ verranno indicati con $a^{-1}$ e $b^{-1}$.
2. Alice manda a Bob $K_1 \equiv K^a \pmod{p}$.
3. Bob manda ad Alice $K_2 \equiv K_1^b \pmod{p}$.
4. Alice manda a Bob $K_3 \equiv K_2^{a^{-1}} \pmod{p}$.
5. Bob calcola $K \equiv K_3^{b^{-1}} \pmod{p}$.

Alla fine di questo protocollo, Alice e Bob hanno entrambi la chiave $K$.
Il motivo per cui questo metodo funziona è che Bob ha calcolato $K^{aba^{-1}b^{-1}} \pmod{p}$. Poiché $aa^{-1} \equiv bb^{-1} \equiv 1 \pmod{p-1}$, il principio fondamentale implica che $K^{aba^{-1}b^{-1}} \equiv K^1 \equiv K \pmod{p}$.
Questa procedura è usualmente attribuita a Shamir e a Massey e Omura. Uno svantaggio è che richiede più comunicazioni tra Alice e Bob. Inoltre, è vulnerabile all'attacco dell'intruso (si veda il Paragrafo 10.1).

## 3.7 Radici primitive

Si considerino le potenze di 3 (mod 7):

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1.$$



Si noti che si ottengono tutte le classi di congruenza non nulle modulo 7 come potenze di 3. Questo significa che 3 è una radice primitiva modulo 7 (il termine *generatore moltiplicativo* sarebbe migliore, ma non è così comune). Analogamente, ogni classe di congruenza non nulla modulo 13 è una potenza di 2 e quindi 2 è una radice primitiva modulo 13. Tuttavia, poiché $3^3 \equiv 1 \pmod{13}$, solo 1, 3, 9 sono potenze di 3. Quindi, 3 non è una radice primitiva modulo 13. Le radici primitive modulo 13 sono 2, 6, 7, 11.
In generale, quando $p$ è un primo, una **radice primitiva** modulo $p$ è un numero le cui potenze danno ogni classe non nulla modulo $p$. Si può dimostrare che ci sono $\varphi(p-1)$ radici primitive modulo $p$. In particolare, ne esiste sempre almeno una. In pratica, non è difficile trovarne una, almeno se la fattorizzazione di $p-1$ è nota (si veda l'Esercizio 21).
Quanto segue riassume le principali proprietà delle radici primitive.

**Proposizione.** *Sia $g$ una radice primitiva per un primo $p$.*

1. *Se $n$ è un intero, allora $g^n \equiv 1 \pmod{p}$ se e solo se $n \equiv 0 \pmod{p-1}$.*
2. *Se $j$ e $k$ sono interi, allora $g^j \equiv g^k \pmod{p}$ se e solo se $j \equiv k \pmod{p-1}$.*

*Dimostrazione.* Se $n \equiv 0 \pmod{p-1}$, allora $n = (p-1)m$ per qualche $m$. Quindi

$$g^n \equiv (g^m)^{p-1} \equiv 1 \pmod{p}$$

per il teorema di Fermat. Viceversa, si supponga che $g^n \equiv 1 \pmod{p}$. Bisogna dimostrare che $p-1$ divide $n$. Quindi basta dividere $n$ per $p-1$ e mostrare che il resto è 0. Sia

$$n = (p-1)q + r, \quad \text{con } 0 \le r < p-1$$

(si tratta semplicemente della divisione con quoziente $q$ e resto $r$). Si ha

$$1 \equiv g^n \equiv (g^q)^{p-1} g^r \equiv 1 \cdot g^r \equiv g^r \pmod{p}.$$

Si supponga $r > 0$. Se si considerano le potenze $g, g^2, \ldots$ di $g \pmod{p}$, allora si torna a 1 dopo $r$ passi. Pertanto

$$g^{r+1} \equiv g, \quad g^{r+2} \equiv g^2, \quad \ldots$$

e quindi le potenze di $g \pmod{p}$ danno solo gli $r$ numeri $g, g^2, \ldots, 1$. Poiché $r < p-1$, è impossibile che ogni numero modulo $p$ sia una potenza di $g$, contro l'ipotesi che $g$ è una radice primitiva. L'unica possibilità che rimane è che $r = 0$. Questo significa che $n = (p-1)q$, ossia che $p-1$ divide $n$. Il punto (1) è pertanto dimostrato.
Per dimostrare il punto (2), si supponga $j \ge k$ (altrimenti, basta scambiare $j$ con $k$). Si supponga che $g^j \equiv g^k \pmod{p}$. Dividendo entrambi i membri per $g^k$ si ha $g^{j-k} \equiv 1 \pmod{p}$. Per la parte (1), $j - k \equiv 0 \pmod{p-1}$, ossia $j \equiv k \pmod{p-1}$. Viceversa, se $j \equiv k \pmod{p-1}$, allora $j - k \equiv 0 \pmod{p-1}$ e quindi $g^{j-k} \equiv 1 \pmod{p}$, ancora per la parte (1). A questo punto basta moltiplicare per $g^k$. □

## 3.8 Inversione di matrici mod $n$

L'inversa di una matrice modulo $n$ può essere determinata mediante l'usuale metodo di inversione di una matrice, pur di applicare le opportune regole relative alle frazioni (viste nel Paragrafo 3.3). Qui il fatto fondamentale è che una matrice quadrata è invertibile modulo $n$ se e solo se il suo determinante e $n$ sono primi tra loro.
Per gli esempi di questo libro sarà sufficiente lavorare con matrici piccole. In questo caso, per trovare l'inversa di una matrice conviene lavorare con i numeri razionali e poi tornare ai numeri modulo $n$. In generale l'inversa di una matrice intera può sempre essere scritta come una matrice intera divisa per il determinante della matrice di partenza. Poiché si assume che il determinante e $n$ sono primi tra loro, il determinante può essere invertito come visto nel Paragrafo 3.3.
Per esempio, nel caso $2 \times 2$ la formula usuale è

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Quindi bisogna trovare un inverso per $ad - bc \pmod n$.

**Esempio.** Si supponga di dover invertire la matrice $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \pmod{11}$. Poiché $ad - bc = -2$, occorre l'inverso di $-2 \pmod{11}$. Poiché $5 \cdot (-2) \equiv 1 \pmod{11}$, si può sostituire $-1/2$ con 5. Pertanto

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} \equiv -\frac{1}{2}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \equiv 5\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \equiv \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix} \pmod{11}.$$

Un rapido calcolo mostra che

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix} = \begin{pmatrix} 23 & 11 \\ 55 & 23 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{11}.$$ ■

**Esempio.** Si supponga di dover calcolare l'inversa della matrice

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix} \pmod{11}.$$

Il determinante è 2 e l'inversa di $M$ sul campo razionale è

$$\frac{1}{2}\begin{pmatrix} 6 & -5 & 1 \\ -6 & 8 & -2 \\ 2 & -3 & 1 \end{pmatrix}.$$



(Per il calcolo dell'inversa di una matrice, si veda un qualunque testo di algebra lineare.) Sostituendo $1/2$ con 6 modulo 11, si ottiene

$$M^{-1} \equiv \begin{pmatrix} 3 & 3 & 6 \\ 8 & 4 & 10 \\ 1 & 4 & 6 \end{pmatrix} \pmod{11}.$$ ■

Perché è necessario che il determinante e $n$ siano primi tra loro? Si supponga che $MN \equiv I \pmod n$, dove $I$ è la matrice identica. Allora

$$\det(M)\det(N) \equiv \det(MN) \equiv \det(I) \equiv 1 \pmod n.$$

Quindi $\det(M)$ ha un inverso modulo $n$ e questo è possibile solo se $\det(M)$ e $n$ sono primi tra loro.

## 3.9 Radici quadrate mod $n$

Si supponga di sapere che l'equazione $x^2 \equiv 71 \pmod{77}$ ha soluzione. Come si può determinare una di queste soluzioni e come si possono trovare tutte le soluzioni? Più in generale, il problema è quello di determinare tutte le soluzioni dell'equazione $x^2 \equiv b \pmod n$, dove $n = pq$ è il prodotto di due primi. Se è nota la fattorizzazione di $n$, questo problema può essere risolto molto facilmente. Viceversa, se si conoscono tutte le soluzioni, allora $n$ può essere facilmente fattorizzato.
Iniziamo con il caso della radice quadrata modulo un primo $p$. Il caso più semplice è quando $p \equiv 3 \pmod 4$ e questo basta per i nostri scopi. Il caso in cui $p \equiv 1 \pmod 4$ è più difficile (vedi [Cohen, pp. 31–34]).

**Proposizione.** *Sia $p \equiv 3 \pmod 4$ un primo e sia $y$ un intero. Sia $x \equiv y^{(p+1)/4} \pmod p$.*

1. *Se $y$ ha una radice quadrata modulo $p$, allora le radici quadrate di $y$ modulo $p$ sono $\pm x$.*
2. *Se $y$ non ha radice quadrata modulo $p$, allora $-y$ ha una radice quadrata modulo $p$ e le radici quadrate di $-y$ sono $\pm x$.*

*Dimostrazione.* Se $y \equiv 0 \pmod p$, tutte le affermazioni sono banali. Si assuma pertanto che $y \not\equiv 0 \pmod p$. Il teorema di Fermat dice che $y^{p-1} \equiv 1 \pmod p$. Quindi

$$x^4 \equiv y^{p+1} \equiv y^2 y^{p-1} \equiv y^2 \pmod p.$$

Questo implica che $(x^2 + y)(x^2 - y) \equiv 0 \pmod p$ e quindi che $x^2 \equiv \pm y \pmod p$ (si veda l'Esercizio 7(a)). Pertanto o $y$ o $-y$ è un quadrato modulo $p$. Si supponga che $y$ e $-y$ siano entrambi quadrati modulo $p$, diciamo $y \equiv a^2$ e $-y \equiv b^2$. Allora $-1 \equiv (a/b)^2$ (si lavori con le frazioni modulo $p$ come nel Paragrafo 3.3), cioè $-1$ è un quadrato modulo $p$. Questo è impossibile quando $p \equiv 3 \pmod 4$ (si veda l'Esercizio 26). Quindi, esattamente uno tra $y$ e $-y$ ha una radice quadrata modulo $p$. Se $y$ ha una radice quadrata modulo $p$, allora $y \equiv x^2$ e le due radici quadrate di $y$ sono $\pm x$. Se $-y$ ha una radice quadrata, allora $x^2 \equiv -y$. □

**Esempio.** Per calcolare la radice quadrata di 5 modulo 11, essendo $(p+1)/4 = 3$, basta calcolare $x \equiv 5^3 \equiv 4 \pmod{11}$. Poiché $4^2 \equiv 5 \pmod{11}$, le radici quadrate di 5 modulo 11 sono $\pm 4$.
Proviamo ora a trovare una radice quadrata di 2 modulo 11. Poiché $(p+1)/4 = 3$, si calcola $2^3 \equiv 8 \pmod{11}$. Ma $8^2 \equiv 9 \equiv -2 \pmod{11}$ e quindi si ha una radice quadrata di $-2$ invece che di 2. Ciò deriva dal fatto che 2 non ha radice quadrata modulo 11. ■

Passiamo a considerare le radici quadrate per un modulo composto. Poiché

$$x^2 \equiv 71 \pmod{77}$$

è equivalente a

$$x^2 \equiv 71 \equiv 1 \pmod{7} \quad \text{e} \quad x^2 \equiv 71 \equiv 5 \pmod{11},$$

si ha

$$x \equiv \pm 1 \pmod{7} \quad \text{e} \quad x \equiv \pm 4 \pmod{11}.$$

Il teorema cinese del resto dice che una congruenza modulo 7 e una congruenza modulo 11 possono essere ricomposte in un'unica congruenza modulo 77. Per esempio, se $x \equiv 1 \pmod{7}$ e $x \equiv 4 \pmod{11}$, allora $x \equiv 15 \pmod{77}$. Pertanto si hanno quattro modi di ricomporre le cose, ottenendo le soluzioni

$$x \equiv \pm 15, \quad \pm 29 \pmod{77}.$$

Viceversa, si supponga ora che $n = pq$ sia il prodotto di due primi e si supponga di conoscere le quattro soluzioni $x \equiv \pm a, \pm b$ di $x^2 \equiv y \pmod{n}$. Dalla costruzione appena vista, si ha che $a \equiv b \pmod{p}$ e $a \equiv -b \pmod{q}$ (o le stesse congruenze con $p$ e $q$ scambiati tra loro). Quindi $p|(a-b)$, ma $q \nmid (a-b)$. Pertanto $\text{MCD}(a-b, n) = p$ è un fattore non banale di $n$ (si tratta essenzialmente del Principio Fondamentale del Paragrafo 6.3).
Nell'esempio precedente si ha che $15^2 \equiv 29^2 \equiv 71 \pmod{77}$. Quindi $\text{MCD}(15 - 29, 77) = 7$ è un fattore non banale di 77. Un altro esempio di calcolo di radici quadrate modulo $n$ è dato nel Paragrafo 13.1.
Si noti che tutte le operazioni usate sono veloci, con l'eccezione della fattorizzazione di $n$. In particolare, il calcolo relativo al teorema cinese del resto può essere svolto rapidamente. E altrettanto rapidamente può essere svolto il calcolo del massimo comune divisore. L'elevamento a potenza modulare richiesto per calcolare le radici quadrate modulo $p$ e modulo $q$ può essere svolto rapidamente usando quadrature successive. Quindi, si può enunciare il seguente principio.

> *Si supponga che $n = pq$ sia il prodotto di due primi congruenti a 3 modulo 4 e si supponga che $y$ non abbia fattori in comune con $n$ e che abbia radice quadrata modulo $n$. Allora la determinazione delle quattro soluzioni $x \equiv \pm a, \pm b$ di $x^2 \equiv y \pmod{n}$ è computazionalmente equivalente alla fattorizzazione di $n$.*

In altre parole, se si possono trovare le soluzioni, allora si può facilmente fattorizzare $n$. Viceversa, se si può fattorizzare $n$, allora si possono trovare facilmente le soluzioni.



## 3.10 Simboli di Legendre e di Jacobi

Si supponga di dover determinare se $x^2 \equiv a \pmod{p}$ ammette soluzione, dove $p$ è primo. Se $p$ è piccolo, si possono elevare a quadrato tutti i numeri modulo $p$ e vedere se $a$ compare in questa lista. Quando $p$ è grande, questo metodo diventa impraticabile. Se $p \equiv 3 \pmod{4}$, allora si può usare la tecnica del paragrafo precedente e calcolare $s \equiv a^{(p+1)/4} \pmod{p}$. Se $a$ ha radice quadrata, allora $s$ è una di esse. In questo caso, basta elevare a quadrato $s$ e vedere se si ottiene $a$. In caso contrario, $a$ non ha radice quadrata modulo $p$. La seguente proposizione fornisce un metodo per decidere se $a$ è un quadrato modulo $p$ che funziona per $p$ dispari arbitrari.

**Proposizione.** *Sia $p$ un primo dispari e sia $a$ un intero con $a \not\equiv 0 \pmod{p}$. Allora $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Inoltre la congruenza $x^2 \equiv a \pmod{p}$ ha una soluzione se e solo se $a^{(p-1)/2} \equiv 1 \pmod{p}$.*

*Dimostrazione.* Se $y \equiv a^{(p-1)/2} \pmod{p}$, allora $y^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ per il teorema di Fermat e quindi $y \equiv \pm 1 \pmod{p}$ (per l'Esercizio 8).
Se $a \equiv x^2$, allora $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. La parte difficile è mostrare il viceversa. Sia $g$ una radice primitiva modulo $p$. Allora $a \equiv g^j$ per qualche $j$. Se $a^{(p-1)/2} \equiv 1 \pmod{p}$, allora

$$g^{j(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Per la proposizione del Paragrafo 3.7, $j(p-1)/2 \equiv 0 \pmod{p-1}$. Questo implica che $j$ deve essere pari, ossia $j = 2k$. Quindi $a \equiv g^j \equiv (g^k)^2 \pmod{p}$ e di conseguenza $a$ è un quadrato modulo $p$. □

Il criterio è molto semplice da implementare su un calcolatore, ma può essere piuttosto complicato da usare a mano. Nel seguito verrà introdotto il simbolo di Legendre e il simbolo di Jacobi, che forniscono un modo semplice per determinare se un numero sia o meno un quadrato modulo $p$. Tali simboli sono utili anche per il test di primalità (si veda il Paragrafo 6.3).
Sia $p$ un primo dispari e sia $a \not\equiv 0 \pmod{p}$. Il **simbolo di Legendre** è definito nel modo seguente:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{se } x^2 \equiv a \pmod{p} \text{ ha soluzione.} \\ -1 & \text{se } x^2 \equiv a \pmod{p} \text{ non ha soluzione.} \end{cases}$$

Le principali proprietà del simbolo di Legendre sono raccolte nella seguente proposizione.

**Proposizione.** *Sia $p$ un primo dispari.*

1. *Se $a \equiv b \not\equiv 0 \pmod{p}$, allora $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *Se $a \not\equiv 0 \pmod{p}$, allora $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.*
3. *Se $ab \not\equiv 0 \pmod{p}$, allora $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

4. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

*Dimostrazione.* Il punto (1) è vero perché, quando $a \equiv b \pmod p$, le soluzioni di $x^2 \equiv a$ sono le stesse di $x^2 \equiv b$.
Il punto (2) deriva dalla definizione del simbolo di Legendre e dalla proposizione precedente.
Per dimostrare il punto (3), basta usare la parte (2):

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p.$$

Poiché il membro di sinistra e quello di destra di questa congruenza sono $\pm 1$ e sono congruenti modulo il primo dispari $p$, essi devono essere uguali.
Per il punto (4), basta usare il punto (2) con $a = -1$:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p.$$

Ancora, poiché la parte di sinistra e quella di destra di questa congruenza sono $\pm 1$ e sono congruenti modulo il primo dispari $p$, esse devono essere uguali. □

**Esempio.** Sia $p = 11$. I quadrati non nulli modulo 11 sono 1, 3, 4, 5, 9. Si ha

$$\left(\frac{6}{11}\right)\left(\frac{7}{11}\right) = (-1)(-1) = +1$$

e (usando la proprietà (1))

$$\left(\frac{42}{11}\right) = \left(\frac{9}{11}\right) = +1.$$

Quindi

$$\left(\frac{6}{11}\right)\left(\frac{7}{11}\right) = \left(\frac{42}{11}\right).$$

■

Il simbolo di Jacobi estende il simbolo di Legendre dai primi $p$ ai numeri interi dispari composti $n$. Si potrebbe essere tentati di definire il simbolo come $+1$ se $a$ è un quadrato modulo $n$ e $-1$ in caso contrario. Tuttavia, questo renderebbe falsa l'importante proprietà (3). Per esempio, 2 non è un quadrato modulo 35 e 3 non è un quadrato modulo 35 (poiché non sono quadrati modulo 5), ma anche il prodotto 6 non è un quadrato modulo 35 (poiché non è un quadrato modulo 7). Se la proprietà (3) valesse, allora si avrebbe $(-1)(-1) = -1$, che è falso.
Per preservare la proprietà (3), il **simbolo di Jacobi** viene definito nel modo seguente. Sia $n$ un intero positivo dispari e sia $a$ un intero non nullo con $\mathrm{MCD}(a,n) = 1$. Sia

$$n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$



una scomposizione di $n$ in fattori primi. Allora

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{b_1}\left(\frac{a}{p_2}\right)^{b_2}\cdots\left(\frac{a}{p_r}\right)^{b_r}.$$

I simboli a secondo membro sono i simboli di Legendre precedentemente introdotti. Se $n = p$, il simbolo di Jacobi si riduce al simbolo di Legendre.

**Esempio.** Sia $n = 135 = 3^3 \cdot 5$. Allora

$$\left(\frac{2}{135}\right) = \left(\frac{2}{3}\right)^3\left(\frac{2}{5}\right) = (-1)^3(-1) = +1.$$

Si noti che 2 non è un quadrato modulo 5 e quindi non è nemmeno un quadrato modulo 135. Quindi, il fatto che il simbolo di Jacobi abbia valore $+1$ non implica che 2 sia un quadrato modulo 135. ■

Le principali proprietà del simbolo di Jacobi sono raccolte nel seguente teorema. I punti (1), (2) e (3) possono essere dedotti da quelli del simbolo di Legendre. I punti (4) e (5) sono molto più profondi.

**Teorema.** *Sia $n$ un intero dispari.*

1. *Se $a \equiv b \pmod n$ e $\mathrm{MCD}(a,n) = 1$, allora* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

2. *Se $\mathrm{MCD}(ab,n) = 1$, allora* $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

3. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

4. $\left(\frac{2}{n}\right) = \begin{cases} +1 & \text{se } n \equiv 1,7 \pmod 8 \\ -1 & \text{se } n \equiv 3,5 \pmod 8. \end{cases}$

5. *Se $m$ è dispari con $\mathrm{MCD}(m,n) = 1$, allora*

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

Non si è inclusa la proprietà $\left(\frac{a}{n}\right) \equiv (-1)^{(n-1)/2}$, perché, in genere, non è vera per $n$ composto (si veda l'Esercizio 31). Il test di primalità di Solovay-Strassen si basa proprio su questo fatto (vedi il Paragrafo 6.3).
Il punto (5) è la famosa **legge di reciprocità quadratica**, dimostrata da Gauss nel 1796. Quando $m$ e $n$ sono primi, essa mette in relazione il fatto che $m$ sia un quadrato modulo $n$ con il fatto che $n$ sia un quadrato modulo $m$.

La dimostrazione del teorema per $m$ e $n$ primi può essere trovata in molti testi elementari di teoria dei numeri. L'estensione al caso in cui $m$ e $n$ sono composti può essere dedotta abbastanza facilmente dal caso precedente. Si veda, per esempio, [Niven et al.] oppure [Rosen].
Se si considera la reciprocità quadratica insieme alle altre proprietà del simbolo di Jacobi, si ha un metodo veloce per valutare questo simbolo. Ecco un paio di esempi.

**Esempio.** Per calcolare il simbolo $\left(\frac{4567}{12345}\right)$ si può procedere nel modo seguente:

$$\begin{aligned}
\left(\frac{4567}{12345}\right) &= +\left(\frac{12345}{4567}\right) && \text{(per (5), poiché } 12345 \equiv 1 \pmod 4\text{)}\\
&= +\left(\frac{3211}{4567}\right) && \text{(per (1), poiché } 12345 \equiv 3211 \pmod{4567}\text{)}\\
&= -\left(\frac{4567}{3211}\right) = -\left(\frac{1356}{3211}\right) && \text{(per (5) e per (1))}\\
&= -\left(\frac{2}{3211}\right)^2\left(\frac{339}{3211}\right) && \text{(per (2), poiché } 1356 = 2^2 \cdot 339\text{)}\\
&= -\left(\frac{339}{3211}\right) && \text{(poiché } (\pm 1)^2 = 1\text{)}\\
&= +\left(\frac{3211}{339}\right) = +\left(\frac{160}{339}\right) && \text{(per (5) e per (1))}\\
&= +\left(\frac{2}{339}\right)^5\left(\frac{5}{339}\right) && \text{(per (2), poiché } 160 = 2^5 \cdot 5\text{)}\\
&= +(-1)^5\left(\frac{5}{339}\right) && \text{(per (4))}\\
&= -\left(\frac{339}{5}\right) = -\left(\frac{4}{5}\right) && \text{(per (5) e per (1))}\\
&= -\left(\frac{2}{5}\right)^2\\
&= -1.
\end{aligned}$$

L'unica fattorizzazione di cui si ha bisogno in questo calcolo è data dall'estrazione delle potenze di 2, operazione facile da eseguire. Il fatto che i calcoli possano essere svolti senza fattorizzare numeri dispari è importante nelle applicazioni. Il fatto che la risposta sia $-1$ implica che 4567 non è un quadrato modulo 12345. Tuttavia, se la risposta fosse stata $+1$, non si sarebbe potuto dedurre se 4567 sia o meno un quadrato modulo 12345 (si veda l'Esercizio 30). ■



**Esempio.** Per calcolare $\left(\frac{107}{137}\right)$ si può procedere nel modo seguente:

$$\begin{aligned}
\left(\frac{107}{137}\right) &= +\left(\frac{137}{107}\right) && \text{(per (5))}\\
&= +\left(\frac{30}{107}\right) && \text{(per (1))}\\
&= +\left(\frac{2}{107}\right)\left(\frac{15}{107}\right) && \text{(per (2))}\\
&= +(-1)\left(\frac{15}{107}\right) && \text{(per (4))}\\
&= +\left(\frac{107}{15}\right) && \text{(per (5))}\\
&= +\left(\frac{2}{15}\right) && \text{(per (1))}\\
&= +1 && \text{(per (5)).}
\end{aligned}$$

Poiché 137 è un primo, questo dice che 107 è un quadrato modulo 137. Nello svolgere il calcolo si è usato il fatto che $\left(\frac{2}{15}\right) = +1$. Questo però non significa che 2 sia un quadrato modulo 15. Infatti 2 non è un quadrato modulo 5 e quindi non può nemmeno essere un quadrato modulo 15. Quindi, benché il risultato finale possa essere interpretato dicendo che 107 è un quadrato modulo il primo 137, i risultati intermedi che coinvolgono numeri composti non devono essere interpretati in questo modo. ■

Si supponga che $n = pq$ sia il prodotto di due primi grandi. Se $\left(\frac{a}{n}\right) = -1$, allora si può concludere che $a$ non è un quadrato modulo $n$. Ma cosa si può concludere se $\left(\frac{a}{n}\right) = +1$? Poiché

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right),$$

ci sono due possibilità:

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1 \qquad \text{oppure} \qquad \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = +1.$$

Nel primo caso, $a$ non è un quadrato modulo $p$ e quindi non può nemmeno essere un quadrato modulo $pq$. Nel secondo caso, $a$ è un quadrato modulo $p$ e modulo $q$. Usando il teorema cinese del resto, si possono mettere insieme una radice quadrata modulo $p$ e una radice quadrata modulo $q$ per ottenere una radice quadrata di $a$ modulo $n$. Quindi $a$ è un quadrato modulo $n$.
In conclusione, se $\left(\frac{a}{n}\right) = +1$, allora $a$ può essere o meno un quadrato modulo $n$. Il problema di decidere quale caso valga è chiamato **problema di residuosità quadratica**. Non si conoscono algoritmi veloci per risolverlo. Naturalmente, se si può fattorizzare $n$, allora il problema può essere risolto facilmente calcolando $\left(\frac{a}{p}\right)$.

## 3.11 Campi finiti

**Nota.** *Questo paragrafo è più avanzato rispetto al resto del capitolo ed è stato incluso perché i campi finiti sono usati spesso in crittografia. In particolare, essi appaiono in quattro punti del libro. In Rijndael che usa il campo finito $GF(2^8)$ (Capitolo 5), nel Paragrafo 2.11 dove sono usati per spiegare alcuni fenomeni ivi menzionati, nel Paragrafo 16.4 e nell'ambito dei codici correttori di errori (Capitolo 18).*

Spesso in questo libro si lavora con interi modulo $p$, dove $p$ è un primo. Possiamo sommare, sottrarre e moltiplicare, ma ciò che distingue il caso in cui si lavora modulo $p$ dal caso in cui si lavora modulo un arbitrario intero $n$ è che nel primo caso si può dividere per un qualunque numero non nullo modulo $p$. Per esempio, per risolvere $3x \equiv 1 \pmod 5$, basta dividere per 3 per ottenere $x \equiv 2 \pmod 5$. Se invece si vuole risolvere $3x \equiv 1 \pmod 6$, allora non si hanno soluzioni, poiché non si può dividere per 3 (mod 6). Parlando alla buona, un insieme munito di operazioni di addizione, moltiplicazione, sottrazione e divisione per elementi non nulli è detto campo. Si richiedono anche la proprietà associativa, commutativa e distributiva.

**Esempi.** Gli esempi fondamentali di campo sono i numeri reali, i numeri complessi, i numeri razionali e gli interi modulo un primo. L'insieme di tutti gli interi non è un campo poiché non sempre si può dividere (per esempio, 4/3 non è un intero). ■

**Esempio.** L'insieme

$$GF(4) = \{0,1,\omega,\omega^2\}$$

forma un campo formato da quattro elementi rispetto alle seguenti leggi:

1. $0 + x = x$ per ogni $x$.
2. $x + x = 0$ per ogni $x$.
3. $1 \cdot x = x$ per ogni $x$.
4. $\omega + 1 = \omega^2$.

$\omega^2 + 1 = 1 + \omega + 1 = \omega$

5. L'addizione e la moltiplicazione sono operazioni commutative e associative e vale la legge distributiva: $x(y+z) = xy + xz$ per ogni $x,y,z$.

Poiché

$$\omega^3 = \omega \cdot \omega^2 = \omega \cdot (1+\omega) = \omega + \omega^2 = \omega + (1+\omega) = 1,$$

si ha che $\omega^2$ è l'inverso moltiplicativo di $\omega$. Quindi ogni elemento non nullo di $GF(4)$ ha un inverso moltiplicativo e pertanto $GF(4)$ è un campo. ■

In generale, un **campo** è un insieme contenente due elementi 0 e 1 (con $1 \neq 0$) che soddisfa le seguenti condizioni.

(non nullo)

1. È munito di un'addizione e di una moltiplicazione che soddisfano le condizioni (1), (3) e (5) nella lista precedente.



2. Ogni elemento ha un inverso addittivo, ossia per ogni $x$ esiste un elemento $-x$ tale che $x + (-x) = 0$.
3. Ogni elemento non nullo possiede un inverso moltiplicativo.

Un campo è chiuso rispetto alla sottrazione. Per calcolare $x - y$, basta calcolare $x + (-y)$.
L'insieme delle matrici $2 \times 2$ a coefficienti reali non è un campo per due motivi. Primo, il prodotto non è commutativo. Secondo, ci sono matrici non nulle che non possiedono inversa. L'insieme dei numeri reali non negativi non è un campo. Possiamo sommare, moltiplicare e dividere, ma non sempre il risultato di una sottrazione appartiene ancora all'insieme in questione.
Per ogni potenza $p^n$ di primo esiste esattamente un campo finito con $p^n$ elementi. Questi campi sono esattamente tutti e soli i campi finiti. Prima di vedere come si costruiscono, si osservi che gli interi modulo $p^n$ non formano un campo per $n > 1$. Poiché la congruenza $px \equiv 1 \pmod{p^n}$ non ammette soluzioni non si può dividere per $p$, anche se $p \not\equiv 0 \pmod{p^n}$. Quindi occorrono costruzioni più complesse per ottenere campi con $p^n$ elementi.
Il campo con $p^n$ elementi è indicato con $GF(p^n)$, dove "GF" significa "Galois field", in onore al matematico francese Evariste Galois (1811–1832), pioniere della teoria dei campi.

**Esempio.** Il campo $GF(4)$ può essere costruito anche nel seguente modo. Sia $\mathbb{Z}_2[X]$ l'insieme di tutti i polinomi a coefficienti interi modulo 2. Per esempio, $1 + X^3 + X^6$ e $X$ appartengono a questo insieme. Anche i polinomi costanti 0 e 1 appartengono a $\mathbb{Z}_2[X]$. Si può sommare, sottrarre e moltiplicare in questo insieme, purché si lavori con i coefficienti modulo 2. Per esempio

$$(X^3 + X + 1)(X + 1) = X^4 + X^3 + X^2 + 1$$

poiché il termine $2X$ sparisce modulo 2. La proprietà importante qui è che si possono effettuare le divisioni con resto, come con gli interi. Per esempio, si supponga di volere dividere $X^4 + X^3 + 1$ per $X^2 + X + 1$. Si può procedere nel modo seguente, come per i numeri interi:

$$\begin{array}{r|l} X^4 + X^3 + 1 & X^2 + X + 1 \\ \underline{X^4 + X^3 + X^2} & \\ X^2 + 1 & \\ \underline{X^2 + X + 1} & \\ X & \end{array}$$

Dividendo per $X^2 + X + 1$ si ottiene $X^2$ come primo termine del quoziente. Poi, moltiplicando $X^2 + X + 1$ per $X^2$, si ottiene $X^4 + X^3 + X^2$ che sottratto a $X^4 + X^3 + 1$ da $X^2 + 1$. Dividendo $X^2 + 1$ per $X^2 + X + 1$ si ottiene il secondo termine del quoziente, ossia 1. Moltiplicando 1 per $X^2 + X + 1$ e poi sottraendo a $X^2 + 1$ rimane il resto $X$. Poiché il grado del polinomio $X$ è minore del grado di $X^2 + X + 1$, ci si ferma. Il quoziente è $X^2 + 1$ e il resto è $X$:

$$X^4 + X^3 + 1 = (X^2 + 1)(X^2 + X + 1) + X.$$

Possiamo scrivere

$$X^4 + X^3 + 1 \equiv X \pmod{X^2 + X + 1}.$$

Quando si divide per $X^2 + X + 1$ si ottiene un resto uguale a 0 o a un polinomio di grado al più 1 (se il resto ha grado almeno 2, si può continuare a dividere). Quindi, si definisce $\mathbb{Z}_2[X] \pmod{X^2 + X + 1}$ come l'insieme

$$\{0, 1, X, X + 1\}$$

dei polinomi di grado al più 1, poiché questi sono i resti che si ottengono quando si divide per $X^2 + X + 1$. La somma, la sottrazione e la moltiplicazione sono modulo $X^2 + X + 1$. Questo è completamente analogo a ciò che accade quando si lavora con gli interi modulo $n$. Nella situazione presente, si dice che due polinomi $f(X)$ e $g(X)$ sono congruenti modulo $X^2 + X + 1$, ossia $f(X) \equiv g(X) \pmod{X^2 + X + 1}$, se $f(X)$ e $g(X)$ hanno lo stesso resto quando vengono divisi per $X^2 + X + 1$. Un altro modo per dire la stessa cosa è che $f(X) - g(X)$ è un multiplo di $X^2 + X + 1$. Questo significa che c'è un polinomio $h(X)$ tale che $f(X) - g(X) = (X^2 + X + 1)h(X)$.
Per quanto riguarda la moltiplicazione in $\mathbb{Z}_2[X] \pmod{X^2 + X + 1}$, per esempio, si ha

$$X \cdot X = X^2 \equiv X + 1 \pmod{X^2 + X + 1}$$

(se si pensa che il membro di destra debba essere $-X - 1$, si tanga presente che, quando si lavora con coefficienti modulo 2, $+1$ e $-1$ sono uguali). Come ulteriore esempio, si ha

$$X^3 \equiv X \cdot X^2 \equiv X \cdot (X + 1) \equiv X^2 + X \equiv 1 \pmod{X^2 + X + 1}.$$

È facile vedere che si sta lavorando con l'insieme $GF(4)$ di prima, con $X$ al posto di $\omega$. ■

- Considerare l'insieme $\mathbb{Z}_2[X]$ modulo un polinomio permette di generare nuovi campi finiti. Tuttavia non si può considerare come modulo un polinomio qualunque. Tale polinomio deve essere irriducibile, cioè non deve fattorizzarsi in polinomi di grado inferiore modulo 2. Per esempio, il polinomio $X^2 + 1$ è irriducibile quando si lavora con i numeri reali, ma non è irriducibile quando i coefficienti sono presi mod 2, poiché in questo caso $X^2 + 1 = (X + 1)(X + 1)$. Invece il polinomio $X^2 + X + 1$ è irriducibile sia con coefficienti reali sia con coefficienti in $\mathbb{Z}_2$. Si supponga che si fattorizzi modulo 2 in polinomi di grado inferiore. I soli fattori possibili modulo 2 sono $X$ e $X + 1$ e $X^2 + X + 1$ non è multiplo di nessuno di essi, nemmeno modulo 2.

- Ecco la procedura generale per costruire a campo finito con $p^n$ elementi, dove $p$ è primo e $n \geq 1$. Sia $\mathbb{Z}_p$ l'insieme degli interi modulo $p$.

  1. $\mathbb{Z}_p[X]$ è l'insieme dei polinomi con coefficienti modulo $p$.
  2. Si sceglie un polinomio $P(X)$ irriducibile modulo $p$, di grado $n$.
  3. Sia $GF(p^n) = \mathbb{Z}_p[X] \pmod{P(X)}$. Allora $GF(p^n)$ è un campo con $p^n$ elementi.



Si vede facilmente che $GF(p^n)$ ha $p^n$ elementi. I possibili resti dopo la divisione per $P(X)$ sono i polinomi della forma $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$, dove i coefficienti sono interi modulo $p$. Ci sono $p$ scelte per ogni coefficiente, e quindi $p^n$ possibili resti.
Poiché per ogni $n$ esiste sempre almeno un polinomio irriducibile modulo $p$ di grado $n$, questa costruzione genera campi con $p^n$ elementi per ogni $n \geq 1$. Ma cosa accade se si ripete la medesima costruzione per due polinomi diversi $P_1(X)$ e $P_2(X)$, entrambi di grado $n$? Si ottengono due campi $GF(p^n)'$ e $GF(p^n)''$ che risultano essere essenzialmente uguali (ossia isomorfi), anche se questo non è affatto ovvio essendo la moltiplicazione modulo $P_1(X)$ diversa della moltiplicazione modulo $P_2(X)$.

### 3.11.1 Divisione

È facile sommare, sottrarre e moltiplicare polinomi in $\mathbb{Z}_p[X]$, mentre dividere è un po' più laborioso. Per esempio, il polinomio $X^8 + X^4 + X^3 + X + 1$ è irriducibile in $\mathbb{Z}_2[X]$ (anche se ci sono metodi più veloci, un modo per mostrare che esso è irriducibile è quello di dividerlo per tutti i polinomi di grado inferiore in $\mathbb{Z}_2[X]$). Si consideri il campo

$$GF(2^8) = \mathbb{Z}_2[X] \pmod{X^8 + X^4 + X^3 + X + 1}.$$

Poiché $X^7 + X^6 + X^3 + X + 1$ non è 0, esso deve avere un inverso. L'inverso può essere determinato usando l'analogo dell'algoritmo euclideo esteso. Come prima cosa, si calcola il massimo comune divisore $\mathrm{MCD}(X^7+X^6+X^3+X+1, X^8+X^4+X^3+X+1)$. La procedura (resto → divisore → dividendo → ignora) è la stessa che per gli interi:

$$\begin{aligned} X^8+X^4+X^3+X+1 &= (X+1)(X^7+X^6+X^3+X+1)+(X^6+X^2+X) \\ X^7+X^6+X^3+X+1 &= (X+1)(X^6+X^2+X)+1. \end{aligned}$$

Poiché l'ultimo resto è 1, il "massimo comune divisore" di $X^7 + X^6 + X^3 + X + 1$ e $X^8+X^4+X^3+X+1$ è 1. Naturalmente deve essere così, poiché $X^8+X^4+X^3+X+1$ è irriducibile e quindi gli unici fattori sono 1 e se stesso.
Ora basta ripercorrere al contrario questo calcolo per esprimere 1 come combinazione lineare di $X^7 + X^6 + X^3 + X + 1$ e $X^8 + X^4 + X^3 + X + 1$ (oppure si possono usare le formule per l'algoritmo euclideo esteso). In ogni passo si prende l'ultimo resto che non si è ancora utilizzato e lo si sostituisce con il dividendo meno il quoziente per il divisore; poiché si sta lavorando modulo 2, il segno meno scompare.

$$\begin{aligned} 1 &= (X^7+X^6+X^3+X+1)+(X+1)(X^6+X^2+X) \\ &= (X^7+X^6+X^3+X+1) \\ &\quad +(X+1)\left((X^8+X^4+X^3+X+1)+(X+1)(X^7+X^6+X^3+X+1)\right) \\ &= (1+(X+1)^2)(X^7+X^6+X^3+X+1)+(X+1)(X^8+X^4+X^3+X+1) \\ &= X^2(X^7+X^6+X^3+X+1)+(X+1)(X^8+X^4+X^3+X+1). \end{aligned}$$

Quindi,

$$1 = X^2(X^7+X^6+X^3+X+1)+(X+1)(X^8+X^4+X^3+X+1).$$

Riducendo modulo $X^8 + X^4 + X^3 + X + 1$, si ottiene

$$X^2(X^7+X^6+X^3+X+1) \equiv 1 \pmod{X^8+X^4+X^3+X+1},$$

da cui segue che $X^2$ è l'inverso moltiplicativo di $X^7+X^6+X^3+X+1$. Ogni volta che si deve dividere per $X^7+X^6+X^3+X+1$, si può invece moltiplicare per $X^2$. Questo è l'analogo di quello che si fa quando si lavora con gli usuali interi modulo $p$.

### 3.11.2 $GF(2^8)$

Più avanti verrà discusso Rijndael che usa $GF(2^8)$ (si veda il Capitolo 5). È pertanto utile studiare un po' più a fondo questo campo. Si lavorerà modulo il polinomio irriducibile $X^8+X^4+X^3+X+1$ (quello usato da Rijndael), anche se ci sono altri polinomi irriducibili di grado 8, ognuno dei quali porta a calcoli analoghi. Ogni elemento può essere rappresentato in modo unico come un polinomio

$$b_7X^7+b_6X^6+b_5X^5+b_4X^4+b_3X^3+b_2X^2+b_1X+b_0,$$

dove ogni $b_i$ è 0 o 1. Poiché gli 8 bit $b_7b_6b_5b_4b_3b_2b_1b_0$ rappresentano un byte, è possibile rappresentare gli elementi di $GF(2^8)$ come byte di 8 bit. Per esempio, il polinomio $X^7+X^6+X^3+X+1$ diventa 11001011. Come addizione si utilizza lo XOR bit a bit:

$$(X^7+X^6+X^3+X+1)+(X^4+X^3+1)\rightarrow$$
$$\rightarrow 11001011\oplus 00011001=11010010\rightarrow X^7+X^6+X^4+X.$$

La moltiplicazione è più delicata e non ha un'interpretazione così semplice. Ciò è dovuto al fatto che si sta lavorando modulo il polinomio $X^8+X^4+X^3+X+1$, che può essere rappresentato dai 9 bit 100011011. Se si moltiplica $X^7+X^6+X^3+X+1$ per $X$ si ha

$$\begin{aligned}(X^7+X^6+X^3+X+1)X &= X^8+X^7+X^4+X^2+X\\ &= (X^7+X^3+X^2+1)+(X^8+X^4+X^3+X+1)\\ &\equiv X^7+X^3+X^2+1 \pmod{X^8+X^4+X^3+X+1}.\end{aligned}$$

La stessa operazione con i bit diventa

$$\begin{aligned}11001011 &\rightarrow 110010110 && \text{(far scorrere a sinistra e concatenare con 0)}\\ &\rightarrow 110010110\oplus 100011011 && \text{(sottrarre } X^8+X^4+X^3+X+1)\\ &= 010001101.\end{aligned}$$

In generale, si può moltiplicare per $X$ mediante il seguente algoritmo.

1. Far scorrere i bit verso sinistra e concatenare uno 0 come ultimo bit.
2. Se il primo bit è 0, stop.
3. Se il primo bit è 1, eseguire uno XOR con 100011011.

Il motivo per cui ci si ferma nel passo 2 è che se il primo bit è 0, allora il polinomio ha ancora grado inferiore a 8 dopo essere stato moltiplicato per $X$ e quindi non ha bisogno di essere ridotto. Per moltiplicare per potenze maggiori di $X$, basta moltiplicare per $X$ più volte. Per esempio, la moltiplicazione per $X^3$ può essere eseguita con tre operazioni di scorrimento *(shift)* e al più tre somme XOR. La moltiplicazione per un polinomio arbitrario può essere eseguita moltiplicando per le varie potenze di $X$ che appaiono nel polinomio e poi sommando (mediante la somma XOR) i vari risultati.



In conclusione, si ha che le operazioni di addizione e moltiplicazione nel campo $GF(2^8)$ possono essere eseguite in modo molto efficiente. In realtà, analoghe considerazioni possono essere fatte per un qualunque campo finito.

L'analogia tra gli interi modulo un primo e i polinomi modulo un polinomio irriducibile è notevole e viene riassunta qui di seguito:

$$\begin{aligned}\text{interi} &\longleftrightarrow \mathbb{Z}_p[X]\\ \text{numero primo } q &\longleftrightarrow P(X) \text{ irriducibile di grado } n\\ \mathbb{Z}_q &\longleftrightarrow \mathbb{Z}_p[X] \pmod{P(X)}\\ \text{campo con } q \text{ elementi} &\longleftrightarrow \text{campo con } p^n \text{ elementi}\end{aligned}$$

Sia $GF(p^n)^*$ l'insieme degli elementi non nulli di $GF(p^n)$. Questo insieme, che ha $p^n-1$ elementi, è chiuso rispetto alla moltiplicazione, esattamente come gli interi non congruenti a 0 modulo $p$ sono chiusi rispetto alla moltiplicazione. Si può dimostrare che esiste un polinomio generatore $g(X)$ tale che ogni elemento di $GF(p^n)^*$ può essere espresso come una potenza di $g(X)$. Questo significa anche che il più piccolo esponente $k$ per cui $g(X)^k\equiv 1$ è $p^n-1$. È l'analogo di una radice primitiva per i primi. Esistono $\varphi(p^n-1)$ di questi polinomi generatori, dove $\varphi$ è la funzione di Eulero. Si ha una situazione interessante quando $p=2$ e $2^n-1$ è primo. In questo caso, ogni polinomio non nullo $f(X)\neq 1$ appartenente a $GF(2^n)$ è un polinomio generatore (infatti l'insieme $GF(2^n)^*$ è un gruppo di ordine primo e per questo motivo ogni elemento diverso dall'identità è un generatore).

Il **problema del logaritmo discreto** modulo un primo, che verrà discusso nel Capitolo 7, ha un analogo per i campi finiti: dato $h(X)$, trovare un intero $k$ tale che $h(X)=g(X)^k$ in $GF(p^n)$. Trovare uno di questi $k$ è molto difficile nella maggior parte dei casi.

### 3.11.3 Successioni LFSR

A questo punto è possibile spiegare un fenomeno di cui si è parlato nel Paragrafo 2.11 riguardante le successioni LFSR. Si supponga di avere una ricorrenza

$$x_{n+m}\equiv c_0x_n+c_1x_{n+1}+\cdots+c_{m-1}x_{n+m-1} \pmod 2.$$

Per semplicità, si assuma che il polinomio associato

$$P(X)=X^m+c_{m-1}X^{m-1}+c_{m-2}X^{m-2}+\cdots+c_0$$

sia irriducibile modulo 2. Allora $\mathbb{Z}_2[X] \pmod{P(X)}$ coincide con il campo $GF(2^m)$, che può essere pensato come spazio vettoriale su $\mathbb{Z}_2$. In questo modo la moltiplicazione per $X$ è una trasformazione lineare di questo spazio. Fissata la base canonica $\{1,X,X^2,X^3,\ldots,X^{m-1}\}$, si ha

$$X\cdot 1=X,\quad X\cdot X=X^2,\quad X\cdot X^2=X^3,\quad \ldots$$
$$X\cdot X^{m-1}=X^m\equiv c_0+c_1X+\cdots+c_{m-1}X^{m-1}$$

e quindi la moltiplicazione per $X$ è rappresentata dalla matrice

$$M_X = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{m-1} \end{pmatrix}.$$

Se si conosce il vettore $(x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m-1})$, allora

$$\begin{aligned}(x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m-1})\, M_X &= \\ &= (x_{n+1}, x_{n+2}, x_{n+3}, \ldots, c_0 x_n + \cdot \mathbf{v} + c_{m-1} x_{n+m-1}) \\ &\equiv (x_{n+1}, x_{n+2}, x_{n+3}, \ldots, x_{n+m}).\end{aligned}$$

La moltiplicazione per $M_X$ fa scorrere gli indici di 1. Di conseguenza la moltiplicazione a destra della matrice $M_X^j$ manda il vettore $(x_1, x_2, \ldots, x_m)$ nel vettore $(x_{1+j}, x_{2+j}, \ldots, x_{m+j})$. Se $M_X^j \equiv I$, dove $I$ è la matrice identità, allora quest'ultimo vettore deve essere il vettore originale $(x_1, x_2, \ldots, x_m)$. Poiché ci sono $2^m - 1$ elementi non nulli in $GF(2^m)$, per il teorema di Lagrange della teoria dei gruppi si ha che $X^{2^m-1} \equiv 1$ e questo implica che $M_X^{2^m-1} = I$. Quindi $x_1 \equiv x_{2^m}$, $x_2 \equiv x_{2^m+1}, \ldots$.
Per ogni insieme di valori iniziali (si assume che almeno uno dei valori iniziali sia non nullo), la successione si ripeterà dopo $k$ termini, dove $k$ è il più piccolo intero positivo tale che $X^k \equiv 1 \pmod{P(X)}$. Si può dimostrare che che $k$ divide $2^m - 1$.
Infatti, il periodo di tale successione è esattamente $k$. Questo può essere dimostrato nel modo seguente, usando alcuni risultati dell'algebra lineare. Sia $v = (x_1, \ldots, x_m) \neq 0$ il vettore riga dei valori iniziali. La successione si ripete quando $vM_X^j = v$. Questo significa che il vettore *riga* non nullo $v$ appartiene allo spazio nullo sinistro della matrice $M_X^j - I$ e quindi che $\det(M_X^j - I) = 0$. Ma questo significa che esiste un vettore *colonna* non nullo $w = (a_0, \ldots, a_{m-1})^T$ appartenente allo spazio nullo destro di $M_X^j - I$, cioé tale che $M_X^j w = w$. Poiché la matrice $M_X^j$ rappresenta la trasformazione lineare data dalla moltiplicazione per $X^j$ rispetto alla base $\{1, X, \ldots, X^{m-1}\}$, tornando ai polinomi si ha

$$X^j(a_0 + a_1X + \cdots + a_{m-1}X^{m-1}) \equiv a_0 + a_1X + \cdots + a_{m-1}X^{m-1} \pmod{P(X)}.$$

Ma $a_0 + a_1X + \cdots + a_{m-1}X^{m-1} \pmod{P(X)}$ è un elemento non nullo del campo $GF(2^m)$ e quindi si può dividere per questo elemento e ottenere $X^j \equiv 1 \pmod{P(X)}$. Poiché questo accade per la prima volta per $j = k$, la successione si ripete per la prima volta dopo $k$ termini, ossia ha periodo $k$.
Come già osservato in precedenza, quando $2^m - 1$ è primo, tutti i polinomi (tolto 0 e 1) sono polinomi generatori di $GF(2^m)$. In particolare, $X$ è un polinomio generatore e quindi $k = 2^m - 1$ è il periodo della ricorrenza.

## 3.12 Frazioni continue

In molte situazioni bisogna approssimare un numero reale mediante un numero razionale. Per esempio, $\pi = 3.14159265\cdots$ può essere approssimato con $314/100 = 157/50$.



Ma $22/7$ è un'approssimazione un poco migliore, anche perché possiede un denominatore più piccolo. Il metodo delle frazioni continue permette di ottenere buone approssimazioni di questo tipo. In questo paragrafo, verranno presentati i primi rudimenti di tale metodo. Per le dimostrazioni e per ulteriori dettagli, si veda, per esempio, [Hardy-Wright], [Niven et al.] e [Rosen].
Un modo semplice per approssimare un numero reale $x$ è di prendere il più grande intero minore o uguale ad $x$, che spesso viene indicato con $\lfloor x \rfloor$. Per esempio $\lfloor \pi \rfloor = 3$. Se si vuole ottenere un'approssimazione migliore bisogna considerare la rimanente parte frazionaria. Per $\pi = 3.14159\cdots$, essa è $.14159\cdots$ e sembra vicina a $1/7 = .142857\cdots$. Un modo per esprimere questo fatto è di considerare il rapporto $1/.14159 = 7.06251$. Poiché esso può essere approssimato da $\lfloor 7.06251\cdots \rfloor = 7$ si può concludere che $1/7$ è effettivamente una buona approssimazione di $.14159$ e che $22/7$ è una buona approssimazione di $\pi$. Continuando in questo modo si possono ottenere approssimazioni migliori. Per esempio, il passo successivo è quello di calcolare $1/.06251 = 15.9966$ e poi di prendere il più grande intero minore di esso, ossia 15 (in effetti 16 è più vicino, ma l'algoritmo effettua una correzione nel passo successivo). Così si ha

$$\pi \approx 3 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106}.$$

Dopo un ulteriore passo, si ottiene

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}} = \frac{355}{113}.$$

Quest'ultima approssimazione è molto accurata:

$$\pi = 3.14159265\cdots \qquad \text{e} \qquad 355/113 = 3.14159292\cdots.$$

Questa procedura funziona per numeri reali arbitrari. Si parte con un numero reale $x$. Si pone $a_0 = \lfloor x \rfloor$ e $x_0 = x$. Poi, se $x_i \neq a_i$ (altrimenti ci si ferma), si pone

$$x_{i+1} = \frac{1}{x_i - a_i} \qquad \text{e} \qquad a_{i+1} = \lfloor x_{i+1} \rfloor.$$

In questo modo si ottiene l'approssimazione

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}.$$

In realtà si ha una successione di numeri razionali $p_1/q_1$, $p_2/q_2$, .... Si può dimostrare che ognuno dei numeri razionali $p_k/q_k$ fornisce un'approssimazione migliore di $x$ di qualunque dei precedenti numeri razionali $p_j/q_j$ con $1 \leq j < k$. Inoltre, si ha il

**Teorema.** *Se $|x - (r/s)| < 1/2s^2$ per due interi $r$ e $s$, allora $r/s = p_i/q_i$ per qualche $i$.*

Per esempio, $|\pi - 22/7| \approx .001 < 1/98$ e $22/7 = p_2/q_2$.

Le frazioni continue permettono di riconoscere in modo semplice i numeri razionali dalla loro rappresentazione decimale. Per esempio, si supponga di incontrare il numero decimale 3.764705882 e di sospettare che sia la parte iniziale dello sviluppo decimale di un numero razionale con denominatore più piccolo. I primi termini della frazione continua sono

$$3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{9803921}}}}.$$

Il fatto che 9803921 è grande indica che la precedente approssimazione è piuttosto buona. Così si può calcolare

$$3+\cfrac{1}{1+\cfrac{1}{3+\frac{1}{4}}}=\frac{64}{17}=3.7647058823529\cdots,$$

che concorda con tutti i termini del numero 3.764605882 originale. Quindi 64/17 è un probabile candidato per la risposta. Si noti che se si fosse incluso anche 9803921, allora si sarebbe ottenuta una frazione che avrebbe concordato ancora con lo sviluppo decimale originale, ma che avrebbe avuto un denominatore significativamente più grande.
Applicando la procedura a 12345/11111, si ottiene

$$\frac{12345}{11111}=1+\cfrac{1}{9+\cfrac{1}{246+\cfrac{1}{1+\frac{1}{4}}}}.$$

Da qui si hanno i numeri

$$1,\quad \frac{10}{9},\quad \frac{2461}{2215},\quad \frac{2471}{2224},\quad \frac{12345}{11111}.$$

Si noti che i numeri 1, 9, 246, 1, 4 sono i quozienti ottenuti durante il calcolo del MCD(12345, 11111) nel Paragrafo 3.1 (si veda l'Esercizio 35).
Calcolare frazioni del tipo

$$\frac{2461}{2215}=1+\cfrac{1}{9+\frac{1}{246}}$$

può diventare piuttosto faticoso quando si procede in modo diretto. Fortunatamente, c'è un metodo piú veloce. Posto

$$\begin{cases} p_{n+1}=a_{n+1}p_n+p_{n-1} \\ q_{n+1}=a_{n+1}q_n+q_{n-1} \end{cases} \quad \text{con} \quad \begin{cases} p_{-2}=0, & p_{-1}=1 \\ q_{-2}=1, & q_{-1}=0, \end{cases}$$

si ha

$$\frac{p_n}{q_n}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\cdots+\frac{1}{a_n}}}}.$$

Usando queste relazioni, si possono calcolare i quozienti parziali $p_n/q_n$ da quelli precedenti, invece di dover iniziare un nuovo calcolo ogni volta che si trova un nuovo $a_n$.



## 3.13 Esercizi

**1.** (a) Trovare due interi $x$ e $y$ tali che $17x+101y=1$.
(b) Trovare $17^{-1} \pmod{101}$.

**2.** (a) Risolvere $7d \equiv 1 \pmod{30}$.
(b) Un messaggio viene scritto come un numero $m \pmod{31}$. Se $m$ viene cifrato come $m^7 \pmod{31}$, come verrà decifrato? (*Suggerimento*: la cifratura viene eseguita elevando il testo in chiaro a una potenza modulo 31. Usare il teorema di Fermat.)

**3.** (a) Trovare tutte le soluzioni di $12x \equiv 28 \pmod{236}$.
(b) Trovare tutte le soluzioni di $12x \equiv 30 \pmod{236}$.

**4.** (a) Usare l'algoritmo euclideo per calcolare MCD(30030, 257).
(b) Usando il risultato della parte (a) e il fatto che $30030 = 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13$, mostrare che 257 è primo. (*Osservazione:* questo metodo per calcolare il massimo comune divisore, al posto di fare varie divisioni per tentativi (per 2, 3, 5, ...), è spesso più veloce per stabilire se primi piccoli dividono un numero)

**5.** (a) Calcolare MCD(4883, 4369).
(b) Fattorizzare 4883 e 4369 in un prodotto di primi.

**6.** (a) I numeri di Fibonacci $1, 1, 2, 3, 5, 8, \ldots$ sono definiti dalla ricorrenza $F_{n+1} = F_n + F_{n-1}$ e dalle condizioni iniziali $F_1 = 1$ e $F_2 = 1$. Usare l'algoritmo euclideo per calcolare $\text{MCD}(F_n, F_{n-1})$ per ogni $n \geq 1$.
(b) Trovare MCD(11111111, 11111).
(c) Calcolare MCD($a$,$b$), dove $a = 111\cdots11$ è formato da $F_n$ cifre tutte uguali a 1 e $b = 111\cdots11$ è formato da $F_{n-1}$ cifre tutte uguali a 1. (*Suggerimento:* utilizzare le parti (a) e (b).)

**7.** (a) Sia $p$ un primo. Siano $a$ e $b$ due interi tali che $ab \equiv 0 \pmod{p}$. Mostrare che $a \equiv 0$ oppure $b \equiv 0 \pmod{p}$.
(b) Mostrare che se $a$, $b$, $n$ sono interi con $n|ab$ e MCD($a$,$n$) = 1, allora $n|b$.

**8.** Sia $p \geq 3$ un primo. Mostrare che le uniche soluzioni di $x^2 \equiv 1 \pmod{p}$ sono $x \equiv \pm 1 \pmod{p}$. (*Suggerimento:* applicare l'Esercizio 7(a) a $(x+1)(x-1)$.)

**9.** Se $x \equiv 2 \pmod{7}$ e $x \equiv 3 \pmod{10}$, a cosa è congruente $x$ modulo 70?

**10.** Un gruppo di persone si deve disporre per una parata. Se si allineano tre per riga, una persona resta fuori. Se si allineano quattro per riga, due persone restano fuori. Infine, se si allineano cinque per riga, tre persone restano fuori. Qual è il minor numero possibile di persone? Qual'è il numero minore successivo? (*Suggerimento*: interpretare questo problema in termini del teorema cinese del resto.)

**11.** Sia $p$ un primo. Mostrare che $a^p \equiv a \pmod{p}$ per ogni $a$.

**12.** Dividere $2^{10203}$ per 101. Qual è il resto?

**13.** Trovare le ultime due cifre di $123^{562}$.

**14.** **(a)** Calcolare $7^7 \pmod{4}$.

**(b)** Usare la parte (a) per trovare l'ultima cifra di $7^{7^7}$. (*Nota:* $a^{b^c}$ significa $a^{(b^c)}$ poiché l'altra interpretazione possibile sarebbe $(a^b)^c = a^{bc}$, che si scrive più semplicemente senza un secondo elevamento a potenza.)

**15.** **(a)** Calcolare $\varphi(d)$ per ognuno dei divisori di 10 (ossia, 1, 2, 5, 10) e trovare la somma di questi $\varphi(d)$.

**(b)** Ripetere la parte (a) per tutti i divisori di 12.

**(c)** Sia $n \geq 1$. Congetturare il valore di $\sum \varphi(d)$, dove la somma è fatta su tutti i divisori di $n$. (Questo risultato è dimostrato in molti testi elementari di teoria dei numeri.)

**16.** **(a)** Sia $p = 7$, 13 o 19. Mostrare che $a^{1728} \equiv 1 \pmod{p}$ per ogni $a$ con $p \nmid a$.

**(b)** Sia $p = 7$, 13 o 19. Mostrare che $a^{1729} \equiv a \pmod{p}$ per ogni $a$. (*Suggerimento:* considerare il caso $p|a$ separatamente.)

**(c)** Mostrare che $a^{1729} \equiv a \pmod{1729}$ per ogni $a$. I numeri composti $n$ per cui $a^n \equiv a \pmod{n}$ per ogni $a$ si chiamano numeri di Carmichael. Questi numeri sono rari (561 è un'altro esempio), ma ce ne sono infiniti [Alford et al. 2].

**17.** **(a)** Mostrare che ogni classe di congruenza non nulla modulo 11 è una potenza di 2 e quindi che 2 è una radice primitiva modulo 11.

**(b)** Osservato che $2^3 \equiv 8 \pmod{11}$, trovare $x$ in modo che $8^x \equiv 2 \pmod{11}$. (*Suggerimento:* qual è l'inverso di 3 (mod 10)?)

**(c)** Mostrare che ogni classe di congruenza non nulla modulo 11 è una potenza di 8 e quindi che 8 è una radice primitiva modulo 11.

**(d)** Sia $p$ un primo e sia $g$ una radice primitiva modulo $p$. Sia $h \equiv g^y \pmod{p}$ con $\text{MCD}(y, p-1) = 1$. Sia $xy \equiv 1 \pmod{p-1}$. Mostrare che $h^x \equiv g \pmod{p}$.

**(e)** Siano $p$ e $h$ come in (d). Mostrare che $h$ è una radice primitiva modulo $p$. (*Osservazione:* poiché ci sono $\varphi(p-1)$ possibilità per l'esponente $x$ in (d), questo produce tutte le $\varphi(p-1)$ radici primitive modulo $p$.)

**18.** **(a)** Trovare l'inversa di $\begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix} \pmod{26}$.

**(b)** Trovare tutti i valori di $b \pmod{26}$ per cui $\begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix} \pmod{26}$ è invertibile.

**19.** Trovare tutti i primi $p$ per cui $\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{p}$ non è invertibile.



**20.** Siano $a$ e $n > 1$ interi con $\text{MCD}(a,n) = 1$. L'**ordine** di $a$ modulo $n$ è il più piccolo intero positivo $r$ tale che $a^r \equiv 1 \pmod{n}$. Si scrive $r = \text{ord}_n(a)$.

**(a)** Mostrare che $r \leq \varphi(n)$.

**(b)** Mostrare che se $m = rk$ è un multiplo di $r$, allora $a^m \equiv 1 \pmod{n}$.

**(c)** Sia $a^t \equiv 1 \pmod{n}$ e $t = qr + s$ con $0 \leq s < r$ (si tratta semplicemente della divisione con resto). Mostrare che $a^s \equiv 1 \pmod{n}$.

**(d)** Usando la definizione di $r$ e il fatto che $0 \leq s < r$, mostrare che $s = 0$ e quindi che $r|t$. Da qui e da (b) si ha che $a^t \equiv 1 \pmod{n}$ se e solo se $\text{ord}_n(a)|t$.

**(e)** Mostrare che $\text{ord}_n(a)|\varphi(n)$.

**21.** Questo esercizio mostra mediante un esempio come usare i risultati dell'Esercizio 20 per dimostrare che un numero è una radice primitiva modulo un primo $p$, una volta nota la fattorizzazione di $p-1$. In particolare, si mostrerà che 7 è una radice primitiva modulo 601. Si noti che $600 = 2^3 \cdot 3 \cdot 5^2$.

**(a)** Mostrare che se un intero $r < 600$ divide 600, allora divide almeno uno dei numeri 300, 200, 120 (ossia 600/2, 600/3 e 600/5).

**(b)** Mostrare che se $\text{ord}_{601}(7) < 600$, allora esso divide uno dei numeri 300, 200, 120.

**(c)** Sapendo che

$$7^{300} \equiv 600, \quad 7^{200} \equiv 576, \quad 7^{120} \equiv 423 \pmod{601},$$

perché si può concludere che $\text{ord}_{601}(7)$ non divide 300, 200, 120?

**(d)** Mostrare che 7 è una radice primitiva modulo 601.

**(e)** In generale, si supponga che $p$ sia un primo e che $p - 1 = q_1^{a_1} \cdots q_s^{a_s}$ sia la fattorizzazione di $p-1$ in primi. Descrivere una procedura per decidere se un numero $g$ è una radice primitiva modulo $p$. (Quindi, se occorre trovare una radice primitiva modulo $p$, si può semplicemente usare questa procedura per controllare i numeri $g = 2, 3, 5, 6, \ldots$ in successione finché non si trova una radice primitiva.)

**22.** Si vuole determinare un esponente $k$ tale che $3^k \equiv 2 \pmod{65537}$.

**(a)** Si osservi che $2^{32} \equiv 1 \pmod{65537}$, ma $2^{16} \not\equiv 1 \pmod{65537}$. Si può dimostrare (Esercizio 32) che 3 è una radice primitiva modulo 65537, cosa che implica che $3^n \equiv 1 \pmod{65537}$ se e solo se $65536|n$. Si usi questo per mostrare che $2048|k$ e che 4096 non divide $k$. (*Suggerimento:* si elevino entrambi i membri di $3^k \equiv 2$ alla 16-esima e alla 32-esima potenza.)

**(b)** Si usi il risultato della parte (a) per concludere che esistono solo 16 possibili scelte per $k$ che devono essere considerate. Si usi questa informazione per determinare $k$. Questo problema mostra che se $p - 1$ ha una speciale struttura, per esempio è una potenza di 2, allora questo può essere usato

per evitare ricerche esaustive. Quindi, tali primi sono crittograficamente deboli. Si veda l'Esercizio 9 del Capitolo 7 per una reinterpretazione del presente problema.

**23.** **(a)** Sia $x = b_1 b_2 \cdots b_w$ un intero scritto in binario (per esempio, quando $x = 1011$ si ha $b_1 = 1$, $b_2 = 0$, $b_3 = 1$, $b_4 = 1$). Siano $y$ e $n$ due interi. Si esegua la seguente procedura.

1. Partire con $k = 1$ e $s_1 = 1$.
2. Se $b_k = 1$, porre $r_k \equiv s_k y \pmod{n}$. Se $b_k = 0$, porre $r_k = s_k$.
3. Porre $s_{k+1} \equiv r_k^2 \pmod{n}$.
4. Se $k = w$, stop. Se $k < w$, aggiungere 1 a $k$ e andare al passo 2.

Mostrare che $r_w \equiv y^x \pmod{n}$.

**(b)** Siano $x$, $y$ e $n$ tre interi positivi. Mostrare che la seguente procedura calcola $y^x \pmod{n}$.

1. Partire con $a = x$, $b = 1$, $c = y$.
2. Se $a$ è pari, porre $a = a/2$ e porre $b = b, c \equiv c^2 \pmod{n}$.
3. Se $a$ è dispari, porre $a = a - 1$ e porre $b \equiv bc \pmod{n}, c = c$.
4. Se $a \neq 0$, andare al passo 2.
5. Output $b$.

(*Osservazione:* questo algoritmo è simile a quello descritto nella parte (a), ma usa i bit binari di $x$ in ordine inverso.)

**24.** Ecco come costruire il numero $x$ garantito dalla forma generale del teorema cinese del resto. Si supponga che $m_1, \ldots, m_k$ siano numeri interi con $\text{MCD}(m_i, m_j) = 1$ per ogni $i \neq j$. Siano $a_1, \ldots, a_k$ numeri interi. Eseguire la seguente procedura.

1. Per $i = 1, \ldots, k$, porre $z_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$.
2. Per $i = 1, \ldots, k$, porre $y_i \equiv z_i^{-1} \pmod{m_i}$.
3. Porre $x = a_1 y_1 z_1 + \cdots + a_k y_k z_k$.

Mostrare che $x \equiv a_i \pmod{m_i}$ per ogni $i$.

**25.** **(a)** Trovare tutte le quattro soluzioni di $x^2 \equiv 133 \pmod{143}$. (Si noti che $143 = 11 \cdot 13$.)

**(b)** Trovare tutte le soluzioni di $x^2 \equiv 77 \pmod{143}$. (Ci sono solo due soluzioni in questo caso, poiché $\text{MCD}(77, 143) \neq 1$.)

**26.** Sia $p \equiv 3 \pmod{4}$ un primo. Mostrare che $x^2 \equiv -1 \pmod{p}$ non ha soluzioni. (*Suggerimento:* supporre che esista una soluzione $x$, elevare entrambi i membri della congruenza alla potenza $(p-1)/2$ e usare il teorema di Fermat.)

**27.** Alice progetta un crittosistema nel modo seguente (questo sistema è dovuto a Rabin). Sceglie due primi distinti $p$ e $q$ (preferibilmente, entrambi congruenti a 3 modulo 4) e li tiene segreti, mentre rende pubblico $n = pq$. Quando Bob vuole mandare ad Alice un messaggio $m$, calcola $x \equiv m^2 \pmod{n}$ e manda $x$ ad Alice. Lei costruisce una macchina di decifrazione che si comporta come segue: quando alla macchina viene dato un numero $x$, essa calcola le radici quadrate di $x \pmod{n}$, conoscendo $p$ e $q$. Normalmente esiste più di una radice quadrata. Essa ne sceglie una a caso e la passa ad Alice. Quando Alice riceve $x$ da Bob, lo inserisce nella macchina. Se l'output della macchina è un messaggio che ha un significato, Alice lo accetta come messaggio corretto. Se invece non ha senso, Alice inserisce $x$ ancora una volta nella macchina e continua in questo modo fino a quando ottiene un messaggio che ha significato.



**(a)** Perché Alice dovrebbe aspettarsi di ottenere un messaggio significativo abbastanza presto?

**(b)** Se Oscar (che già conosce $n$) intercetta $x$, perché dovrebbe essere difficile per lui determinare il messaggio $m$?

**(c)** Se Eva irrompe nell'ufficio di Alice e riesce a provare alcuni attacchi di testo cifrato scelto alla macchina di decifrazione di Alice, come può determinare la fattorizzazione di $n$?

**28.** Questo esercizio mostra che l'algoritmo euclideo calcola il massimo comune divisore. Siano $a$, $b$, $q_i$, $r_i$ come nel Paragrafo 3.1.

**(a)** Sia $d$ un divisore comune di $a$ e di $b$. Mostrare che $d | r_1$ e usare questo fatto per mostrare che $d | r_2$.

**(b)** Sia $d$ come in (a). Usare l'induzione per mostrare che $d | r_i$ per ogni $i$. In particolare, $d | r_k$, l'ultimo resto non nullo.

**(c)** Usare l'induzione per mostrare che $r_k | r_i$ per $1 \leq i \leq k$.

**(d)** Usando il fatto che $r_k | r_1$ e $r_k | r_2$, mostrare che $r_k | b$ e quindi che $r_k | a$. Quindi $r_k$ è un divisore comune di $a$ e di $b$.

**(e)** Usare (b) per mostrare che $r_k \geq d$ per ogni divisore comune $d$ e che pertanto $r_k$ è il massimo comune divisore.

**29.** Usare il simbolo di Legendre per determinare quale delle seguenti congruenze ha soluzione (ogni modulo è primo):

**(a)** $x^2 \equiv 123 \pmod{401}$

**(b)** $x^2 \equiv 43 \pmod{179}$

**(c)** $x^2 \equiv 1093 \pmod{65537}$

**30.** **(a)** Sia $n$ dispari e si assuma che $\text{MCD}(a,n) = 1$. Mostrare che se $\left(\frac{a}{n}\right) = -1$, allora $a$ non è un quadrato modulo $n$.

**(b)** Mostrare che $\left(\frac{3}{35}\right) = +1$.

**(c)** Mostrare che 3 non è un quadrato modulo 35.

**31.** Sia $n = 15$. Mostrare che $\left(\frac{2}{n}\right) \not\equiv 2^{(n-1)/2} \pmod{n}$.

**32.** **(a)** Mostrare che $\left(\frac{3}{65537}\right) = -1$.

**(b)** Mostrare che $3^{(65537-1)/2} \not\equiv 1 \pmod{65537}$.

**(c)** Usare la procedura dell'Esercizio 21 per mostrare che 3 è una radice primitiva modulo 65537. (*Osservazione:* la stessa argomentazione mostra che 3 è una radice primitiva per ogni primo $p \geq 5$ tale che $p-1$ sia una potenza di 2. Tuttavia, ci sono solo sei primi noti per cui $p-1$ è una potenza di 2, ossia 2, 3, 5, 17, 257, 65537. Essi sono chiamati *primi di Fermat.*)

**33.** **(a)** Mostrare che gli unici polinomi irriducibili in $\mathbb{Z}_2[X]$ di grado al più 2 sono $X$, $X+1$ e $X^2+X+1$.

**(b)** Mostrare che $X^4+X+1$ è irriducibile in $\mathbb{Z}_2[X]$. (*Suggerimento:* se fosse fattorizzabile, dovrebbe avere almeno un fattore di grado al più 2.)

**(c)** Mostrare che $X^4 \equiv X+1$, $X^8 \equiv X^2+1$ e $X^{16} \equiv X \pmod{X^4+X+1}$.

**(d)** Mostrare che $X^{15} \equiv 1 \pmod{X^4+X+1}$.

**34.** **(a)** Mostrare che $X^2+1$ è irriducibile in $\mathbb{Z}_3[X]$.

**(b)** Trovare l'inverso moltiplicativo di $1+2X$ in $\mathbb{Z}_3[X] \pmod{X^2+1}$.

**35.** Mostrare che i quozienti nell'algoritmo euclideo per MCD($a$,$b$) sono esattamente i numeri $a_0, a_1, \ldots$ che appaiono nella frazione continua di $a/b$.

**36.** **(a)** Calcolare un po' di termini delle frazioni continue di $\sqrt{3}$ e $\sqrt{7}$ e vedere se si nota una qualche regolarità. (Si può mostrare che la successione degli $a_i$ che compaiono nella frazione continua di ogni numero irrazionale della forma $a+b\sqrt{d}$ con $a$, $b$, $d$ razionali e $d>0$ è sempre definitivamente periodica.)

**(b)** Per $d = 3, 7$, sia $n$ l'indice per cui $a_{n+1} = 2a_0$ nella frazione continua di $\sqrt{d}$. Calcolare $p_n$ e $q_n$ e mostrare che $x = p_n$ e $y = q_n$ danno una soluzione dell'equazione di Pell $x^2 - dy^2 = 1$.

**(c)** Usare il metodo della parte (b) per risolvere $x^2 - 19y^2 = 1$.

**37.** Calcolare vari termini della frazione continua di $e$. Si nota qualche regolarità? (Al contrario, la frazione continua di $\pi$ sembra essere abbastanza casuale.)

**38.** Calcolare vari termini della frazione continua di $(1+\sqrt{5})/2$ e calcolare i corrispondenti numeri $p_n$ e $q_n$ (definiti nel Paragrafo 3.12). Le successioni $p_0, p_1, p_2, \ldots$ e $q_1, q_2, \ldots$ formano una qualche successione famosa di numeri?

**39.** Siano $p$ e $q$ due primi distinti.

**(a)** Mostrare che tra gli interi $m$ tali che $1 \leq m < pq$, ci sono $q-1$ multipli di $p$ e ci sono $p-1$ multipli di $q$.

**(b)** Supposto MCD($m$,$pq$) $> 1$, mostrare che $m$ è un multiplo di $p$ o un multiplo di $q$.

**(c)** Mostrare che se $1 \leq m < pq$, allora $m$ non può essere un multiplo di entrambi $p$ e $q$.

**(d)** Mostrare che il numero di interi $m$ con $1 \leq m < pq$ e MCD($m$,$pq$) $= 1$ è $pq-1-(p-1)-(q-1) = (p-1)(q-1)$. (*Osservazione:* questo dimostra che $\varphi(pq) = (p-1)(q-1)$.)



**40.** **(a)** Dare un esempio di interi $m \neq n$ con MCD($m$,$n$) $> 1$ e di interi $a$, $b$ tali che le congruenze simultanee

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}$$

non abbiano soluzione.

**(b)** Dare un esempio di interi $m \neq n$ con MCD($m$,$n$) $> 1$ e di interi $a \neq b$ tali che le congruenze simultanee

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}$$

non abbiano soluzione.

## 3.14 Problemi al calcolatore

**1.** Calcolare MCD(8765,23485).

**2.** **(a)** Trovare due interi $x$ e $y$ tali che $65537x + 3511y = 1$.

**(b)** Trovare due interi $x$ e $y$ tali che $65537x + 3511y = 17$.

**3.** Trovare le ultime cinque cifre di $3^{1234567}$ (non si chieda al calcolatore di visualizzare $3^{1234567}$: è troppo grande!).

**4.** Risolvere $314x \equiv 271 \pmod{11111}$.

**5.** Trovare tutte le soluzioni di $216x \equiv 66 \pmod{606}$.

**6.** Trovare un intero tale che, diviso per 101, dia resto 17, diviso per 201, dia resto 18 e diviso per 301, dia resto 19.

**7.** Sia $n = 391 = 17 \cdot 23$. Mostrare che $2^{n-1} \not\equiv 1 \pmod{n}$. Trovare un esponente $j > 0$ tale che $2^j \equiv 1 \pmod{n}$.

**8.** Sia $n = 84047 \cdot 65497$. Trovare $x$ e $y$ con $x^2 \equiv y^2 \pmod{n}$, ma $x \not\equiv \pm y \pmod{n}$.

**9.** Verificare che 3 è una radice primitiva per il primo 65537. (*Suggerimento:* usare il metodo dell'Esercizio 21.)

**10.** Sia $M = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 5 & 25 \\ 1 & 14 & 196 \end{pmatrix}$.

**(a)** Trovare l'inversa di $M \pmod{101}$.

**(b)** Per quali primi $p$ la matrice $M$ non ha un'inversa modulo $p$?

**11.** Trovare la radice quadrata di 26055 modulo il primo 34807.

**12.** Trovare tutte le radici quadrate di 1522756 modulo 2325781.

**13.** Provare a trovare una radice quadrata di 48382 modulo il primo 83987 usando il metodo del Paragrafo 3.9. Elevare al quadrato la risposta per vedere se è corretta. Di quale numero si è trovata la radice quadrata?