

## 0. Numeri interi.

Sia  $\mathbf{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  l'insieme dei numeri interi e sia  $\mathbf{N} = \{1, 2, 3, \dots\}$  il sottoinsieme dei numeri interi positivi. Sappiamo bene come addizionare, sottrarre e moltiplicare i numeri interi. In questo paragrafo discuteremo la divisione fra numeri interi e alcune sue conseguenze. Introduciamo i numeri *primi* e dimostreremo il Teorema Fondamentale dell' Aritmetica: ogni intero positivo può essere scritto in modo unico come prodotto di numeri primi.

**Teorema (0.1).** (*Divisione con resto*) Siano  $a, b \in \mathbf{Z}$  con  $b > 0$ . Allora esistono unici due interi, il quoziente  $q$  ed il resto  $r$ , tali che

$$\begin{aligned} a &= qb + r, \\ 0 &\leq r < b. \end{aligned}$$

**Definizione.** Siano  $a, b \in \mathbf{Z}$ . Si dice che  $a$  divide  $b$  se esiste un intero  $c \in \mathbf{Z}$  tale che

$$b = ac.$$

Per esempio, 3 divide 15, perché  $15 = 3 \cdot 5$ . Ogni intero divide 0. Se  $a$  divide  $b$ , si dice anche che  $a$  è un *divisore* di  $b$  oppure che  $b$  è *divisibile* per  $a$ . In tal caso si scrive  $a|b$ . Si verifica facilmente che 1 è un divisore di ogni numero e che  $b$  divide  $a \pm a'$  quando divide sia  $a$  che  $a'$ . Se  $a \neq 0$  e  $b$  divide  $a$ , allora  $|b| \leq |a|$ . Per quest'ultima proprietà la seguente definizione ha senso.

**Definizione.** Se  $a$  e  $b$  sono interi non entrambi nulli, il *massimo comun divisore*  $\text{mcd}(a, b)$  di  $a$  e  $b$  è il più grande intero che divide  $a$  e  $b$ . Definiamo  $\text{mcd}(0, 0) = 0$ .

**Osservazione (0.2).** Siano  $a, b \in \mathbf{Z}$ .

- (i)  $\text{mcd}(b, a) = \text{mcd}(a, b)$ ,
- (ii)  $\text{mcd}(-a, b) = \text{mcd}(a, b)$ ,
- (iii) Per ogni  $q \in \mathbf{Z}$  si ha che  $\text{mcd}(a, b + qa) = \text{mcd}(a, b)$ .

**Dimostrazione.** Dimostriamo soltanto la parte (iii) perché le dimostrazioni delle altre parti sono simili e più facili. Sia  $q \in \mathbf{Z}$ . Se  $d$  divide  $a$  e  $b$ , allora  $d$  divide  $b + qa$ . Viceversa, se  $d$  divide  $a$  e  $b + qa$  allora  $d$  divide  $b = (b + qa) - qa$ . Dunque l'insieme dei divisori comuni di  $a$  e  $b$  è uguale all'insieme dei divisori comuni di  $a$  e  $b + qa$ . Questo dimostra (iii).

**Teorema (0.3).** Siano  $a, b \in \mathbf{Z}$ , non entrambi nulli. Allora il massimo comun divisore di  $a$  e  $b$  è uguale al più piccolo elemento positivo nell'insieme

$$A = \{ax + by : x, y \in \mathbf{Z}\}.$$

**Dimostrazione.** Osserviamo innanzitutto che  $A$  contiene degli elementi positivi, ossia  $A \cap \mathbf{N} \neq \emptyset$ . Infatti i numeri  $a, -a, b, -b$  sono elementi di  $A$ , ottenuti rispettivamente per  $x = 0, y = \pm 1$  e  $x = \pm 1, y = 0$ . Sia  $d = ax + by$  il più piccolo elemento positivo in  $A$ . Un tale elemento esiste perché  $A \cap \mathbf{N} \subset \mathbf{N}$  che è un insieme bene ordinato.

Gli elementi in  $A$  sono somme di un multiplo intero di  $a$  e uno di  $b$ . Allora tutti, ed in particolare  $d$ , sono divisibili per  $\text{mcd}(a, b)$ . Questo implica che

$$\text{mcd}(a, b) \leq d.$$

D'altra parte, se  $c = ax' + by' \in A$ , utilizzando il Teorema 0.1, possiamo dividere l'intero  $c$  per  $d$  con quoziente  $q$  e resto  $r$ :

$$c = qd + r \quad \text{con } 0 \leq r < d.$$

Sostituendo  $c = ax' + by'$  e  $d = ax + by$ , si vede che  $r = a(x' - qx) + b(y' - qy) \in A$ . Siccome  $r < d$  e  $d$  era minimo, dobbiamo avere che  $r = 0$ . Dunque  $c = qd$  e  $d$  divide  $c$ . Siccome  $c$  era un elemento arbitrario di  $A$ , concludiamo che  $d$  divide *ogni*  $c \in A$ . In particolare  $d$  divide  $a, b \in A$ . Risulta che

$$d \leq \text{mcd}(a, b)$$

e la dimostrazione è completa.

Il teorema appena dimostrato ha una importante conseguenza:

**Corollario (0.4).** *Siano  $a, b \in \mathbf{Z}$ . Allora esistono  $x, y \in \mathbf{Z}$  tali che*

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

A partire dal Corollario (0.4) si possono dimostrare inoltre i seguenti fatti:

**Corollario (0.5)** Siano  $a, b \in \mathbf{Z}$ . Se l'intero  $d$  divide  $a$  e  $b$ , allora  $d$  divide  $\text{mcd}(a, b)$ .

**Corollario (0.6)** Siano  $a, b, c \in \mathbf{Z}$ . Se  $\text{mcd}(a, b) = 1$  e  $a|bc$  allora  $a|c$ .

*Dim.* Per il Corollario 0.4 esistono  $x, y \in \mathbf{Z}$  tale che  $ax + by = 1$ . Moltiplicando per  $c$  otteniamo:

$$cax + bcy = c.$$

Siccome  $a$  divide  $bc$ , esiste  $m \in \mathbf{Z}$  tale che  $am = bc$ . Troviamo  $c = cax + amy = a(cx + my)$  e vediamo che  $a$  divide  $c$ .

## I numeri primi.

**Definizione.** Un intero  $p$  si dice che è un *numero primo*, se è positivo e se i soli divisori positivi di  $p$  sono 1 e  $p$ .

Esempi di numeri primi sono 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ..., 94291, 94307, 94309, ..., 772865886177933052632667046915246737827100790144773744195236265619879496879953539649, .... Come vedremo in seguito, i numeri primi sono infiniti.

**Proposizione (0.7).** *Siano  $b, c \in \mathbf{Z}$  e sia  $p$  un numero primo. Se  $p|bc$  allora  $p|b$  oppure  $p|c$ .*

**Dimostrazione.** Ovviamente, il massimo comun divisore di  $b$  e  $p$  divide  $p$ . Quindi  $\text{mcd}(b, p) = 1$  oppure  $p$ . Se  $p$  non divide  $b$  allora  $\text{mcd}(b, p) = 1$  e per il Cor.0.6 abbiamo che  $p$  divide  $c$ .

**Teorema (0.8).** *(Teorema Fondamentale dell'Aritmetica). Per ogni intero  $n > 1$  esistono numeri primi  $p_1, p_2, \dots, p_t$  tali che*

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_t.$$

*I primi  $p_1, \dots, p_t$  sono unici a meno dell'ordine.*

Il teorema vale anche per  $n = 1$  ponendo il prodotto vuoto uguale a 1. Se  $n$  è *negativo*, si applica il teorema precedente a  $-n$  e si trova che esistono numeri primi  $p_1, p_2, \dots, p_t$ , unici a meno dell'ordine, tali che

$$n = -p_1 \cdot p_2 \cdot \dots \cdot p_t.$$

**Teorema (0.9).** *(Dimostrazione di Euclide). I numeri primi sono infiniti.*

**Dimostrazione.** Se i numeri primi fossero in numero finito  $p_1, p_2, \dots, p_n$  allora il numero

$$N = p_1 p_2 \dots p_n + 1$$

sarebbe un numero intero privo di divisori primi, contro il Teorema Fondamentale dell'Aritmetica.

Diamo adesso un *algoritmo* per calcolare il mcd di due interi. Questo metodo si chiama *algoritmo di Euclide*: siano  $a, b \in \mathbf{Z}$  e supponiamo che  $a, b > 0$ . Per la Proposizione 0.2(i) non è una restrizione seria. Definiamo i numeri interi  $r_k$  per  $k = 0, 1, 2, 3, \dots$  come segue. Poniamo  $r_0 = a$  e  $r_1 = b$ . Poi, utilizzando il Teorema 0.1, dividiamo  $r_0$  per  $r_1$  con quoziente  $q_1$  e resto  $r_2$  dove  $0 \leq r_2 < r_1$ . Se  $r_2$  non è zero, dividiamo  $r_1$  per  $r_2$  con quoziente  $q_2$  e resto  $r_3$  soddisfacendo  $0 \leq r_3 < r_2 \dots$  eccetera. In generale, se  $r_k$  non è zero, dividiamo  $r_{k-1}$  per  $r_k$  con quoziente  $q_k$  e resto  $r_{k+1}$ :

$$\begin{aligned} r_{k-1} &= q_k r_k + r_{k+1}, \\ 0 &\leq r_{k+1} < r_k. \end{aligned}$$

Si vede che  $r_1 > r_2 > r_3 > \dots$ . Ad un certo punto il resto  $r_k$  diventa zero e si smette. Il resto precedente  $r_{k-1}$  è uguale a  $\text{mcd}(a, b)$ , come vedremo nella prossima proposizione.

**Esempio.**  $a = 7007$  e  $b = 1991$ :

$$\begin{array}{rcl} & & r_0 = 7007 \\ & & r_1 = 1991 \\ q_1 = 3 & \text{ed} & r_2 = r_0 - 3 \cdot r_1 = 1034 \\ q_2 = 1 & \text{ed} & r_3 = r_1 - 1 \cdot r_2 = 957 \\ q_3 = 1 & \text{ed} & r_4 = r_2 - 1 \cdot r_3 = 77 \\ q_4 = 12 & \text{ed} & r_5 = r_3 - 12 \cdot r_4 = 33 \\ q_5 = 2 & \text{ed} & r_6 = r_4 - 2 \cdot r_5 = 11 \\ q_6 = 3 & \text{ed} & r_7 = r_5 - 3 \cdot r_6 = 0 \end{array}$$

Allora, si trova che  $\text{mcd}(7007, 1991) = 11$ .

**Proposizione (0.10).** *L'algoritmo di Euclide è un algoritmo corretto: termina e dà come risposta il massimo comun divisore.*

**Dimostrazione.** L'algoritmo termina perché i resti  $r_k$  sono non-negativi, ma diventano sempre più piccoli. Ad un certo punto il resto diventa zero e l'algoritmo termina.

Siccome  $r_{k-1} = q_k \cdot r_k + r_{k+1}$  si ha per la Prop.0.2(iii)

$$\text{mcd}(r_{k-1}, r_k) = \text{mcd}(r_k, r_{k+1}).$$

Si trova

$$\text{mcd}(a, b) = \text{mcd}(r_0, r_1) = \text{mcd}(r_1, r_2) = \dots = \text{mcd}(r_{k-1}, r_k) = \dots$$

Alle fine, quando  $r_k$  diventa 0, abbiamo  $\text{mcd}(r_{k-1}, r_k) = \text{mcd}(r_{k-1}, 0) = r_{k-1}$ . Concludiamo che  $\text{mcd}(a, b) = \dots = \text{mcd}(r_{k-1}, 0) = r_{k-1}$  come richiesto.

Ecco una versione estesa dell'algoritmo di Euclide, che calcola anche i due interi  $x, y \in \mathbf{Z}$  del Cor.0.4 tali che

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

**Algoritmo.** Scriviamo

$$\begin{aligned} 1 \cdot a + 0 \cdot b &= a = r_0 \\ 0 \cdot a + 1 \cdot b &= b = r_1 \end{aligned}$$

adesso facciamo i calcoli dell'algoritmo di Euclide, non solo con i resti  $r_1, r_2, r_3, \dots$  ecc., ma ogni volta con l'intera equazione. Come spiegazione prendiamo l'esempio sopra con  $a = 7007$  e  $b = 1991$ . Sottraiamo la seconda uguaglianza  $q_1 = 3$  volte dalla prima, la terza  $q_2 = 1$  volta dalla seconda e così via.

$$\begin{array}{rll}
 1 \cdot 7007 & + 0 \cdot 1991 = & 7007 \\
 0 \cdot 7007 & + 1 \cdot 1991 = & 1991 & (\text{sottrarre } q_1 = 3 \text{ volte}) \\
 1 \cdot 7007 & - 3 \cdot 1991 = & 1034 & (\text{sottrarre } q_2 = 1 \text{ volta}) \\
 -1 \cdot 7007 & + 4 \cdot 1991 = & 957 & (\text{sottrarre } q_3 = 1 \text{ volta}) \\
 2 \cdot 7007 & - 7 \cdot 1991 = & 77 & (\text{sottrarre } q_4 = 12 \text{ volte}) \\
 -25 \cdot 7007 & + 88 \cdot 1991 = & 33 & (\text{sottrarre } q_5 = 2 \text{ volte}) \\
 52 \cdot 7007 & - 183 \cdot 1991 = & 11 & (\text{sottrarre } q_6 = 3 \text{ volte}) \\
 -181 \cdot 7007 & + 637 \cdot 1991 = & 0 & 
 \end{array}$$

Si trova che  $52 \cdot 7007 - 183 \cdot 1991 = 11$ .

### Equazioni diofantee di primo grado $ax + by = c$ .

Consideriamo un'equazione di primo grado a coefficienti interi

$$ax + by = c, \quad a, b, c \in \mathbf{Z}, \quad ab \neq 0. \quad (0.1)$$

Di questa equazione cerchiamo le soluzioni intere, ossia tutte le coppie  $(x, y) \in \mathbf{Z} \times \mathbf{Z}$  che sostituite in (0.1) danno un'identità. C'è da osservare innanzitutto che un'equazione (0.1) non ammette necessariamente soluzioni intere. Se consideriamo ad esempio l'equazione  $2x + 2y = 3$ , vediamo subito che per ogni coppia  $x, y$  di interi,  $2x + 2y$  è un numero pari, mentre 3 è un numero dispari. Dunque, non ci sono soluzioni intere. I risultati del paragrafo precedente ci permettono di caratterizzare le equazioni (0.1) che ammettono soluzioni intere e di risolverle completamente.

**Proposizione (0.11).** *Un'equazione  $ax + by = c$ , con  $a, b, c \in \mathbf{Z}$ , ammette soluzioni intere se e solo se  $\text{mcd}(a, b)$  divide  $c$ .*

**Dimostrazione.** Se un'equazione  $ax + by = c$ , con  $a, b, c \in \mathbf{Z}$ , ammette soluzioni intere, allora per il Cor(0.4) si ha che  $\text{mcd}(a, b) | c$ . Viceversa,  $c = md$  e se  $M, N \in \mathbf{Z}$  soddisfano  $aM + bN = d$  (cf. Cor(0.4)), allora  $(mM, mN)$  sono interi che soddisfano  $amM + bmN = md$ .

Se  $\text{mcd}(a, b) | c$ , possiamo dividere tutti i coefficienti dell'equazione per  $\text{mcd}(a, b)$  e ricondurci ad un'equazione equivalente  $Ax + By = C$ , con coefficienti  $A, B, C \in \mathbf{Z}$  e  $\text{mcd}(A, B) = 1$ .

**Proposizione (0.12).** *Sia data l'equazione  $ax + by = c$ , con  $a, b, c \in \mathbf{Z}$  e  $\text{mcd}(a, b) = 1$ .*

- (1) *Se  $c = 0$ , la soluzione generale dell'equazione  $ax + by = 0$  è data da  $\{(bM, -aM)\}$ , al variare di  $M \in \mathbf{Z}$ .*
- (2) *Siano  $(x_0, y_0)$  e  $(x_1, y_1)$  due soluzioni intere dell'equazione  $ax + by = c$ . Allora la loro differenza  $(x_0 - x_1, y_0 - y_1)$  è una soluzione intera dell'equazione omogenea associata  $ax + by = 0$ .*
- (3) *La soluzione generale dell'equazione  $ax + by = c$  è data da  $(x, y) = (x_0, y_0) + (bM, -aM)$ ,  $M \in \mathbf{Z}$ , dove  $(x_0, y_0)$  è una soluzione particolare e  $\{(bM, -aM)\}_{M \in \mathbf{Z}}$  è la soluzione generale della equazione omogenea associata  $ax + by = 0$ .*

(1) Dall'equazione  $ax + by = 0$  ricaviamo  $x = -\frac{b}{a}y$ . Si ha che  $x \in \mathbf{Z}$  se e solo se  $y = Ma$ , con  $M \in \mathbf{Z}$ . Dunque tutte e sole le soluzioni dell'equazione  $ax + by = 0$  sono della forma  $(x, y) = (bM, -aM)$ , al variare di  $M \in \mathbf{Z}$ .

(2) Se  $ax_0 + by_0 = c$  e  $ax_1 + by_1 = c$ , sottraendo un'equazione dall'altra si ottiene che  $a(x_0 - x_1) + b(y_0 - y_1) = 0$ .

(3) Questo segue immediatamente dai punti (1) e (2).

**Esempio (0.13).** Consideriamo l'equazione  $21x + 56y = 121$ . Poiché  $\text{mcd}(21, 56) = 7$  e 7 non divide 121, l'equazione non ammette soluzioni intere.

**Esempio (0.14).** Consideriamo l'equazione  $623x + 413y = 21$ . Con l'algoritmo di Euclide, calcoliamo  $\text{mcd}(623, 413) = 7$  e verifichiamo che  $7|21$ . Dunque l'equazione ammette soluzioni intere. Dividendo tutti i coefficienti per 7, ci riconduciamo all'equazione equivalente

$$89x + 59y = 3, \quad \text{mcd}(89, 59) = 1. \quad (0.2)$$

Cerchiamo una soluzione particolare di (0.2). Per il Cor.(0.4), sappiamo che esistono  $M, N \in \mathbf{Z}$  tali che  $89M + 59N = 1$  e una coppia di tali interi  $(M, N)$  può essere calcolata con la versione estesa dell'algoritmo di Euclide.

$$r_0 = 89, \quad r_1 = 59, \quad r_0 = q_1 r_1 + r_2, \quad q_1 = 1, r_2 = 30, \quad r_1 = q_2 r_2 + r_3, \quad q_2 = 1, r_3 = 29$$

$$r_2 = q_3 r_3 + r_4, \quad q_3 = 1, r_4 = 1.$$

$$1 \cdot 89 + 0 \cdot 59 = 89$$

$$0 \cdot 89 + 1 \cdot 59 = 59$$

$$1 \cdot 89 + (-1) \cdot 59 = 30$$

$$(-1) \cdot 89 + 2 \cdot 59 = 29$$

$$2 \cdot 89 + (-3) \cdot 59 = 1.$$

Dunque  $(2, -3)$  è una soluzione particolare dell'equazione ausiliaria  $89M + 59N = 1$  e  $(x_0, y_0) = (6, -9)$  è una soluzione particolare dell'equazione (0.2). La soluzione generale dell'equazione (0.2) si trova sommando alla soluzione particolare  $(x_0, y_0) = (6, -9)$  la soluzione generale dell'omogenea associata, ed è data da

$$(x, y) = (6, -9) + (59m, -89m), \quad m \in \mathbf{Z}.$$

## Congruenze.

**Definizione.** Siano  $a, b$  numeri interi e sia  $n \in \mathbf{N}$  un intero positivo. Si dice che  $a$  è congruo a  $b$  modulo  $n$  se  $a$  e  $b$  danno lo stesso nella divisione per  $n$ . Ciò equivale a dire che  $a = b + kn$ , per  $k \in \mathbf{Z}$ , e si indica con  $a \equiv b \pmod{n}$ .

**Proposizione (0.14).** La congruenza modulo  $n$  è una relazione di equivalenza su  $\mathbf{Z}$ .

**Dimostrazione.** La congruenza è riflessiva: infatti  $a = a + 0 \cdot n$  e vale  $a \equiv a \pmod{n}$ .

La congruenza è simmetrica: infatti se  $a \equiv b \pmod{n}$  e  $a = b + kn$ , si ha che  $b = a - kn$ , con  $k \in \mathbf{Z}$ , e  $a \equiv b \pmod{n}$ . La congruenza è transitiva: infatti se  $a \equiv b \pmod{n}$  e  $b \equiv c \pmod{n}$ , vale  $a = b + kn$  e  $b = c + hn$ , con  $k, h \in \mathbf{Z}$ . Ne segue che  $a = b + kn = c + (h + k)n$ , con  $h + k \in \mathbf{Z}$  e dunque  $a \equiv c \pmod{n}$ .

La congruenza modulo  $n$  individua  $n$  classi di equivalenza in  $\mathbf{Z}$ , tante quanti sono i resti distinti nella divisione per  $n$ , ossia  $0, 1, 2, \dots, n - 1$ . Ognuna di esse contiene rispettivamente i numeri della forma

$$\{kn\}_{k \in \mathbf{Z}}, \{kn + 1\}_{k \in \mathbf{Z}}, \{kn + 2\}_{k \in \mathbf{Z}}, \dots, \{kn + (n - 1)\}_{k \in \mathbf{Z}}.$$

Ad esempio, se  $n = 2$  le due classi di equivalenza in  $\mathbf{Z}$  rispetto alla congruenza modulo 2 consistono rispettivamente nei numeri pari e nei numeri dispari. Se  $n = 3$  le tre classi di equivalenza in  $\mathbf{Z}$  rispetto alla congruenza modulo 3 sono date da

$$\{k3\}_{k \in \mathbf{Z}} = \{0, \pm 3, \pm 6, \dots\}, \{k3+1\}_{k \in \mathbf{Z}} = \{1, -2, 4, -5, 7, \dots\}, \{k3+2\}_{k \in \mathbf{Z}} = \{2, -1, 5, -4, 8, \dots\}.$$

**Proposizione (0.15).** La relazione di congruenza modulo  $n$  ha le seguenti proprietà:

- (i) Se  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , allora  $a + c \equiv b + d \pmod{n}$ ;
- (ii) Se  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , allora  $ac \equiv bd \pmod{n}$ ;
- (iii) Sia  $d > 0$  un intero che divide  $a, b, n$ . Allora  $a \equiv b \pmod{n}$  se e solo se  $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ .

**Dimostrazione.** (i)(ii) Se  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , allora  $a = b + kn$  e  $c = d + hn$ , con  $h, k \in \mathbf{Z}$ . Da cui  $a + c = b + d + (h + k)n$ , con  $h + k \in \mathbf{Z}$ , e  $a + c \equiv b + d \pmod{n}$ , come richiesto. Similmente,  $ac = (b + kn)(d + hn) = bd + (k + h + hkn)n$ , con  $(h + k + hkn) \in \mathbf{Z}$ , da cui  $ac \equiv bd \pmod{n}$ .

(iii) Per definizione,  $a \equiv b \pmod{n}$  se e solo se  $a = b + kn$ , con  $k \in \mathbf{Z}$ , che è equivalente a  $\frac{a}{d} = \frac{b}{d} + k\frac{n}{d}$ . Poiché  $d$  divide  $a, b, n$ , si ha che  $\frac{a}{d}, \frac{b}{d}, \frac{n}{d}$  sono interi e l'equazione  $\frac{a}{d} = \frac{b}{d} + k\frac{n}{d}$  è a sua volta equivalente a  $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ , come richiesto.

Consideriamo adesso una congruenza

$$ax \equiv b \pmod{n}, \quad a, b, n \in \mathbf{Z}, \quad n > 0. \quad (0.3)$$

Risolvere questa congruenza significa trovare tutti i numeri interi  $x \in \mathbf{Z}$  tali che  $ax = b + kn$ , con  $k \in \mathbf{N}$ . In altre parole, significa trovare tutti i numeri interi  $x \in \mathbf{Z}$  per cui esiste  $y \in \mathbf{Z}$ , tale che la coppia  $(x, y)$  sia una soluzione dell'equazione  $ax + ny = b$ . È evidente che c'è una stretta relazione fra la congruenza (0.3) e un'equazione del tipo (0.1). Valgono i seguenti fatti:

**Proposizione (0.16).** Una congruenza  $ax \equiv b \pmod{n}$ , con  $a, b, n \in \mathbf{Z}$ ,  $n > 0$ , ammette soluzioni se e solo se  $\text{mcd}(a, n)$  divide  $b$ .

**Dimostrazione.** La proposizione segue direttamente dalla Proposizione (0.11).

Se  $\text{mcd}(a, n) | b$ , possiamo dividere tutti i coefficienti della congruenza per  $\text{mcd}(a, n)$  e ricondurci ad una congruenza equivalente (vedi Prop.(0.15)(iii)) della forma  $Ax \equiv B \pmod{N}$ , con  $A, B, N \in \mathbf{Z}$ ,  $N > 0$  e  $\text{mcd}(A, N) = 1$ .

**Proposizione (0.17).** Sia data la congruenza  $ax \equiv b \pmod{n}$ , con  $a, b, n \in \mathbf{Z}$ ,  $n > 0$  e sia  $\text{mcd}(a, n) = 1$ .

- (1) Se  $b = 0$ , la soluzione generale della congruenza  $ax \equiv 0 \pmod{n}$  è data da  $x = nM$ , al variare di  $M \in \mathbf{Z}$ .
- (2) Se  $x_0$  e  $x_1$  sono due interi tali che  $ax_0 \equiv b \pmod{n}$  e  $ax_1 \equiv b \pmod{n}$ , la loro differenza  $x_0 - x_1$  soddisfa  $a(x_0 - x_1) \equiv 0 \pmod{n}$ .
- (3) La soluzione generale della congruenza  $ax \equiv b \pmod{n}$  è data da  $x = x_0 + nM$ ,  $M \in \mathbf{Z}$ , dove  $x_0$  è una soluzione particolare e  $\{nM\}_{M \in \mathbf{Z}}$  è la soluzione generale della congruenza  $ax \equiv 0 \pmod{n}$ .

**Dimostrazione.** La proposizione segue direttamente dalla Proposizione (0.12).

**Osservazione (0.18).** Una congruenza  $ax \equiv b \pmod{n}$  è risolubile ed ha soluzione generale  $x = x_0 + nM$ , con  $M \in \mathbf{Z}$ , se e solo se è equivalente alla congruenza  $x \equiv x_0 \pmod{n}$ .

**Esempio (0.19)** Consideriamo la congruenza  $2x \equiv 5 \pmod{8}$ . Poiché  $\text{mcd}(2, 8) = 2$  e 2 non divide 5, la congruenza non ha soluzioni.

**Esempio (0.20)** Consideriamo la congruenza  $8x \equiv 4 \pmod{12}$ . Poiché  $\text{mcd}(8, 12) = 4$  e 4 divide 4, la congruenza ha soluzioni. Per prima cosa dividiamo tutti i coefficienti per  $\text{mcd}(8, 12) = 4$  e otteniamo la congruenza equivalente

$$2x \equiv 1 \pmod{3}, \quad \text{mcd}(2, 3) = 1.$$

Poiché  $\text{mcd}(2, 3) = 1$ , per il Cor.(0.4) esistono  $P, Q \in \mathbf{Z}$  tali che  $2P + 3Q = 1$ . Ad esempio  $P = -1$  e  $Q = 1$ . Ne segue che  $x_0 = -1$  è una soluzione particolare della congruenza  $2x \equiv 1 \pmod{3}$ . La soluzione generale della congruenza  $2x \equiv 0 \pmod{3}$  è data da  $x = 3M$ , al variare di  $M \in \mathbf{Z}$ . Pertanto, la soluzione generale della congruenza  $2x \equiv 1 \pmod{3}$  è data da  $x = -1 + 3M$ , con  $M \in \mathbf{Z}$ .

### Il Teorema Cinese del Resto.

In questo paragrafo discutiamo sistemi di congruenze, ossia famiglie congruenze che devono essere soddisfatte *simultaneamente*. Il risultato principale è il seguente.

**Teorema (0.21).** (*Teorema Cinese del Resto*). Sia dato il sistema di congruenze

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m}, \end{cases} \quad a, b, n, m \in \mathbf{Z}, \quad n, m > 0, \quad \text{con} \quad \text{mcd}(n, m) = 1. \quad (0.4)$$

(1) Il sistema ammette soluzioni.

(2) La soluzione generale del sistema è della forma  $x = x_0 + M(nm)$ , dove  $x_0$  è una soluzione particolare ed  $M$  varia in  $\mathbf{Z}$ . In altre parole, la soluzione del sistema è unica modulo  $nm$ .

**Dimostrazione.** È evidente che le congruenze del sistema (0.4) hanno singolarmente soluzioni. Sostituiamo la soluzione generale della prima congruenza  $x = a + nk$ ,  $k \in \mathbf{Z}$ , nella seconda:

$$a + nk \equiv b \pmod{m} \quad \Leftrightarrow \quad nk \equiv (b - a) \pmod{m}. \quad (0.5)$$

Otteniamo così una congruenza in  $k$  che ammette soluzioni perché  $1 = \text{mcd}(n, m)$  divide  $(b - a)$  (cf. Proposizione (0.16)). Se risolviamo la seconda congruenza in  $k$  e sostituiamo la soluzione generale nell'espressione  $x = a + nk$ , otteniamo la soluzione generale del sistema. Questo dimostra il punto (1). Per dimostrare il punto (2), osserviamo che la soluzione generale della (0.5) è data da  $k = k_0 + hm$ , dove  $k_0$  è una soluzione particolare e  $h \in \mathbf{Z}$ . Di conseguenza, la soluzione generale del sistema risulta

$$x = a + n(k_0 + hm) = (a + nk_0) + hnm, \quad h \in \mathbf{Z}.$$

È immediato verificare che  $x_0 = (a + nk_0)$  è una soluzione particolare del sistema. Poiché tutte le soluzioni del sistema differiscono per multipli interi di  $nm$ , possiamo dire che la soluzione è unica modulo  $nm$ .

### Osservazione (0.22).

(a) Il Teorema Cinese del Resto dice che il sistema di congruenze (0.4) è equivalente alla singola congruenza  $x \equiv (a + nk_0) \pmod{nm}$  che a sua volta è equivalente alla congruenza

$$x \equiv c \pmod{nm},$$

dove  $c$  è l'unico intero  $0 \leq c \leq (nm - 1)$  nella stessa classe resto di  $(a + nk_0)$  modulo  $nm$ . Questo fatto può essere così riformulato: *se  $n$  ed  $m$  sono interi relativamente primi, il resto della divisione di un intero per  $nm$  è completamente determinato dai resti delle divisioni per  $n$  e per  $m$ .* Da qui il nome del teorema.

(b) Nel Teorema Cinese del Resto si assume  $d = \text{mcd}(n, m) = 1$ . Nel caso in cui  $d > 1$ , il sistema (0.4) ha soluzioni se e solo se la congruenza (0.5) ha soluzioni. Ciò avviene se e solo se  $\text{mcd}(n, m)$  divide  $(b - a)$  (vedi Propo.(0.16)). In tal caso, dividendo tutti i coefficienti della congruenza (0.5) per  $d$  si ottiene la congruenza equivalente

$$\frac{n}{d}k \equiv \frac{b - a}{d} \pmod{\frac{m}{d}}, \quad \text{mcd}\left(\frac{n}{d}, \frac{m}{d}\right) = 1.$$

Dopodiché la soluzione generale del sistema (0.4) è data da  $x = x_0 + h\frac{mn}{d}$ . Questo è esattamente quello che si fa in pratica quando si risolvono i sistemi di congruenze.

(c) Un sistema con  $p \geq 2$  di due congruenze

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_p \pmod{n_p}, \end{cases} \quad a_i, n_i \in \mathbf{Z}, n_i > 0$$

può essere trattato applicando ripetutamente il Teorema Cinese del Resto, a mano a mano che si procede per sostituzione dall'alto in basso. Si trova che se per ogni  $i \neq j$  vale  $\text{mcd}(n_i, n_j) = 1$ , allora il sistema ammette soluzioni e la soluzione è *unica modulo*  $n_1 \cdot \dots \cdot n_p$ .

**Osservazione (0.23).** A volte può essere conveniente spezzare una singola congruenza in un sistema di congruenze. Siano  $n, m$  interi con  $\text{mcd}(n, m) = 1$ . Allora per  $x \in \mathbf{Z}$  vale

$$x \equiv a \pmod{mn} \quad \Leftrightarrow \quad \begin{cases} x \equiv a \pmod{m} \\ x \equiv a \pmod{n}. \end{cases} \quad (0.6)$$

*Sol.* L'implicazione  $\Rightarrow$  è immediata. Vicersa, sia  $x \in \mathbf{Z}$  che soddisfa il sistema (0.6). Allora valgono simultaneamente

$$\begin{cases} x = a + kn \\ x = a + hm \end{cases}, \quad h, k \in \mathbf{Z}.$$

Ciò equivale a  $kn = hm \Leftrightarrow k = Pm, h = Qn, P, Q \in \mathbf{Z}$ .

**Esercizio (0.24).** Consideriamo il sistema

$$\begin{cases} 2x \equiv 3 \pmod{5} \\ 3x \equiv 2 \pmod{7}. \end{cases}$$

Poiché 5 e 7 sono primi,  $\text{mcd}(2, 5) = \text{mcd}(3, 7) = 1$  e le congruenze del sistema sono singolarmente risolubili. La soluzione generale della prima è data da  $x = 4 + 5k, k \in \mathbf{Z}$  e quella della seconda è data da  $x = 3 + 7h, h \in \mathbf{Z}$ . Dunque (cf. Osservazione (0.18)) il sistema è equivalente al sistema

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{7}. \end{cases} \quad (0.7)$$

Poiché  $\text{mcd}(5, 7) = 1$ , il Teorema Cinese del Resto assicura che il sistema ha soluzioni e che sono tutte della forma  $x = x_0 + M35, M \in \mathbf{Z}$ . Per determinare  $x_0$ , soluzione particolare del sistema, procediamo per sostituzione: sostituiamo  $x = 4 + 5k$  nella seconda equazione del sistema (0.7) e otteniamo la congruenza in  $k$

$$4 + 5k \equiv 3 \pmod{7} \quad \Leftrightarrow \quad 5k \equiv -1 \pmod{7}.$$

È a questo punto che la condizione  $\text{mcd}(5, 7) = 1$  garantisce la risolubilità di questa congruenza e del sistema. La soluzione generale di questa congruenza è  $k = 4 + 7N, N \in \mathbf{Z}$  e la soluzione generale del sistema è

$$x = 4 + 5(4 + 7N) = 24 + 35N, \quad N \in \mathbf{Z}.$$

**Esercizio (0.25).** Consideriamo il sistema

$$\begin{cases} x \equiv 3 \pmod{6} \\ x \equiv 5 \pmod{8} \\ x \equiv 2 \pmod{18}. \end{cases} \quad (0.8)$$

Procediamo per sostituzione e sostituiamo la soluzione generale della prima congruenza  $x = 3 + 6k$ ,  $k \in \mathbf{Z}$  nella seconda. Otteniamo la congruenza in  $k$

$$3 + 6k \equiv 5 \pmod{8} \quad \Leftrightarrow \quad 6k \equiv 2 \pmod{8}.$$

Poiché  $\text{mcd}(6, 8) = 2$  divide 2, la congruenza ha soluzione. Dividendo tutti i suoi coefficienti per  $\text{mcd}(6, 8) = 2$ , otteniamo la congruenza equivalente

$$3k \equiv 1 \pmod{4}, \quad \text{mcd}(3, 4) = 1,$$

che ha soluzione generale  $k = 3 + 4N$ ,  $N \in \mathbf{Z}$ . La soluzione generale del sistema formato dalle prime due equazioni del sistema è

$$x = 3 + 6(3 + 4N) = 21 + 24N, \quad N \in \mathbf{Z}. \quad (0.9)$$

In altre parole, il sistema formato dalle prime due equazioni del sistema (0.8) è equivalente alla singola congruenza  $x \equiv 21 \pmod{24}$ . Sostituendo la soluzione (0.9) nella terza equazione del sistema (0.8), troviamo una nuova congruenza in  $N$

$$21 + 24N \equiv 2 \pmod{18} \quad \Leftrightarrow \quad 24N \equiv -19 \pmod{18}. \quad (0.10)$$

Poiché  $\text{mcd}(24, 18) = 6$  e 6 non divide  $-19$ , la congruenza (0.10) non ammette soluzioni. Di conseguenza anche il sistema (0.8) risulta incompatibile.