Corso di Algebra 1

A. Machì

a.a. 2006–2007

Dispensa I

1. Principio di induzione e principio del minimo intero

Teorema 1. *Il principio di induzione e il principio del minimo intero sono equivalenti.*

Dim. i) Minimo intero $\Rightarrow$ induzione.

Per assurdo (cioè, siano vere le due premesse dell'induzione e falsa la conclusione). Sia

i) $P(1)$ vera;

ii) $P(n)$ vera $\Rightarrow P(n+1)$ vera,

e supponiamo che la P non si vera per ogni n. Esiste allora un intero k tale che $P(k)$ è falsa. L'insieme degli interi per i quali $P(n)$ è falsa è quindi non vuoto (contiene almeno k), e dunque, per il principio del minimo intero, contiene un minimo, e sia m. $P(m)$ è falsa, e poiché m è il minimo intero per cui la P è falsa, $P(m-1)$ è vera. Allora, per *ii*), anche $P(m-1+1) = P(m)$ è vera, una contraddizione. □

La conclusione si può enunciare così come segue le quattro proposizioni

i) il principio del minimo intero è vero;

ii) $P(1)$ vera;

iii) $P(n)$ vera $\Rightarrow P(n+1)$ vera,

iv) Esiste un intero k tale che $P(k)$ è falsa,

sono contraddittorie.

ii) Induzione $\Rightarrow$ minimo intero.

Per assurdo. Sia $A \neq \emptyset$ un insieme di interi positivi che non contenga un minimo. Dimostriamo per induzione che, per ogni n, si ha

$$P(n): \text{ "}x \in A \Rightarrow x \geq n\text{"}.$$

$P(1)$ è vera (ogni intero x è ≥ 1). Sia $P(n)$ vera. Allora $n \notin A$ (altrimenti, avendosi $x \geq n$ per ogni $x \in A$, n sarebbe un intero minimo di A). Sia $k \in A$; allora $k \geq n$, ma poiché $n \notin A$, non può essere $k = n$, e perciò $k \geq n+1$.

Ne segue che $P(n)$ vera implica $P(n+1)$ vera, e dunque P è vera per ogni n. Con $n = k+1$ si ha $k \geq k+1$, una contraddizione. □

Nota. Un insieme di premesse, o assiomi, è non contraddittorio se ammette un modello, cioè un'intepretazione nella quale esse sono verificate. Ad esempio, se si toglie l'ultima delle quattro proposizioni del teorema precedente, le tre proposizioni risultanti non sono più contraddittorie: c'è un modello nel quale sono verificate, e cioè gli interi. Ma è interessante osservare che si può togliere una qualunque delle quattro, e le tre che restano non sono più contraddittorie. Ad esempio, se togliamo "$P(1)$ è vera", le altre tre sono soddifatte con il modello dato, ad esempio, dalla $P(n)$: "$n > 100$":

1. Resta vero

3. $P(n) \Rightarrow P(n+1)$: se $n > 100$ allora $n+1 > 100$. Dunque la 3. è vera.

4. Esiste n tale che $P(n)$ è falsa : basta prendere un qualunque numero $n < 100$. Dunque la 4. è vera.

Se si toglie la 3., le restanti 1., 2., e 4. non sono più contraddittorie; un modello è dato, ad esempio, dalla $P(n)$: "$n < 100$".

2. Divisione intera con resto

Teorema 2. *Dati due numeri interi m, n con $n > 0$, esistono due numeri interi q ed r tali che*

$$i)\ m = nq + r, \quad ii)\ 0 \leq r < n.$$

Inoltre, gli interi q ed r che soddisfano $i)$ e $ii)$ sono unici.

Dim. Il numero r sarà determinato come minimo di un insieme di interi non negativi. Consideriamo l'insieme delle differenze $D = m - nt$ al variare di t negli interi positivi, negativi o zero. Tra gli elementi di D vi sono certamente numeri non negativi: ad esempio, se $t = -|m|$ si ha $m - n(-|m|) = m + n|m| \geq 0$. Se $m \geq 0$ ciò è ovvio. Se $m < 0$, avendosi $n \geq 1$ si ha $m + n|m| \geq 0$. L'insieme $D' \subseteq D$ delle differenze non negative è quindi non vuoto, e pertanto, per il principio del minimo intero, contiene un intero non negativo minimo, e sia r. Allora, per un certo q, $r = m - nq$, ovvero $m = nq + r$, cioè $i)$. Dimostriamo ora che la $ii)$ è soddisfatta. Per assurdo, sia $r \geq n$. Allora, $r = n + x$, con $x \geq 0$, e pertanto $m = nq + r = nq + n + x$, da cui $x = m - (q+1)n$, numero che è della forma $m - nt$; si tratta perciò di un elemento non negativo di D, e come tale appartiene a D'. Ma $x \leq r$, ed essendo $x \geq 0$, se $x < r$ si contraddice la minimalità di r. Allora $x = r$,

e $r = n + x$ implica $n = 0$, contro l'ipotesi. Ne segue la *ii*), ovvero: *il resto non è mai negativo ed è minore del divisore.*

Per quanto riguarda l'unicità, supponiamo che esistano due coppie q, r e q_q, r_1 tali che

$$m = nq + r = nq_1 + r_1.$$

Sia $r < r_1$; allora,

$$r_1 - r = n(q - q_1) < n, \tag{1}$$

(r ed r_1 sono minori di n, e dunque anche la loro differenza lo è). Inoltre, essendo $r_1 - r$ non negativo, anche $q - q_1$ è non negativo, e se fosse $q - q_1 > 0$ si avrebbe $n(q - q_1) > n$, contro la (1). Allora $q - q_1 = 0$ e $q = q_1$. Dalla (1) segue allora anche $r = r_1$. □

Esempio. $m = 6, n = 4$. L'insieme $D = \{m - nt\}$, al variare di t, è l'insieme:
...
$t = -5 :\ 6 - 4(-5) = 26;$
$t = -3 :\ 6 - 4(-3) = 18;$
$t = -2\ 6 - 4(-2) = 14;$
$t = -1,\ 6 - 4(-1) = 10;$
$t = 0 :\ 6 - 4 \cdot 0 = 6,$
$t = 1 :\ 6 - 4 \cdot 1 = 2,$
$t = 2 :\ 6 - 4 \cdot 2 = -2,$
$t = 3 :\ 6 - 4 \cdot 3 = -6$
...
L'insieme D' è $\{\ldots, 26, 18, 14, 10, 6, 2\}$, il cui minimo è $r = 2$, che si ottiene per $t = q = 1$: $6 - 4 \cdot 1 = 2$, ovvero $6 = 4 \cdot 1 + 2$.

Gli interi q ed r si chiamano rispettivamente *quoziente* e *resto* della divisione di m per n. Se $r = 0$, allora $m = qn$, e si dice che n *divide* m; si scrive $n|m$.

Un altro modo di dimostrare il Teorema 2 è il seguente. Formiamo i multipli di n (positivi, negativi e zero), e disponiamoli in successione:

$$\ldots, -3 \cdot n, -2 \cdot n, -1 \cdot n, 0, 1 \cdot n, 2 \cdot n, 3 \cdot n, \ldots$$

Allora esistono sempre due termini successivi che sono uno minore e l'altro maggiore di m. Infatti, avendosi $n \geq 1$, basta prendere un intero $k \geq |m|$ perché si abbia

$$kn > n|m| \geq |m| \geq m, \quad -kn \leq -|m| \leq m.$$

Esistono quindi due termini successivi, uno $qn \leq m$, l'altro $(q+1)n > m$ tali che

$$qn \leq m < (q+1)n. \tag{2}$$

Se $m \geq 0$, il numero q è il massimo numero il cui prodotto per n non supera m ed è il quoziente della divisione, mentre la differenza $r = m - qn$ è il resto. (Se $m < 0$, q è il minimo numero il cui prodotto per n supera m). Se sottraiamo qn dai tre membri della (2) otteniamo

$$0 \leq r < n.$$

Esempio. Sia $m = 8$, $n = 6$. 8 si trova tra $1 \cdot 6$ e $2 \cdot 6$. Dunque $q = 1$, e il resto è $r = 8 - 1 \cdot 6 = 2$.

Sia $m = -8$, $n = 6$. -8 si trova tra $-2 \cdot 6 = -12$ e $-1 \cdot 6 = -6$, e pertanto $q = -2$. La differenza $-8 - (-2 \cdot 6) = 4$ è il resto della divisione, e si ha $-8 = -2 \cdot 6 + 4$.

3. Massimo comun divisore

La ricerca dei divisori comuni di due numeri interi si riduce alla ricerca dei divisori di *un solo* numero intero grazie al seguente teorema.

Teorema 3. *Dati due numeri m ed n, esiste un numero d tale che i divisori comuni di m ed n coincidono con i divisori di d. Il numero d è unico a meno del segno.*

Dim. Sia S l'insieme delle combinazioni lineari positive di m ed n a coefficienti interi (positivi, negativi o zero):

$$S = \{am + bn > 0,\ a, b \in Z\}.$$

S è non vuoto. Infatti, se $m, n > 0$, si prendano $a, b > 0$; se $m > 0$ e $n < 0$, si prendano $a < 0$ e $b < 0$; se $m < 0$ e $n > 0$, si prendano $a < 0$ e $b > 0$. Per il principio del minimo intero S contiene un minimo d, e per certi h e k allora:

$$d = hm + kn.$$

Si ha:

i) $c|m$ e $c|n$, allora $c|d$.

ii) $d|m$. Infatti, sia $m = dq + r$, $0 \leq r < d$. Si ha $r = m - dq = m - (hm + kn)q = (1 - h)m + (kq)n$. Se $r > 0$, allora r è un elemento di S, ma essendo minore di d si contraddice la minimalità di r in S. Allora $d|m$, e

analogamente $d|n$. In particolare, se un intero divide d, questo intero divide m ed n, e quindi ha la proprietà richiesta dal teorema.

È chiaro che d è il più grande dei divisori comuni di m ed n, e perciò è unico. Dimostriamo tuttavia l'unicità in base al fatto che i suoi divisori coincidono con quelli di m ed n. Se infatti d e d' sono entrambi tali che i loro divisori coincidono con quelli di m ed n, d', dividendo m ed n divide d, e dunque $d = hd'$, e analogamente $d' = kd$. Allora $d = hkd$, per cui se $d \neq 0$ è $hk = 1$ da cui $h = k = \pm 1$ e $d' = \pm d$. □

4. Algoritmo euclideo per il calcolo del MCD

Dati due interi m ed n, la divisione euclidea fornisce un quoziente e un resto: $m = nq + r$, $0 \leq r < n$. Un numero che divide m ed n divide allora anche r, e d'altra parte un intero che divide n ed r divide anche m, e dunque divide m ed n. Abbiamo così che i divisori comuni di m ed n sono i divisori comuni di n ed r. Se $r \neq 0$, dividendo ora n per r, si ha un resto r', $0 \leq r' < r$ e come prima i divisori comuni di n ed r (e dunque anche di m ed n) sono quelli di r ed r'. Proseguendo in questo modo si ha una successione di divisioni che a un certo punto trova resto zero in quanto resti successivi non nulli sono interi positivi descrescenti (abbiamo posto $r = r_1$), e non si può più proseguire (non si può dividere per zero):

$$\begin{aligned}
m &= nq_1 + r_1, \quad 0 \leq r_1 < n, \\
n &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2, \\
&\vdots \\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, \quad 0 \leq r_{k-1} < r_{k-2}, \\
r_{k-2} &= r_{k-1} q_k + 0, \quad r_k = 0.
\end{aligned}$$

Per quanto visto sopra, un divisore di m ed n è anche un divisore di n ed r_1, e quindi di r_1 ed r_2. Proseguendo in questo modo si ha che un divisore di m ed n è anche un divisore di r_{k-1} e 0, e poiché ogni numero divide 0, i divisori comuni di m ed n sono divisori di r_{k-1}. Viceversa, dall'ultimo passo dell'algoritmo si ha che un divisore di r_{k-1} divide anche r_{k-2}; dal penultimo, che un divisore di r_{k-1} e di r_{k-2} divide anche r_{k-3}, ecc., finché si arriva al secondo passo: un divisore di r_{k-1} divide r_2 ed r_1, e quindi divide n. Dal primo passo si ha allora che un divisore di di r_1 ed n divide m, e quindi divide m ed n. Per il Teorema 3, r_{k-1}, *cioè l'ultimo resto non nullo, è il*

massimo comun divisore $d = (m, n)$ *di* m *ed* n. Il procedimento ora visto per determinare $d = (m, n)$ va sotto il nome di *algoritmo di Euclide*.

Esempio. $m = 40$, $n = 25$.

$$\begin{aligned} 40 &= 25 \cdot 1 + 15, \\ 25 &= 15 \cdot 1 + 10, \\ 15 &= 10 \cdot 1 + 5, \\ 10 &= 5 \cdot 2 + 0. \end{aligned}$$

L'ultimo resto non nullo è 5, che dunque è il MCD tra 40 e 25.

In forma di programma per un sistema di calcolo simbolico si può esprimere come segue:

input: m, n
$u := m$, $v := n$,
finché $v \neq 0$ fare:
(q: quoziente(u, v),
$t := u$,
$u := v$,
$v := t - qv$)
output: u.

Esempio. $m = 40, n = 25$
PRIMO PASSO:
$u := 40$, $v := 25$,
$v \neq 0$? Sì
(q:=quoziente(40,25)=1,
$t := 40$,
$u := 25$,
$v := 40 - 1 \cdot 25 = 15$)
[i nuovi valori di u e v sono ora $u = 25$, $v = 15$]
SECONDO PASSO:
$v \neq 0$? Sì
(q:=quoziente(25,15)=1,
$t := 25$,
$u := 15$,
$v := 25 - 1 \cdot 15 = 10$)
[i nuovi valori di u e v sono ora $u = 15$, $v = 10$]

$v \neq 0$? Sì
ecc.

Se $d = (m, n) = 1$, m e n non hanno divisori comuni diversi da 1: si dicono allora *primi tra loro* (o *relativamente primi*).

Il resto $r_1 = m - qn$ è una combinazione lineare di m e n:

$$r_1 = 1 \cdot m + (-q_1) \cdot n,$$

e ciò è vero anche per r_2: si ha $r_2 = n - q_2 r_1 = n - q_2 m + q_1 q_2 n$, da cui:

$$r_2 = (-q_2) \cdot m + (1 + q_1 q_2) \cdot n,$$

e proseguendo si vede che ciò accade per tutti i resti r_i, $i = 1, 2, \ldots, k$, e dunque anche per $r_{k-1} = d$. Si ha così:

Teorema 4. (IDENTITÀ DI BÉZOUT) *Dati due interi m e n, esistono due interi h e k tali che $d = (m, n)$ è combinazione lineare di m e n:*

$$d = hm + kn. \qquad \diamondsuit$$

Nota. I due interi h e k del Teorema 1.1 non sono univocamente determinati. Per ogni intero s si ha infatti:

$$d = (h \pm sn)m + (k \mp sm)n.$$

Esempio. Con un algoritmo che consta di quattro passi:

$$\begin{aligned} m &= nq_1 + r_1, \\ n &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ r_4 &= r_3 q_3, \end{aligned}$$

e dunque $d = r_3$, abbiamo, con r_1 ed r_2 visti sopra,

$$\begin{aligned} d &= r_3 = r_1 - r_2 q_3 = m - q_1 n + q_2 q_3 m - q_3 n - q_1 q_2 q_3 n \\ &= (1 + q_2 q_3)m - (q_1 + q_3 + q_1 q_2 q_3)n. \end{aligned}$$

Nell'esempio con $m = 40$ ed $n = 25$ abbiamo $q_1 = q_2 = q_3 = 1$, e dunque

$$d = r_3 = (1 + 1 \cdot 1)40 - (1 + 1 + 1 \cdot 1 \cdot 1) = 2 \cdot 40 - 3 \cdot 75) = 80 - 75 = 5.$$

Il programma per l'algoritmo di Euclide fornisce anche la terna $[h, k, d]$ (poiché si cerca una terna, al posto di due numeri l'input deve avere due terne).

input: m, n,
$u := [1, 0, m], v := [0, 1, n]$,
finché $v_3 \neq 0$ fare:
$(q := quoziente(u, v)$,
$t := u$,
$u := v$,
$v : t - qv)$
output: u.

L'input dell'algoritmo consta dei due interi m e n. Nella forma data dall'identità di Bézout essi si scrivono:

$$m = 1 \cdot m + 0 \cdot n,\ n = 0 \cdot m + 1 \cdot n,$$

e queste le due terne iniziali dell'algoritmo.

Vediamo due importanti applicazioni del lemma di Bézout.

Teorema 5. *i) Se $c|ab$ e $(c, a) = 1$ allora $c|b$;*
ii) se $a|c, b|c$ e $(a, b) = 1$, allora $ab|c$.

Dim. i) Per Bézout esistono due interi h e k tali che $1 = hc + ka$; moltiplicando questa uguaglianza per b si ha $b = hcb + kab$. Ma c divide i due addendi della somma, e pertanto divide b.

ii) Sia $c = qa = q_1 b$, $1 = ha + kb$. Moltiplichiamo quest'ultima per qq_1: $qq_1 = haqq_1 + kbqq_1 = hq_1 c + kqc$. Ma $qq_1 = \frac{c^2}{ab}$, da cui semplificando c si ha $\frac{c}{ab} = hq_1 + kq$, che è un intero, e dunque $ab|c$. □

Se $(m, n) = 1$, sia $hm + kn = 1$. Posto $e = hm$, $e_1 = kn$, si ha

$$e^2 = am \cdot am = am(1 - kn) = hm - hkmn \equiv hm = e \bmod mn$$

e analogamente $e_1^2 \equiv e_1 \bmod mn$. Si dice allora che e ed e_1 sono *idempotenti* modulo mn. Inoltre sono *ortogonali* (sempre modulo mn:

$$ee_1 = hm \cdot kn = hkmn \equiv 0 \bmod mn,$$

e a somma 1: $e + e_1 = 1$.

Ci poniamo ora il seguente problema: dati tre interi a,b,c, esistono due interi a' e b' tali che $aa' + bb' = c$? In altri termini, l'*equazione diofantea*

$$ax + by = c \tag{3}$$

ammette soluzioni intere? Intanto, se una soluzione esiste, e qualunque siano x e y che risolvono l'equazione, se un numero divide a e b allora divide c. Abbiamo allora una condizione necessaria affinché la (3) ammetta soluzioni: *il massimo comun divisore d tra a, b deve dividere c.* Ma questa condizione è anche sufficiente: se d divide c, sia $c = dt$. Per l'identità di Bézout, $d = ah + bk$, da cui $c = dt = a(ht) + b(kt)$, e dunque $x = ht$ e $y = kt$ risolvono la (3). (Ovviamente la soluzione non è unica, perché gli interi h e k di Bézout non sono unici. Inoltre, ogniqualvolta $(a, b) = 1$, l'equazione ha sempre soluzione, qualunque sia c). Abbiamo quindi:

Teorema 6. *Condizione necessaria e sufficiente affinché la* (3) *ammetta soluzioni è che il massimo comun divisore $d = (a, b)$ divida c.*

Esempi 1. $12x + 18y = 48$. Qui $d = 6$. Scriviamo $6 = -1 \cdot 12 + 1 \cdot 18$, e proseguendo come sopra, $48 = 6 \cdot 8 = 12(-1 \cdot 8) + 18(1 \cdot 8)$.

2. $12x + 18y = 14$. Qui $d = 6$, ma 6 non divide 14, e dunque l'equazione non ha soluzioni.

3. $7x + 13y = 5$. Qui $d = (7, 13) = 1$, $1 = 2 \cdot 7 + (-1) \cdot 13$, da cui, moltiplicando quest'ultima uguaglianza per 5, $5 = 2 \cdot (7 \cdot 5) + (-1) \cdot (13 \cdot 5)$.

Il massimo comun divisore si estende al caso di più numeri.

Teorema 7. *Dati n numeri $a_1, a_2, \ldots, a_n$, esiste un numero d tale che i divisori comuni dei numeri dati coincidono con i divisori di d.*

Dim. Il teorema è vero per due numeri (Teorema 3); diciamo allora che $T(2)$ è vero. Per induzione su n: supponiamo il teorema vero per $n - 1$ numeri (supponiamo vero $T(n - 1)$), e dimostriamolo vero per n numeri (dimostriamo che $T(n)$ è vero). Consideriamo $a_1, a_2, \ldots, a_{n-1}$. Per l'ipotesi $T(n - 1)$ vero, esiste un numero d' tale che i divisori comuni dei numeri $a_1, a_2, \ldots, a_{n-1}$ coincidono con i divisori di d'. Ne segue che i divisori comuni di $a_1, a_2, \ldots, a_{n-1}$ e a_n coincidono con i divisori comuni di d' ed a_n. Ci siamo così ridotti al caso di due numeri, caso in cui sappiamo che il teorema è vero: esiste cioè un numero d che con i suoi divisori esaurisce i divisori comuni di d' ed a_n, e dunque i divisori comuni di $a_1, a_2, \ldots, a_n$. □

5. Congruenze

Definiamo la seguente relazione ρ nell'insieme degli interi relativi: fissato un intero positivo n,

$a \rho b$ se a e b divisi per n danno lo stesso resto.

Si tratta di una relazione di equivalenza (le tre proprietà riflessiva, simmetrica e transitiva sono immediate), detta *relazione di congruenza modulo n*. Se a è nella relazione ρ con b si dice che a e b sono *congrui modulo n*, e si scrive:

$$a \equiv b \bmod n,$$

Sia $a \equiv b \bmod n$; allora $a = nq + r$, $b = nq' + r$, e sottraendo i due membri $a - b = n(q - q')$, cioè n *divide* $a - b$. Viceversa, se $n|(a - b)$, sia $a = nq_1 + r_1$, $b = nq_2 + r_2$; allora $a - b = n(q_1 - q_2) + r_1 - r_2$, e $a - b = nq$ implicano $r_1 - r_2 = 0$, cioè $r_1 = r_2$, ovvero: *a e b divisi per n danno lo stesso resto*. Abbiamo così:

Teorema 8. *Fissato un intero n, le seguenti proprietà sono equivalenti per ogni coppia di interi a e b*:

i) a e b divisi per n danno lo stesso resto

ii) la differenza a–b è divisibile per n. □

I resti possibili nella divisione di un intero per n sono $0, 1, \ldots n - 1$. Gli interi si ripartiscono quindi in n classi:

1. gli interi che divisi per n danno resto 0 (i multipli di n); denotiamo questa classe con $[0]$ ("classe 0");

2. gli interi che divisi per n danno resto 1; denotiamo questa classe con $[1]$ ("classe 1");

. . . . . .

2. gli interi che divisi per n danno resto $n - 1$; denotiamo questa classe con $[n - 1]$ ("classe $n - 1$").

Queste n classi costituiscono l'insieme quoziente di Z rispetto alla relazione ρ:

$$Z/\rho = \{[0], [1], \ldots, [n - 1]\}.$$

Vediamo alcune proprietà della relazione di congruenza.

1. Moltiplicando una congruenza modulo n per un intero si ottiene ancora una congruenza modulo n. Sia $a \equiv b \bmod n$, e $c \in Z$. Allora:

$$ac \equiv bc \bmod n.$$

Infatti, se $n|(a - b)$, allora $n|(a - b)c = ac - bc$.

2. Viceversa, non si può sempre dividere per uno stesso numero. Ad esempio,

$$2 \cdot 6 \equiv 7 \cdot 6 \bmod 15,$$

(la differenza $12 - 42 = -30$ è divisibile per 15), ma dividendo per 6 si ha $2 \not\equiv 7 \bmod 15$.

Tuttavia si ha:

Teorema 9. Se $ac \equiv bc \bmod n$ e $d = (c, n)$, allora:

$$a \equiv b \bmod \frac{n}{d}.$$

Dim. $ac - bc = kn$ implica $(a-b)\frac{c}{d} = k\frac{n}{d}$. Ma $(\frac{n}{d}, \frac{c}{d}) = 1$ implica $\frac{n}{d} | (a-b)$ (Teorema 5). □

Nell'esempio precedente, $2 \cdot 6 \equiv 7 \cdot 6 \bmod 15$, si ha $(6, 15) = 3$, e dividendo per 3 si ha $2 \equiv 7 \bmod 5$.

Ci chiediamo ora, dati a, b ed n, sotto quali condizioni l'equazione:

$$ax \equiv b \bmod n \tag{4}$$

ammette soluzione. Ci si riduce al caso delle equazioni diofantee. Infatti, se esiste una soluzione c, allora $ac - b = nk$ per un certo k, e dunque $ac - nk = b$, cioè l'equazione

$$ax - my = b$$

ha la soluzione $x = c$ e $y = k$, e viceversa. Allora (Teorema 7):

Teorema 10. *Condizione necessaria e sufficiente affinché la* (4) *abbia una soluzione è che il massimo comun divisore tra a ed n divida b.* □

Corollario. *i) Se c e c' sono soluzioni, e* $d = (a, n)$ *allora* $c' \equiv c \bmod \frac{n}{d}$*;*
ii) se $d = 1$*, la soluzione è unica*

Dim. Se $ac \equiv b \bmod n$ e $ac' \equiv b \bmod n$, allora, sottraendo, $a(c' - c) \equiv 0 \bmod n$, e si ha $\frac{a}{d}(c' - c) \equiv 0 \bmod \frac{n}{d}$. Allora $\frac{n}{d}$ divide $\frac{a}{d}(c' - c)$, ma essendo $(\frac{a}{d}, \frac{n}{d}) = 1$, $\frac{n}{d}$ divide $c' - c$, ovvero $c' \equiv c \bmod \frac{n}{d}$. La *ii)* segue dalla *i)*. □

Esempio. $6x \equiv 4 \bmod 8$; l'equazione è $6x - 8y = 4$. $d = (6, -8) = -2$, e $-2 = 1 \cdot 6 - 1 \cdot 8$; ne segue $4 = -2 \cdot -2 = 6(1 \cdot -2) - 8(1 \cdot -2)$, e la soluzione $x = y = -2$.

Vediamo ora alcune proprietà.

i) Più congruenze rispetto allo stesso modulo si possono sommare membro a membro, ottenendo ancora una congruenza modulo n. Se

$$a \equiv b \bmod n, \quad c \equiv d \bmod n,$$

le differenze $a-c$ e $b-d$ sono divisibili per n, e dunque anche la loro somma lo è. Allora

$$(a-c)+(b-d)=(a+b)-(c+d)$$

è divisibile per n, cioè $(a+b)\equiv(c+d) \bmod n$. Lo stesso risultato vale per un numero qualunque di congruenze.

ii) Due o più congruenze rispetto a uno stesso modulo si possono moltiplicare per uno stesso numero: se $a\equiv b \bmod n$, allora $a-b$ è divisibile per n, e perciò lo è anche $(a-b)k=ak-bk$ per ogni k, ovvero $ak\equiv bk \bmod n$.

iii) Due o più congruenze rispetto a uno stesso modulo si possono moltiplicare membro a membro: se $a\equiv b \bmod n$ e $c\equiv d \bmod n$, allora per la *ii*), moltiplicando i due membri della prima per c, si ha $ac\equiv bc \bmod n$, e quelli della seconda per b, $bc\equiv bd \bmod n$. Per la proprietà transitiva delle relazioni di equivalenza segue allora $ac\equiv bd \bmod n$, come si voleva.

Esempi. 1. Determiniamo il resto della divisione per 2 di 7235. Scriviamo $7215=7\cdot 10^3+2\cdot 10^2+1\cdot 10+5$, e consideriamo i resti degli addendi della divisione per 2; essi sono tutti 0, meno l'ultimo che è 1:

$$7\cdot 10^3\equiv 0 \bmod 2,\ 2\cdot 10^2\equiv 0 \bmod 2,\ 3\cdot 10\equiv 0 \bmod 2,\ 5\equiv 1 \bmod 2.$$

Per quanto visto sopra, la somma dei primi membri, che è il numero dato 7215, è congrua a 1 modulo 2; in altre parole, il numero dato diviso per 2 dà resto 1. Analogamente, il numero dato diviso per 5 dà resto 0.

2. Determiniamo il resto della divisione per 4 di 7215. Proseguendo come prima, poiché 10^3 e 10^2 divisi per 4 danno resto zero, rimangono solo i resti di $3\cdot 10$ e di 5, cioè 2 e 1; il resto cercato è quindi 3. In generale, un numero scritto in base 10:

$$m=a_k10^k+a_{k-1}10^{k-1}+\cdots+a_210^2+a_110^1+a_0 \tag{5}$$

il resto della divisione di m per 2 è uguale al resto della divisione di a_0 per 2 (in altre parole, un numero dà resto 0 o 1 quando è diviso per 2, cioè è pari o dispari, se è pari o dispari la sua ultima cifra. Il resto della divisione di m per 4 è lo stesso di quello della divisione di $a_110^1+a_0$ per 4, ecc.

3. Qualunque potenza di 10 divisa per 3 dà resto 1, e dunque il resto della divisione di m della (5) per 3 è lo stesso di quello della divisione della somma delle cifre $a_k+a_{k-1}+\cdots+a_0$ per 3. Se il numero m è divisibile per 3, cioè il resto della divisione per 3 è zero, allora la somma delle cifre di m

deve essere un multiplo di 3, e viceversa. Quindi, un numero è divisibile per 3 se e solo se lo è la somma delle sue cifre.

4. Anche qualunque potenza di 10 divisa per 9 dà resto 1, e dunque il resto della divisione di m della (5) per 9 è lo stesso di quello della divisione della somma delle cifre. Su questo fatto si basa la prova del 9: il risultato di una moltiplicazione $a \times b = c$ si può controllare verificando se la somma delle cifre di a moltiplicata per la somma delle cifre di b è congrua, modulo 9, alla somma delle cifre di c. Se il risultato della prova è negativo, l'operazione è sbagliata; ma se è positivo, non è detto che sia giusta: lo è a meno di multipli di 9. Ad esempio, $13 \times 43 = 559$ (operazione giusta), la somma delle cifre è $4 \times 7 \equiv 19$, da cui $28 \equiv 10$, e $10 \equiv 1 \bmod 9$, che è vero. Ma anche per $13 \times 43 = 586$ la prova del 9 dà un risultato positivo (i due risultati differiscono per 27, che è un multiplo di 9). In altri termini, la prova positiva dice che il risultato è giusto a meno di multipli di 9.

5. Osserviamo che $10 \equiv -1 \bmod 11$, e dunque per una potenza di 10, $10^k \equiv (-1)^k \bmod 11$. Ne segue che modulo 11 la (5) diventa $(-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots + (-1)a_1 + a_0$. Le potenze pari di –1 danno 1, quelle dispari –1, e dunque:

$$m \equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) \bmod 11$$

ovvero: il resto della divisione di m per 11 è lo stesso che si ottiene dividendo per 11 la differenza tra la somma delle cifre di posto pari e quella delle cifre di posto dispari, cominciando da destra. In particolare, un numero è divisibile per 11 se questa differenza è un multiplo di 11.

6. Teorema cinese dei resti.

Ci poniamo ora il seguente problema: date due coppie di interi m, n e a, b, esiste un intero c che diviso per m dà resto a, e diviso per n dà resto b? In altre parole, esiste una soluzione comune delle due congruenze $x \equiv a \bmod m$ e $x \equiv b \bmod n$? Non sempre. Ad esempio, con $m = 4, n = 6, a = 1, b = 2$, se $c \equiv 1 \bmod 4$ e $c \equiv 2 \bmod 6$ si avrebbe $c = 4q_1 + 1$, un numero dispari, e $c = 4q_2 + 2$, un numero pari. Con $a = 2, b = 4$ si ha la soluzione $c = 10$: $10 = 4 \cdot 2 + 2$, e $10 = 1 \cdot 6 + 4$. L'esistenza o meno di una soluzione dipende quindi dalla scelta di a e b. In quale caso esiste una soluzione qualunque siano a e b?

Teorema 11. *Se $(m, n) = 1$, una soluzione delle congruenze*

$$x \equiv a \bmod m$$

$$x \equiv b \bmod n$$

esiste qualunque siano a e b, ed è unica modulo il prodotto mn.

Dim. Il risultato è una conseguenza dell'identità di Bézout. Poiché $(m, n) = 1$, esistono due interi h e k tali che $hm + kn = 1$. Allora $c = bhm + akn$ è una soluzione. Infatti,

$$c \equiv a \cdot kn \equiv a \cdot 1 \equiv a \bmod m, \quad \text{e} \quad c \equiv b \cdot hm \equiv b \cdot 1 \equiv b \bmod m.$$

Riguardo all'unicità, se c_1 è un'altra soluzione, allora $c_1 \equiv c \bmod m$ e mod$n$, e pertanto m ed n dividono $c_1 - c$, ed essendo $(m, n) = 1$ anche mn divide $c_1 - c$ (Teorema 5, *ii*)), e dunque $c_1 \equiv c \bmod mn$. In altri termini, esiste ed è unica una soluzione c dove $0 \leq c < mn$. □

Nota. Come mostrano gli esempi visti prima del teorema, la condizione che i moduli siano relativamente primi a due a due non è necessaria per l'esistenza di una soluzione delle congruenze. Si tratta solo di una condizione sufficiente.

Corollario. *Se $m_1, m_2, \ldots, m_n$ sono n interi a due a due relativamente primi ($(m_i, m_j) = 1, i \neq j$), allora il sistema di congruenze:*

$$\begin{aligned} x &\equiv a_1 \bmod m_1, \\ x &\equiv a_2 \bmod m_2, \\ &\vdots \\ x &\equiv a_{n-1} \bmod m_{n-1} \\ x &\equiv a_n \bmod m_n \end{aligned} \tag{6}$$

ammette soluzioni qualunque siano gli interi $a_1, a_2, \ldots, a_n$. La soluzione è unica modulo il prodotto $m_1 m_2 \cdots m_n$.

Dim. Induzione su n. Se $n = 1$ basta prendere $x = a_1$. Supponiamo allora il teorema vero per $n - 1$ congruenze (ad esempio, le prime $n - 1$). Esiste allora una soluzione $x \equiv c \bmod m'$, dove $m' = m_1 m_2 \cdots m_{n-1}$, e siamo così ridotti al caso di due congruenze:

$$x \equiv c \bmod m', \quad x \equiv a_n \bmod m_n,$$

le quali, essendo $(m', m_n) = 1$, ci rimandano al Teorema 11. □

Nel IV sec EV il cinese Sun Tsu Suan–Ching pose il teorema seguente: dato un certo numero di oggetti, se disposti a gruppi di 3 ne restano 2, se

disposti a gruppi di 5 ne restano 3, e se disposti a gruppi di 7 ne restano 2. Quanti sono gli oggetti? Si tratta di risolvere il sistema di congruenze:

$$\begin{aligned} x &\equiv 2 \bmod 3, \\ x &\equiv 3 \bmod 5, \\ x &\equiv 2 \bmod 7. \end{aligned}$$

Da (3,5)=1 abbiamo $1 = 2\cdot 5 - 3\cdot 3$, per cui $5\cdot 2\cdot 5 - 3\cdot 3\cdot 3 = 23 \equiv 8 \bmod 15$ risolve le prime due. Restiamo allora con:

$$\begin{aligned} x &\equiv 8 \bmod 15, \\ x &\equiv 2 \bmod 7. \end{aligned}$$

Con $1 = 1\cdot 15 - 2\cdot 7$ abbiamo la soluzione $2\cdot 15 - 8\cdot 2\cdot 7 = 30 - 112 = -82$. Se vogliamo una soluzione non negativa aggiungiamo 105: otteniamo 23, che è anche l'unica non negativa e minore del prodotto dei moduli $15 \cdot 7 = 105$.

Un altro modo di enunciare il teorema cinese è il seguente: un sistema di congruenze nel quale i moduli sono relativamente primi è equivalente a una sola congruenza. Infatti, se il sistema ha una soluzione, e sia a, allora il sistema è equivalente alla sola congruenza $x \equiv a \bmod m$, dove m è il prodotto dei moduli.

Ci chiediamo ora: dati due interi a ed m, qual è la probabilità che un numero scelto a caso sia congruo ad a modulo m? Poiché le classi resto modulo m sono in numero di m, la probabilità che il numero appartenga alla stessa classe di a è $1/m$.

Siano ora $m_1, m_2, \ldots, m_n$ interi a due a due primi tra loro. Il teorema cinese afferma, come visto sopra, che un sistema di congruenze nel quale i moduli sono relativamente primi è equivalente a una sola congruenza:

$$x \equiv a \bmod m \tag{7}$$

dove m è il prodotto dei moduli m_i. Per quanto detto, la (7) ha probabilità $1/m$ di verificarsi; ma

$$\frac{1}{m} = \frac{1}{m_1} \cdot \frac{1}{m_2} \cdots \frac{1}{m_n}$$

In altri termini, la probabilità del verificarsi simultaneo delle (6), cioè la probabilità del verificarsi della (7), è il prodotto delle probabilità del verificarsi di ciascuna di esse. Se ne conclude che *le congruenze i cui moduli sono a due a due relativamente primi sono statisticamente indipendenti.*