

ALGEBRA DELLE CLASSI DI RESTO 1

dalle classi di resto al teorema cinese e ai sistemi di congruenze lineari

di Leonardo Calconi

Publicato il 15/05/2007

Che cos'è una classe di resto ?

E' l'insieme di quei numeri interi che danno lo stesso resto se divisi per uno stesso intero.

{..., -7, -5, -3, 1, 3, 5, 7,...} formano una classe di resto [1] perchè divisi per 2 danno lo stesso resto 1.

L'argomento è intrigante: utilizzare classi di resto anzichè numeri nelle operazioni.

Le applicazioni pratiche sono di grande interesse: basti pensare che attualmente (e almeno fin quando i computer quantistici non saranno realtà), l'esistenza delle transazioni commerciali e bancarie via Internet è resa possibile grazie alle cifrature basate sull'algebra delle classi di resto.

Ho iniziato con alcune premesse sulle definizioni fondamentali, e perchè rimanessero brevi e compatte ne ho tralasciato le dimostrazioni che non sono funzionali agli scopi di questo lavoro.

Ho proseguito dalla definizione di classe di resto fino ai sistemi di congruenze lineari, cercando di dimostrare tutto ed inserendo un buon numero di esempi di calcolo pratico.

Ho tralasciato la matematica ricreativa, argomenti molto popolari quali la prova del nove e i criteri di divisibilità, ed altri interessanti come la RSA sui quali è stato scritto molto e molto meglio di quanto potrei fare io.

1 Premesse

pagg.2-3

- 1.1 Relazione
- 1.2 Relazione di equivalenza
- 1.3 Relazione di uguaglianza
- 1.4 Classe di equivalenza
- 1.5 Partizione
- 1.6 Combinazione lineare
- 1.7 Identità di Bezout
- 1.8 Algoritmo di Euclide e MCD
- 1.9 Equazione diofantea

2 Classi di resto

pagg.4-9

- 2.1 Relazione di congruenza modulo n
- 2.2 Proprietà delle relazioni di congruenza
- 2.3 Classe di resto
- 2.4 Anello delle classi di resto
- 2.5 Dominio d'integrità delle classi di resto
- 2.6 Campo delle classi di resto ed inversi
- 2.7 Calcolo degli inversi nell'anello delle classi di resto
 - 2.7.1 Teorema di Lagrange
 - 2.7.2 Corollario del Teorema di Lagrange
 - 2.7.3 Teorema di Eulero
 - 2.7.4 Piccolo Teorema di Fermat
- 2.8 Calcolo degli inversi nel campo delle classi di resto
- 2.9 Inversi banali

3 Congruenze lineari

pagg. 10-13

- 3.1 Equazione diofantea
- 3.2 Definizione di congruenza lineare
- 3.3 Compatibilità, soluzioni fondamentali e classi di congruenza
- 3.4 Forma delle soluzioni
- 3.5 Soluzioni non congruenti e congruenti; calcolo
- 3.6 Riduzione del modulo

4 Sistemi di congruenze lineari

pagg. 14-18

- 4.1 Teorema cinese del resto
 - 4.1.1 Compatibilità
 - 4.1.2 Soluzioni
- 4.2 Sistemi di congruenze lineari ad una incognita

1 PREMESSE

1.1 Relazione

Descritta in modo *informale* una relazione è una legge che associa un elemento di un insieme ad un elemento di un altro insieme, oppure che associa uno ad uno gli elementi di uno stesso insieme.

Descritta in modo *formale* una relazione \underline{r} è un'applicazione $\underline{r}: A \rightarrow B$, ovvero un sottoinsieme del prodotto cartesiano $A \times B$. Se $A = B = \mathbb{Z}$ l'applicazione è $\underline{r}: \mathbb{Z} \rightarrow \mathbb{Z}$ ed è definita in \mathbb{Z} stesso.

1.2 Relazione di equivalenza

È una relazione \underline{r} definita nell'insieme A per la quale valgono le proprietà *riflessiva*, *simmetrica* e *transitiva*:

$a \underline{r} b, a, b \in A$ se

- $a \underline{r} a$
- $a \underline{r} b \Rightarrow b \underline{r} a$
- $a \underline{r} b, b \underline{r} c \Rightarrow a \underline{r} c$

► Esempi

\underline{r} = similitudine, A = insieme dei triangoli nel piano

\underline{r} = parallelismo, A = insieme dei piani nello spazio

► Contro-esempi

\underline{r} = normalità, A = insieme dei piani nello spazio \rightarrow 1 e 3 non sono verificate

\underline{r} = essere multiplo di, $A = \mathbb{N} \rightarrow$ 2 non è verificata

1.3 Relazione di uguaglianza

È una relazione di equivalenza cui viene applicata la proprietà restrittiva *antisimmetrica*:

- $a \underline{r} b, b \underline{r} a \Leftrightarrow a = b$

► Esempio

\underline{r} = dividere

$A = \mathbb{Z}$

Come è evidente, questo e qualunque altro esempio si voglia portare è tautologico.

Si può discutere sul fatto che la relazione di uguaglianza sia un caso particolare delle relazione di equivalenza oppure che quest'ultima sia una generalizzazione della relazione di uguaglianza.

1.4 Classe di equivalenza modulo \underline{r}

Tutti gli elementi di A per i quali vale \underline{r} rispetto ad a

$[a] = \{b \in A / b \underline{r} a\}$

► Esempio

\underline{r} = coordinate $\leq q$

A = insieme dei punti dello spazio

$[a]$ = sfera di raggio q .

Naturalmente le classi di equivalenza modulo \underline{r} possono essere più d'una, come mostrato nel paragrafo seguente.

1.5 Partizione

È l'insieme $[A]$ delle parti di A che verifica le proprietà:

- $[A] = A$
- $A_m \cap A_n = \emptyset$
- $A_m \cap A_n \neq \emptyset \Leftrightarrow A_m = A_n$

Quindi una partizione esaurisce l'insieme al quale si riferisce.

► **Esempio**

r = dare resto m nella divisione per n intero

$$A = \mathbb{Z}$$

$$[A] = [a_0] \cup [a_1] \cup [a_2] \cup \dots \cup [a_{n-1}]$$

1.6 Combinazione lineare

In \mathbb{Z} è definita tale una scrittura come $bx + cy$. Per essa se $a | b, a | c \Rightarrow a | (ax + by)$.

1.7 Identità di Bezout

E' una scrittura del MCD. In \mathbb{Z} se $d = (a, b) \Rightarrow d = ha + kb$ per h, k opportuni.

La coppia di valori (h, k) non è unica in quanto per ogni $i \in \mathbb{Z}$ si ha $d = a(h + ib) - b(k + ia)$.

► **Esempio:** $(77, 99) = 11 = 77 \cdot 4 - 99 \cdot 3 = 77(4 + 567 \cdot 99) - 99(3 + 567 \cdot 77)$

In base all'identità risulta che se $a | c, b | c, (a, b) = d$ allora $ab | cd$.

1.8 Algoritmo di Euclide e MCD

Per $a, b \in \mathbb{Z}$ e, senza inficiare la validità del procedimento con $a > b$, ecco come calcolare il MCD e una coppia di valori per l'identità di Bezout col metodo delle divisioni successive:

► **Esempio:** $(758, 242) = 2 = 758 \cdot 53 - 242 \cdot 166$:

$a = bq_1 + r_1$	$758 = 242 \cdot 3 + 32$	$2 = 14 - 4 \cdot 3, 4 = 18 - 14 \cdot 1 \Rightarrow$
$b = r_1q_2 + r_2$	$242 = 32 \cdot 7 + 18$	$2 = 14 - (18 - 14) \cdot 3 = 14 \cdot 4 - 18 \cdot 3, 14 = 32 - 18 \cdot 1 \Rightarrow$
$r_1 = r_2q_3 + r_3$	$32 = 18 \cdot 1 + 14$	$2 = (32 - 18) \cdot 4 - 18 \cdot 3 = 32 \cdot 4 - 18 \cdot 7, 18 = 242 - 32 \cdot 7 \Rightarrow$
$r_{n-2} = r_{n-1}q_n + r_n$	$18 = 14 \cdot 1 + 4$	$2 = 32 \cdot 4 - (242 - 32 \cdot 7) \cdot 7 = 32 \cdot 53 - 242 \cdot 7, 32 = 758 - 242 \cdot 3 \Rightarrow$
$r_{n-1} = r_nq_n + 1$	$14 = 4 \cdot 3 + 2$	$2 = (758 - 242 \cdot 3) \cdot 53 - 242 \cdot 7 \Rightarrow$
	$4 = 2 \cdot 2 + 0$	$2 = 758 \cdot 53 + (-166) \cdot 242$

► **Esempio:** $(726, 275) = 11 = 726 \cdot 11 - 275 \cdot 29$:

$726 = 275 \cdot 2 + 176$	$11 = 77 - 22 \cdot 3 = 77 - (99 - 77) \cdot 3 \Rightarrow 77 - 99 \cdot 3 + 77 \cdot 3 \Rightarrow 77 \cdot 4 - 99 \cdot 3$
$275 = 176 \cdot 1 + 99$	$11 = (176 - 99) \cdot 4 - 99 \cdot 3 \Rightarrow 176 \cdot 4 - 99 \cdot 4 - 99 \cdot 3 = 176 \cdot 4 - 99 \cdot 7$
$176 = 99 \cdot 1 + 77$	$11 = 176 \cdot 4 - (275 - 176) \cdot 7 \Rightarrow 176 \cdot 11 - 275 \cdot 7$
$99 = 77 \cdot 1 + 22$	$11 = (726 - 275 \cdot 2) \cdot 11 - 275 \cdot 7 \Rightarrow 726 \cdot 11 - 275 \cdot 22 - 275 \cdot 7 \Rightarrow 11 \cdot 726 - 29 \cdot 275$
$77 = 22 \cdot 3 + 11$	$11 = 11 \cdot 726 + (-29) \cdot 275$
$22 = 11 \cdot 2 + 0$	

Notare come l'identità di Bezout sia stata scritta e in forma *canonica* $ha + kb$ e in forma *non canonica* $ha - kb$, forma che ritroveremo nell'equazione diofantea.

1.9 Equazione diofantea.

In generale è un'equazione di grado g in k incognite a coefficienti interi della quale si cercano soluzioni intere.

Per esempio, l'equazione (di Pitagora !) $x^2 + y^2 = z^2$ è un'equazione di Diofanto...

Un tipo particolare di equazione diofantea che interessa questo lavoro è quella lineare in due incognite, ovvero l'identità di Bezout:

► $ax + ny = b$

La ricerca di una coppia di valori per l'identità di Bezout equivale alla ricerca di una soluzione per l'equazione diofantea corrispondente.

L'argomento è di importanza fondamentale e sarà sviluppato nel capitolo 3.■

2 CLASSI DI RESTO

2.1 Relazione di congruenza modulo n

Se $n \in \mathbb{N}$ si definisce “di congruenza modulo n ” una relazione su \mathbb{Z} tale che:

$$\blacktriangleright a \equiv b \pmod{n} \Leftrightarrow a - b = nq, \Rightarrow \frac{a - b}{n} = q, q \in \mathbb{Z}$$

ovvero tale che a e b divisi per n danno lo stesso resto r

$$\blacktriangleright a \pmod{n} = b \pmod{n} = r$$

2.2 Proprietà delle relazioni di congruenza

In linea generale le proprietà seguenti non sono invertibili.

Ad esempio, per la 2, se $a + c \equiv b + c \pmod{n}$ non è necessariamente vero che $a \equiv b \pmod{n}$.

Ancora, per la 10, se $ac \equiv bc \pmod{n}$ non è necessariamente vero che $a \equiv b \pmod{n}$.

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

1. $a^c \equiv b^c \pmod{n}$
2. $a + c \equiv b + c \pmod{n}$
3. $ac \equiv bc \pmod{n}$

Se $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$

4. $a + c \equiv b + d \pmod{n}$
5. $ac \equiv bd \pmod{n}$

Se $a \equiv b \pmod{n}$, $d \mid n$

6. $a \equiv b \pmod{d}$

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

7. $a \equiv b \pmod{[n, m]}$

Se n è primo

8. $(a + b)^n \equiv (a^n + b^n) \pmod{n}$

Se $ac \equiv bc \pmod{n}$, $d = (c, n)$ prima proprietà di cancellazione del prodotto

9. $a \equiv b \pmod{n/d}$

Se $ac \equiv bc \pmod{n}$, $(c, n) = 1$ seconda proprietà di cancellazione del prodotto

10. $a \equiv b \pmod{n}$

2.3 Classe di resto

La relazione di congruenza ci permette di definire una classe di resto $[r]$ modulo n come insieme degli interi che danno lo stesso resto r se divisi per n , ovvero che

$$\blacktriangleright b \pmod{n} = r$$

Pertanto avremo che $\{b, n \in \mathbb{Z} : b \pmod{n} = r\} = [r]$

Tale relazione è una relazione di equivalenza che gode quindi delle tre proprietà:

1. $a \equiv a \pmod{n}$ riflessiva
2. $b \equiv a \pmod{n}$ simmetrica

3. $a \equiv b \pmod{n}$, $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ transitiva

Una relazione di congruenza modulo n determina la partizione di \mathbb{Z} in n classi di resto che lo esauriscono. La compilazione delle classi di resto è elementare partendo dalla classe $[0]$ o dalla colonna dei primi elementi.

<p>► Esempio con modulo $n = 3$</p> <p>$[0] = [\dots, -9, -6, -3, 0, 3, 6, 9, \dots]$ $[1] = [\dots, -8, -5, -2, 1, 4, 7, 10, \dots]$ $[2] = [\dots, -7, -4, -1, 2, 5, 8, 11, \dots]$</p> <p>► Esempio con modulo $n = 4$</p> <p>$[0] = [\dots, -12, -8, -4, 0, 4, 8, 12, \dots]$ $[1] = [\dots, -11, -7, -3, 1, 5, 9, 13, \dots]$ $[2] = [\dots, -10, -6, -2, 2, 6, 10, 14, \dots]$ $[3] = [\dots, -9, -5, -1, 3, 7, 11, 15, \dots]$</p>	<p>► Esempio con modulo $n = 5$</p> <p>$[0] = [\dots, -15, -10, -5, 0, 5, 10, 15, \dots]$ $[1] = [\dots, -14, -9, -4, 1, 6, 11, 16, \dots]$ $[2] = [\dots, -13, -8, -3, 2, 7, 12, 17, \dots]$ $[3] = [\dots, -12, -7, -2, 3, 8, 13, 18, \dots]$ $[4] = [\dots, -11, -6, -1, 4, 9, 14, 19, \dots]$</p>
---	--

L'insieme quoziente \mathbb{Z}_n delle classi di resto $[0], \dots, [n-1]$ modulo n gode di diverse proprietà.

2.4 Anello delle classi di resto

Le proprietà di \mathbb{Z}_n sono quelle di un anello commutativo con unità:

- Chiusura rispetto all'addizione e alla moltiplicazione
- Esistenza dell'elemento neutro rispetto all'addizione e alla moltiplicazione
- Esistenza dell'elemento opposto rispetto all'addizione
- Associatività rispetto all'addizione e alla moltiplicazione
- Distributività rispetto all'addizione e alla moltiplicazione
- Commutatività rispetto all'addizione e alla moltiplicazione

Verifichiamo queste proprietà nelle tabelle seguenti:

$n = 3$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

•	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$n = 4$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

•	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

$n = 5$

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

•	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Osservando queste tabelle si intuisce che insiemi \mathbb{Z}_n diversi possono non godere delle stesse proprietà e pertanto conviene dotarci di un paio di definizioni in più.

2.5 Dominio d'integrità delle classi di resto

E' dominio d'integrità I un anello commutativo che non abbia divisori dello zero:

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ o } b = 0, a, b \in I$$

Dalle tabelle moltiplicative si vede immediatamente che \mathbb{Z}_4 non è un dominio d'integrità:

$$[2] \cdot [2] = [0] \Rightarrow \frac{[0]}{[2]} = [2]$$

mentre lo sono \mathbb{Z}_3 e \mathbb{Z}_5 .

► **Contro Esempio** \mathbb{Z}_8

•	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Gli elementi di \mathbb{Z}_n si calcolano riga/colonna semplicemente così:

$$[r_{r,c}] = [r_r r_c \pmod n]$$

Riassumendo:

- ✓ \mathbb{Z}_n è dominio d'integrità se n è un numero primo.
- ✓ se n non è primo, saranno divisori dello zero tutti gli elementi di \mathbb{Z}_n tali che $(r, n) \neq 1$

Notiamo infine come essendo $\circ(I) = n$ \mathbf{I} sia finito, e poichè un dominio d'integrità finito è un campo arriviamo agevolmente a parlare di inversi.

Per dimostrare ciò è necessario provare l'esistenza dell'elemento neutro moltiplicativo (l'unità) e l'esistenza degli inversi per tutti gli elementi di \mathbf{I} .

Ecco una bella dimostrazione di *I.N. Herstein*.

Principio dei cassetti.

Se n oggetti devono essere distribuiti in m cassetti e il numero degli oggetti è maggiore di quello dei cassetti, allora uno o più cassetti conterranno due o più oggetti. Chiaramente, se $n = m$ ogni cassetto contiene esattamente un oggetto.

Prova dell'esistenza dell'elemento neutro.

Se \mathbf{I} è finito avrà un certo numero di elementi x_1, x_2, \dots, x_n e se $a \neq 0$ è uno di questi, anche gli elementi $x_1 a, x_2 a, \dots, x_n a$ appartengono ad \mathbf{I} e sono in numero di n .

Se essi sono tutti distinti, per il principio dei cassetti sono tutti gli elementi di \mathbf{I} .

Ma essi sono tutti distinti.

Se infatti fosse $x_i a = x_j a$ per $i \neq j$ allora sarebbe $(x_i - x_j) a = 0$, ed essendo \mathbf{I} dominio d'integrità dovrebbe necessariamente essere $(x_i - x_j) = 0 \Rightarrow x_i = x_j$ contro l'ipotesi $i \neq j$.

Allora $x_1 a, x_2 a, \dots, x_n a$ sono tutti gli elementi di \mathbf{I} che possono essere scritti in tale maniera.

Quindi a stesso può essere scritto in modo analogo, ovvero $a = x_{i_0} a = a x_{i_0}$.

Ora, se $y = x_i a$ è un elemento di \mathbf{I} sarà $y x_{i_0} = (x_i a) x_{i_0} = x_i (a x_{i_0}) = x_i a = y$.

Ma questa è proprio la scrittura secondo la quale $x_{i_0} = 1$ è l'elemento neutro moltiplicativo di \mathbf{I} .

Prova dell'esistenza degli inversi.

Semplicemente, possiamo scrivere l'elemento neutro come multiplo di a come abbiamo fatto in precedenza, $1 = b a$, il che dimostra che b è l'inverso di a e viceversa. E poichè a è un elemento qualsiasi di \mathbf{I} tutti i suoi elementi hanno l'inverso e quindi \mathbf{I} è un campo.

2.6 Campo delle classi di resto e inversi

Se il modulo n è un numero primo, ogni elemento diverso da zero ammette l'inverso ed un anello commutativo con unità con questa proprietà è un campo.

Dato $[a] \in \mathbb{Z}_n$ se $(a, n) = 1$ esiste $[a_i] \in \mathbb{Z}_n : [a][a_i] = [1]$ ovvero è $aa_i \equiv 1 \pmod{n}$.

Ciò significa che $aa_i - 1 = kn \Rightarrow aa_i - kn = 1$, e quest'ultima è un'equazione diofantea che, data l'ipotesi, ammette soluzioni in \mathbb{Z}_n , delle quali una è senz'altro $\langle a_i, k \rangle$.

L'inverso di $[0]$ non esiste in quanto $(0, n) = n \neq 1$.

L'esistenza degli inversi conferma l'assenza di divisori dello zero.

Infatti, dati $[a], [b] \neq 0$ se fosse vero che $[a][b] = 0$ potremmo scrivere

$[a_i][a][b] = [a_i][0] \Rightarrow [b] = [a_i][0] \Rightarrow [b] = [0]$ il che va contro l'ipotesi.

Concludiamo sottolineando che se la primalità di n garantisce l'esistenza degli inversi di tutti gli elementi della classe di resti, non è vero che se n non è primo tali inversi non esistono del tutto.

Se \mathbb{Z}_n non è un campo essi esisteranno solo per quegli elementi dell'anello che non sono divisori dello zero.

Ma come si calcola un inverso ?

2.7 Calcolo degli inversi nell'anello \mathbb{Z}_n delle classi di resto modulo n

Se il modulo n della classe di resti non è primo, possiamo calcolare gli inversi solo di quegli elementi che con n sono primi: $aa_i \equiv 1 \pmod{n} \Leftrightarrow (a, n) = 1$

Se $aa_i \equiv 1 \pmod{n}$ allora esiste un k intero per cui $aa_i = 1 + kn$. Di qui $(a, n) \mid 1 \Rightarrow (a, n) = 1$

Del resto se $(a, n) = 1$ si può scrivere l'identità di Bezout $aa_i + ny = 1$, $a_i, y \in \mathbb{Z}$ e da questa la congruenza $aa_i \equiv 1 \pmod{n}$ per la quale a_i è l'inverso di a .

Quindi in generale possiamo ridurre il problema del calcolo di un inverso alla ricerca della soluzione $\langle a_i, y \rangle$ dell'equazione diofantea

$$aa_i + ny = 1$$

ottenuta scrivendo l'identità di Bezout .

Come visto nelle *Premesse*, tale soluzione può essere ricavata con l'algoritmo di Euclide per divisioni successive, ottenendo una coppia di valori che non è unica e appartenendo tutte le a_i delle coppie di valori alla classe di resto inversa che è pertanto univocamente determinata.

► **Esempio:** in $\mathbb{Z}_{16} : 117 \equiv 5 \pmod{16}$

Con l'algoritmo di Euclide troviamo immediatamente la coppia

$$(a_{i_0} = 13, y_0 = -95)$$

come soluzione della diofantea

$$117a_i + 16y = 1 \Rightarrow 117 \cdot 13 - 16 \cdot 95 = 1$$

Quindi 13 è l'inverso di 117 $\Rightarrow 117 \cdot 13 \equiv 1 \pmod{16}$

Ma anche (29, -212) è soluzione così come sono soluzioni tutte le coppie

$$a_{ik} = 13 + 16k, y_k = -95 - 117k, k \in \mathbb{N}$$

e poichè tutte le $a_{ik} \in [13]$, questo è l'elemento inverso di $[5] \Rightarrow [5] \cdot [13] = [1]$

Un metodo di calcolo elegante, benchè valido solo per n primo, è il *piccolo teorema di Fermat* per arrivare al quale occorre una catena di teoremi T :

T . di Lagrange \rightarrow Corollario del T . di Lagrange \rightarrow T . di Eulero \rightarrow Piccolo T . di Fermat

2.7.1 Teorema di Lagrange

Se \mathcal{G}' è un sottogruppo di \mathcal{G} di ordine finito, allora $\circ(\mathcal{G}') \mid \circ(\mathcal{G})$.

Dati \mathcal{G} di ordine n finito e il suo sottogruppo $\mathcal{G}' \neq \mathcal{G}$ di ordine m con elementi z_1, z_2, \dots, z_m , per un elemento $a_1 \in \mathcal{G}, a_1 \notin \mathcal{G}'$ possiamo sicuramente costruire almeno due laterali destri di \mathcal{G}' in \mathcal{G} :

$$z_1 e, z_2 e, \dots, z_m e = z_1, z_2, \dots, z_m$$

$$z_1 a_1, z_2 a_1, \dots, z_m a_1$$

Tutti gli elementi dei due laterali sono distinti e se essi esauriscono \mathcal{G} allora $\circ(\mathcal{G}) = 2 \circ(\mathcal{G}')$ ed il teorema è dimostrato.

Se così non è possiamo iterare il procedimento sino ad che \mathcal{G} non sia esaurito (è un gruppo di ordine finito) il che avverrà per il suo k -esimo elemento a_k .

A questo punto si ha che $\circ(\mathcal{G}) = k \circ(\mathcal{G}')$ e quindi $\circ(\mathcal{G}') \mid \circ(\mathcal{G})$.

2.7.2 Corollario del teorema di Lagrange

Se \mathcal{G} è di ordine finito e $a \in \mathcal{G}$ allora $\circ(a) \mid \circ(\mathcal{G})$.

La dimostrazione è immediata considerando un sottogruppo ciclico \mathcal{G}' di \mathcal{G} generato da a il cui ordine è $\circ(a)$. Pertanto poichè $\circ(\mathcal{G}') \mid \circ(\mathcal{G})$ segue che $\circ(a) \mid \circ(\mathcal{G})$.

2.7.3 Teorema di Eulero

Se $(a, n) = 1$ allora è $a^{\varphi(n)} \equiv 1 \pmod{n}$

Ricordiamo che la funzione di Eulero $\varphi(n)$ è una funzione moltiplicativa che esprime il numero di interi minori di n e con esso relativamente primi.

Per il teorema di Lagrange se a è primo con n allora appartiene al gruppo moltiplicativo Z_n che ha ordine $\varphi(n)$. Per il corollario del teorema di Lagrange l'ordine di a è allora un divisore di $\varphi(n)$ e quindi $a^{\circ(a)} \equiv 1 \pmod{n} \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$.

2.7.4 Piccolo teorema di Fermat

Se $n = p$ è primo si ha un caso particolare del teorema di Eulero per cui:

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

e se $(a, p) = 1$ si ha

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

Si dimostra per induzione.

Come quasi sempre in questo tipo di dimostrazione, per il primo elemento, $a = 0$, il risultato è ovvio. Allora supposto vero per a , dobbiamo dimostrare che è vero anche per l'elemento successivo $a + 1$. Notando che per la proprietà 8 $(a + 1)^p \equiv a^p + 1^p \pmod{p}$ e che $1^p \equiv 1 \pmod{p}$, si avrà che $(a + 1)^p \equiv (a + 1) \pmod{p}$ *cvd.*

Questo teorema di Fermat è detto *Piccolo* non perchè di scarsa importanza, ma per distinguerlo dal popolarissimo *Ultimo* che è il *Grande*.

2.8 Calcolo degli inversi nel campo \mathbb{Z}_p delle classi di resto modulo p

Il piccolo teorema di Fermat ci permette di calcolare gli inversi con p primo e $(a, p) = 1$:

- $a_i : aa_i \equiv 1 \pmod{p}$
- $[a_i] : [a][a_i] \in [1]$.

Infatti possiamo scrivere $a^{p-1} = aa^{p-2} \Rightarrow aa^{p-2} \equiv 1 \pmod{p}$ dove

- $a^{p-2} = a_i$ è l'inverso di $a \pmod{p}$
- $[a^{p-2}] = [a_i]$ è l'inverso di $[a] \pmod{p}$.

► **Esempio:** $7 \equiv 2 \pmod{5} \Rightarrow 7^3 \equiv 3 \pmod{5} \Rightarrow 8 \equiv 3 \pmod{5}$

Quindi $a = 7$, $a_i = 7^3 \Rightarrow a_i = 8 \Rightarrow 7 \cdot 8 \equiv 1 \pmod{5}$

$7^3, 8 \in [3]$, $[a] = 2$, $[a_i] = 3 \Rightarrow [2] \cdot [3] = [1]$

come risulta dalla tabella seguente

$[a] = [2]$	-12	-7	2	7	12	17	22
$[a_i] = [3]$	-13	-8	3	8	13	18	23
$[a][a_i] \in [1]$	-156	-56	6	56	156	306	506

► **Esempio:** $21 \equiv 4 \pmod{17} \Rightarrow 21^{15} \equiv 13 \pmod{17} \Rightarrow 13 \equiv 13 \pmod{17}$

Quindi $a = 21$, $a_i = 21^{15} \Rightarrow a_i = 13 \Rightarrow 21 \cdot 13 \equiv 1 \pmod{17}$

$21^{15}, 13 \in [13]$, $[a] = 4$, $[a_i] = 13 \Rightarrow [4] \cdot [13] = [1]$

Come si vede, nei due esempi il Teorema di Eulero conferma gli inversi trovati.

Ci sono dei dubbi ?

In ogni caso ricordiamo che dato un gruppo \mathcal{G} ed un suo sottogruppo \mathcal{G}' , se $a, b \in \mathcal{G}$ allora

$a \equiv b \pmod{\mathcal{G}'} \Leftrightarrow ab^{-1} \in \mathcal{G}'$. Nel secondo esempio se \mathcal{G} è il gruppo delle classi di resto modulo 17 e

\mathcal{G}' il sottogruppo classe di resto [1], sarà esattamente $aa^{-1} \equiv 1 \pmod{17} \Leftrightarrow [a][a^{-1}] \in [1]$.

Il fatto che possiamo calcolare gli inversi per tutti gli elementi diversi da zero dell'insieme quoziente delle p classi di resto modulo p prova che tale insieme è un campo.

2.9 Inversi banali

Capita che per alcuni \mathbb{Z}_n ci siano degli inversi banali, ovvero degli elementi che sono gli inversi di se stessi. Per rendersi praticamente conto della cosa basta osservare la tabella di \mathbb{Z}_8 .

Ma quando accade ciò ?

Ecco alcune evidenze:

- L'inverso è sempre banale quando $[a]^2 \equiv 1 \pmod{n}$
- [1] e [n-1] hanno sempre inversi banali
- Escludendo [1] e [n-1] \mathbb{Z}_n non ha inversi banali quando n è primo

All'indirizzo www.4dmatrix.it/math è disponibile un software gratuito per lo studio della distribuzione degli inversi banali.■

3 CONGRUENZE LINEARI

3.1 Equazione diofantea

L'equazione diofantea lineare in due incognite che interessa è la
 $ax + ny = b$

Se $(a, n) \mid b$ l'equazione è compatibile e una soluzione è data da

$$x_0 = \frac{kn}{d}, y_0 = -\frac{ka}{d}, k \in \mathbb{Z}, d = (a, n), \text{ mentre tutte le soluzioni sono date da}$$

$$x_j = x_0 + \frac{kn}{d}, y_j = y_0 - \frac{ka}{d} \text{ e se } d = 1 \text{ ovviamente da } x_j = x_0 + kn, y_j = y_0 - ka.$$

Dimostriamolo.

Se $(a, n) \mid b$ possiamo scrivere d come combinazione lineare di a e n , $d = ai_1 + bi_2$, e poichè b è multiplo di d , $b = md$, il tutto per $i_1, i_2, m \in \mathbb{Z}$ opportuni, potremo moltiplicare la combinazione lineare per m , $md = ai_1m + ai_2m = b$, e trovare così che $\langle x = i_1m, y = i_2m \rangle$ è una soluzione intera della diofantea.

Viceversa, se $\langle x, y \rangle$ è una soluzione intera della diofantea allora poichè $d \mid a$, $d \mid b$ sarà $d \mid ax + ny \Rightarrow d \mid b$.

Le coppie di valori $\langle x, y \rangle$ che sono soluzione dell'equazione lineare diofantea sono infinite.

Per rendersene conto basta pensare che, geometricamente, tale equazione rappresenta una retta.

► **Esempio:** $2x + 5y = 3$

$(2, 5) \mid 3$ quindi l'equazione ha soluzioni.

Una soluzione è $\langle -6, 3 \rangle$. Poichè $(2, 5) = 1$, tutte le altre soluzioni sono date da

$$x_j = -6 + k5, y_j = 3 - k2, \text{ per } k \text{ intero.}$$

► **Esempio:** $2x + 4y = 3$

Non ha soluzioni perchè $(2, 4) \nmid 3$

► **Esempio:** $364x + 124y = 8$

Calcoliamo $d = (364, 124)$ con l'algoritmo di Euclide:

$$364 = 124 \cdot 2 + 116$$

$$124 = 116 \cdot 1 + 8$$

$$116 = 8 \cdot 14 + 4$$

$$8 = 4 \cdot 2$$

$$d = 4 \mid 8$$

Una soluzione è $\langle -1, 3 \rangle$; tutte le soluzioni sono $x = -1 + \frac{k124}{4} = -1 + k31, y = 3 - \frac{k364}{4} = 3 - k91$

Il che dimostra che l'equazione data può essere ridotta alla forma $91x + 31y = 4 \Rightarrow (91, 31) = 1$.

Possiamo scrivere un'equazione diofantea anche in una forma *non canonica*, forma che verrà utile nel paragrafo successivo:

► **Esempio:** $2x - 5y = 3$

Se il criterio di compatibilità e il numero delle soluzioni non dipendono dal segno dei coefficienti, la forma ne dipende. Infatti, se una soluzione è $\langle -6, -3 \rangle$, tutte le soluzioni

sono $x_j = -6 + k5, y_j = -3 + k2$, per k intero.

3.2 Definizione di congruenza lineare

Una congruenza lineare è una relazione di congruenza in incognita x del tipo:

$$3.2.1 \quad ax \equiv b \pmod{n}$$

Le domande su tale congruenza lineare sono:

- Ammette soluzioni ?
- Se si, di che forma sono e quante sono ?
- Di esse, quante sono non congruenti tra di loro ?
- Come si calcolano ?

Iniziamo col dire che tali soluzioni, se esistono, sono anche soluzioni dell'equazione

$$3.2.2 \quad ax + ny = b$$

Infatti dalla relazione di congruenza 3.2.1 abbiamo che

$$3.2.3 \quad \frac{ax - b}{n} = y \Rightarrow ax - ny = b, \quad y \in \mathbb{Z}$$

Poichè delle soluzioni $\langle x_j, y_j \rangle$ di questa diofantea ci interessano solo i valori dell'incognita x , possiamo tranquillamente scrivere la 3.2.3 nella *forma canonica* 3.2.2 a prescindere dal segno di y .

3.3 Compatibilità, soluzioni fondamentali e classi di congruenza

Poichè per la congruenza lineare 3.2.1 si parla di soluzioni intere esse saranno, se esistono, anche soluzioni dell'equazione 3.2.2, la quale essendo a coefficienti interi e soluzioni intere abbiamo visto essere un'equazione diofantea lineare in due incognite x e y .

Quindi il criterio di compatibilità per la 3.2.1 è

$$3.3.1 \quad (a, n) \mid b \text{ o il caso particolare } (a, n) = 1$$

Prima di procedere esaminiamo alcune definizioni.

Soluzioni fondamentali di una congruenza lineare: tutte le soluzioni della congruenza lineare per x intero $< n$.

Classi di congruenza: sono individuate dalle soluzioni fondamentali e sono le classi di resto modulo n i cui elementi sono tutti soluzioni x della congruenza lineare. E poichè le classi di resto sono n , tale è il numero massimo di soluzioni fondamentali comprese tra 0 e $n-1$.

Soluzione unica: la classe di congruenza i cui elementi sono tutte e sole le soluzioni x della congruenza lineare.

d Soluzioni: le (a, n) classi di congruenza i cui elementi sono tutte e sole le soluzioni x della congruenza lineare.

Se il criterio di compatibilità è $(a, n) = 1$, la soluzione è unica, una sola classe di congruenza.

Se il criterio di compatibilità è $d = (a, n) \mid b$, le soluzioni sono in numero di d classi di congruenza comprese tra 0 e $n-1$.

► **Esempio con soluzione unica**: $3x \equiv 2 \pmod{4} \Rightarrow 3x + 4y = 2$

Poichè $(3, 4) = 1$, $1 \mid 2$ la soluzione sarà *unica modulo* $n = 4$. Infatti per l'equazione diofantea, con x intero da 0 a 3, solo per $x = 2$ si ha una soluzione intera per y e quindi la soluzione della congruenza lineare è la classe di resto [2] modulo 4, ovvero tutti gli elementi di questa classe: $\dots, -10, -6, -2, 2, 6, 10, \dots$

sono soluzioni della congruenza lineare e conseguentemente le soluzioni $\langle x, y \rangle$ della diofantea sono: $\langle \dots, \dots \rangle, \langle -10, 8 \rangle, \langle -6, 5 \rangle, \langle -2, 2 \rangle, \langle 2, -1 \rangle, \langle 6, -4 \rangle, \langle 10, -7 \rangle, \langle \dots, \dots \rangle$

► **Esempio senza soluzioni**: $2x \equiv 3 \pmod{4} \Rightarrow 2x + 4y = 3$

Applicando il criterio di compatibilità scopriamo che *non esistono soluzioni*; infatti si ha che $(2, 4) = 2 \nmid 3$.

► **Esempio con d soluzioni:** $6x \equiv 2 \pmod{4} \Rightarrow 6x + 4y = 2$

Qui abbiamo che $d = (6, 4) = 2$, $2 \mid 4$, quindi le soluzioni saranno in numero di due.

Calcoleremo le soluzioni di questo esempio nel paragrafo 3.5.

3.4 Forma delle soluzioni

Abbiamo affermato che ogni soluzione di una congruenza lineare che abbia soluzioni è soluzione dell'equazione diofantea corrispondente e quindi è del tipo:

$$3.4.1 \quad x_0 + \frac{kn}{d}$$

dove x_0 è una soluzione, $k \in \mathbb{Z}$ e $(a, n) \neq 1 = d$, $d \mid b$. Ora dobbiamo dimostrarlo.

Che 3.4.1 sia effettivamente una soluzione è evidente dal fatto che

$$a \left(x_0 + \frac{kn}{(a, n)} \right) = ax_0 \pm k[a, n] = b \pm mn$$

Ma tutte le altre soluzioni che forma hanno? La stessa? Sì, infatti date *due* soluzioni

$$\begin{cases} ax_1 = b + pn \\ ax_0 = b + qn \end{cases}$$

sottraendo e dividendo per d si avrà

$$\frac{a}{d}(x_1 - x_0) = (p - q)\frac{n}{d}$$

ovvero, dal momento che $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$ e che quindi $\frac{n}{d} \mid (x_1 - x_0)$:

$$x_1 = x_0 + \frac{kn}{d} \dots \text{et voilà!}$$

3.5 Soluzioni non congruenti e congruenti: calcolo

Continuiamo nel nostro percorso dimostrando che le soluzioni *non congruenti* modulo n tra loro sono in numero di $d = (a, n)$ e che quindi, come già detto, per $(a, n) = 1$ la soluzione è unica.

Secondo il risultato del paragrafo precedente e per $k_j = 0, 1, \dots, (d - 1)$ si dimostra che le sole soluzioni non congrue sono

$$x_0 + \frac{k_0 n}{d}, x_0 + \frac{k_1 n}{d}, x_0 + \frac{k_2 n}{d}, \dots, x_0 + \frac{k_{d-1} n}{d}$$

Supponiamo per assurdo di avere due soluzioni congruenti tra loro modulo n :

$$x_0 + \frac{k_1 n}{d} \equiv x_0 + \frac{k_2 n}{d} \pmod{n}, \quad k_1, k_2 \in \mathbb{Z} \quad 0 \leq k_1 < k_2 \leq d-1$$

Applicando la proprietà di cancellazione del prodotto con cambio di modulo si avrebbe

$$\frac{k_1 n}{d} \equiv \frac{k_2 n}{d} \pmod{n} \Rightarrow k_1 \equiv k_2 \pmod{\frac{n}{n/d}} \Rightarrow k_1 \equiv k_2 \pmod{d}$$

il che è appunto assurdo perchè $0 < k_2 - k_1 < d$.

Ora sappiamo *quante* sono le soluzioni non congruenti. Sappiamo anche *quali* sono ?

Sì, lo sappiamo. Sono esattamente i primi d interi positivi della classe di congruenza ridotta.

E le *soluzioni congruenti* ? Sono tutte le altre, infinite quindi, e ciascuna di esse è congruente ad una delle soluzioni di cui sopra.

► **Esempio:** $6x \equiv 2 \pmod{4} \Rightarrow 6x + 4y = 2$

Qui abbiamo che $d = (6, 4) = 2$, $2 \mid 4$, quindi le soluzioni non congruenti fra loro modulo 4 saranno in numero di due.

Poichè $x_0 = 1$ è una soluzione, l'altra sarà $x_0 + \frac{4}{2} = 3$; infatti $3 \not\equiv 1 \pmod{4}$, $1 \not\equiv 3 \pmod{4}$.

Le classi di congruenza modulo 4 saranno quindi:

$$[1] = \dots, -17, -13, -9, -5, -1, \mathbf{1}, 5, 9, 13, 17, \dots$$

$$[3] = \dots, -19, -15, -11, -7, -3, \mathbf{3}, 7, 11, 15, 19$$

Ora, ricordando la proprietà (9) secondo la quale se $ac \equiv bc \pmod{n}$, $d = (c, n)$ allora è $a \equiv b \pmod{n/d}$, calcoliamo la congruenza ridotta e la sua classe di congruenza:

$$3 \cdot 2 \equiv 1 \cdot 2 \pmod{\frac{4}{2}} \Rightarrow 3 \equiv 1 \pmod{2}$$

Allora le soluzioni non congruenti tra loro modulo 4 sono i primi $d = 2$ elementi positivi della classe di congruenza [1] modulo 2, ovvero: $\mathbf{1}, \mathbf{3}, 5, 7, \dots$

Tutti gli altri elementi sono congruenti modulo 4 con una delle soluzioni non congruenti.

► **Esempio:** $21x \equiv 6 \pmod{15} \Rightarrow 21x + 15y = 6$

$(21, 15) = 3$, $3 \mid 15$ quindi le soluzioni sono 3. Vedremo che sono [7], [12], [17].

Riduciamo la congruenza con cambio di modulo:

$$3 \cdot 7 \equiv 3 \cdot 2 \pmod{\frac{15}{3}} \Rightarrow 7x \equiv 2 \pmod{5}$$

La classe di congruenza è quindi [2] modulo 5 e le soluzioni non congruenti tra loro modulo 15 saranno $S = (7, 12, 17)$, ovvero i primi tre elementi positivi di questa classe.

Tutti gli altri elementi della classe di congruenza $\{[2] - S\}$ sono congrui modulo 15 con uno degli elementi di S : $37 \equiv 7 \pmod{15}$ ecc.

3.6 Riduzione del modulo

Se il modulo è un numero grande non primo esso può essere fattorizzato e la congruenza lineare può essere decomposta in un sistema di congruenze lineari modulo i fattori del modulo fattorizzato, sistema la cui soluzione sarà soluzione contemporanea di tutte le congruenze lineari che lo compongono e quindi della congruenza lineare originale.

$$3x \equiv 11 \pmod{2275} \Rightarrow 2275 = 5^2 \cdot 7 \cdot 13 \Rightarrow \begin{cases} 3x \equiv 11 \pmod{25} \\ 3x \equiv 11 \pmod{7} \\ 3x \equiv 11 \pmod{13} \end{cases}$$

La soluzione dei sistemi di congruenze lineari è argomento del prossimo capitolo. ■

4 SISTEMI DI CONGRUENZE LINEARI

Ci siamo posti il problema di trovare le soluzioni di una congruenza lineare, ovvero tutti quegli interi x che verificano una congruenza del tipo $ax \equiv b \pmod{n}$, e lo abbiamo risolto.

Ora potremmo chiederci se esistono degli interi x che verificano una *serie* di congruenze di questo tipo. Ovvero, se esistono soluzioni a sistemi del tipo

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \dots \\ a_m x \equiv b_m \pmod{n_m} \end{cases}$$

Per arrivare alla soluzione di questo sistema possiamo servirci di un suo caso particolare ponendo $a_1, a_2, \dots, a_m = 1$, ossia del *Teorema Cinese dei Resti*.

4.1 Teorema cinese dei resti

$$\text{Un sistema } \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \dots \\ x \equiv b_m \pmod{n_m} \end{cases} \text{ ha soluzione se e solo se } (n_i, n_j) \mid b_i - b_j$$

Dimostriamo il criterio di compatibilità, la forma e il numero delle soluzioni, e quindi troviamo una procedura di calcolo delle medesime.

4.1.1 Compatibilità

Partiamo da un sistema molto semplice di due congruenze lineari:

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{cases} \Rightarrow \begin{cases} x = b_1 - n_1 y_1 \\ x = b_2 - n_2 y_2 \end{cases}$$

che ovviamente ammette soluzioni se ciascuna equazione l'ammette, ovvero, in base al criterio di compatibilità 3.3.1, se e solo se $n_1 \mid b_1$, $n_2 \mid b_2$.

Dal sistema di diofantee possiamo ricavare per sottrazione l'uguaglianza

$$b_1 - n_1 y_1 = b_2 - n_2 y_2 \Rightarrow b_1 - b_2 = n_1 y_1 - n_2 y_2$$

ovvero un'equazione diofantea con incognite y_1, y_2 .

Sempre in base al criterio 3.3.1 questa equazione è compatibile se e solo se

$$(n_1, n_2) \mid b_1 - b_2 \Rightarrow b_1 \equiv b_2 \pmod{(n_1, n_2)}$$

E' ovvio che se $(n_1, n_2) = 1$ sarà sempre vero che $(n_1, n_2) \mid b_1 - b_2$

E' quindi evidente che un sistema di m congruenze lineari avrà soluzioni se i criteri di compatibilità saranno verificati per tutte le coppie di congruenze lineari, e pertanto potremo scrivere i due criteri di compatibilità:

A) $(n_1, n_2) \mid b_1 - b_2$, *criterio generale*

B) $(n_1, n_2) = 1$, *criterio standard*

In buona sostanza, se è verificato **B** il sistema è sicuramente compatibile.

Se **B** non è verificato bisogna controllare **A** prima di concludere che il sistema non ammette soluzioni.

► **Esempio 1:**

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 3 \pmod{5} \end{cases} \Rightarrow (9, 5) = 1 \mid (7 - 3); \mathbf{B} \text{ è verificato e quindi lo è anche } \mathbf{A}$$

► **Esempio 2:**

$$\begin{cases} x \equiv 6 \pmod{22} \\ x \equiv 2 \pmod{12} \end{cases} \Rightarrow (22, 12) = 2 \nmid (6 - 2); \mathbf{B} \text{ non è verificato ma lo è } \mathbf{A}$$

► **Esempio 3:**

$$\begin{cases} x \equiv 15 \pmod{14} \\ x \equiv 2 \pmod{4} \end{cases} \Rightarrow (14, 4) = 2 \nmid (15 - 2); \mathbf{B} \text{ ed } \mathbf{A} \text{ non verificati, sistema non compatibile.}$$

Ora ci dobbiamo preoccupare di sapere quante e di che forma sono le soluzioni.

4.1.2 Soluzioni

► **B)**

Se è valido il criterio di compatibilità *standard* allora la soluzione è unica modulo il prodotto dei

moduli $x \equiv x_0 \pmod{N}$, $N = \prod_{j=1}^k n_j$ ed è del tipo

4.1.2.1 $x = \sum_{j=1}^k b_j w_j N_j$

dove si ha $N_j = \frac{N}{n_j}$, il suo inverso $w_j = (N_j)^{-1} \Rightarrow w_j \cdot N_j \equiv 1 \pmod{n_j}$ ed è $(N_j, n_j) = 1$.

Se è $(N_j, n_j) = 1$ (B), possiamo scrivere un'identità di Bezout $w_i N_i + q_i n_i = 1$ dalla quale risulta che $w_i N_i \equiv 1 \pmod{n_i}$ ovvero che w_i è l'inverso di N_i . Ma allora possiamo scrivere che $b_1 w_1 N_1 + b_2 w_2 N_2 + \dots + b_k w_k N_k \equiv b_i \pmod{n_i}$ e quindi una soluzione del sistema sarà $x = b_1 w_1 N_1 + b_2 w_2 N_2 + \dots + b_k w_k N_k$. Inoltre, se \tilde{x} è un'altra soluzione del sistema, allora $n_i \mid x - \tilde{x}$ e quindi $x - \tilde{x}$ è divisibile per N . La soluzione del sistema è dunque unica modulo N .

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 3 \pmod{5} \end{cases} \Rightarrow N_1 = 5, N_2 = 9, w_1 = 2, w_2 = 4$$

Si trovano gli inversi con un semplice calcolo diretto e quindi, con la 4.1.2.1, la soluzione che è:

$$x = 7 \cdot 2 \cdot 5 + 3 \cdot 4 \cdot 9 = 178$$

Ma in realtà questa è solo *una molteplicità* della soluzione unica la cui forma generale è:

$$x = 43 + k45, k \in \mathbb{Z} \Rightarrow \dots, -2, 43, 88, 133, 178, \dots$$

Infatti, poichè la soluzione è unica modulo il prodotto dei moduli, sarà

$$178 \pmod{45} = 43 \Rightarrow 178 \equiv 43 \pmod{45}$$

e di qui la forma generale della soluzione.

Riflettete sul fatto che la forma generale della soluzione del sistema soddisfacendo contemporaneamente ciascuna delle congruenze lineari soddisfa anche le equazioni diofantee corrispondenti.

In 3.4 abbiamo visto che un'equazione diofantea $ax + ny = b$ ha soluzione

$$x_j = x_0 + \frac{kn}{d}, y_j = y_0 - \frac{ka}{d}$$

Nel nostro esempio la forma generale della diofantea è $x + ny = b$, $d = 1$ e la soluzione è

$$x = x_0 + kn, \text{ ovvero esattamente la forma generale trovata per il nostro esempio.}$$

Infatti, avremmo potuto anche procedere diversamente, cercando le soluzioni del corrispondente sistema di diofantee

$$\begin{cases} x = 7 - y_1 9 \\ x = 3 - y_2 5 \end{cases}$$

dal quale otteniamo l'equazione diofantea

$$7 - y_1 9 = 3 - y_2 5 \Rightarrow y_1 9 - y_2 5 = 4$$

per la quale c'è sicuramente una soluzione $\langle 1, 1 \rangle$, mentre tutte le altre sono date da

$$y_1 = 1 - k5, y_2 = 1 - k9$$

Allora la soluzione del sistema di congruenze lineari sarà

$$x = -2 + k45 \Rightarrow -2 \pmod{45} = 43 \Rightarrow x = 43 + k45$$

Questa procedura sarà quella che dovremo adottare nel caso seguente.

► **A)**

Se è valido il criterio *generale* di compatibilità ma non quello *standard*, la soluzione è sempre unica ma è modulo il mcm dei moduli $M = [n_1, \dots, n_i, n_j, \dots, n_k]$.

Si tratta di una generalizzazione del criterio B). Infatti basta tenere presente che il mcm è dato da

$$\frac{n_1 \cdot n_2 \cdot \dots \cdot n_k}{(n_1, n_2, \dots, n_k)} = \frac{N}{d} \text{ e che se è valido il criterio di compatibilità B) è } d = 1.$$

► **Soluzione dell'esempio 2:**

$$\begin{cases} x \equiv 6 \pmod{22} \\ x \equiv 2 \pmod{12} \end{cases} \Rightarrow \begin{cases} x = 6 - 22y_1 \\ x = 2 - 12y_2 \end{cases} \Rightarrow [22, 12] = 132$$

Essendo $(22, 12) \neq 1$ non possiamo adoperare la 4.1.2.1. Per rendersene conto basta osservare che

$$(N_1, n_1) \neq 1, (N_2, n_2) \neq 1 \text{ e che quindi non esistono inversi.}$$

Allora procediamo ricavando dal sistema l'equazione diofantea:

$$22y_1 - 12y_2 = 4$$

che avrà sicuramente la soluzione $\langle 4, 7 \rangle$. Tutte le altre saranno date da:

$$y_1 = 4 - k12, y_2 = 7 - k22$$

quindi la soluzione unica del sistema sarà data da:

$$x = 6 - 22(4 - k12) = 2 - 12(7 - k22) = -82 + k264 \Rightarrow -82 \pmod{132} = 50 \Rightarrow x = 50 + k132$$

E' evidente a questo punto che un sistema

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_i \pmod{n_i} \\ x \equiv b_j \pmod{n_j} \\ x \equiv b_k \pmod{n_k} \end{cases}$$

avrà soluzioni sempre alle stesse condizioni, ovvero che B) o A) siano verificati per ogni coppia i, j di equazioni.

Infatti poichè i criteri di compatibilità devono essere verificati *solo per coppie* di congruenze lineari, dimostrazioni e procedimenti di calcolo validi per sistemi a due congruenze lineari sono validi anche per sistemi a k congruenze lineari i quali avranno per soluzione le soluzioni di sistemi ridotti formati da una coppia qualsiasi di congruenze lineari.

4.2 Sistemi di congruenze lineari ad una incognita

Possiamo generalizzare i risultati ottenuti col teorema cinese dei resti per risolvere un sistema di congruenze lineari ad una incognita

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \dots \\ a_m x \equiv b_m \pmod{n_m} \end{cases}$$

e dimostrare che se è valido il criterio di compatibilità B) la soluzione è esattamente la 4.1.2.1.

Infatti, se gli interi x_1, x_2, \dots, x_m sono le soluzioni di ciascuna congruenza lineare, ovvero se è

$$a_j x_j \equiv b_j \pmod{n_j}, \text{ posto } N = n_1 \cdot n_2 \cdot \dots \cdot n_m \text{ e } N_j = \frac{N}{n_j} \text{ avremo che } (N_j, n_j) = 1$$

Quindi possiamo trovare degli interi w_j tali che $N_j w_j \equiv 1 \pmod{n_j}$.

La soluzione del sistema sarà pertanto unica e del tipo

$$x = \sum_{j=1}^m x_j w_j N_j$$

che è esattamente la 4.1.2.1.

Ci sono dubbi ?

Se è valido il criterio di compatibilità B) *standard* allora è valido anche il A) *generale*, ovvero

$d_j = (a_j, n_j) \mid b_j$. Allora possiamo riscrivere il sistema dividendo per d_j

$$\begin{cases} a'_1 x \equiv b'_1 \pmod{n'_1} \\ a'_2 x \equiv b'_2 \pmod{n'_2} \\ \dots \\ a'_m x \equiv b'_m \pmod{n'_m} \end{cases} \text{ dove } a'_j = \frac{a_j}{d_j} \text{ e } (a'_j, n'_j) = 1$$

Ma allora il sistema avrà una soluzione unica $c_j \pmod{n'_j}$ e potrà essere scritto come

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \dots \\ x \equiv c_m \pmod{n_m} \end{cases}$$

e quindi potremo risolverlo col teorema cinese dei resti che come soluzione prevede la 4.1.2.1.

► **Esempio**

$$\begin{cases} 2x \equiv 3 \pmod{7} \\ 3x \equiv 4 \pmod{5} \\ 5x \equiv 46 \pmod{51} \end{cases}$$

La condizione di compatibilità è rispettata, quindi siamo certi che il sistema avrà soluzioni.

Ora possiamo trovare una soluzione a ciascuna congruenza lineare:

$$x_1 = 5, x_2 = 3, x_3 = 50$$

Quindi poniamo

$$N = 7 \cdot 5 \cdot 51 = 1785$$

$$N_1 = \frac{1785}{7} = 255, N_2 = \frac{1785}{5} = 357, N_3 = \frac{1785}{51} = 35$$

Ora vediamo che è $(N_j, n_j) = 1$ e quindi possiamo trovare tre interi m_j tali che $N_j m_j \equiv 1 \pmod{n_j}$.

Tali interi sono 5, 3, 35.

La soluzione è pertanto $5 \cdot 255 \cdot 5 + 3 \cdot 357 \cdot 3 + 50 \cdot 35 \cdot 35 = 70838 \equiv 1223 \pmod{1785}$. ■

Leonardo Calconi
leo@4dmatrix.it

Una versione aggiornata e corretta potrebbe essere disponibile all'indirizzo:
www.4dmatrix.it/math