CONGRUENZE

1. Cosa afferma il principio di induzione?

Sia P(n) una proposizione definita per ogni $n \geq n_0$ (n_0=naturale)
e siano dimostrate le seguenti proposizioni:

a) $P(n_0)$ è vera
b) Se P(n) è vera allora P(n+1) è vera

Segue che P(n) è vera per ogni naturale.

2. Può fare un esempio di applicazione del principio di induzione?

Dimostriamo che la somma dei primi n interi vale $S_n=n(n+1)/2$
Se $n=n_0=1$ risulta S=1 . Perciò $P(n_0)$ è vera.
Se $S_n= n(n+1)/2$ la S(n+1) si ottiene sommando ad S_n il numero n+1
Si ottiene $\frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+2)(n+1)}{2}$
La formula risulta vera anche per n+1. Per induzione è allora vera per ogni n.

3. E' corretto affermare che l'insieme dei naturali è ben ordinato?

Si è detto che un insieme è ben ordinato se ogni suo sottoinsieme ha un minimo.
L'insieme N dei numeri naturali è ben ordinato secondo l'usuale relazione d'ordine $\leq$
[x<=y $\Leftrightarrow$ (x=y) oppure esiste un $z \in N$ tale che x+z=y]

4. Cosa si può dedurre dall'esistenza dell'algoritmo della divisione ?

Siano a,b due numeri naturali appartenenti ad N_0, (a sia detto dividendo, b sia detto divisore) e sia $b \neq 0$. L'esistenza dell'algoritmo della divisione consente di dedurre che esistono e sono unici due interi q, r tali che

$$a=q \bullet b+r$$

con $0 \leq r < b$. Il numero intero q è detto quoziente, il numero intero r è detto resto. Il resto r è sempre minore del divisore. Se il resto è zero il divisore b divide il dividendo a e ciò viene indicato scrivendo b|a.
L'algoritmo precedente può estendersi al caso in cui a,b appartengono a Z (insieme dei numeri interi RELATIVI).
Se q è un numero reale (razionale od irrazionale), definiamo col simbolo $\lfloor q \rfloor$ l'approssimazione per difetto di q.
Ad esempio se q=2.3 allora $\lfloor q \rfloor$ =2, mentre se q=−2.3 allora $\lfloor q \rfloor$ =−3

> Diciamo divisione intera dei numeri interi relativi a,b la coppia ordinata (q,r) tale che $q=\lfloor a/b \rfloor$, (approssimazione per difetto di a/b) mentre r=a−qb

Ad esempio −18:10=(−2,2) [si noti che −18/10=−1.8, e che $\lfloor -1.8 \rfloor = -2$
−8:10=(−1,2)

5. Cos'è il massimo comun divisore MCD fra due interi a,b?

E' un intero d tale che $\frac{a}{d}$ =intero e $\frac{b}{d}$ =intero. Inoltre non esiste alcun intero maggiore di d che divida sia a che b. Se d divide sia a che b, divide anche la loro differenza, ovvero $\frac{a-b}{d} = k$ (k intero)

6. Qual è l'algoritmo di Euclide per la ricerca del MCD fra a e b?

- Si divide a per b ricavando il quoziente q ed il resto r_0:

$a=qb+r_0$

- Si divide b per r_0:

$b=q_0 r_0+r_1$

- Si divide r_0 per r_1

$r_0=q_1 * r_1+r_2$

Si divide r_1 per r_2

$r_1=q_2 * r_2+r_3$

Si prosegue fino a che qualche resto r_n sia nullo. Allora il resto r_{n-1} è il MCD

Esempio MCD(64,50)

64= 1• 50 + 14
50= 3• 14 + 8
14= 1• 8 + 6
8= 1• 6 + 2
6= 3• 2 + 0

L'ultimo resto non nullo è il 2, allora MCD(64,50)=2. Si noti che:

> Il precedente algoritmo di Euclide consente di esprimere d come combinazione lineare di a e b. Ovvero **$d=\lambda a+\mu b$** con λ,μ interi (identità di Bezout).

Infatti $2=1•8-1•6= 1•8-1(14-1•8)=2•8-14=2(50-3•14)-14= 2•50-7•14= 2•50-7(64-1•50)=-7•64+9•50$

Allora $\lambda=-7$, $\mu=9$ (Infatti $-7•64+9•50=2$)

Notiamo che possiamo scrivere l'identità di Bezout $d=\lambda a+\mu b$ nella forma:

$d=(\lambda+kb)a+(\mu-ka)b$

> Se (λ,μ) rappresenta una soluzione particolare dell'identità di Bezout **$d=\lambda a+\mu b$** , la soluzione generale è $(\lambda+kb,\mu-ka)$ con k intero relativo.

7. Può fare un esempio di utilizzo dell'identità di Bezout?

Supponiamo che si abbiano assegni da 2000 ∈ e da 3500 ∈. Vogliamo stabilire se con un certo numero di tali assegni è possibile ottenere la somma di 11000 ∈. Chiaramente in questo esempio la soluzione è immediata (2 assegni da 2000 e 2 da 3500). Ma vi sono molti casi in cui la soluzione non è altrettanto semplice.

Per risolvere il problema con Bezout scriviamo:

$2000x+3500y=11000$

Dividendo per 500:
a)4x+7y=22
Facciamo riferimento all'equazione:
b) 4x+7y=1 che è una identità di Bezout ($d=\lambda a+\mu b$) e ricerchiamo x,y col metodo di Euclide:

7=1•4+3
4=1•3+1
Segue 1=1•4−1•(7−1•4)
1=2•4−1•7
Allora $(\lambda,\mu)=(2,-1)$ (soluzione particolare della b)
La soluzione particolare della (a) si ottiene moltiplicando per 22
Allora $(\lambda,\mu)=(44,-22)$
La soluzione generale è: $(\lambda,\mu)=(44+7k,-22-4k)$
Il problema richiede che il numero di assegni sia positivo. Allora
44+7k>=0 44+7k>=0 k>=−44/7 k>=−6.2
−22−4k>=0 22+4k<=0 k<=−22/4 k<=−5.5

L'unica soluzione l'otteniamo con k=−6.
Con k=−6 otteniamo $(\lambda,\mu)=(44+7k,-22-4k)=(2,2)$

8. Può fare un altro esempio?
Dati degli assegni da 2000 ∈ e 3500∈, in quanti modi è possibile ottenere la somma di 25000∈ ?

La equazione è
2000x+3500y=25000
Dividendo per 500:
1)4x+7y=50
Consideriamo l'equazione
2) 4x+7y=1 che è una identità di Bezout. Allora

7=1•4+3
4=1•3+1 $\Rightarrow$1=1•4−1(1•7−1•4)
1=2•4−1•7
$(\lambda,\mu)=(2,-1)$ [soluzione particolare della 2]
Moltiplicando per 50 si ottiene una soluzione particolare della 1:
$(\lambda,\mu)=(100,-50)$. La soluzione generale della 1 è allora:
$(\lambda,\mu)=(100+7k,-50-4k)$.
Dovendo essere λ,μ positivi segue:
100+7k>=0 7k>=−100 k>=−100/7 k>=−14.2
−50−4k>=0 50+4k<=0 k<=−50/4 k<=−12.5
Vi sono allora solo due soluzioni: k=−13, k=−14
$(\lambda1,\mu1)=(100-13*7,-50-4(-13).=(9,2)$
$(\lambda2,\mu2)=(100-14*7,-50-4(-14).=(2,6)$

9. Quando un numero è primo?

Un numero x è detto divisore proprio di n quando divide n ed è diverso sia da 1 che da n.
Il numero naturale n è primo quando non ha divisori propri.

10. Studiare la validità della proposizione: Se p divide ab allora divide a oppure divide b.

Tale proposizione è falsa se p non è primo.
Infatti 6 divide 4*3, ma non divide né il 3, né il 4
Il motivo per cui $\frac{4*3}{6}$ è intero nonostante né $\frac{4}{6}$, né $\frac{3}{6}$ sia intero, è che $\frac{4}{6}$ si può semplificare (in modo da fornire un denominatore che sia un divisore del numero 3).
Ma se il denominare p è primo allora non si potrà semplificare né con a, né con b. Perciò l'unica possibilità che ab/p sia intero è che p divida a oppure b.

11. Quando due interi si dicono COPRIMI?
Quando il loro MCD è l'unità.

12. Quando due interi relativi a,b si dicono congrui modulo n ?
Quando, divisi per n, hanno lo stesso resto.
La relazione di congruenza fra a e b, viene indicata con $a \equiv b \pmod n$
Ad esempio $2 \equiv 12 \pmod{10}$
Ma è anche $2 \equiv 22 \pmod{10}$
Oppure $2 \equiv 32 \pmod{10}$
Ma è anche $-8 \equiv 2 \pmod{10}$

Infatti -8:10=(-1,2), ovvero -8:10 ha quoziente -1 e resto 2. Si noti che il quoziente della divisione intera a:b l'abbiamo definito come il numero $\lfloor a/b \rfloor$=approssimazione per difetto del numero a/b. Mentre se q è il quoziente di a:b, il resto è r=a-qb

Si noti che ogni numero a è congruo col suo resto nella divisione per il modulo.
Ad esempio $12 \equiv 2 \pmod{10}$. Infatti il resto della divisione di 12 per 10 è proprio 2.

> Se $a \equiv b \pmod n$ allora $a-b=kn$, con k intero relativo.
> Due numeri sono congrui se e solo se la loro differenza è un multiplo del modulo.

Infatti sia r_1 il resto della divisione di a per n
r_2 il resto della divisione di b per n

Dall'algoritmo della divisione:
$a=hn+r_1 \quad \Rightarrow r_1=a-hn$
$b=mn+r_2 \quad \Rightarrow r_2=b-mn$
Essendo per definizione $r_1=r_2$ segue $a-hn=b-mn \Rightarrow a-b=(h-m)n$
Ovvero $a-b=kn$

13. Quali sono le proprietà più comuni delle congruenze?

a) Se $a \equiv b \pmod n$ possiamo aggiungere o togliere lo stesso intero ad entrambi i membri della congruenza.

Infatti $a \equiv b \pmod n$ significa $a-b=kn$ da cui, sottraendo e sommando c a primo membro:

$$(a-c)-(b-c)=kn$$
$$(a-c) \equiv (b-c) \pmod n$$

b) Se $a \equiv b \pmod n$ possiamo moltiplicare per lo stesso numero intero entrambi i membri della congruenza

Infatti da $a-b=kn$, moltiplicando i due membri per l'intero h

$ah-bh=hk\,n$ $ah-bh=p\,n$ $ah \equiv bh \pmod n$

In generale non possiamo dividere per uno stesso numero i due membri di una congruenza. Ad esempio $6*3 \equiv 6*10 \pmod{14}$. Ma non vale $3 \equiv 10 \pmod{14}$

c) possiamo dividere entrambi i membri di una congruenza per uno stesso numero r a condizione di dividere il modulo n per il MCD(r,n)

Ad esempio avendo $6*3 \equiv 6*10 \pmod{14}$

possiamo scrivere $3 \equiv 10 \pmod{14/MCD(14,6)}$

$3 \equiv 10 \pmod 7$

Per capire come mai da $ra \equiv rb \pmod n$ segue $a \equiv b \pmod{n/MCD(r,n)}$

si noti che avendo una congruenza $a \equiv b \pmod n$,

se d è un divisore di n vale anche $a \equiv b \pmod d$

Infatti $a \equiv b \pmod n$, significa $a-b=kn$

Ma se d è un divisore di n allora $hd=n$ (h intero).

Segue $a-b=hk\,d$ ovvero $a-b$ è un multiplo intero di d, e perciò a,b sono congrui modulo d.

d) Se abbiamo due congruenze: $a \equiv b \pmod n$

$c \equiv d \pmod n$

possiamo sommare membro a membro, sottrarre membro a membro, moltiplicare membro a membro. In particolare da $a \equiv b \pmod n$ segue $a^k \equiv b^k \pmod n$ con k intero.

14. E' corretto affermare che la relazione di congruenza è una relazione di equivalenza?

Si. Essa è riflessiva (un numero è congruente a se stesso).

E' simmetrica (se a ha lo stesso resto di b allora b ha lo stesso resto di a)

E' transitiva (se a ha lo stesso resto di b e b ha lo stesso resto di c allora a ha lo stesso resto di c)

15. Nelle relazioni di equivalenza è possibile definire un insieme quoziente. Come viene indicato tale insieme nel caso della relazione di congruenza?

Viene indicato con Zn e viene detto insieme quoziente delle classi di congruenza.

Ad esempio per n=5 abbiamo l'insieme quoziente Z_5.

Dato che ogni relazione di equivalenza su un insieme Z definisce una partizione dell'insieme Z medesimo, anche la relazione di congruenza (mod n) definirà una partizione

su Z. Ovvero l'insieme dei numeri interi relativi Z sarà suddiviso dalla relazione (congruenza mod n) in un certo numero di sottoinsiemi, disgiunti fra loro, la cui unione fornirà Z.

Dato l'intero positivo n (modulo) indichiamo con [0] l'insieme di tutti i numeri interi relativi che sono congrui con 0 (mod n). Ovvero l'insieme di tutti i multipli interi di n.
Indichiamo con [1] l'insieme di tutti i numeri che divisi per il modulo n danno resto 1.
E in generale indichiamo con [a] l'insieme formato da tutti i numeri che divisi per il modulo n danno come resto a.
Dato che i possibili resti della divisione di un numero x per un numero n sono n, abbiamo n classi di congruenza: [0],[1],[2],…..[n−1].
Tali insiemi formano una partizione di Z.
Indichiamo con Zn l'insieme quoziente di Z mediante la relazione di congruenza mod n. Gli elementi di Zn sono le classi di congruenza, ovvero
Zn={[0],[1],…[n−1]}

Riassumiamo. Consideriamo la classe di congruenza [0] in Z_5.
Si ha [0]={….−25,−20,−15,−10,−5,0,5,10,15,…}
La classe di congruenza [0] in Z_5 è allora formata da tutti i multipli, positivi e negativi, di 5.
La classe [1] in Z_5 è invece: [1]={ −14,−9,−4,1,6,11,16,…}
Ovvero è formata da tutti gli interi che divisi per il modulo cinque hanno come resto 1.
Analogamente:
[2]={ −13,−8,−3,2,7,12,17,…}
[3]={ −12,−7,−2,3,8,13,18,…}
[4]={ −11,−6,−1,4,9,14,19,…}
Le cinque classi di congruenza sono fra loro disgiunte ed danno come unione l'insieme Z dei numeri interi relativi.
Costituiscono perciò una partizione di Z.
L'insieme quoziente Z_5 è per definizione: Z_5={[0],[1],[2],[3],[4]}
Si noti che tale insieme NON E' Z, poiché è costituito solo da cinque elementi, (ciascuno dei quali è un insieme).

Si noti anche che se se a,b sono due interi qualsiasi ed $a \equiv b \pmod n$ allora la classe di congruenza a cui appartiene a coincide con la classe di congruenza a cui appartiene b. Indichiamo tale fatto scrivendo [a]=[b] che significa: a,b appartengono entrambi ad uno degli insiemi: [0],[1],[2],[3],[4],…[n−1].

Su Zn si possono definire le seguenti operazioni:
[a]+[b]=[a+b]
[a]*[b]=[a*b]

Nelle precedenti [a] indica la classe di congruenza, modulo n, di a.

16. Quali proprietà comuni su Z sono valide anche su Zn?

Commutativa e associativa delle due operazioni di somma e prodotto.

Distributività del prodotto rispetto alla somma. Cancellazione rispetto alla somma (uno stesso elemento sommato ai due membri di una congruenza, può essere cancellato),
Non vale la proprietà di cancellazione rispetto al prodotto.
Ad esempio [6]*[3]=[6]*[10]=[4] (su Z_{14})
ma [3]≠[10] (su Z_{14})

Ovvero 3*6≡6*10 (mod 14)
Ma non vale 3≡10 (mod 14)

17. Quali proprietà delle congruenze sono legate al modulo?

a) Se a≡b (mod n) ed m divide n allora a≡b mod m
b) se a≡b (mod n) e a≡b (mod m) allora a≡b [mod mcm(m,n)]
c) se r•a≡r•b (mod n) allora è possibile dividere per r ottenendo a≡b [mod n/MCD(r,n)]

15. Quand'è che l'equazione ax≡b (mod n) ha soluzioni intere?

Quando il massimo comun divisore fra a ed n divide b. Ovvero quando MCD(a,n)|b.
Infatti tale equazione significa ax−ny=b (x,y interi)
Se indichiamo con d=MCD(a,n), dividendo per d si ottiene:

$$\frac{a}{d}x - \frac{n}{d}y = \frac{b}{d}$$

Il numero d divide a, e divide anche n, perciò a primo membro vi è un intero.
A secondo membro vi è un intero solo se d divide b.

Se x_0 è una soluzione parziale di ax≡b (mod n), tutte le soluzioni saranno

$x_0+\lambda\ n/d$ con d=MCD(a,n)

Infatti sostituendo si ottiene $a(x_0+\lambda \frac{n}{d})\equiv b$

$a\ x_0 + a\ \lambda\frac{n}{d}\equiv b \pmod n$

Infatti essendo d il MCD(a,n) segue $\frac{an}{d} = mcm(a,n)$. Allora $a\ \lambda\frac{n}{d}\equiv 0 \pmod n$.

[esempio MCD(8,12)=4 8*12/4=24 =mcm(8,12)]

16. Come si ricavano le soluzioni dell'equazione precedente?

Un primo metodo segue dalla osservazione che se x_0 è una soluzione allora
$a \bullet x_0 \equiv b \pmod n$,
ovvero $(a \bullet x_0 - b) = y_0 \bullet n$.
$a \bullet x_0 - n \bullet y_0 = b$
se b è il MCD tra a ed n la precedente è l'identità di Bezout, ed i due numeri x_0, y_0 si possono ricavare col metodo di Euclide che abbiamo già visto.
Se invece b non è il MCD tra a ed n allora si risolve l'identità di Bezout:
$ax_0 - ny_0 = d$
con d =MCD fra a ed n, e poi si moltiplicano entrambi i membri per un numero k tale che k•d=b

Esempio:
Risolvere $81y \equiv 6 \pmod{15}$

Dividendo per 3:
$27y \equiv 2 \pmod 5$

Il MCD fra 27 e 5 divide il 2, perciò è risolubile.

La scriviamo nella forma:
(a)$27y-5x=2$;

Il 2 non è il MCD fra 27 e 5. Perciò risolviamo la seguente:
$27y'-5x'=1$ Ponendo $-x'=z'$ si ha:

$27\,y'+5\,z'=1$ (identità di Bezout)

$27=5\bullet 5+2$
$5=2\bullet 2+1$
Segue $1=1\bullet 5-2(27-5\bullet 5)$
$1=-2\bullet 27+11\bullet 5$
$(y'=-2;\ z'=11) \Rightarrow y'=-2;\ x'=-11$
La soluzione parziale della (a) si ottiene moltiplicando per 2:
$(y=-4;\ x=-22)$
La soluzione completa è $(y=-4-5k;\ x=-22-27k)$
Si può scrivere $y=-4-5(k-1)$ $x=-22-27(k-1)$
$y=1-5k$ $x=5-27k$

Un secondo metodo sfrutta il teorema di Eulero:

> Se MCD(a,n)=1 allora $a^{\varphi} \equiv 1 \pmod n$
> essendo φ il numero di coprimi inferiori a n (funzione di Eulero)

Ad esempio risolvere:

$24x \equiv 21 \pmod 9$. Dividendo per 3:
$8x \equiv 7 \pmod 3$

Si ha MCD(a,n) divide b [infatti MCD(8,3)=1 che divide 7]

Inoltre $\varphi_3=2$
Allora $8^2 \equiv 1 \pmod 3$ (Eulero)

$8^2\,7 \equiv 1\bullet 7 \pmod 3$ [moltiplicando i membri per 7]
$8\bullet 8\bullet 7 \equiv 7 \pmod 3$
Allora $x=56+3k$ (k intero)

(trovata una soluzione λ_0,μ_0 dell'equazione $\lambda a+\mu b=d$ allora anche $\lambda_0+\lambda b$ ed $\mu_0-\lambda a$

sono soluzioni : $(\lambda_0+\lambda b)a+(\mu_0-\lambda a)b=\lambda_0 a+\mu_0 b=d$.
L'equazione $8\lambda\equiv 7 \pmod 3$ equivale a $8\lambda-7=3\mu$ ovvero $8\lambda-3\mu=7$)

18. Esiste un metodo pratico per calcolare la potenza $a^n \pmod m$?

Sia da calcolare $25^{17} \pmod{54}$. Esprimiamo l'esponente n in base 2 ottenendo:
$17=(10001)_2$
Quindi partiamo dall'uno più significativo ed effettuiamo le seguenti operazioni

$1\Rightarrow 1^2 *25 \equiv 25 \pmod{54}$
$0\Rightarrow 25^2 \equiv 31 \pmod{54}$
$0\Rightarrow 31^2 \equiv 43 \pmod{54}$
$0\Rightarrow 43^2 \equiv 13 \pmod{54}$
$1\Rightarrow 13^2*25 \equiv 13 \pmod{54}$

Allora $25^{17}= 13 \pmod{54}$

In pratica al primo uno facciamo corrispondere la base. Dopodiché quando la cifra binaria è zero gli facciamo corrispondere il quadrato del risultato precedente (modulo m).
Quando la cifra binaria è uno gli facciamo corrispondere il quadrato del risultato precedente moltiplicato per la base.

Facciamo un altro esempio

$5^{11} \pmod 7$
$11=(1011)_2$
$1\Rightarrow 5 \pmod 7$
$0\Rightarrow 5*5 \equiv 4 \pmod 7$
$1\Rightarrow 4*4*5\equiv 3 \pmod 7$
$1\Rightarrow 3*3*5\equiv 3 \pmod 7$

Tuttavia notiamo che $5^{11}= 5^2*5^2*5^2*5^2*5^2*5\equiv 4^5*5\equiv 3 \pmod 7$

19. Cosa afferma il teorema cinese del resto?

Che se si ha il sistema di congruenze:
$x\equiv a_1 \pmod{n_1}$
$x\equiv a_2 \pmod{n_2}$
.....
$x\equiv a_t \pmod{n_t}$

e se i moduli sono tutti coprimi fra loro, allora il sistema è risolubile.
e la soluzione vale:
$x_0+\lambda*n$ essendo n il prodotto dei moduli ed x_0 una soluzione particolare.

Esempio:

$x \equiv 1 \pmod 5$
$x \equiv 9 \pmod{12}$
$x \equiv 10 \pmod{11}$

essendo i moduli coprimi fra loro il sistema e risolubile e la soluzione vale
$x=x_0+\lambda \bullet 660$

Per trovare x_0 notiamo che $\alpha_1=m_2\, m_3=12*11=132$ è coprimo con $m_1=5$. Allora

$132\,\lambda_1+5\mu_1=1$ (bezout)

$132=26*5+2$
$5=2*2+1 \Rightarrow 1=5-2(132-26*5)$
$1=53*5-2*132$
$1=132(-2)+5(53)$
$\lambda_1=-2+5k \qquad \mu_1=53-132k$

La minima soluzione positiva è $\lambda_1=8$
Analogamente:
$\alpha_2=5*11=55$ è coprimo con 12
Allora $55\lambda_2+12\mu_2=1$
$55=4*12+7$
$12=1*7+5$
$7=1*5+2$
$5=2*2+1 \Rightarrow 1=5-2(7-1*5)$
$1=3*5-2*7$
$1=3*(12-1*7)-2*7$
$1=3*12-5*(55-4*12)$
$1=23*12-5*55$
$1=55(-5)+12*(23)$
$\lambda_2=-5+12k \qquad \mu_2=23-55k$
La minima positiva è $\lambda_2=7$

Infine $\alpha_3=m_1*m_2=5*12=60$ è coprimo con $m_3=11$
$60\lambda_3+11\mu_3=1$
$60=5*11+5$
$11=2*5+1 \Rightarrow 1=11-2(60-5*11)$
$1=11*11-2*60$
$1=60(-2)+11(11)$
$\lambda_3=-2+11k \qquad \mu_3=11-60k$
La soluzione minima positiva è $\lambda_3=9$
$x_0=\alpha_1*\lambda_1*a_1+\alpha_2*\lambda_2*a_2+\alpha_3*\lambda_3*a_3$
$x_0=132*8*1+55*7*9+60*9*10=9921$
$x=x_0+k\ 5*12*11=9921+k*660=21+k*660$