DIVISIBILITA' DÌ INTERI

Definizione.
Siano a e b due interi. Si dice che *a divide b* o che *b è divisibile per a* (e si indica con $a|b$) se esiste ed è unico un intero q tale che $b=q\cdot a$.
In simboli si ha:

per ogni $a,b \in \mathbf{Z}$, $a|b$ se esiste $q \in \mathbf{Z}$ tale che $b=q\cdot a$.

Questa relazione di divisibilità gode di semplici proprietà:
per ogni $a,b,c \in \mathbf{Z}$, allora

1) se $a|b$ e $b|c$, allora $a|c$;
2) se $a|b$ e $b\neq 0$, allora $1 \leq |a| \leq |b|$;
3) $1|b$ e $b|b$;
4) se $a|b$ e $b|a$, allora $a = \pm b$;
5) se $a|1$, allora $a = \pm 1$;
6) se $a\neq 0$, allora $a|0$;
7) $a|b$ se e solo se $a|(-b)$ se e solo se $(-a)|(b)$ se e solo se $(-a)|(-b)$;
8) se $a|b$ e $a|c$ e presi $m,n \in \mathbf{Z}$, allora $a|(mb+nc)$; l'intero $mb+nc$ si dice *combinazione lineare* di b e c;
9) se $a|b$ e $a|(b+c)$, allora $a|c$.

Dimostrazione.
1) Se $a|b$, allora esiste un intero q tale che $b=q\cdot a$ e se $b|c$ allora esiste un intero p tale che $c=p\cdot b$, quindi si ha che $c=p\cdot b=p\cdot q\cdot a$. Se poniamo $k= p\cdot q$, avremo un intero k tale che $c=k\cdot a$, allora $a|c$.
2) Prendiamo $a \in \mathbf{R}$, allora per definizione di valore assoluto avremo che

$$|a| = \begin{cases} a, & \text{se } a>0; \\ -a, & \text{se } a<0. \end{cases}$$

Ora se $a|b$, possiamo scrivere che $b= q\cdot a$ e, poiché $b\neq 0$, questo implica che sia a che q sono diversi da zero, allora sia ha che $|b| = |q|\cdot|a|$. Da queste relazioni si deduce che: $|a| \geq 1$, poiché $a\neq 0$; $|b| \geq |a|$, perché è uguale al prodotto di $|a|$ per una quantità positiva non nulla.
3) Dimostrazione immediata tramite l'applicazione della definizione.
4) Se $a|b$, allora esiste un intero q tale che $b=q\cdot a$,
se $b|a$, allora esiste un intero t tale che $a= t\cdot b$,
quindi sostituendo otteniamo che $b= q\cdot t\cdot b$, da cui abbiamo che $q\cdot t=1$. Essendo q e t numeri interi, questo implica che $q=t=1$, oppure $q=t=-1$, da cui si ha che $a = \pm b$.
5) Dalla definizione segue immediatamente che esiste un intero t tale che $1= t\cdot a$, per cui, essendo a e t due interi, abbiamo $a=t=\pm 1$.
6) Si ha che $0= q\cdot a$, condizione verificata da $q=0$ per ogni elemento a di $\mathbf{Z}$, Se però $a=0$, allora $0=q\cdot 0$ è vera per ogni q, contro la richiesta che q sia unico. Quindi 0 non divide 0.
7) Dimostrazione immediata.
8) Dalle ipotesi abbiamo che esistono due interi p,q tali che $b=q\cdot a$, $c=p\cdot a$, allora la combinazione lineare $mb+nc$ diventa $mb+nc =mq\cdot a+n\, p\cdot a = (mq+np)\cdot a = t\cdot a$, per $t= mq+np \in \mathbf{Z}$, per cui si ha che $a|\,(mb+nc)$.
9) Poniamo $c=(b+c)-b$. Ora sappiamo che $a|(b+c)$ per ipotesi, $a|(-b)$ per la proprietà 7), quindi a divide la somma dei due termini per la proprietà 8), per cui $a|c$.

Definizione.
Un intero p è *primo* se $p\geq 2$ e se i suoi soli divisori sono 1 e p.
In particolare, per la proprietà 7), se p è un primo e a un intero allora $a|p$ se $a \in \{\pm 1, \pm p\}$.
Quindi possiamo anche concludere che se a è un intero positivo, allora a non è un primo se e solo se $a=1$ o se esistono due interi b,c con $b\geq 2$, $c\geq 2$ tali che $a=b\cdot c$.

La scomposizione in fattori primi gode di 3 proprietà fondamentali:

Proposizione 1.
Ogni intero maggiore o uguale a 2 è primo od è un prodotto di primi. In altre parole, preso un qualunque intero a, esistono $p_1,\dots,p_r$ primi (non necessariamente distinti) tali che

$$a= p_1\cdot\dots\cdot p_r \quad (r>0).$$

Dimostrazione.
Se a è primo non c'è niente da dimostrare.
Consideriamo ora $a\geq 2$, intero non primo.
Procediamo per assurdo e supponiamo che a non sia prodotto di primi, allora per il principio del minimo, esiste il più piccolo intero positivo $a\geq 2$ che gode di questa proprietà.
Se a non è primo, allora si potrebbe scrivere come prodotto di b,c con $b,c\geq 2$ e sia b che c sono minori di a e saranno prodotti di primi, per cui il loro prodotto, e cioè a, sarà ancora prodotto di primi, il che contraddice l'ipotesi.
Abbiamo ipotizzato che i fattori della scomposizione non siano necessariamente distinti, infatti si ha che:

Proposizione 2.
Sia $a\geq 2$ un intero. Allora esistono dei primi $p_1,\dots,p_r$ con $p_1<p_2<\dots<p_r$ degli interi positivi $m_1,\dots,m_r$ tali che

$$a=p_1^{m_1}\cdot p_2^{m_2}\cdot\dots\cdot p_r^{m_r},$$

dove $p_1,\dots,p_r$ sono chiamati *fattori primi* di a, mentre m_i è l'*esponente* di p_i per $i=1,\dots r$ di a.
In seguito proveremo che questa scomposizione è unica.
Una conseguenza fondamentale di questa proposizione è che ogni intero maggiore di 2 è divisibile per almeno un primo. Questa osservazione ci permette di dimostrare il seguente teorema:

Teorema 3.
Esiste un numero infinito di primi.

Dimostrazione.
Procediamo per assurdo, supponendo che esista un numero finito di primi e dimostrando che ne possiamo sempre costruire un altro che non appartiene a quell'insieme.
Sia $\{p_1,\dots,p_r\}$ l'insieme di tutti i primi e consideriamo un intero a diverso da questi, $a = p_1\cdot\dots\cdot p_r +1$.
Abbiamo costruito a in modo tale che non sia divisibile per nessun primo (dividendo a per un p_i si ha resto 1), quindi a deve essere primo esso stesso, in contraddizione con il fatto che i soli primi siano $\{p_1,\dots,p_r\}$.
Ora sappiamo che esistono primi divisibili solo per 1 e per se stessi e interi scomponibili in fattori primi.

Possiamo quindi studiare le relazioni che esistono fra i divisori di due numeri:

Definizione.
Siano a e b due interi non entrambi nulli. Chiameremo *massimo comun divisore* di a e b, e lo denoteremo con il simbolo MCD, il più grande intero positivo che divide sia a che b.In simboli si ha:

$$\forall a,b \in \mathbf{Z},\ \ \mathrm{MCD}(a,b)=d,\ d\in \mathbf{Z} \Leftrightarrow$$

i) $d|a$ e $d|b$,
ii) preso $c\in\mathbf{Z}$, se $c|a$ e $c|b \Rightarrow c|d$.

In particolare, presi $a,b \in \mathbf{Z}$, se $\mathrm{MCD}(a,b)=1$, allora a e b sono detti *relativamente primi*, cioè non esiste un intero che sia divisore di entrambi eccetto l'unità.
Possiamo osservare che se consideriamo due interi nulli, cioè se $a=b=0$, non esiste il $\mathrm{MCD}(a,b)$, poiché ogni numero intero divide entrambi, mentre se prendiamo due numeri tali che p sia primo e a un intero qualsiasi, si ha che:

- $\mathrm{MCD}(p,a) = p$, se $p|a$,
- $\mathrm{MCD}(p,a) = 1$ altrimenti.

La definizione di massimo comun denominatore può essere estesa anche a n numeri:

Definizione.
Siano $a_1,\dots, a_n$ interi non tutti nulli. Allora il MCD($a_1,\dots, a_n$) è il più grande intero positivo che divide ogni termine, in simboli:

$$\text{presi } a_1,\dots, a_n \in \mathbf{Z}, \text{MCD}(a_1,\dots, a_n) = d \Leftrightarrow$$

1) $d|a_i \qquad \forall i=1,\dots,n;$
2) preso $c\in\mathbf{Z}$, se $c|a_i \quad \forall i=1,\dots,n$, allora $c|d$.

Analogamente se MCD($a_1,\dots, a_n$) = 1, allora gli n termini si dicono *relativamente primi*, cioè l'unico fattore che divide tutti gli n interi è l'unità.
Il seguente lemma risulterà di fondamentale importanza per il proseguo della trattazione:

Lemma di divisione.
Siano a,b due interi con $a \neq 0$.
Allora sono univocamente determinati due interi q,r tali che:

i) $b = q\cdot a + r,$
ii) $0 \le r < |a|,$

dove q è il *quoziente della divisione* e r è il *resto della divisione* fra a e b.

Dimostrazione.
Imposteremo la dimostrazione in due parti: nella prima verificheremo l'unicità dimostrando che se per assurdo esistessero due coppie di valori che soddisfano tale proprietà, allora i valori devono essere uguali; mentre nella seconda parte proveremo che i) si può sempre scrivere come $r=b-q\cdot a$, da cui discende la relazione ii).
Unicità.
Supponiamo esistano per assurdo due coppie di valori q_1, r_1 e q_2, r_2 che soddisfano tale proprietà. Allora si ha:

$$b = q_1\cdot a + r_1 \quad \text{e} \quad b = q_2\cdot a + r_2 \quad \text{con } 0 \le r_1 < |a| \ \text{ e } \ 0 \le r_2 < |a|,$$

quindi $q_1\cdot a + r_1 = q_2\cdot a + r_2$.
Supponiamo che $r_1 \le r_2$, allora

$$r_2 - r_1 = a(q_1-q_2), \ \text{ con } \ 0 \le r_2 - r_1 < r_1 < |a|$$

da cui abbiamo che $a|\,(r_2-r_1)$.
Ma se a divide c e c è diverso da 0, allora $1 \le |a| \le |c|$ per la proprietà della divisione fra interi, quindi nel nostro caso diventa $1 \le |a| \le |\,r_2-r_1| = r_2-r_1$, da cui possiamo concludere che $r_2-r_1 = 0$, allora $r_1 = r_2$, da cui si ha

$$0 = a(q_1-q_2), \ \text{ cioè } q_1-q_2=0 \ \text{ e quindi } \ q_1 = q_2.$$

Esistenza.
Senza perdere di generalità, possiamo supporre $a>0$, perché se proviamo la tesi per $a>0$, la verifichiamo immediatamente anche per $a<0$:
posto $-a>0$, esistono due interi q, r tali che $b = q\cdot(-a)+r$ con $0 \le r < |-a| = |a|$ da cui diventa:

$$q\cdot(-a)+r = (-q)\cdot a + r$$

ritornando così al caso di a intero positivo.
Supponiamo quindi $a>0$ e consideriamo l'insieme S degli interi non negativi della forma $b = q\cdot a$ con $q \in \mathbf{Z}$, cioè

$$S = \{c\ge 0 \ / \ c=b-q\cdot a, \ \text{con } q\in \mathbf{Z}\}.$$

S è un sottoinsieme di $\mathbf{Z}$, quindi per il principio del minimo S ha minimo e poniamo min$S=r$.
Per costruzione $r \ge 0$ e cerchiamo di dimostrare che $r<|a|$, cioè che $r<a$, visto che abbiamo definito a positivo.
Per assurdo supponiamo $r \ge a$, da cui $r-a \ge 0$.
Sappiamo che $r-a \ge 0$ e $r-a<r$, quindi $r-a$ è ancora un valore che appartiene a S e inoltre è minore di r che è il min$S$, infatti

$$r-a = b-q\cdot a-a = b-(q+1)\cdot a \ \in S$$

e questo contraddice l'ipotesi che r sia il minimo di S; pertanto deve essere che $r<a$.

Come conseguenza di questo lemma, possiamo studiare un teorema fondamentale per la nostra trattazione che dice che il MCD di due interi a e b è una combinazione lineare di a e di b:

Teorema. Dati $a,b \in \mathbf{Z}$ non entrambi nulli, esistono due interi $s,t \in \mathbf{Z}$ tali che

$$\text{MCD}(a,b) = sa + tb.$$

Dimostrazione.
Poniamo $d = \text{MCD}(a,b)$ e sia m il minimo dell'insieme S di tutte le combinazioni di a e di b, cioè $m = \min S$, dove $S = \{sa+tb \,/\, s,t \in \mathbf{Z}, \text{ con } sa+tb>0\}$.
Se dimostriamo che $d=m$ l'enunciato resta dimostrato.
Se $d = \text{MCD}(a,b)$, allora d è un divisore di tutte le combinazioni lineari di a e di b e in particolare d divide m, da cui si ha che $d \le m$.
Quindi se dimostriamo che $m|d$ avremo nucessariamente che $d=m$.
Usando il lemma di divisione, si ha che

$$a = q \cdot m + r, \quad \text{con } 0 \le r < m$$

da cui diventa

$$r = a - q \cdot m = a - q \cdot (sa+tb) = (1-qs)a - qtb,$$

quindi r è combinazione lineare di a e di b e $r<m$, ma da ciò deriva che $r=0$ perché se fosse positivo non nullo cadremmo in contraddizione in quanto m deve essere il minimo di S. Quindi $a = q \cdot m$, da cui si ha che $m|a$.
Con un ragionamento analogo per b, abbiamo che $m|b$.
Quindi se un intero c divide sia a che b, c divide ogni combinazione lineare di a e di b, pertanto c divide $sa+tb=d$, per definizione di MCD, per cui $m|d$, quindi $d>m$.

Osservazioni.
I coefficienti s e t della combinazione lineare non sono unici, infatti presi $s'=s+b$ e $t'=t-a$ si ha

$$s'a+t'b = (s+b)a+(t-a)b = sa+ba+tb-ab = sa+tb.$$

Inoltre si deduce che un numero divide sia a che b se e solo se divide anche $\text{MCD}(a,b)$.
Ora indichiamo quattro corollari che sfruttano questo risultato:

Corollario 1)
Due interi a e b sono primi fra loro se e solo se esistono due interi s,t tali che $sa+tb = 1$.

Dimostrazione.
Se a e b sono primi fra loro, allora $\text{MCD}(a,b) = d = 1$, da cui si ha che $sa+tb=d=1$ per il teorema precedente.
Viceversa, se $sa+tb=1$, allora $\text{MCD}(a,b)$ deve dividere 1, quindi $\text{MCD}(a,b)=1$.

Corollario 2)
Se un intero a divide un prodotto $b \cdot c$ e a è relativamente primo con b, allora a divide c. In simboli:
se $a|bc$ e $\text{MCD}(a,b)=1$, allora $a|c$.

Dimostrazione.
Se $\text{MCD}(a,b)=1$, allora esistono s,t interi tali che $1=sa+tb$, quindi $c = c(sa+tb) = csa+tbc$.
Abbiamo che $a|(csa)$ e $a|(tbc)$ in quanto $a|bc$ per ipotesi, quindi $a|(csa+tbc)$, da cui $a|c$.

Corollario 3)
Se un primo p divide un prodotto di n interi $a_1,\ldots,a_n$, allora p divide almeno un fattore a_i , per $i=1,\ldots,n$.
(Questo corollario ci permetterà di dimostrare l'unicità della scomposizione in fattori primi).

Dimostrazione.
Dimostriamo il corollario per induzione su n:
per $n=1$, è immediato;
per $n=2$, abbiamo che $p|(a_1 \cdot a_2)$.
Se p non divide a_1, allora, poiché $\text{MCD}(p,a_1)=1$, abbiamo che $p|a_2$ per il corollario precedente;
supponiamo il corollario vero per $n=r$;
consideriamo il caso $n=r+1$.
Se $p|((a_1 \cdot \ldots \cdot a_r) \cdot a_{r+1})$, allora $p|(a_1 \cdot \ldots \cdot a_r)$ oppure $p|a_{r+1}$.
Se $p|a_{r+1}$ siamo a posto, mentre se $p|\, p|(a_1 \cdot \ldots \cdot a_r)$ per ipotesi induttiva abbiamo che $p|a_i$ per $i=1,\ldots,r$.

Corollario 4)

Se $m|a$ e $n|a$ e se MCD$(m,n)=1$, allora $m\cdot n = a$.

Dimostrazione.

Per ipotesi, a sarà della forma $a=q\cdot m$ e $n|q\cdot m$.
Poiché MCD$(n,m)=1$, abbiamo che $n|q$, quindi esiste un intero s tale che $q=s\cdot n$.
Concludendo, si ha che $a=s\cdot n\cdot m$, da cui $n\cdot m|a$.
Ora abbiamo tutte le conoscenze necessarie per dimostrare che la scomposizione in fattori primi è unica.

Esistono diversi procedimenti per ottenere questo risultato e qui riportiamo la soluzione che a nostro avviso è più trasparente:

Teorema.

Ogni intero maggiore di 1 ha un'unica scomposizione in fattori primi. In simboli:
per ogni $a\in\mathbf{Z}$, $a>1$, esistono e sono unici $p_1,\dots,p_r$ primi e $m_1,\dots,m_r$ naturali tali che

$$a= {p_1}^{m_1}\cdot {p_2}^{m_2}\cdot\dots\cdot {p_r}^{m_r}, \quad \text{con } p_1<p_2<\dots<p_r.$$

Dimostrazione.

Abbiamo già appurato l'esistenza della scomposizione in fattori primi per ogni intero diverso dall'unità, quindi ci riserviamo di verificare solo l'unicità di questa affermazione.
Procediamo per assurdo, cercando di dimostrare che se esistono due scomposizioni di a, queste devono essere uguali. Supponiamo che

$$a = {p_1}^{m_1}\cdot {p_2}^{m_2}\cdot\dots\cdot {p_r}^{m_r}, \quad \text{con } p_1<p_2<\dots<p_r$$
$$a = {q_1}^{n_1}\cdot {q_2}^{n_2}\cdot\dots\cdot {q_s}^{n_s}, \quad \text{con } q_1<q_2<\dots<q_s.$$

e proviamo che $r=s$ e $p_i=q_i$ per ogni $i=1,\dots,r$.

Consideriamo un fattore p_i della prima scomposizione: certamente p_i divide il prodotto ${q_1}^{n_1}\cdot{q_2}^{n_2}\cdot\dots\cdot{q_s}^{n_s}$ in quanto $p|a$ e quindi dividerà un valore q_j per un certo j appartenente a $\{1,\dots,s\}$.
Ragionando in modo analogo per ogni fattore p_i, avremo che l'insieme dei p_i è incluso in quello dei fattori q_j, cioè

$$\{p_1,\dots,p_r\}<\{q_1,\dots,q_n\},$$

e ripetendo lo stesso procedimento, se consideriamo prima i fattori q_j avremo che

$$\{q_1,\dots,q_n\}<\{p_1,\dots,p_r\}.$$

Dalla doppia conclusione e dal fatto che $p_1<p_2<\dots<p_r$ e $q_1<q_2<\dots<q_s$, otteniamo che $r=s$ e $p_1=q_1$, $p_2=q_2$, .. , $p_r=q_r$.
Rimane da dimostrare che anche gli esponenti sono uguali:
consideriamo

$${p_1}^{m_1}\cdot {p_2}^{m_2}\cdot\dots\cdot {p_r}^{m_r} = {p_1}^{n_1}\cdot {p_2}^{n_2}\cdot\dots\cdot {p_r}^{n_r}$$

e dividiamo entrambi i membri per un certo ${p_i}^{m_i}$, allora avremo che

$${p_1}^{m_1}\cdot\dots\cdot {p_{i-1}}^{m_{i-1}}\cdot{p_{i+1}}^{m_{i+1}}\cdot\dots\cdot {p_r}^{m_r} = {p_1}^{n_1}\cdot\dots\cdot {p_{i-1}}^{n_{i-1}}\cdot {p_i}^{(n_i-m_i)}\cdot{p_{i+1}}^{n_{i+1}}\cdot\dots\cdot {p_r}^{n_r}.$$

Siccome n_i-m_i deve essere positivo, abbiamo che il termine p_i può dividere nuovamente il primo membro, mentre non può più dividere il secondo perché non divide più alcun fattore e questo è assurdo, quindi $m_i=n_i$ per $i=1,\dots,r$.

Ora tutte queste nozioni sono propedeutiche per studiare l'*algoritmo euclideo*, un procedimento quasi "meccanico" che consiste in una serie di divisioni successive che consentono di calcolare il massimo comun divisore di due numeri a,b e gli interi s,t tali che

$$\text{MCD}(a,b) = d \quad \text{e} \quad d=sa+tb,$$

senza scomporre a e b in fattori primi.

ALGORITMO EUCLIDEO

Prendiamo a,b interi con $a,b>0$ e supponiamo $0<a<b$.
Dividiamo b per a, avremo che:

$$b = q_1 \cdot a + r_1, \quad \text{con } 0 \leq r_1 < a.$$

Osserviamo che:

i) se $r_1=0$, allora $b = q_1 \cdot a$ e abbiamo già che $\text{MCD}(a,b)=a$;
ii) altrimenti, preso un intero positivo d
   1) se d divide sia a che b, allora dividerà anche r_1 in quanto combinazione lineare di a e b;
   2) viceversa, se d divide a e r_1, dividerà anche b per la stessa proprietà sopra.

Quindi possiamo concludere che

$$\text{MCD}(a,b) = \text{MCD}(a,r_1),$$

con il vantaggio che $r_1<a<b$.
Ora ripetiamo lo stesso procedimento sostituendo al posto di a e b i nuovi valori a e r_1 con $r_1<a$:

$$a = q_2 \cdot r_1 + r_2, \quad \text{con } 0 \leq r_2 < r_1$$

dove

i) se $r_2=0$, si ha che $r_2 | a$, quindi $\text{MCD}(a,b) = \text{MCD}(a,r_1) = r_2$;
ii) altrimenti, si ripetono le stesse conclusioni giungendo a definire che $\text{MCD}(a,b)=\text{MCD}(a,r_1)=\text{MCD}(r_1,r_2)$.

Continuiamo a costruire queste successioni di resto sino ad arrivare all'i-esima iterazione dove

$$r_{i-1} = q_{i+1} \cdot r_i + r_{i+1}, \quad \text{con } 0 \leq r_{i+1} < r_i$$

e avremo che

i) se $r_i=0$, allora $\text{MCD}(a,b) = r_{i-1}$;
ii) altrimenti, continuiamo il procedimento.

Poiché gli r_i sono interi non negativi e la successione di resti è decrescente, ad un certo punto ci dovremo fermare, cioè esisterà un r_n diverso da zero tale che $r_{n+1}=0$, allora il nostro $\text{MCD}(a,b)$ sarà uguale all'ultimo resto diverso da zero della catena di divisioni. Questo procedimento è vantaggioso perché non dobbiamo scomporre in fattori primi e si utilizzano divisioni sempre più facili. Proviamo ora a ricostruire s,t procedendo a ritroso nell'algoritmo euclideo:
presi $\text{MCD}(a,b) = r_n$ e $sa+tb = r_n$, possiamo scrivere

$$r_n = r_{n-2} - q_n \cdot r_{n-1},$$

e andiamo a sostituire il valore di r_{n-1} che si ricava dall'uguaglianza $r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1}$:

$$r_n = r_{n-2} - q_n \cdot (r_{n-3} - q_{n-1} \cdot r_{n-2}) = (1+q_n q_{n-1})\, r_{n-2} - q_n \cdot r_{n-3}.$$

Ora sostituiamo in questa equazione il valore di r_{n-2} che si ottiene da $r_{n-4} = q_{n-2} \cdot r_{n-3} + r_{n-2}$ e avremo r_n come espressione in r_{n-3} e r_{n-4}, quindi andremo a sostituire r_{n-3} e continueremo questo procedimento fino ad ottenere r_n come combinazione lineare dei soli a e b.

CONGRUENZE

Le congruenze sono un linguaggio alternativo per trattare la divisibilità fra interi:

Definizione.

Siano a e b due interi e m un intero strettamente positivo, detto *modulo*.
Si dice che a e b sono *congruenti modulo m*, in simboli

$$a \equiv b \pmod{m}$$

se m divide $a-b$.
In altre parole, possiamo dire che a è *congruo* a b modulo m se a e b differiscono per un multiplo di m, cioè

$$a \equiv b \pmod{m} \Leftrightarrow m|(a-b) \Leftrightarrow \text{esiste un } k \in \mathbf{Z} \text{ tale che } a-b = km \Leftrightarrow$$
$$a = b + km, \text{ con } k \in \mathbf{Z}.$$

In particolare, affermare che m divide a è equivalente a dire che a è congruo a 0 modulo m (basta porre $b=0$ nelle equivalenze sopra).
Possiamo così riformulare il lemma di divisione studiato nella divisibilità fra interi per il caso delle congruenze:

Lemma di divisione.

Dati due interi a,b con a positivo, esiste ed è unico un intero r con $0 \le r < a$ e tale che

$$b \equiv r \pmod{a}$$

ove r si dice *resto* di a modulo m (è l'equivalente di dire $b=q\cdot a+r$).

Poiché la relazione di congruenza è una relazione di equivalenza, gode delle seguenti proprietà:

1) proprietà riflessiva: $a \equiv a \pmod{m}$ per ogni $a \in \mathbf{Z}$;
2) proprietà simmetrica: se $a \equiv b \pmod{m}$, allora $b \equiv a \pmod{m}$;
3) proprietà transitiva: se $a \equiv b \pmod{m}$ e $c \equiv b \pmod{m}$, allora $a \equiv c \pmod{m}$.

Infatti è facile dimostrare che:

1) $a-a=0$ è sempre divisibile per ogni intero m diverso da zero;
2) se $m|(a-b)$, allora $m|(b-a)$ per le proprietà della divisibilità fra interi;
3) se $m|(a-b)$ e $m|(c-b)$, allora esistono due interi $k.t$ tali che $a-b = km$ e $c-b = tm$, quindi se consideriamo $c-a = c-b-a+b = tm+km = (t+k)m$ abbiamo che $m|(c-a)$.

Di seguito riporteremo altre facili proprietà della relazione di congruenza:

Proprietà i)

Dati a,b interi, allora $a \equiv b \pmod{m}$ se e solo se a e b hanno lo stesso resto modulo m.

Dimostrazione.

Verifichiamo la doppia implicazione, ponendo r_1 e r_2 come i resti di a e b modulo m:
$a = q_1\cdot m+r_1$, con $0 \le r_1<m$, quindi $a-r_1=q_1\cdot m$;
$b = q_2\cdot m+r_2$, con $0 \le r_2<m$, quindi $b-r_2=q_2\cdot m$;
abbiamo cioè che $a \equiv r_1 \pmod{m}$ e $b \equiv r_2 \pmod{m}$.
Se supponiamo che $a \equiv b \pmod{m}$, poiché che $b \equiv r_2 \pmod{m}$, allora per la transitività della congruenza si ha che $a \equiv r_2 \pmod{m}$ e per l'unicità del resto (derivante dal lemma di divisione) si ha che $r_1=r_2$.
Viceversa, se supponiamo che $r_1=r_2$, allora per la simmetria e la transitività della relazione di congruenza si ha che $a \equiv b \pmod{m}$.

Proprietà ii)

Se $a \equiv b \pmod{m}$, per ogni intero k, avremo $ak \equiv bk \pmod{m}$ e $a+k \equiv b+k \pmod{m}$.
In altre parole, moltiplicando o sommando ad entrambi i membri un numero intero, il risultato non cambia.

Dimostrazione.

Per la somma basta notare che $(a+k)-(b+k) = a+k-b-k = a-b$; per la moltiplicazione che $ak - bk = k(a-b)$, quindi in entrambi i casi se m divide $a-b$, divide anche $k(a-b)$.

Osservazione.
In generale però non è sempre vera l'implicazione opposta, cioè se $ak \equiv bk \pmod{m}$, allora non è detto che $a \equiv b \pmod{m}$; questo viene verificato solo quando k e m sono relativamente primi fra loro.

Proprietà iii)
Se $ak \equiv bk \pmod{m}$ e MCD$(k,m)=1$, allora $a \equiv b \pmod{m}$.

Dimostrazione.
Dalle ipotesi si ha che m divide $ak-bk$, quindi $m|k(a-b)$ e poiché MCD$(k,m)=1$, allora $m|(a-b)$.

Generalizzando la proprietà ii) possiamo concludere che la relazione di congruenza è chiusa rispetto alla moltiplicazione e alla somma:

Proprietà iv)
Posto $a \equiv b \pmod{m}$ e $a' \equiv b' \pmod{m}$, allora abbiamo
1) $(a+a') \equiv (b+b') \pmod{m}$,
2) $aa' \equiv bb' \pmod{m}$.

Dimostrazione.
1) Se $a \equiv b \pmod{m}$, allora $a+a' \equiv b+a' \pmod{m}$ per proprietà ii), analogamente se $a' \equiv b' \pmod{m}$, allora $a'+b \equiv b'+b \pmod{m}$; quindi per la proprietà transitiva abbiamo:
$$a+a' \equiv b+b' \pmod{m}.$$
2) Si procede in modo analogo per 1).

Proprietà v)
Se $a \equiv b \pmod{m}$, allora per ogni n naturale positivo, $a^n \equiv b^n \pmod{m}$.

Dimostrazione.
Procediamo per induzione su n.
Posto n=1, diventa $a \equiv b \pmod{m}$ ed è verificato per ipotesi.
Supponiamo sia vero per n, cioè poniamo che la relazione $a^n \equiv b^n \pmod{m}$ sia verificata e consideriamo il caso $n+1$: $a^{n+1} \equiv b^{n+1} \pmod{m}$.
Per proprietà iv) si ha
$$a^{n+1}=a^n \cdot a \equiv b^n \cdot b = b^{n+1} \pmod{m}.$$

Proprietà vi)
Se $a \equiv b \pmod{m}$, allora $(-a) \equiv (-b) \pmod{m}$.

Dimostrazione.
Discende direttamente dalle proprietà delle divisibilità fra interi.
Il teorema che segue dice che se a è un intero non divisibile per un primo p, allora c'è una periodicità nei resti delle potenze di a.

Teorema di Fermat.
Sia p un primo e a un intero relativamente primo con p, allora
$$a^{p-1} \equiv 1 \pmod{p} \qquad \text{I formulazione;}$$
$$a^p \equiv a \pmod{p} \qquad \text{II formulazione.}$$
Le due formulazioni sono equivalenti.

Dimostrazione.
Iniziamo con il dimostrare che le due formulazioni sono equivalenti, cioè che la veridicità di una implica quella dell'altra.
Supponiamo sia vera la prima formulazione, cioè che $a^{p-1} \equiv 1 \pmod{p}$ e consideriamo le due possibilità: o p non divide a, o p divide a.

Nel primo caso, possiamo moltiplicare entrambi i membri dell'uguaglianza per a e avremo immediatamente che $a^{p-1}\cdot a \equiv 1\cdot a \pmod p$ da cui segue la seconda affermazione: $a^p \equiv a \pmod p$.
Nel secondo caso, sappiamo che

$$a \equiv 0 \pmod p \text{ e } a^p \equiv 0 \pmod p,$$

da cui, per la transitività delle congruenze, avremo che $a^p \equiv a \pmod p$.
Viceversa, supponiamo vera la seconda formulazione del teorema: ora poiché a e p sono relativamente primi fra loro, possiamo semplificare per a la congruenza:

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

e ottenere

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

Ora se verifichiamo il teorema per la prima formulazione, questa implicherà anche la veridicità della seconda formulazione, poiché abbiamo dimostrato che le due affermazioni sono equivalenti.

Prendiamo un intero k non divisibile per p, allora p non dividerà neanche ak e quindi, per il lemma di divisione, esisterà un unico intero r con $0<r<p$ tale che $ak \equiv r \pmod p$.
Definiamo la funzione

$$\psi_a : \{1,2, \dots , p-1\} \longrightarrow \{1,2, \dots , p-1\}$$
$$\text{tale che } \psi_a(k) = r ,$$

ove r è l'unico intero tale che $ak \equiv r \pmod p$.
La funzione ψ_a è iniettiva, infatti presi due elementi k e l di $\{1,2,\dots,p-1\}$, abbiamo che

$$\psi_a(k) = \psi_a(l) \text{ se e solo se } ak \equiv al \pmod p,$$

e, poiché MCD(a,p)=1, avremo che questo è vero se e solo se $k \equiv l \pmod p$ e quindi se solo se $k = l$, perché entrambi compresi fra 1 e p-1.
Inoltre, poiché ψ_a è iniettiva in se stessa, la sua iniettività implica anche la suriettività.
Ora abbiamo che

$$a^{p-1}\cdot (p-1)! = a^{p-1}\cdot 1\cdot 2\cdot \dots \cdot (p-1) = (a\cdot 1)(a\cdot 2)\dots (a\cdot(p-1)) = \psi_a(1)\cdot\psi_a(2)\cdot\dots\cdot\psi_a(p-1)=(p-1)!$$

in particolare l'ultima uguaglianza segue dal fatto che gli interi $\psi_a(1)\cdot\psi_a(2)\cdot\dots\cdot\psi_a(p-1)$ sono gli interi $1,2,\dots,p-1$ in ordine inverso.
Adesso, poiché MCD$((p-1)!,p) = 1$, possiamo semplificare l'uguaglianza sopra per $(p-1)!$, da cui avremo l'equazione cercata $a^{p-1} \equiv 1 \pmod p$.

Osservazione.
Se si omette la condizione che MCD(a,p)=1, cioè che a e p siano relativamente primi fra loro, la tesi del teorema di Fermat non è più verificata.

CRITERI DI DIVISIBILITÀ

All'interno delle congruenze, trovano una loro naturale collocazione i criteri di divisibilità per i numeri in rappresentazione decimale.

Definizione
Per convenzione, quando scriviamo un numero $m= a_n..a_0$, sottintendiamo che le cifre $a_n,..,a_0$ che lo compongono siano interi compresi fra 0 e 9 e la scrittura $a_n..a_0$ indica *in forma decimale* l'intero

$$a_0+10\cdot a_1+10^2\cdot a_2+..+10^n\cdot a_n \text{ , dove } 0\le a_i \le 9 \text{ per } i=0,..n.$$

Ora, all'interno di questo paragrafo, indicheremo con $a_n..a_0$ il numero intero $a_0+10\cdot a_1+10^2\cdot a_2+..+10^n\cdot a_n$ e non il suo prodotto $a_n\cdot..\cdot a_0$.
I più noti criteri di divisibilità sono:
preso un numero $m= a_n..a_0$, con $0\le a_i \le 9$ per $i=0,..n$, allora

a) 5 divide m se e solo se 5 divide a_0, quindi se e solo se $a_0=0$ oppure $a_0=5$;
b) 4 divide m se e solo se 4 divide $a_0+10\cdot a_1$, quindi se e solo se 4 divide a_1a_0;
c) 3 divide m se e solo se 3 divide $a_0+ a_1+\dots+ a_n$;
d) 9 divide m se e solo se 9 divide $a_0+ a_1+\dots+ a_n$;
e) 11 divide m se e solo se 11 divide $a_0- a_1+a_2+\dots+(-1)^n a_n$;
f) 7 divide m se e solo se 7 divide $a_0+3a_1+2a_2-a_3-3a_4-2a_5+a_6+3a_7+\dots$.

Dimostrazione.
Questi criteri si giustificano attraverso le congruenze; in particolare ora tratteremo i casi più complessi, lasciando all'utente quelli più semplici la cui dimostrazione è analoga a quella che riportiamo di seguito.
Osserviamo che nel caso b), abbiamo che

$$10 \equiv 2 \pmod 4$$
$$10^2 \equiv 2^2 \equiv 0 \pmod 4$$
$$10^3 \equiv 10 \cdot 10^2 \equiv 0 \pmod 4$$

e, poiché preso 10^n con $n \geq 2$, si ha $10^n \equiv 0 \pmod 4$, si deduce per induzione che

$$a_n..a_0 \equiv a_0 + 10 \cdot a_1 = a_1 a_0 \pmod 4.$$

Il criterio di divisibilità segue dal fatto che se i due numeri sono congrui modulo 4, allora uno è divisibile per 4 se e solo se lo è anche l'altro.

Continuando così per gli altri criteri, avremo che nel caso c)

$$10 \equiv 1 \pmod 3$$
$$10^2 \equiv 1^2 \equiv 1 \pmod 3$$
$$10^3 \equiv 1^3 \equiv 1 \pmod 3,$$

ossia, preso 10^n con $n \geq 2$, si ha $10^n \equiv 1 \pmod 3$, da cui abbiamo che

$$a_n..a_0 \equiv a_0 + a_1 + \ldots + a_n \pmod 3.$$

Il caso d) è del tutto analogo a quello appena discusso, mentre per il caso e) abbiamo che

$$10 \equiv -1 \pmod{11}$$
$$10^2 \equiv (-1)^2 \equiv 1 \pmod{11}$$
$$10^3 \equiv (-1)^3 \equiv -1 \pmod{11},$$

per cui, proseguendo nelle congruenze, avremo che $10^n \equiv (-1)^n \pmod{11}$ e quindi il valore 1 per le potenze pari di 10, mentre –1 per quelle dispari, da cui segue

$$a_n..a_0 \equiv a_0 - a_1 + a_2 - \ldots + (-1)^n a_n \pmod{11}.$$

Il caso f) risulta essere il più complesso e questo è un motivo per cui il suo utilizzo non è molto diffuso:

$$10 \equiv 3 \pmod 7$$
$$10^2 \equiv 3^2 \equiv 2 \pmod 7$$
$$10^3 \equiv 3 \cdot 2 \equiv -1 \pmod 7$$
$$10^4 \equiv 3 \cdot (-1) \equiv -3 \pmod 7$$
$$10^5 \equiv 3 \cdot (-3) \equiv -2 \pmod 7$$
$$10^6 \equiv 3 \cdot (-2) \equiv 1 \pmod 7$$
$$10^7 \equiv 3 \cdot 1 \equiv 3 \pmod 7$$

da notare che, poiché i resti si ripetono ciclicamente come previsto dal teorema di Fermat, è sufficiente conoscere i primi 7 coefficienti per comporre la serie completa di resti, per cui

$$a_n..a_0 \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + .. \pmod 7$$

CLASSI DÌ CONGRUENZA

Una relazione di equivalenza sull'insieme degli interi divide gli interi in classi di equivalenza; nel nostro caso la congruenza modulo un intero strettamente positivo m dividerà $\mathbf{Z}$ in *classi di congruenza (modulo m)*.

Definizione.
Se a è un intero, la *classe di congruenza* di a modulo m è definita come

$$[a]_m = \{ x \in \mathbf{Z} / x \equiv a \pmod m \} = \{ x \in \mathbf{Z} / x = a + km, \text{ con } k \in \mathbf{Z} \},$$

cioè è l'insieme di tutti gli interi che sono congrui ad a modulo m.

Osservazioni.
Se due classi di congruenza hanno un elemento in comune, allora coincidono.
Inoltre, ogni intero a sta in una ed una sola classe di congruenza, da cui segue che se a e b non sono congruenti modulo m, allora le loro classi di congruenza sono disgiunte.

In simboli, se $a \equiv b \pmod m$, allora

$$x \equiv a \pmod m \text{ se e solo se } x \equiv b \pmod m;$$

e se $a \neq b \pmod m$, allora

$$[a]_m \cap [b]_m = \varnothing,$$

poiché se esiste un x che appartiene all'insieme formato dall'intersezione delle loro classi di congruenza, cioè se esiste $x \in [a]_m \cap [b]_m$, allora $x \equiv a \pmod m$ e $x \equiv b \pmod m$, da cui discende che $a \equiv b \pmod m$ per le proprietà studiate della congruenza, e questo è assurdo.

Possiamo nuovamente riformulare il

Lemma di divisione.

Ogni classe di congruenza modulo m contiene uno ed un solo intero r con $0 \leq r < m$, dove

$$[a]_m = \{\, r \in \mathbf{Z} \,/\, a = q \cdot m + r, \text{ con } r \in \mathbf{Z} \,\}.$$

Una conseguenza del lemma è il seguente corollario:

Corollario.

Esistono precisamente m classi di congruenza modulo m, ossia

$$\mathbf{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Le classi di congruenza si possono sommare e moltiplicare, quindi sono chiuse rispetto alla somma e alla moltiplicazione con le operazioni definite come:

1) $[a]_m + [b]_m := [a+b]_m$,
dove $+, \quad \mathbf{Z}_m \times \mathbf{Z}_m \longrightarrow \mathbf{Z}_m$
$([a]_m, [b]_m) \rightarrow [a+b]_m$;
2) $[a]_m \cdot [b]_m := [a \cdot b]_m$,
dove $\cdot, \quad \mathbf{Z}_m \times \mathbf{Z}_m \longrightarrow \mathbf{Z}_m$
$([a]_m, [b]_m) \rightarrow [a \cdot b]_m$.

dove $[0]_m$ sarà l'elemento neutro della somma e $[1]_m$ sarà l'elemento neutro della moltiplicazione.

Le operazioni $+, \cdot$ sono ben definite, ossia il comportamento delle seguenti operazioni non dipende dalla scelta del valore che appartiene alla classe di congruenza, ma se scegliamo valori diversi per a e b, le classi che abbiamo definito non cambiano, cioè

Proposizione.

Supponiamo che $[a]_m = [a']_m$ e $[b]_m = [b']_m$, allora

$$[a+b]_m = [a'+b']_m \text{ e } [a \cdot b]_m = [a' \cdot b']_m.$$

Inoltre $+, \cdot$ definite su $\mathbf{Z}_m$ godono delle stesse proprietà di $+, \cdot$ definite su $\mathbf{Z}$, per cui valgono ancora la proprietà associativa e distributiva:
presi $\alpha = [a]_m$, $\beta = [b]_m$, $\gamma = [c]_m \in \mathbf{Z}_m$ si possono facilmente dimostrare che valgono le seguenti regole di calcolo:

$(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$;
$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$;
$\alpha \cdot (\beta+\gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$;
$\alpha + 0 = \alpha$;
$\alpha \cdot 0 = 0$;
$\alpha \cdot 1 = \alpha$.

La potenza n-esima di α viene invece definita come il prodotto di n copie di α, quindi si ha che:

$$\alpha^n = ([a]_m)^n = [a^n]_m.$$

Nell'anello degli interi, gli unici valori a per cui esiste un intero b tale che $ab=1$ sono $a=1$, $a=-1$, mentre in $\mathbf{Z}_m$ si ha che:

Proposizione.
In $\mathbf{Z}_m$, data $\alpha=[a]_m$, esiste un $\beta=[x]_m$ tale che $[a]_m\cdot[x]_m=[1]_m$ se e solo se MCD$(a,m)=1$, cioè se e solo se a e m sono primi fra loro. Inoltre se β esiste è unico.

In particolare, l'elemento α si dice *invertibile*, l'elemento β si dice *inverso* di α e si denota con α^{-1}.

Dimostrazione.
Se $[a]_m\cdot[x]_m=[1]_m$, allora $ax \equiv 1 \pmod m$, che è equivalente a scrivere $ax = 1+km$, con k intero. Da questo abbiamo che

$$ax-km=1,$$

quindi MCD$(a,m)=1$.
Viceversa, se MCD$(a,m)=1$, allora esistono due interi s,t tali che $1=sa+tm$, quindi

$$[1]_m = [sa]_m+[tm]_m = [sa]_m = [s]_m\cdot[a]_m$$

e ponendo $\beta=[s]_m$ abbiamo che $\beta=\alpha^{-1}$.
Inoltre β è unico perché se ne esistessero due, per le proprietà delle classi di congruenze, devono coincidere.
Se p è un primo, allora ogni intero non divisibile per p è relativamente primo con p, da cui

Corollario.
Se p è primo, ogni elemento di $\mathbf{Z}_p$ diverso da zero è invertibile.

La nuova formulazione del teorema di Fermat diventa:

Teorema di Fermat. Sia p primo. Se $\alpha\in\mathbf{Z}_p$, allora

$$\alpha^p=\alpha.$$

Se $\alpha\neq0$, abbiamo che $\alpha^{p-1}=1$.

L'insieme $\mathbf{Z}_m$ con le operazioni di addizione e moltiplicazione è una struttura chiamata *anello commutativo*.