Aritmetica modulare

Prof. Giuseppe Caputo

Congruenze

Iniziamo da alcune nozioni di base.

Definizione: Assegnati gli interi $a, b \in \mathbb{Z}$, dire che a divide b oppure che b è un multiplo di a, vuol dire che esiste un intero $c \in \mathbb{Z}$ tale che $b = a \cdot c$. Se usiamo il simbolo $a|b$ per indicare che a divide b (da non confondere col simbolo di frazione), ciò si sintetizza in

$$a|b \overset{def}{\Longleftrightarrow} b = a \cdot c, \quad con\ c \in \mathbb{Z} \text{ opportuno intero}$$

Tra i divisori di un intero a vi sono i divisori banali a, -a, 1, -1, potendo in genere esserci degli altri.

Definizione:Un intero $p \in \mathbb{Z}$ non nullo e diverso dall'unità positiva o negativa si dice primo se i suoi unici divisori sono quelli banali.

Definizione: Si dice che due interi non nulli $a, b \in \mathbb{Z}$ hanno l'intero $d \in \mathbb{Z}$ per massimo comun divisore, se d è un divisore comune di a e b, nel senso che divide entrambi, inoltre tra i divisori c comuni di a, b, d è il massimo ovvero il più grande, significando questo che d è multiplo di ogni divisore comune c di a, b. In simboli, se a,b,c$\in \mathbb{Z}$

$$\begin{cases} 1)\ d|a \wedge d|b \\ 2)\ c|a \wedge c|b \Rightarrow c|d \end{cases}$$

Per indicare il M.C.D.(a,b) di due interi a e b, useremo la notazione (a,b) da non con fondersi con il simbolo di coppia ordinata. E' ovvio che se d è il massimo comun divisore di a,b allora anche – d lo è.

Definizione: Due interi $a, b \in \mathbb{Z}$ si dicono relativamente primi o primi tra loro o coprimi se (a,b)=1, ovvero se il loro massimo comun divisore è l'unità, per cui a e b non hanno divisori comuni propri (cioè diversi dall'unità).

E' ovvio che coppie di numeri primi sono anche relativamente primi avendosi (p,q) = 1, ma non è detto che se due numeri sono relativamente primi allora sono primi, come nel caso di (4,9) =1, dove 4 e 9 non sono primi. Vale il seguente,

Teorema fondamentale dell'Aritmetica (scomposizione in fattori primi)

Se $n \in \mathbb{Z} - \{0, -1, 1\}$ allora se t $\in \mathbb{N}$ vale ed è unica la scomposizione di n in fattori primi

$$n = \mp p_1^{\alpha_1} \cdot p_2^2 \cdot \ldots \cdot p_t^{\alpha_t},$$

dove i fattori $p_1^{\alpha_1}, p_2^2, \ldots, p_t^{\alpha_t}$del prodotto sono numeri interi primi positivi.

Nota: Si definisce minimo comune multiplo di due interi a,b, e si indica col simbolo [a,b], un multiplo comune ai due interi che risulta il più piccolo dei multipli comuni nel senso che è sottomultiplo di tutti i multipli comuni ad a e b.

Lemma di Euclide: Se $n, a, b \in \mathbb{Z}$ sono tre interi non nulli, si ha che n, dividendo il prodotto ab, risulta primo con a, allora necessariamente n divide b, cioè

$$\mathbf{n|ab, (n, a) = 1 \Rightarrow n|b}$$

Teorema di Euclide: Se il numero primo p$\in \mathbb{Z}$ divide il prodotto ab con $a \neq b \in \mathbb{Z}$, allora p deve dividere almeno uno dei due fattori a,b, cioè

$$\mathbf{p|ab, p\ primo \Rightarrow p|a \vee p|b}$$

Da questo segue che se p divide il prodotto di più interi $a_1, a_2, \dots, a_n$, con $n \in \mathbb{N}$, allora p divide almeno uno dei fattori a_i, $(i = 1,2, \dots, n)$

Dimostrazione: Se p è primo, allora, essendo $a \neq b$, si ha che o p è primo con a, oppure p è primo con b, ma, dividendo il prodotto per ipotesi, non può essere contemporaneamente primo con entrambi , perché per il lemma di Euclide, se p è primo con uno dei due interi a o b, dividendo il prodotto ab, necessariamente deve dividere l'altro, e ciò prova la prima parte del teorema. Considerato ora il prodotto $a_1 \cdot a_2 \cdot \dots \cdot a_n$, con $n \in \mathbb{N}$, associamo le parentesi con due elementi alla volta in modo che possiamo applicare iterativamente la prima parte del teorema. Allora, in $n-1$ passi, p dividendo il prodotto $(a_i) \cdot (a_{i+1} \cdot \dots \cdot a_n)$, con $(i = 1,2, \dots, n-1)$, p divide o il primo fattore oppure il secondo, conseguendone che p deve dividere almeno uno dei fattori a_i.

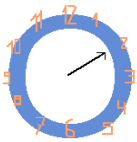
Proposizione: Si ha che n$\in \mathbb{Z}$ è primo col prodotto ab se e solo se n è primo sia con a che con b,

$$\mathbf{(n, ab) = 1 \Leftrightarrow (n, a) = 1 \wedge (n, b) = 1}$$

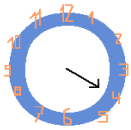
Dimostrazione: La condizione è necessaria perché se n è primo con ab, allora essendo $(n, ab) = 1$, n non ha fattori comuni con ab e quindi né con a né con b, donde $(n, a) = 1$ e $(n, b) = 1$, per cui n risulta primo sia con a che con b. La condizione è sufficiente perché, supposto n primo sia con a che con b, per cui $(n, a) = 1$ e $(n, b) = 1$, se per assurdo n non fosse primo col prodotto ab, allora dovrebbe aversi $(n, ab) \neq 1$ e quindi esistere un numero primo p tale che $p|n$ e $p|ab$. In particolare allora si avrebbe che $p|a$ oppure $p|b$, per cui p sarebbe un fattore comune sia alla scomposizione di n che a quella di a o di b, contro il fatto che per ipotesi n è primo sia con a che con b. Di qui l'asserto.

L'orologio di Gauss

Circa duecento anni fa, K.F.Gauss introdusse i concetti base dell'aritmetica modulare. Se la lancetta delle ore di un orologio punta sulle due:



12 ore dopo, la lancetta punta sempre sulle 2 (abbiamo fatto un giro completo). Quindi aggiungere 12 non cambia niente al numero delle ore:



2 + 12 = 2.

I matematici, per indicare che stanno contando le ore su un orologio a 12 ore, scrivono:

2 + 12 = 2 (mod 12) oppure $\mathbf{2 + 12 \equiv 2 (\ mod\ 12\ )}$

(da ora in poi useremo questa seconda notazione).

Anzi, se facciamo un numero qualsiasi, n, di giri, la lancetta punterà sempre sulle 2:

$$2 + 12n \equiv 2 (\text{mod } 12)$$

Invece 14 ore dopo la lancetta punterà sulle 4:

Strano però perchè: 2 + 14 = 16 e non 4?!

In realtà non è cosi strano perchè: 2 + 14 = 2 + (2 + 12) = (2 + 2) + 12 = 4 + 12 = 4 (mod 12)

Stiamo contando "modulo 12"

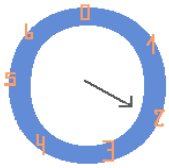
Se aggiungiamo 47, cosa succedde?

Per vederlo si divide 47 per 12: 47 = 3·12 + 11. Aggiungere 47 è come aggiungere 11, quindi: 11 + 2 = 13,

ma 13 = 1 + 12. Finalmente 47 + 2 = 1 (mod 12).cioè

47+2=3·12+11+2=3·12+12+1=4·12+1=1(mod 12)

Vediamo che per il numero delle ore, quello che importa non è il numero n ma il suo resto nella divisione per 12. Ci sono 12 resti possibili: 0, 1, 2, ..., 11. Sono le ore dell'orologio (12 = 0 (mod 12))



Altri orologi.

Possiamo considerare orologi con un numero diverso di ore, ecco, per esempio, un <u>orologio con 7 ore</u> (come <u>i giorni della settimana</u>)

Con questo orologio: 2 + 20 = 1 (mod 7)

Scriviamo (mod 7) per indicare che stiamo usando un orologio con 7 ore.

Infatti: 20 = 2·7 + 6 = 6 (mod 7) e 2 + 6 = 8 = 1 (mod 7)

(Se 1 = Lunedi, 2 = Martedi, ..., 0 = Domenica e se aggiungo 20 giorni a un Martedi, viene un Lunedi.,poiché 20+2=2·7+6+2=2·7+7+1=3·7+1=1(mod 7))

<u>Esercizio</u>: se oggi è mercoledì 6 dicembre, in quale giorno della settimana è Natale?

<u>Risposta</u>:

Sommando 25 - 6 = 19 giorni a 3 = mercoledì , si ha 3+19 =22 = 3·7+1, da cui 22 = 1 (mod 7) essendo rest(22,7) = 1, quindi essendo 1 = lunedì, si ha che Natale viene di lunedì.

Chiaramente possiamo considerare orologi con un numero n qualsiasi di ore.

Per riassumere:

- La scrittura $\boldsymbol{a \equiv b\ (mod\ n)}$ significa che a e b hanno lo stesso resto nella divisione per n (dopo avere aggiunto a ore, la lancetta dell'orologio con n ore punterà alla stessa ora che se io avessi aggiunto b ore). Dire che a e b hanno lo stesso resto nella divisione per n significa che a-b è divisibile per n (a = kn+r , $k \in \mathbb{Z}$, b=tn+r, $t \in \mathbb{Z}$ dove $0 \le r < n$ 0≤r<n, quindi a-b=n(k-t))
- Dire che $\boldsymbol{a \equiv r\ (mod\ n)}$, con 0≤ r <n, è equivalente a dire che a è della forma a = kn+r (un multiplo di n più r).

Precisiamo:

<u>Definizione</u> : Si dice che due interi **a,b∈ℤ** sono **<u>congrui modulo n</u>** e si scrive

$$\mathbf{a \equiv b\ (mod\ n)}$$

se la loro differenza è un multiplo di n, ovvero se esiste un opportuno intero

q∈ℤ tale che risulti

$$\boldsymbol{a - b = q \cdot n.}$$

Se ciò non si verifica i due interi a,≢b si dicono <u>incongrui modulo n</u> e si scrive

$$\boldsymbol{a \not\equiv b\ (mod\ n)}$$

Nell'insieme ℤ dei numeri interi **<u>la congruenza è una relazione di equivalenza</u>**. poiché si prova facilmente che gode delle proprietà

1) <u>riflessiva:</u> $a \equiv a(\mathrm{mod}\, n)$.∀a∈ℤ

Infatti $\exists 0 \in \mathbb{Z} / a - a = 0 \cdot n. \Rightarrow n/a - a \Rightarrow a \equiv a(mod\ n)$

2) <u>simmetrica:</u> $a \equiv b(\mathrm{mod}\, n) \Rightarrow b \equiv a(\mathrm{mod}\, n)$.∀a,b∈ℤ

Infatti $a \equiv b(mod\ n) \Rightarrow n/a - b \Rightarrow n/b - a \Rightarrow b \equiv a(mod\ n)$,per la proposizione7 pag.1 cap I

3) <u>transitiva:</u> $a \equiv b(\mathrm{mod}\ n), b \equiv c(\mathrm{mod}\ n) \Rightarrow a \equiv c(\mathrm{mod}\ n)$.∀a,b,c∈ℤ

Infatti
$a \equiv b(mod\ n) \wedge b \equiv c(mod\ n) \Rightarrow n/a - b \wedge n/b - c \Rightarrow a - b = k \cdot n \wedge b - c = h \cdot n, k, h \in \mathbb{Z} \Rightarrow a - c = a - b - (b - c) = k \cdot n - h \cdot n = (k - h) \cdot n \Rightarrow n/a - c.$

Per quello che riguarda le classi di equivalenza diremo dopo,osservando che ci possiamo limitare a considerare congruenze solo per n≥0 poiché $a \equiv b\ (mod\ n) \Leftrightarrow a - b = \mathrm{n} \cdot \mathrm{q} = (-\mathrm{n})(-\mathrm{q}) = (-\mathrm{n})\mathrm{q}' \Leftrightarrow \mathrm{a} \equiv \mathrm{b}\ (\mathrm{mod}\ -\mathrm{n})$, inoltre è immediato verificare che $a \equiv b(\mathrm{mod}\, n) \Leftrightarrow (-a) \equiv (-b)(\mathrm{mod}\, n)$.

Indicato con rest(a,n) il resto della divisione di a per n, si ha

Proposizione: **Se $a \in \mathbb{Z}, n \in \mathbb{N}$, si ha**

$$\mathbf{a \equiv rest(a,n)\ (mod\ n)}$$

Dimostrazione:

Per il teorema della divisione pag.5 cap. I dividendo a per n, si ha che $\exists q \in \mathbb{Z}\ /\ a = q \times n + rest(a,n), 0 \leq rest(a,n) < n \Rightarrow a - rest(a,n) = q \times n \Rightarrow a \equiv rest(a,n)(mod\ n)$

Per semplificare la notazione di congruenza modulo n, da ora in poi invece di scrivere $a \equiv b (\text{mod}\, n)$, scriveremo semplicemente $a \equiv b$ salvo i casi in cui tale notazione abbreviata possa generare confusione.

E' fondamentale la seguente

Proposizione:

$$\mathbf{a \equiv b\ (mod\ n) \Leftrightarrow rest\ (a,n) = rest\ (b,n)}$$

Dimostrazione:

La condizione è necessaria perché se $a \equiv b$, da $a \equiv rest(a,n)$ e $b \equiv rest(b,n)$,segue ,applicando la

proprietà simmetrica e transitiva, che

$[rest(a,n) \equiv a] \wedge [a \equiv b] \wedge [b \equiv rest(b,n)] \Rightarrow rest(a,n) \equiv rest(b,n) \Leftrightarrow rest(a,n) - rest(b,n) = kn, k \in \mathrm{Z}$
.

intero opportuno, da cui si ha:

$[0 \leq rest(a,n) < n] \wedge [0 \leq rest(b,n) < n] \Rightarrow [0 \leq rest(a,n) - rest(b,n) < n] \Rightarrow [0 \leq kn < n, k \in \mathrm{Z}] \Rightarrow k = 0 =$

$\Rightarrow rest(a,n) - rest(b,n) = 0 \Rightarrow rest(a,n) = rest(b,n)$.

Viceversa la condizione è sufficiente poiché,dall' ipotesi e per la proprietà simmetrica e transitiva ,si ha

$[rest(a,n) = rest(b,n)] \wedge [a \equiv rest(a,n)] \wedge [b \equiv rest(b,n)] \Rightarrow [rest(a,n) = rest(b,n)] \wedge [a \equiv rest(a,n)] \wedge$

$\wedge [rest(b,n) \equiv b] \Rightarrow [a \equiv rest(a,n)] \wedge [rest(a,n) \equiv b] \Rightarrow a \equiv b$.

Proposizione1: $\mathbf{a \equiv b \pmod{n} \Rightarrow k + a \equiv k + b \pmod{n} \wedge ka \equiv kb \pmod{n}, \forall k \in \mathbb{Z}}$

Dimostrazione: Si ha $k + a \equiv k + b \pmod{n}$ osservando che $(k + a) - (k + b) = a - b$; analogamente si ha $ka \equiv kb \pmod{n}$ poiché $ka - kb = k(a - b)$.

Osservazione: In generale per la moltiplicazione non vale l'implicazione opposta che risulta valere solo quando k ed n sono relativamente primi. Infatti si ha:

Proposizione2: $\mathbf{ka \equiv kb \pmod{n}, \ (k,n) = 1 \Rightarrow a \equiv b \pmod{n}}$

Dimostrazione: $ka \equiv kb \pmod{n}, M.C.D.(k,n) = 1 \Rightarrow n|ka - kb \Rightarrow n|k(a - b) \Rightarrow n|a - b \Rightarrow a \equiv b \pmod{n}$

La proposizione seguente mostra che la relazione di congruenza risulta chiusa sia rispetto alla somma che al prodotto, come vedremo in modo più approfondito tra breve.

Proposizione3:

$$\mathbf{a \equiv b \pmod{n} \wedge a' \equiv b' \pmod{n} \Rightarrow a + a' \equiv b + b' \pmod{n} \wedge a \cdot a' \equiv b \cdot b' \pmod{n}}$$

Dimostrazione:

Per la proposizione1 $a \equiv b \pmod{n} \Rightarrow a + a' \equiv b + a' \pmod{n}$ e $a' \equiv b' \pmod{n} \Rightarrow a' + b \equiv b' + b \pmod{n} \Rightarrow b + a' \equiv b + b' \pmod{n} \Rightarrow a + a' \equiv b + b' \pmod{n}$ per la proprietà transitiva. Analogamente $a \equiv b \pmod{n} \Rightarrow a \cdot a' \equiv b \cdot a' \pmod{n}$ e $a' \equiv b' \pmod{n} \Rightarrow a' \cdot b \equiv b' \cdot b \pmod{n} \Rightarrow b \cdot a' \equiv b \cdot b' \pmod{n} \Rightarrow a \cdot a' \equiv b \cdot b' \pmod{n}$.

Proposizione4: $a \equiv b \pmod{n} \Rightarrow a^m \equiv b^m \pmod{n}, \forall m \in \mathbb{N}$

Dimostrazione: Ragioniamo per induzione. Per $m = 1$ il teorema è ovviamente vero. Se il teorema è vero per $m \in \mathbb{N}$, si ha che vale anche per m+1. Infatti, applicando la proposizione3 $a \equiv b \pmod{n} \Rightarrow a^m \equiv b^m \pmod{n} \Rightarrow a^m a \equiv b^m b \pmod{n} \Rightarrow a^{m+1} \equiv b^{m+1} \pmod{n}$. Un'altra dimostrazione è la seguente: $a \equiv b (mod\ n) \Leftrightarrow a - b = nn, l \in \mathbb{Z}$, ora $a^n - b^n = (a^{n-1} + ba^{n-2} + \cdots + ab^{n-2} + b^{n-1}) = (nl)r = (lr)n = vn, v, r \in \mathbb{Z} \Rightarrow a^n \equiv b^n \pmod{n}$.

Proposizione4 bis: Se $n \in \mathbb{Z}$-$\{0\}$ la proposizione precedente si inverte

$$a^m \equiv b^m \pmod{n}, \forall m \in \mathbb{N} \Rightarrow a \equiv b (mod\ n).$$

Dimostrazione: Stante l'ipotesi, si ha la tesi per m = 1.

Proposizione5: $\mathbf{a \equiv b \pmod{n} \Rightarrow a \cdot m \equiv b \cdot m \pmod{n \cdot m}, \forall m \in \mathbb{N}}$

Dimostrazione:

$a \equiv b \pmod{n} \Rightarrow a - b = n \cdot q, q \in \mathbb{Z} \Rightarrow m \cdot a - m \cdot b = (n \cdot m)q \Rightarrow a \cdot m \equiv b \cdot m \pmod{n \cdot m}$.

Proposizione6: $\mathbf{a \equiv b \pmod{n}, m \mid n \Rightarrow a \equiv b \pmod{m}}$

Dimostrazione: $a \equiv b \pmod{n} \Rightarrow a - b = n \cdot q, q \in \mathbb{Z}, m|n \Rightarrow n = m \cdot h, h \in \mathbb{Z} \Rightarrow a - b = n \cdot q = m(h \cdot q) \Rightarrow a \equiv b \pmod{m}$.

Proposizione7: Se $k \in \mathbb{Z}$, $\mathbf{ka \equiv kb \pmod{n} \Rightarrow a \equiv b \left(\mathrm{mod}\ \frac{n}{(k,n)}\right)}$

Dimostrazione: Posto $d =. (k, n)$, $ka \equiv kb \pmod{n} \Rightarrow k(a - b) = n \cdot q \Rightarrow a - b = \frac{nq}{k} \in \mathbb{Z} \Rightarrow k|nq$,

perchè k, essendo un divisore del 1°membro, deve dividere anche il secondo, per cui $\frac{nq}{k} \Leftrightarrow k|n \vee k|q$

è un intero e quindi anche $\frac{n}{d}\frac{dq}{k} \in \mathbb{Z}$ e $\frac{n}{d} \in \mathbb{Z}$, $\frac{dq}{k} \in \mathbb{Z}$ ($\frac{dq}{k} = \frac{(sk + tn)q}{k} = sq + t\frac{nq}{k} \in \mathbb{Z}$ applicando il teorema pag.6 cap.I).Allora posto q' = $\frac{dq}{k} \in \mathbb{Z}$, si ha a-b = $\frac{nq}{k} = \frac{n}{d}\frac{dq}{k} = q'\frac{n}{d} \Rightarrow a \equiv b(\mathrm{mod}\frac{n}{d})$

Osservazione: Se M.C.D.(k,n) = 1, si ritrova la proposizione 2.

Proposizione7:

Se per $k,n \in \mathbb{Z}$ e $k|n$, allora si ha $ka \equiv kb(\mathrm{mod}\, n) \Leftrightarrow a \equiv b(\mathrm{mod}\frac{n}{k})$

Dimostrazione: $ka \equiv kb \pmod{n} \Leftrightarrow k(a - b) = n \cdot q \Rightarrow a - b = \frac{n}{k}q \Leftrightarrow a \equiv b\,\mathrm{mod}(\frac{n}{k})$

Proposizione8: $\boldsymbol{a \equiv b \pmod{n} \wedge a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{n \cdot m}}$

Dimostrazione:

La condizione è necessaria poiché $\begin{cases} a \equiv b \pmod{n} \Leftrightarrow a - b = nk, k \in \mathbb{Z} \\ a \equiv b \pmod{m} \Leftrightarrow a - b = mh, h \in \mathbb{Z} \end{cases} \Rightarrow \begin{cases} n|a - b \\ m|a - b \end{cases}$ per cui, essendo n e m entrambi fattori della scomposizione di $a - b$, deve esistere un opportuno intero $t \in \mathbb{Z}$ tale che $a - b = (nm)t \Rightarrow a \equiv b \pmod{n \cdot m}$ **.** Viceversa la condizione è pure sufficiente in quanto se $a \equiv b \pmod{n \cdot m}$, allora $a - b = (nm)t$, da cui $a - b = n(mt) = nk \Rightarrow a \equiv b \pmod{n}$ e $a - b = m(nt) = mh \Rightarrow a \equiv b \pmod{m}$.

Un po' di teoria

Arrivati a questo punto ci proponiamo di introdurre nell'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ una struttura algebrica simile a quella di $\mathbb{Z}$ (+,×), cioè quella che abbiamo nell'insieme $\mathbb{Z}$ rispetto all'ordinaria addizione e moltiplicazione tra interi..

In sostanza si tratta di definire in $\mathbb{Z}/n\mathbb{Z}$ un'operazione di somma e di prodotto tra classi, ovvero di definire un'applicazione $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$di modo che si abbia $[x]_{Z/nZ} + [y]_{Z/nZ} = [x+y]_{Z/nZ}$ e $[x]_{Z/nZ} \bullet [y]_{Z/nZ} = [x \cdot y]_{Z/nZ}$, con tali classi univocamente determinate.

Il problema consiste nel fatto che se si cambia il rappresentante delle classi, cioè al posto di $[x]_{Z/nZ}$ scriviamo $[x']_{Z/nZ}$, con x'∈ $[x]_{Z/nZ}$ e al posto di $[y]_{Z/nZ}$ scriviamo $[y']_{Z/nZ}$, con y'∈ $[y]_{Z/nZ}$, risulti che $[x+y]_{Z/nZ} = [x'+y']_{Z/nZ}$ ed analogamente $[x \cdot y]_{Z/nZ} = [x' \cdot y']_{Z/nZ}$ perché altrimenti al cambiare del rappresentante delle classi cambierebbe la somma ed il prodotto delle classi e non sarebbe univocamente determinato il risultato delle operazioni.tra le classi.

Ricordiamo quindi che se $\mathcal{S}(\perp)$ è una struttura algebrica rispetto all'operazione binaria univoca interna ⊥ e Σ una relazione di equivalenza in $\mathcal{S}$, l'operazione **<u>⊥ si può trasportare al quoziente $\mathcal{S}/\Sigma$</u>** ,ovvero **<u>Σ è compatibile con ⊥</u>** o **<u>Σ è una congruenza</u>**, se

$\forall x,y,x',y' \in \mathcal{S}$ fissati si ha $[x' \equiv x \ (mod\ \Sigma)] \wedge [y' \equiv y \ (mod\ \Sigma)] \Longrightarrow x' \perp y' \equiv x \perp y \ (mod\ \Sigma)$.

Ciò vuol dire che se gli elementi x e x' appartengono ad una stessa classe $[x]_\Sigma$ ed y e y' ad una stessa classe $[y]_\Sigma$, allora il composto x⊥y ed il composto x'⊥y' devono appartenere ad una stessa classe che possiamo indicare con il simbolo $[x \perp y]_\Sigma = [x]_\Sigma \perp [y]_\Sigma$;in questo modo un qualsiasi elemento della classe $[x]_\Sigma$ composto con un qualsiasi elemento della classe $[y]_\Sigma$ dà sempre come risultato un elemento che si trova in una stessa classe d'equivalenza, in genere distinta dalle precedenti, che possiamo prendere quindi come composta delle due classi precedenti. In sintesi $x' \in [x]_\Sigma \wedge y' \in [y]_\Sigma \Longrightarrow x' \perp y' \in [x \perp y]_\Sigma$. .Ha perciò quindi senso la scrittura di composizione tra classi $[x \perp y]_\Sigma = [x]_\Sigma \perp [y]_\Sigma$ .e questa risulta l'unica classe che contiene tutti gli elementi che si hanno componendo un qualunque elemento della prima classe con un qualunque elemento della seconda classe, inoltre tale definizione risulta indipendente dai particolari elementi scelti nelle classi e dipende solo dalle classi stesse.

Si dimostra che tutte e sole le congruenze Σ sono compatibili (a destra e a sinistra) con l'operazione ⊥, nel senso che se due elementi sono congruenti, allora sono ancora congruenti gli elementi ottenuti componendo (a destra e a sinistra) entrambi tali elementi con uno stesso elemento e viceversa, in simboli $x \equiv y \Leftrightarrow x \perp z \equiv y \perp z, \wedge\ z \perp x \equiv z \perp y$, $\forall z \in \mathcal{S}$. o in maniera equivalente $[x]_\Sigma = [y]_\Sigma \Leftrightarrow [x \perp z]_\Sigma = [y \perp z]_\Sigma = [z \perp x]_\Sigma = [z \perp y]_\Sigma$ .Infatti la condizione è necessaria perché se Σ è una

congruenza deve aversi $\forall x,y,z \in S$, $x \equiv y \wedge z \equiv z \Longrightarrow x \perp z \equiv y \perp z \Rightarrow \Sigma$ è compatibile a destra ed analogamente $z \equiv z \wedge x \equiv y \Longrightarrow z \perp x \equiv z \perp y \Rightarrow \Sigma$ è compatibile a sinistra .Viceversa se Σ è compatibile a destra e a sinistra , deve aversi per la compatibilità a destra $x \equiv x' \Rightarrow x \perp y \equiv x' \perp y$ e per la compatibilità a sinistra $y \equiv y' \Rightarrow x' \perp y \equiv x' \perp y'$.Per la proprietà transitiva dell'equivalenza si ha $x \perp y \equiv x' \perp y \wedge x' \perp y \equiv x' \perp y' \Longrightarrow x \perp y \equiv x' \perp y'$. Si è quindi provato che $\forall x,x',y,y' \in S$, se $x \equiv x'$ e $y \equiv y'$ allora $x \perp y \equiv x' \perp y'$cioè Σ è una congruenza.

Dobbiamo quindi dimostrare che <u>la relazione $n\mathbb{Z}$ di congruenza in $\mathbb{Z}$ è compatibile sia con la somma che con il prodotto in $\mathbb{Z}$.</u> Infatti è **compatibile con la somma** poiché $\boldsymbol{x \equiv x'(mod\ n)} \wedge \boldsymbol{y \equiv y'(mod\ n)} \Rightarrow x - x' = hn \wedge y - y' = kn \Longrightarrow x - x' + y - y' = (h+k)n \Longrightarrow x + y - (x' + y') = (h+k)n \Longrightarrow \boldsymbol{x + y \equiv x' + y'(mod\ n)}$, ed è **compatibile con il prodotto** in quanto si ha $\mathbf{x} \equiv \boldsymbol{x'(mod\ n)} \wedge \boldsymbol{y \equiv y'(mod\ n)} \Rightarrow x - x' = hn \wedge y - y' = kn \Longrightarrow x = x' + hn \wedge y = y' + kn \Rightarrow xy = (x' + hn)(y' + kn) = x'y' + x'kn + y'hn + hkn^2 = x'y' + (x'k + y'h + hkn)n \Longrightarrow xy - x'y' = (x'k + y'h + hkn)n \Longrightarrow \boldsymbol{xy \equiv x'y'\ (mod\ n)}$. Ciò equivale a

$$[x]_n = [\boldsymbol{x'}]_{\boldsymbol{n}} \wedge [\boldsymbol{y}]_{\boldsymbol{n}} = [\boldsymbol{y'}]_{\boldsymbol{n}} \Rightarrow [x+y]_n = [\boldsymbol{x'} + \boldsymbol{y'}]_{\boldsymbol{n}} \wedge [xy]_n = [\boldsymbol{x'y'}]_{\boldsymbol{n}}.$$

Si ha così che $\mathbb{Z}/_{n\mathbb{Z}}(+,\bullet)$ è una struttura algebrica che, come $\mathbb{Z}$ (+), risulta <u>un gruppo abeliano rispetto all'addizione</u>, valendo le proprietà:di facile verifica.

- <u>Associativa</u>: $([x]_n + [y]_n) + [z]_n = [x]_n + ([y]_n + [z]_n)$
- <u>Commutativa</u> : $[x]_n + [y]_n = [y]_n + [x]_n$
- <u>Esistenza dell'elemento neutro</u>: $\exists!\ [0]_n \in \mathbb{Z}/_{n\mathbb{Z}} / [x]_n + [0]_n = [0]_n + [x]_n = [x]_n$
- <u>Esistenza dell'opposto</u> $\forall [x]_n \in \mathbb{Z}/_{n\mathbb{Z}}, \exists!\ [-x]_n = -[x]_n \in \mathbb{Z}/_{n\mathbb{Z}} / [x]_n + [-x]_n = [-x]_n + [x]_n = [0]_n$

Per quanto riguarda <u>il prodotto $\mathbb{Z}/_{n\mathbb{Z}}(+,\bullet)$ è un gruppoide</u> o semigruppo abeliano, perché non esiste l'inverso di ogni elemento valendo solo le proprietà anch'esse di facile verifica

- <u>Associativa</u>: $([x]_n \bullet [y]_n) \bullet [z]_n = [x]_n \bullet ([y]_n \bullet [z]_n)$
- <u>Commutativa</u> : $[x]_n \bullet [y]_n = [y]_n \bullet [x]_n$
- <u>Esistenza dell'elemento neutro</u>: $\exists!\ [1]_n \in \mathbb{Z}/_{n\mathbb{Z}} / [x]_n \bullet [1]_n = [1]_n \bullet [x]_n = [x]_n$

Poiché, come in $\mathbb{Z}$ (+,•), vale anche la <u>proprietà distributiva del prodotto rispetto alla somma</u> tra classi, $[x]_n \bullet ([y]_n + [z]_n) = [x]_n \bullet [y]_n + [x]_n \bullet [z]_n$, si ha che <u>$\mathbb{Z}/_{n\mathbb{Z}}(+,\bullet)$ è un anello</u>. Infatti . $[x]_n \bullet ([y]_n + [z]_n) = [x]_n \bullet [y+z]_n = [x(y+z)]_n = [xy + xz]_n = [xy]_n + [xz]_n = [x]_n \bullet [y]_n + [x]_n \bullet [z]_n$

<u>Proposizione</u>: **Le classi di equivalenza di $\mathbb{Z}/_{n\mathbb{Z}}$ sono tante quanti i possibili resti della divisione di interi per n, cioè le n classi $[0]_n$, $[1]_n$, $[2]_n$,…, $[n-1]_n$**

Dimostrazione:

Infatti poiché $\forall x \in \mathbb{Z}\ 0 \leq rest(x,n) < n$, si hanno gli n interi 0,1,2,…,n-1, per cui se h,k sono due tra essi, con k<h, si ha 0<h-k<n e quindi h-k non è un multiplo di n essendo minore di n. Risulta allora $k \not\equiv h\ (mod\ n) \Rightarrow [k]_n \neq [h]_n \Longrightarrow [0]_n \neq [1]_n \neq [2]_n \neq, \dots, \neq [n-1]_n$ .ossia tutte queste classi sono distinte. Sono poi le sole classi di congruenza poiché, se per assurdo esistesse una classe $[x]_n$ con $x \in \mathbb{Z}$ distinta dalle precedenti, essendo $x \equiv rest(x,n)\ (mod\ n), con\ 0 \leq rest(x,n) < n$, si ha $[x]_n = [rest(x,n)]_n$ ovvero la classe $[x]_n$ risulta una delle precedenti classi, contro l'ipotesi.

Proposizione: $\forall k \in \mathbb{Z}$ fissato, ogni classe $[k]_n, [k+1]_n, \dots, [k+n-1]_n$ coincide con una ed una sola delle classe di resti modulo n $[0]_n$, $[1]_n$, $[2]_n$,…, $[n-1]_n$, in modo equivalente, per ogni intero k fissato, un qualsiasi intero è congruente modulo n ad uno ed uno solo degli interi del sistema dei residui modulo n {k, k+1,…,k+n-1}.

Dimostrazione: Poiché $\forall a \in \mathbb{Z}$ si ha, in base alla proposizione precedente, che a è un elemento di una ed una sola tra le classi $[0]_n$, $[1]_n$, $[2]_n$,…, $[n-1]_n$, segue che si ha una ed una sola tra le eventualità $a \equiv 0(mod\ n), a \equiv 1(mod\ n), \dots, a \equiv n-1(mod\ n)$, da cui, in base alla proposizione1 pag.6, segue che si ha una ed una sola tra le eventualità $a+k \equiv k(mod\ n), a+k \equiv k+1(mod\ n), \dots, a+k \equiv k+n-1(mod\ n)$, per cui posto t = a+k$\in \mathbb{Z}$ si ha che t è un elemento di una ed una sola tra le classi distinte di interi incongrui modulo n $[k]_n, [k+1]_n, \dots, [k+n-1]_n$, cioè t è congruo ad uno ed uno solo tra gli interi k, k+1,…,k+n-1.

Sistema dei minimi residui modulo n

Per ottenere il sistema dei minimi residui(relativi) modulo n consideriamo due casi:

1. Il modulo n della congruenza è dispari. In tale caso n-1 è pari, quindi divisibile per 2 per cui si ha $\frac{n-1}{2} \in \mathbb{Z}$. Allineando gli n termini, si ha

$$..0 \quad 1 \dots\dots\dots\dots\dots\dots \frac{n-1}{2} \dots\dots\dots\dots n\text{-}1$$

$$*\dots\dots \frac{n-1}{2} \text{ termini}\dots\dots *\dots \frac{n-1}{2} \text{ termini}\dots\dots *.$$

Da cui traslando verso sinistra di $\frac{n-1}{2}$ termini dopo lo 0, si ricava

$$-\frac{n-1}{2}\ldots\ldots\ldots\text{-1}\quad 0\quad 1\ldots\ldots\ldots\frac{n-1}{2}$$

.....n termini.....

Per cui posto $k=-\frac{n-1}{2}$, si ha sostituendo nel sistema k, k+1,…,k+n-1, si ha

$\{-\frac{n-1}{2},\ldots,-1,0,1,\ldots,\frac{n-1}{2}\}=\{0,\pm1,\ldots,\pm\frac{n-1}{2}\}$ <u>sistema dei minimi residui modulo n con n dispari.</u>

Ad esempio per n = 7 si ha {-3,-2,-1,0,1,2,3}

2) <u>Il modulo n della congruenza è pari</u>. In tale caso n-1 è dispari, quindi $\frac{n}{2}\in\mathbb{Z}$. Allineando gli n termini, si ha..0 $1\ldots\ldots\ldots\ldots\frac{n}{2}-1\quad\frac{n}{2}\ldots\ldots\ldots\ldots$n-1

... $\frac{n}{2}$ termini..... *... $\frac{n}{2}$ termini.....*.

E traslando verso sinistra di $\frac{n}{2}-1$ termini dopo lo 0 si ricava

$$-\frac{n}{2}+1\ldots\ldots\text{-1}\quad 0\quad 1\ldots\ldots\ldots\frac{n}{2}$$

... $\frac{n}{2}$ termini.......... $\frac{n}{2}$ termini...*

per cui si ha il <u>sistema dei minimi residui modulo n con n pari</u>

$$\{-\frac{n}{2}+1,-\frac{n}{2}+2,\ldots,-1,0,1,\ldots,\frac{n}{2}-1,\frac{n}{2}\}$$

Ad esempio per n = 8 si ha {-3,-2,-1,0,1,2,3,4}.

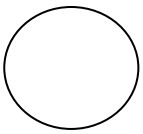
Per concludere: L'aritmetica dell'orologio è (più o meno) come quella usuale in cui possiamo sommare e moltiplicare gli interi,bisogna però dire che certe volte queste operazioni si comportano in modo strano...

<u>Definizione</u>:Una struttura algebrica A(+,•) è un **anello** se:1) A(+) è un gruppo abeliano.2)A(•) è un monoide.3) vale la proprietà distributiva del prodotto rispetto alla somma.

Operazioni con l'aritmetica dell'orologio.

Orologio mod 0

L'anello $\mathbb{Z}/o\mathbb{Z}(+,\bullet) = \{[n]_0, n\in\mathbb{Z}\}$



Orologio con zero ore.(mod 0)

Per n=0 la relazione diviene $a \equiv b(\mathrm{mod}\,0) \Leftrightarrow a-b=k\times 0=0 \Rightarrow a=b$ *,per cui la congruenza modulo zero si riduce alla relazione di eguaglianza tra interi.Si avranno di conseguenza tante classi di equivalenza quanti sono gli interi ,* $[a]_0=\{x\in\mathbb{Z}/x=a\}=\{a\}$*.Quindi* $\mathbb{Z}/o\mathbb{Z}=\{\{a\},a\in\mathbb{Z}\}$*.*

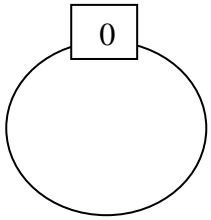
L'anello $\mathbb{Z}/1\mathbb{Z}(+,\bullet) = \{[0]_1\} = \mathbb{Z}$

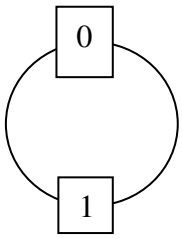
Orologio con un' ora.(mod 1)

Per n=1 la relazione diviene $a \equiv b(\mathrm{mod}\,1) \Leftrightarrow a-b=k\times 1=k, k\in \mathrm{Z}$ *,detta* <u>*relazione totale*</u> *essendo ciò possibile per ogni coppia di interi* $a,b\in\mathbb{Z}$*.ottenendosi un'unica classe di equivalenza* $[0]_1=\mathbb{Z}$ *per cui l'insieme quoziente è* $\mathbb{Z}/1\mathbb{Z}=\{\mathbb{Z}\}$*. Si hanno le seguenti tavole di addizione e moltiplicazione poiché* $[0]_1 + [0]_1 = [0+0]_1 = [0]_1$ e $[0]_1 \bullet [0]_1 = [0\bullet 0]_1 = [0]_1$

+	$[0]_1$	•	$[0]_1$
$[0]_1$	$[0]_1$	$[0]_1$	$[0]_1$

Orologio mod 1





L'anello $\mathbb{Z}/2\mathbb{Z}(+,\bullet) = \{[0]_2, [1]_2\}$

$x,y\in\mathbb{Z}$, $x\equiv y \pmod 5 \Leftrightarrow x-y=5h$, $h\in\mathbb{Z}$

Orologio con due ore.(mod 2)

Prendiamo un orologio con due ore: 0 e 1. (Abbiamo scritto 0 e 1 invece di 1 e 2 perchè i possibili resti nella divisione per 2 sono 0 e 1. Se facciamo la somma delle ore con questo orologio viene:

$0 + 0 \equiv 0 \pmod 2$	$1 + 0 \equiv 0 + 1 \equiv 1 \pmod 2$	$1 + 1 \equiv 0 \pmod 2$	ovvero
$[0]_2 + [0]_2 = [0]_2$	$[1]_2 + [0]_2 = [0]_2 + [1]_2 = [1]_2$	$[1]_2 + [1]_2 = [0]_2$	

Tutto regolare tranne l'ultima uguaglianza, ma se guardiamo all'orologio, anche questa torna. Analizziamo più in profondità. Per n = 2 *la relazione diviene* $a \equiv b \pmod 2 \Leftrightarrow a - b = k \times 2 = 2k, k \in \mathbb{Z}$, per cui due interi sono congrui modulo due se la loro differenza è un numero pari. Ora, essendo un numero pari del tipo 2k, $k\in\mathbb{Z}$, e un numero dispari del tipo 2k+1, si ha che la differenza di due numeri pari è un numero pari in quanto 2k-2h=2(k-h), $h-k\in\mathbb{Z}$, la differenza tra due dispari è un pari avendosi 2k+1-(2h+1)=2(k-h), mentre è banale verificare che la differenza tra un pari e un dispari e viceversa è un dispari per cui, indicato con $\mathcal{P}$ l'insieme dei numeri pari e con $\mathcal{D}$ quello dei dispari, si ha che vale l'equivalenza $(a,b\in \mathrm{P}) \vee (a,b\in D) \Leftrightarrow a \equiv b \pmod 2$ .Ne consegue che in $\mathbb{Z}$ vi sono solo due classi di congruenza modulo due, la classe dei numeri pari e la classe dei numeri dispari e quindi l'insieme quoziente è $\mathbb{Z}/2\mathbb{Z}=\{[0]_2,[1]_2\}=\{\mathcal{P},\mathcal{D}\}$,.dove $[0]_2 = \mathrm{P}, [1]_2 = D$ perché $a\in\mathcal{P}\Leftrightarrow a=2k\Longrightarrow a-0=2k\Leftrightarrow$ ---$a\equiv 0 \pmod 2 \Leftrightarrow a\in[0]_2$ e $[1]_2=\mathcal{D}$ perché $a\in\mathcal{D}\Leftrightarrow a=2k+1\Leftrightarrow a-1=2k\Leftrightarrow a\equiv 1 \pmod 2\Leftrightarrow a\in[1]_2$.

Allora: <u>a≡ 0 (mod 2) se e solo se n è pari; invece a≡1 (mod 2) se e solo se a è dispari.</u>la somma di due numeri pari è un numero pari (cioè $0+0\equiv 0 \pmod 2$)-la somma di un numero pari e di un numero dispari è un numero dispari (cioè $1+0\equiv 1 \pmod 2$)-la somma di due numeri dispari è un numero pari (cioè $1+1\equiv 0 \pmod 2$). Possiamo riassumere la legge dell'addizione dei numeri dell'orologio con due ore (congruenze degli interi modulo 2) con

+	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

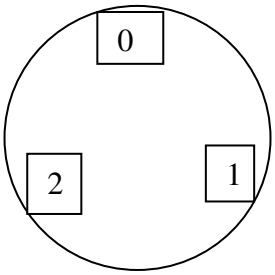
Passiamo ora alla moltiplicazione. Abbiamo: $0 \bullet 0 \equiv 0 \pmod 2$, $1 \bullet 0 = 0 \bullet 1 \equiv 0 \pmod 2$ e $1 \bullet 1 \equiv 1 \pmod 2$

Infatti il prodotto di due numeri pari è un numero pari; il prodotto di un numero pari con un numero dispari è un numero pari; il prodotto di due numeri dispari è un numero dispari.

Abbiamo quindi la seguente tabella per la moltiplicazione:

•	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

Orologio mod 3



L'anello $\mathbb{Z}/3\mathbb{Z}(+,\bullet) = \{[0]_3,[1]_3,[2]_3\}$

$x,y\in\mathbb{Z}$, $x\equiv y \pmod 3 \Leftrightarrow x-y=3h$, $h\in\mathbb{Z}$

Orologio con tre ore.(mod 3)

+	$[0]_3$	$[1]_3$	$[2]_3$	•	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$	$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$	$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$	$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

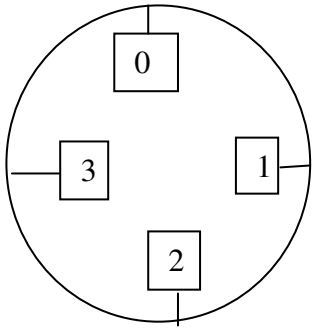
$\mathbb{Z}/3\mathbb{Z}(+)$ è un gruppo abeliano,valendo le quattro proprietà come si verifica facilmente, mentre poiché ogni elemento non nullo ha inverso, si ha che $\mathbb{Z}/3\mathbb{Z}$-{0}(•) è un gruppo abeliano.Si noti che 3 è numero primo.

L'anello $\mathbb{Z}/4\mathbb{Z}(+,\bullet) = \{[0]_4, [1]_4, [2]_4, [3]_4\}$

.

Orologio con quattro ore

$x,y\in\mathbb{Z}$, $x\equiv y \pmod 4 \Leftrightarrow x-y=4h$, $h\in\mathbb{Z}$



Questa volta il nostro orologio ha quattro ore: 0, 1, 2, 3 (sono i possibili resti nella divisione per 4) .Abbiamo: $0+0 \equiv 0 \pmod 4 \Leftrightarrow [0]_4 + [0]_4 = [0]_4$; $0+1 \equiv 1 \pmod 4 \Leftrightarrow [0]_4 + [1]_4 = [1]_4$ $0+2 \equiv 2 \pmod 4 \Leftrightarrow [0]_4 + [2]_4 = [2]_4$; $0+3 \equiv 3 \pmod 4 \Leftrightarrow [0]_4 + [3]_4 = [3]_4$; e poi: $1+1 \equiv 2 \pmod 4 \Leftrightarrow$; $[1]_4 + [1]_4 = [2]_4$ $1+2 \equiv 3 \pmod 4 \Leftrightarrow [1]_4 + [2]_4 = [3]_4$; $1+3 \equiv 0 \pmod 4 \Leftrightarrow [1]_4 + [3]_4 = [0]_4$, $2+2 \equiv 0 \pmod 4 \Leftrightarrow$. $[2]_4 + [2]_4 = [0]_4$. Si noti che: $1+3 \equiv 0 \pmod 4$ e $2+2 \equiv 0 \pmod 4$. Infatti 1+3 = 4 e il resto nella divisione di 4 per 4 è 0. Stessa cosa per 2+2. Si ha quindi la seguente tabella

+	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Infatti guardiamo alla tabella dell'addizione modulo 4:

$[0]_4 + [0]_4 = [0+0]_4 = [0]_4$, $[0]_4 + [1]_4 = [0+1]_4 = [1]_4$, si noti però che $[3]_4 + [1]_4 = [3+1]_4 = [4]_4 = [rest(4,4)]_4 = [0]_4$ e così $[2]_4 + [3]_4 = [5]_4 =$

$[rest\ (5,4)]_4 = [1]_4$

Vediamo che grazie proprio a queste stranezze, l'addizione verifica due proprietà che la solita addizione (con numeri interi positivi e negativi) verifica, cioè:

- esiste lo zero 0 (cioè $[0]_4$) che verifica:

$n + 0 = 0 + n = n$ per ogni numero n (cioè $[n]_4 + [0]_4 = [n+0]_4 = [n]_4$) (aggiungere 0 non cambia nulla, si dice che 0 , cioè$[0]_4$, è "elemento neutro" per l'addizione)

- per ogni numero n esiste un numero -n tale che: $n + (-n) = (-n) + n = 0$,cioè $\forall n\in\mathbb{Z}, \exists -n\in\mathbb{Z} / [n]_3 + [-n]_4 = [n+(-n)]_4 = [0]_4$, per cui si dice che –n, cioè $[-n]_4$ è il "simmetrico" di n, ovvero $[n]_4$, per l'addizione. Per esempio -2 è il simmetrico di 2 (e 2 è il simmetrico di -2,cioè $[-2]_4$ è il simmetrico di $[2]_4$.

Anche i nostri numeri dell'orologio con 4 ore godono di queste proprietà:

- l'elemento neutro è sempre lo zero. $[0]_4$

- ogni elemento ha un simmetrico: il simmetrico di 1 è 3 (e viceversa), ossia il simmetrico di $[1]_4$ è $[3]_4$ poiché $[1]_4 + [3]_4 = [0]_4$, il simmetrico di 2 è 2, cioè il simmetrico di $[2]_4$ è $[2]_4$ poiché $[2]_4 + [2]_4 = [0]_4$.

Siccome i nostri numeri, cioè le classi di congruenza, come quelli "normali", verificano le proprietà:

- per ogni n e per ogni m: n + m = m + n ("commutatività"), ossia $[m]_4 + [n]_4 = [n]_4 + [m]_4$

- per ogni n, per ogni m e per ogni t: t + (n +m) = (t + n) + m ("associatività"), ovvero $[t]_4 +([n]_4 + [m]_4) = ([t]_4 + [n]_4) +[m]_4$

Allora, malgrado (o grazie) alle sue stranezze, l'addizione dei numeri congrui modulo 4 è

strutturalmente *uguale* a quella dei numeri interi

Attenzione!!!

Le cose non vanno così con la moltiplicazione

La tabella della moltiplicazione dei numeri modulo 4 è

•	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$\mathbf{[0]_4}$	$\mathbf{[0]_4}$	$\mathbf{[0]_4}$	$\mathbf{[0]_4}$
$[1]_4$	$\mathbf{[0]_4}$	$\mathbf{[1]_4}$	$\mathbf{[2]_4}$	$\mathbf{[3]_4}$
$[2]_4$	$\mathbf{[0]_4}$	$\mathbf{[2]_4}$	$\mathbf{[0]_4}$	$\mathbf{[2]_4}$
$[3]_4$	$\mathbf{[0]_4}$	$\mathbf{[3]_4}$	$\mathbf{[2]_4}$	$\mathbf{[1]_4}$

Abbiamo che in $\mathbb{Z}/4\mathbb{Z}$ **non vale la legge di annullamento del prodotto**

$$\forall a,b\in\mathbb{Z},\ a\bullet b = 0, \Rightarrow (a = 0) \vee (b = 0)$$

Infatti : **$2 \bullet 2 \equiv 0 \pmod 4$**$\Leftrightarrow$ $[2]_4 \bullet [2]_4 = [2 \bullet 2]_4 = [4]_4 = [\mathrm{rest}(4,4)]_4 = [0]_4$ .Gli elementi come . $[2]_4$ diversi dallo zero $[0]_4$ il cui prodotto è lo zero $[0]_4$,prendono il nome di <u>divisori dello zero</u>.Inoltre <u>non tutti gli elementi hanno l'inverso</u> perché, pur se per la classe $[3]_4$ c'è l'inverso avendosi $[3]_4 \bullet [3]_4 = [1]_4$,ossia esiste un'altra classe che composta con l'operazione di prodotto con la classe data è uguale alla classe elemento neutro $[1]_4$,e così pure per $[1]_4$, per la classe $[2]_4$ non esiste alcuna classe che moltiplicata per classe $[2]_4$ dia per risultato $[1]_4$.

<u>**Nota**</u>:

Nell'insieme **Q** dei razionali abbiamo che: per ogni frazione o intero $n \neq 0$, esiste $1/n$ tale che: $n \bullet (1/n) = 1$ Se $n = a/b$ è una frazione, allora $1/n = b/a$). Come per la somma dei numeri interi positivi e negativi, la moltiplicazione conferisce alle frazioni (escluso 0) una struttura di "gruppo" rispetto alla moltiplicazione usuale dove l'elemento neutro è $1 = 1/1$; il simmetrico di n è $1/n$..

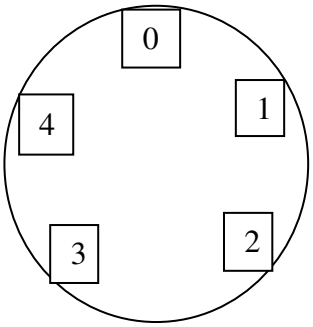
La moltiplicazione <u>NON</u> conferisce una struttura di "gruppo" ai numeri modulo 4 (escluso lo 0), perchè 3 ha un simmetrico avendosi $3 \bullet 3 \equiv 1 \pmod 4$) ma 2 non ha simmetrico cioè inverso..

<u>Questa volta c'è una differenza strutturale</u>, ben illustrata dal fatto che $2 \bullet 2 \equiv 0 \pmod 4$, cioè vi sono divisori dello zero (d'altra parte se $[2]_4$ avesse un simmetrico,$[\bar{2}]_4$, si avrebbe da un lato $[\bar{2}]_4 \bullet ([2]_4 \bullet [2]_4) = [\bar{2}]_4 \bullet [4]_4 = [\bar{2}]_4 [0]_4 = [\bar{2} \bullet 0]_4 = [0]_4$, e dall'altro $[\bar{2}]_4 \bullet ([2]_4 \bullet [2]_4) = ([\bar{2}]_4 \bullet [2]_4) \bullet [2]_4 = [\bar{2} \bullet 2]_4 \bullet [2]_4 = [1]_4 \bullet [2]_4 = [1 \bullet 2]_4 = [2]_4$ donde $[2]_4 = [0]_4$, assurdo)..

Si noti che 4 non è numero primo.

L'anello $\mathbb{Z}/5\mathbb{Z}(+,\bullet) = \{[0]_5,[1]_5,[2]_5,[3]_5,[4]_5\}$

Orologio con cinque ore



$x,y\in\mathbb{Z}$, $x\equiv y \pmod 5 \Leftrightarrow x-y=5h$, $h\in\mathbb{Z}$

Avendosi

$[2]_5 \bullet [3]_5 = [2\bullet 3]_5 = [6]_5 = [rest(6,5)]_5 = [1]_5$

$[2]_5 \bullet [4]_5 = [2\bullet 4]_5 = [8]_5 = [rest(8,5)]_5 = [3]_5$

$[3]_5 \bullet [3]_5 = [3\bullet 3]_5 = [9]_5 = [rest(9,5)]_5 = [4]_5$ *ecc.*

La struttura $\mathbb{Z}/5\mathbb{Z}(+,\bullet)$ gode della proprietà che ogni suo elemento non nullo è simmetrizzabile , ovvero invertibile nella moltiplicazione, mentre in $\mathbb{Z}(\bullet)$ ciò non avviene in quanto $\forall x\in\mathbb{Z}, x\neq 1, \nexists\, x'\in\mathbb{Z}/xx'=1$ (solo 1 e-1 sono invertibili).

Infatti si ha: $[1]_5 \bullet [1]_5 = [1]_5$, $[2]_5 \bullet [3]_5 = [1]_5$, $[3]_5 \bullet [2]_5 = [1]_5$, $[4]_5 \bullet [4]_5 = [1]_5$.

Quindi, eccetto $[0]_5$.,per cui non esiste un elemento $x\in \mathbb{Z}/5\mathbb{Z}$ tale che $[0]_5 \bullet [x]_5 = [1]_5$, tutti gli elementi sono invertibili in. $\mathbb{Z}/5\mathbb{Z}$.

Si verifica facilmente che $\mathbb{Z}/5\mathbb{Z}(+)$ è un gruppo abeliano, mentre $\mathbb{Z}/5\mathbb{Z}(\bullet)$ è solo un monoide commutativo. dotato di elemento neutro $[1]_5$.Invece è un gruppo abeliano $\mathbb{Z}/5\mathbb{Z}-\{0\}(\bullet)$.

Si noti che 5 è numero primo.

Si ha la seguente tavola

+	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	•	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Orologio mod n

Orologi con n ore. L'anello $\mathbb{Z}/n\mathbb{Z}(+,\bullet) = \{ [0]_n , [1]_n , [2]_n ,[3]_n ,\ldots,[n-1]_n \}$

$x,y\in\mathbb{Z}$, $n\in\mathbb{Z}$, $x\equiv y \pmod n \Leftrightarrow x-y=nh$, $h\in\mathbb{Z}$

Come già detto possiamo considerare orologi con un numero (intero) n, qualsiasi di ore. Il nostro orologio avrà n ore: 0, 1, 2, ..., (n-1) (sono i resti possibili nella divisione per n). Non è troppo difficile convincersi che per l'addizione le cose vanno sempre bene (il simmetrico, cioè l'opposto di 1 è n-1; quello di 2, n-2; quello di 3, n-3; ecc...).

Per la moltiplicazione possono esserci dei problemi. poiché la moltiplicazione si comporta "bene", cioè tutti gli elementi non nulli sono invertibili e non vi sono divisori dello zero (in ogni riga corrispondente a x ≠0 compare 1). se e solo se n è un numero primo.

A titolo d'esempio vedi la tabella della moltiplicazione per i numeri modulo 3 e modulo5.

Utile per gli sviluppi ulteriori è la seguente proposizione.

<u>Proposizione</u>: Consideriamo <u>l'equazione congruenziale</u>

$$\mathbf{kx \equiv h \pmod{n}}$$

nell'incognita $x \in \mathbb{Z}$ e $k,h,n \in \mathbb{Z}$, M.C.D.(k,n)=1, ossia k ed n siano relativamente primi. In tali ipotesi si ha che tutte e sole le soluzioni dell' equazione sono interi congrui tra loro modulo n, ovvero se $\bar{x} \in \mathbb{Z}$ è una soluzione particolare, la soluzione generale è la classe $[\bar{x}]_n$.

<u>Nota1</u>: L'equazione si può studiare nell'ipotesi più generale che M.C.D.(k,n) $\neq 1$.

<u>Dimostrazione</u>:

Detto $\mathbb{S} = \{\bar{x} \in \mathbb{Z} / k\bar{x} \equiv h \pmod{n}\}$ l'insieme delle soluzioni, si ha che $\mathbb{S} \neq \emptyset$, cioè $\exists\, \bar{x} \in \mathbb{Z} / k\bar{x} \equiv h$ (mod n). A questo scopo consideriamo i possibile resti della divisione di interi per n, ossia l'n-pla 0,1,…,n-1, che sappiamo essere tutti incongrui tra loro modulo n, e che moltiplichiamo per k ottenendo l'n-pla 0,k,…,(n-1)k. Ora osserviamo che la compatibilità della congruenza con il prodotto ci assicura che $x \equiv y \Rightarrow ax \equiv ay$ ma ciò non si inverte poiché $ax \equiv ay$ $\Longrightarrow$x≡y potendosi avere x≡y, quindi non possiamo subito dire che i numeri dell'n-pla 0,k,…,(n-1)k sono incongrui tra loro modulo n. Ragionando per assurdo, se $\exists\, kx', ky' \in \{0, k, \ldots, (n-1)k\} / kx' \equiv ky' (mod\ n), con\ \ x', y' \in \{0,1, \ldots, n-1\}$, per la compatibilità rispetto alla somma si avrebbe $kx' \equiv ky' (mod\ n) \Rightarrow kx' - ky' \equiv ky' - ky' = 0\ (mod\ n) \Rightarrow k(x' - y') \equiv 0\ (mod\ n) \Rightarrow k(x' - y') = hn, h \in \mathbb{Z} \Rightarrow n / k(x' - y') \Rightarrow n/(x'-y')$, essendo (n,k) =1$\Rightarrow x' - y' = nc, c \in \mathbb{Z} \Rightarrow x' \equiv y' (mod\ n)$, assurdo poiché i resti 0,1,…,n-1 sono tra loro incongrui modulo n. Abbiamo provato che gli interi 0,k,…,(n-1)k sono tra loro incongrui modulo n.. Ricordando che numeri congrui tra loro hanno uguali resti, dividendo per n gli interi 0,k,…,(n-1)k, devono ottenersi in corrispondenza resti distinti che dovranno quindi necessariamente coincidere con i soli possibili resti 0,1,…,n-1.della divisione di interi per n. Ora dividendo h per n si ottiene $h = nq + rest\ (h,n),\ 0 \leq rest(h,n) < n \Longrightarrow \exists\, k\bar{x} \in \{0,k,\ldots,(n-1)k\},\ \bar{x} \in \{0,1,\ldots,n-1\} / rest\ (k\bar{x}, n) = rest\ (h,n) \Rightarrow k\bar{x} \equiv h\ (mod\ n) \Longrightarrow \mathbb{S} \neq \emptyset$.

Proviamo infine che $\mathbb{S} = [\bar{x}]_n$ Si ha $\mathbb{S} \subseteq [\bar{x}]_n$ poiché $\forall y \in \mathbb{S} \Rightarrow ky \equiv h\ (mod\ n)$, ma d'altra parte $k\bar{x} \equiv h$ (mod n), per la proprietà simmetrica e transitiva segue che $ky \equiv k\bar{x}\ (mod\ n)$, e quindi per la compatibilità rispetto alla somma $k\bar{x} - ky \equiv 0\ (mod\ n) \Longrightarrow k(\bar{x} - y) \equiv 0\ (mod\ n) \Longrightarrow$

$k(\bar{x} - y) = nq, q \in \mathbb{Z} \Longrightarrow n \nmid (\bar{x} - y)$, poiché

$(k,n) = 1 \Longrightarrow \bar{x} - y = nc, c \in \mathbb{Z} \Longrightarrow \bar{x} \equiv y \ (mod\ n) \Longrightarrow y \in [\bar{x}]_n$.

Si ha $[\bar{x}]_n \subseteq \mathbb{S}$ in quanto $\forall y \in [\bar{x}]_n . \Longrightarrow y \equiv \bar{x} \ (mod\ n) \Longrightarrow ky \equiv k\bar{x} \ (mod\ n)$, per la compatibilità rispetto al prodotto. Ma , essendo $\bar{x}$ soluzione dell'equazione congruenziale, si

$ha\ k\bar{x} \equiv hh \ (mod\ n)$ e quindi per la proprietà transitiva, $ky \equiv k\bar{x} \ (mod\ n) \wedge k\bar{x} \equiv h \ (mod\ n) \Longrightarrow ky \equiv h \ (mod\ n) \Longrightarrow y \in \mathbb{S}$.

Si conclude allora che $\mathbb{S} = [\bar{x}]_n$.

<u>Nota2</u>:

Poiché M.C.D.(k,n) = 1, per la proposizione a pag.25 la classe $[k]_n$ è invertibile$\Rightarrow \exists [k']_n \in \mathbb{Z}/n\mathbb{Z} \wedge [k]_n \bullet [k']_n = [1]_n \Leftrightarrow [k \bullet k']_n = [1]_n \Leftrightarrow k\ k' \equiv 1 \ (mod\ n)$, quindi l'equazione $kx \equiv h \ (mod\ n)$ ha come soluzione un'unica classe modulo n che si trova moltiplicando per k' ambo i membri, $kx \equiv h \Rightarrow k'kx \equiv k'h (mod\ n) \Rightarrow x \equiv k'h (mod\ n)$. Per la determinazione dell'inverso della classe $[k]_n$, vedere la nota pag.19.

Studiamo ora l'equazione nell'ipotesi più generale che il coefficiente a dell' incognita x ed il modulo n della congruenza non siano primi tra loro. A tale scopo se a,b∈ℤ, n∈ℕ, d = M.C.D.(a,n) ≠1,si ha il seguente teorema:

<u>Teorema</u>: Se a,b∈ℤ, n∈ℕ, **d = M.C.D.(a,n) ≠1, l'equazione congruenziale lineare**

$$\boxed{\mathbf{ax \equiv b \ (mod\ n)}}$$

ammette soluzioni x∈ℤ se e solo se d | b. Se ciò si verifica, detta $x_0 \in \mathbb{Z}$ una soluzione, rappresentano la soluzione generale dell'equazione tutti e soli gli elementi della classe completa di congruenza modulo $\frac{n}{d}$, $[x_0]_{\frac{n}{d}}$ = { $x_0 + h\frac{n}{d}, \forall h \in \mathbb{Z}$}, anzi risultando che

$[x_0]_{\frac{n}{d}} = \bigcup_{h \in Z} [x_0 + h\frac{n}{d}, \forall h \in Z]_n$ **, tutte e sole le soluzioni dell'equazione sono distribuite nelle d classi distinte di resti modulo n,** $[x_0]_n, [x_0 + \frac{n}{d}]_n, [x_0 + 2\frac{n}{d}]_n, \ldots, [x_0 + (d-1)\frac{n}{d}]_n$ **, i cui rappresentanti sono interi incongrui modulo n.**

Nota: Nel caso d = 1, si ha come caso particolare il teorema precedente, riducendosi le classi ad una sola classe di congruenza modulo n poiché $[x_0]_n = [x_0 + hn]_n$ ∀ h∈{0,1,…,d-1} in quanto $x_0 \equiv x_0 + hn (\mathrm{mod}\, n)$ poiché $x_0 - (x_0 + hn) = -hn = nq$ per $q = -h$.

Dimostrazione:

La condizione è necessaria.

Infatti se esiste una soluzione $x_0 \in \mathbb{Z}$, allora deve aversi a x_0 ≡ b (mod n), per cui ∃q∈ℤ tale che a x_0 - b = nq⇒ a x_0 - nq = b. Ora il primo membro dell'eguaglianza è divisibile per d poiché, essendo d il massimo comun divisore di a ed n, in particolare d è un divisore comune di a ed n, allora d deve dividere, per la proposizione8 pag.2 cap.I, anche una qualsiasi combinazione lineare di a ed n, quindi si ha d|a,d|n⇒d|(a x_0 -nq)⇒d|b, pertanto anche b è divisibile per d.
Viceversa la condizione è sufficiente.

Supposto allora che d|b⇔∃c∈ℤ/b = cd, per il teorema pag.6 cap. I si ha che esistono almeno due interi s,t∈ℤ,quindi s e –t, tali che il massimo comun divisore d si possa esprimere come combinazione lineare tramite essi, cioè d = sa – tn, da cui, moltiplicando tale eguaglianza per l'intero c∈ℤ (per ipotesi d|b), si ha cd = a(sc)-(tc)n, ma cd = b. quindi sostituendo a(sc)-(tc)n = b, e ponendo x_0 = sc, h = tc, segue a x_0 -b = hn⇔ a x_0 ≡ b (mod n), ovvero x_0 è soluzione dell'equazione.

Abbiamo quindi dimostrato che, nell'ipotesi che d|b, esiste almeno una soluzione particolare

x_0 dell' equazione congruenziale ax≡b (mod n) per cui si verifica $ax_0 \equiv b (\mathrm{mod}\, n)$.

Proviamo adesso che, tutti e soli gli elementi della classe $[x_0]_{\frac{n}{d}}$ sono soluzione dell'equazione ax≡b (mod n). Infatti tutti gli elementi della classe $[x_0]_{\frac{n}{d}}$ sono soluzione dell'equazione ax≡b (mod n)

perché se x∈$[x_0]_{\frac{n}{d}}$, allora x≡ x_0 (mod $\frac{n}{d}$)⇒∃h∈ℤ/x- x_0 = h $\frac{n}{d}$, da cui, moltiplicando per a∈ℤ, segue

a(x- x_0) = ($\frac{a}{d}h$) n⇔ax - a x_0 = h'n, dove h'= $\frac{a}{d}h \in \mathbb{Z}$ essendo $\frac{a}{d} \in \mathbb{Z}$, donde si ha ax ≡ a x_0 (mod n).
Allora poiché x_0 è soluzione dell'equazione, deve aversi a x_0 ≡ b (mod n) e quindi per la proprietà

transitiva segue ax ≡ b (mod n), cioè x è una soluzione dell'equazione.

Gli elementi della classe $[x_0]_{\frac{n}{d}}$ sono pure i soli ad essere soluzioni dell'equazione ax ≡ b (mod n)

perché, se ξ è una soluzione dell'equazione, per cui si verifica che aξ≡ b (mod n) e $\xi \notin [x_0]_{\frac{n}{d}} \Leftrightarrow \xi \not\equiv$

x_0 (mod $\frac{n}{d}$), da a $x_0 \equiv$ b(mod n) segue per la proprietà transitiva che a$\xi \equiv$ a x_0 (mod n) $\Rightarrow \exists$k$\in\mathbb{Z}$ / a(ξ- x_0) = kn $\Rightarrow \frac{a}{d}(\xi - x_0) = k\frac{n}{d} \Rightarrow \frac{n}{d} | (\xi - x_0)$ in quanto $\frac{n}{d}$ dividendo il prodotto $\frac{a}{d}(\xi - x_0)$ ed essendo primo con $\frac{a}{d}$ per la proposizione pag.5 cap.I, per il corollario2 pag.8 cap.I deve dividere l'altro fattore. Allora da $\frac{n}{d} | (\xi - x_0) \Rightarrow \xi - x_0 = h\frac{n}{d}$, h$\in\mathbb{Z} \Rightarrow \xi \equiv x_0$ (mod $\frac{n}{d}$), contro l'ipotesi.

Proviamo ora che $[x_0]_{\frac{n}{d}} = \{ x_0 + h\frac{n}{d}, \forall h \in \mathbb{Z}\}$, ovvero che se x_0 è una soluzione dell'equazione, allora ogni intero del tipo $x_0 + h\frac{n}{d}$ al variare di h in $\mathbb{Z}$ è pure una soluzione. Infatti si ha che x$\in$ $[x_0]_{\frac{n}{d}} \Leftrightarrow$ x$\equiv x_0$ (mod $\frac{n}{d}$) $\Leftrightarrow \exists$h$\in\mathbb{Z}$/x- $x_0 = h\frac{n}{d} \Leftrightarrow$ x = $x_0 + h\frac{n}{d}$.

Nell'ipotesi non restrittiva che h≥0 (per h<0 si hanno le stesse classi di –h>0), proviamo infine che $[x_0]_{\frac{n}{d}} = \bigcup_{h\in \mathrm{N}} [x_0 + h\frac{n}{d}]_n$ nei casi h<d e h≥d.

Se 0≤h<d⇒h∈{0,1,2,…,d-1}, allora, poiché $[x_0]_{\frac{n}{d}} = \{ x_0 + h\frac{n}{d}, \forall h \in \mathbb{Z}/0 \le h < d \}$, si ha

$[x_0]_{\frac{n}{d}} \subseteq \bigcup_{0\le h<d} [x_0 + h\frac{n}{d}]_n$ poiché ∀x∈$[x_0]_{\frac{n}{d}}$

$$x = x_0 + h\frac{n}{d}, h = 0,1,..d-1 \Rightarrow (x\in[x_0]_n) \vee \left(x\in[x_0 + \frac{n}{d}]_n \right) \vee \left(x\in[x_0 + 2\frac{n}{d}]_n \right) \vee ... \vee \left(x\in[x_0 + (d-1)\frac{n}{d}]_n \right) \Rightarrow x \in \bigcup_{0\le h<d} [x_0 + h\frac{n}{d}]_n$$

Ed anche $[x_0]_{\frac{n}{d}} \supseteq \bigcup_{0\le h<d} [x_0 + h\frac{n}{d}]_n$ da cui $[x_0]_{\frac{n}{d}} = \bigcup_{0\le h<d} [x_0 + h\frac{n}{d}]_n$ poiché

$$\forall x \in \bigcup_{0\le h<d} [x_0 + h\frac{n}{d}]_n \Rightarrow (x \in [x_0]_n) \vee \left(x \in [x_0 + \frac{n}{d}]_n \right) \vee ... \vee \left(x \in [x_0 + (d-1)\frac{n}{d}]_n \right) \Rightarrow$$

$$(x \equiv x_0 (\mathrm{mod}\, n)) \vee \left(x \equiv x_0 + \frac{n}{d} (\mathrm{mod}\, n) \right) \vee ... \vee \left(x \equiv x_0 + (d-1)\frac{n}{d} (\mathrm{mod}\, n) \right) \Rightarrow$$

$$(x - x_0 = h_0 n) \vee \left(x - (x_0 + \frac{n}{d}) = h_1 n \right) \vee ... \vee \left(x - (x_0 + (d-1)\frac{n}{d}) = h_{d-1} n \right) \Rightarrow$$

$$(x = x_0 + h_0 n) \vee \left(x = x_0 + h_1 n + \frac{n}{d} \right) \vee ... \vee \left(x = x_0 + h_{d-1} n + (d-1)\frac{n}{d} \right)$$ e poiché si ha

$$x_0 + h_0 n \equiv x_0 (\text{mod}\,\frac{n}{d}) \Leftrightarrow x_0 + h_0 n - x_0 = k_0 \frac{n}{d}, k_0 = h_0 d$$

$$x_0 + h_1 n + \frac{n}{d} \equiv x_0 (\text{mod}\,\frac{n}{d}) \Leftrightarrow x_0 + h_1 n + \frac{n}{d} - x_0 = k_1 \frac{n}{d}, k_1 = h_1 d + 1$$

.....

$$x_0 + h_{d-1} n + (d-1)\frac{n}{d} \equiv x_0 (\text{mod}\,\frac{n}{d}) \Leftrightarrow x_0 + h_{d-1} n + \frac{n}{d} - x_0 = k_{d-1} \frac{n}{d}, k_{d-1} = h_{d-1} d + 1$$

segue che $x \in [x_0]_n$.

Se invece h≥d, dividendo h per d si ha h = qd + r, 0≤r<d, quindi

$\forall x \in [x_0]_{\frac{n}{d}} \Leftrightarrow x = x_0 + h\frac{n}{d} = x_0 + (qd + r)\frac{n}{d} = x_0 + qn + r\frac{n}{d} \equiv x_0 + r\frac{n}{d}$ (mod n)

(poiché si ha che

$x_0 + qn + r\frac{n}{d} - (x_0 + r\frac{n}{d}) = qn) \Leftrightarrow x \equiv x_0 + h\frac{n}{d}$ (mod n), $r \in \{0,1,\dots,d-1\} \Leftrightarrow$

$x \in \bigcup_{h \geq d} [x_0 + h\frac{n}{d}]_n$. Si è quindi provato che $[x_0]_{\frac{n}{d}} = \bigcup_{h \in Z} [x_0 + h\frac{n}{d}]_n = \bigcup_{h=0}^{d-1} [x_0 + h\frac{n}{d}]_n$ ossia che l'unione

$\bigcup_{h \in Z} [x_0 + h\frac{n}{d}]_n$ si riduce all'unione $\bigcup_{h=0}^{d-1} [x_0 + h\frac{n}{d}]_n$ di classi che devono necessariamente essere distinte.

Per provare ciò è sufficiente far vedere che gli interi $x_0, x_0 + \frac{n}{d}, \dots, x_0 + (d-1)\frac{n}{d}$ sono due a due

incongrui modulo n. Presi 0≤h'≤h≤d-1, se per assurdo si avesse $[x_0 + h\frac{n}{d}]_n = [x_0 + h'\frac{n}{d}]_n$, allora

$$x_0 + h\frac{n}{d} \equiv x_0 + h'\frac{n}{d} (\text{mod}\, n) \Rightarrow \exists k \in \text{N} / x_0 + h\frac{n}{d} - (x_0 + h'\frac{n}{d}) = kn \Rightarrow (h - h')\frac{n}{d} = kn \Rightarrow h - h' = kd$$

cioè h-h' è un multiplo positivo di d, contro il fatto che $0 \leq h - h' \leq h < d$, assurdo.

Così il teorema è completamente provato.

.**<u>Nota</u>**:

<u>Per</u> <u>risolvere</u> <u>l'equazione</u> ax ≡ b (mod n) si procede nel modo seguente:

1. usare l'algoritmo esteso di Euclide per determinare d,s,t∈ℤ / d = M.C.D.(a,n) = sa + tn (vedi cap. I pag.7).

2. controllare che d | b, altrimenti non ci sono soluzioni.

3. d | b⇔b = dc = (sa + tn)c = asc + tnc ⇒ a(sc) – b = (tc)n ⇒ a(sc) ≡ b(mod n)⇒ x_0 = sc è una soluzione particolare, dove $c = \frac{b}{d}$.

4. la soluzione generale è la classe $[x_0]_{\frac{n}{d}} = [sc]_{\frac{n}{d}}$ di tutti gli $x \in \mathbb{Z}$ / $x \equiv x_0 \pmod{\frac{n}{d}} \Rightarrow$

$x \equiv sc \pmod{\frac{n}{d}} \Leftrightarrow x - sc = h\frac{n}{d}, h \in \mathbb{Z} \Leftrightarrow x = sc + h\frac{n}{d}$, al variare di $h \in \mathbb{Z}$.

5. Quindi la soluzione generale si esprime come la classe $[x_0]_{\frac{n}{d}} = \{x_0 + h\frac{n}{d}, \forall h \in \mathbb{Z}\} = \bigcup_{h=0}^{d-1} [x_0 + h\frac{n}{d}]_n$ unione di d classi modulo n.

Esempio 1: l'equazione congruenziale $6x \equiv 3 \pmod{15}$ ha soluzioni perché, in base al teorema pag.19, posto a = 6, b = 3, n = 15, d = M.C.D.(6,15) = 3, si ha che $d|b \Leftrightarrow 3|3$, e poiché $d|b \Leftrightarrow b = dc$, $3|3 \Leftrightarrow 3 = 3 \cdot 1$, segue c = 1 In base al teorema pag.6 cap. I con l'algoritmo euclideo delle divisioni successive determiniamo due interi s e t tali che d =sa+tn, che nel nostro caso diviene 3 = 6s+15t ovvero 2s+5t =1(si noti che questa è un'equazione diofantea del tipo ax+by = c studiata a pag.12 cap.I, che ammette soluzioni in $\mathbb{Z}$ se e solo se M.C.D.(a,b)|c, il che nel nostro caso si verifica). Le divisioni successive per determinare il M.C.D.(2,5) = 1 sono 5 = $2 \cdot 2+1$, 2 = $2 \cdot 1+0$, da cui si ottiene 1 = 2(-2)+5 $\cdot$ 1$\Rightarrow$ s = -2, t = 1. Quindi una soluzione particolare dl'equazione è x_0 = s $\cdot$ c = -2 $\cdot$ 1 = -2. Infatti sostituendo si ha $6(-2) \equiv 3 \pmod{15} \Rightarrow -12 \equiv 3 \pmod{15}$ il che è vero avendosi -12-3 = 15q$\Rightarrow$ -15 =15q per q = -1.Ora $[-2]_{15} = [13]_{15}$ poichè $-2 \equiv 13 \pmod{15}$. Quindi $[x_0]_{15} = [13]_{15}$ è una soluzione particolare; le altre d = 3 soluzioni sono $[x_0 + \frac{n}{d}]_n = [13 + 5]_{15} = [18]_{15} = [rest\ (18,15)]_{15} = [3]_{15}$; $[x_0 + 2\frac{n}{d}]_n = [13 + 10]_{15} = [23]_{15} = [rest\ (23,15)]_{15} = [8]_{15}$. La soluzione cercata è allora $\bigcup_{h=0}^{2} [3 + 5h]_{15} = [3]_{15} \cup [8]_{15} \cup [13]_{15}$ .Infatti

$$[3]_5 = \{3 + 5h, h = 0,1,2\} = \left\{\begin{array}{lll} \rightarrow & h = 3k + 0 & [3]_{15} = \{3 + 15k, k \in Z\} \\ \rightarrow & h = 3k + 1 & [8]_{15} = \{8 + 15k, k \in Z\} \\ \rightarrow & h = 3k + 2 & [13]_{15} = \{13 + 15k, k \in Z\} \end{array}\right\} \text{ poiché}$$

$$\left\{\begin{array}{lll} 3 + 5h = 3 + 15k & \Rightarrow & h = 3k + 0 \\ 3 + 5h = 8 + 15k & \Rightarrow & h = 3k + 1 \\ 3 + 5h = 13 + 15k & \Rightarrow & h = 3k + 2 \end{array}\right\}$$. L'insieme $\{3k, 3k + 1, 3k + 2, k \in Z\} = Z^- \cup Z_0^+ = Z$,perché per k = 0, ±1, ±2, ±3,…si ottiene $\mathbb{Z}$ come si può osservare dallo schema

$$\begin{array}{ccccc} 0 & 3 & 6 & 9 & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ 1 & 4 & 7 & 10 & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ 2 & 5 & 8 & 11 & \ldots \end{array}$$

Esempio2: l'equazione congruenziale $3x \equiv 4 \pmod{15}$, dove a = 3, b= 4, n = 5, ammette soluzioni in quanto d = M.C.D.(a,n) = M.C.D.(3,5) = 1 per cui in base al teorema pag.18 si ha una sola classe di congruenza $[x_0]_n$ modulo n, cioè la classe $[x_0]_5$. Deve aversi quindi $3x_0 \equiv 4 \pmod 5 \Leftrightarrow 3x_0 - 4 = 5h, h \in Z \Leftrightarrow 3x_0 - 5h = 4$ che è un'equazione diofantea nelle incognite intere x_0 ed h del tipo ax+by=c studiata a pag.12 cap.I, la quale ha soluzioni in $\mathbb{Z}$ se e solo se M.C.D.(3,-5)|4, il che si verifica. In base all'osservazione di pag.13 cap.I, il rapporto $r = \frac{c}{d} = 4$, per cui una soluzione è data da x_0 = s $\cdot$ r = 4s, allora per il teorema pag.6 cap.I si ha d = 3s+5t$\Leftrightarrow$3s+5t = 1. Per trovare s determiniamo con le divisioni successive il M.C.D.(3,5) = 1. Si ha

$$\begin{array}{ccccccccc} 5 & : & 3 & 3 & : & 2 & 2 & : & 1 \\ & & - & & & - & & & - \\ 2 & & 1 & 1 & & 1 & 0 & & 2 \end{array} \quad \text{quindi} \quad \begin{array}{lll} 5 & = & 3 \bullet 1 + 2 \\ 3 & = & 2 \bullet 1 + 1 \\ 2 & = & 1 \bullet 2 + 0 \end{array} \quad \text{da cui} \quad \begin{array}{ll} 2 = & 5 - 3 \bullet 1 \\ 1 = & 3 - 2 \bullet 1 \end{array}$$

e sostituendo 1 = 3 –(5-3 $\cdot$ 1) $\cdot$ 1$\Rightarrow$ 1 = 3(1+1) - 5 $\cdot$ 1 = 3 $\cdot$ 2- 5 $\cdot$ 1$\Rightarrow$3 $\cdot$ 2+5 $\cdot$ (-1) = 1$\Rightarrow$ s = 2, t = -1$\Rightarrow$ x_0 = 4s = 8$\Rightarrow [x_0]_5 = [8]_5 = [rest\ (8,5)]_5 = [3]_5$ è la soluzione cercata.

Esempio3: l'equazione congruenziale $36x \equiv 10 \pmod{12}$ non ha soluzioni perché, in base al teorema pag.19, posto a = 36, b = 10, d = M.C.D.(36,12) = 12, si hanno soluzioni se il massimo comun divisore d del coefficiente a dell'incognita x e del modulo della

congruenza n divide il termine noto b, mentre in questo caso d = 12 non divide b = 10. D'altra parte $[36]_3 = [0]_3$ per cui l'equazione è equivalente all'equazione 0x≡10 (mod 12) che ovviamente non ha soluzioni.

Esempio4: l'equazione congruenziale 6x≡5 (mod 9) non ha soluzioni perché, in base al teorema pag.19, posto a = 6, b = 5, d = M.C.D.(6,9) =3, si hanno soluzioni se il massimo comun divisore d del coefficiente a dell'incognita x e del modulo della congruenza n divide il termine noto b, mentre in questo caso d = 3 non divide b = 5.

Esempio5: l'equazione congruenziale 4x≡16 (mod 20) ha soluzioni perché, in base al teorema pag.19, posto a = 4, b = 16, n = 20, d = M.C.D.(4,20) = 4, si ha che d|b ⇔ 4|16⇔16 = 4c ⇒ c = 4. In base al teorema pag.6 cap. I con l'algoritmo euclideo delle divisioni successive determiniamo due interi s e t tali che d =sa+tn, che nel nostro caso diviene 4 = 4s+20t ovvero s+5t =1(si noti che questa è un'equazione diofantea del tipo ax+by = c studiata a pag.12 cap.I, che ammette soluzioni in ℤ se e solo se M.C.D.(a,b)|c, il che nel nostro caso si verifica). Le divisioni successive per determinare il M.C.D.(4,20) = 4 si riducono a 20 = 4 · 5+0 ma non necessarie perché una soluzione dell' equazione s+5t =1è s = 1, t = 0. Quindi una soluzione particolare dell'equazione è $x_0 = s \cdot c = 1 \cdot 4 = 4$. Poiché $\frac{n}{d} = 5$ la soluzione generale è

$[4]_5 = [4]_{20} \cup [4+5]_{20} \cup [4+10]_{20} \cup [4+15]_{20} = [4]_{20} \cup [9]_{20} \cup [14]_{20} \cup [19]_{20}$. Infatti

$$[4]_5 = \{4+5h, h = 0,1,2,3\} = \left\{\begin{array}{llll} \rightarrow & h = 4k+0 & [4]_{20} = & \{4+20k, k \in Z\} \\ \rightarrow & h = 4k+1 & [9]_{20} = & \{9+20k, k \in Z\} \\ \rightarrow & h = 4k+2 & [14]_{20} = & \{14+20k, k \in Z\} \\ \rightarrow & h = 4k+3 & [19]_{20} = & \{19+20k, k \in Z\} \end{array}\right\} \text{ poiché}$$

$$\left\{\begin{array}{lll} 4+5h = 4+20k & \Rightarrow & h = 4k+0 \\ 4+5h = 9+20k & \Rightarrow & h = 4k+1 \\ 4+5h = 14+20k & \Rightarrow & h = 4k+2 \\ 4+5h = 19+20k & \Rightarrow & h = 4k+3 \end{array}\right\}$$. L'insieme $\{4k, 4k+1, 4k+2, 4k+3, k \in Z\} = Z^- \cup Z_0^+ = Z$,perché per

k = 0, ±1, ±2, ±3,…si ottiene ℤ come si può osservare dallo schema

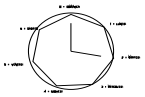
$$\begin{array}{ccccc} 0 & 4 & 8 & 12 & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ 1 & 5 & 9 & 13 & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ 2 & 6 & 10 & 14 & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ 3 & 7 & 11 & 15 & \ldots \end{array}$$

Esempio6: l'equazione congruenziale 3x≡2 (mod 11), dove a = 3, b= 2, n = 11, ammette soluzioni in quanto d = M.C.D.(a,n) = M.C.D.(3,11) = 1 per cui in base al teorema pag.18 si ha una sola classe di congruenza $[x_0]_n$ modulo n, cioè la classe $[x_0]_{11}$. Deve aversi quindi $3x_0 \equiv 2 \pmod{11} \Leftrightarrow 3x_0 - 2 = 11h, h \in Z \Leftrightarrow 3x_0 - 11h = 2$ che è un'equazione diofantea nelle incognite intere x_0 ed h del tipo ax+by=c studiata a pag.12 cap.I, la quale ha soluzioni in ℤ se e solo se M.C.D.(3,-11)|2, il che si verifica. In base all'osservazione di pag.13 cap.I, il rapporto $r = \frac{c}{d} = 2$, per cui una soluzione è data da $x_0 = s \cdot r = 2s$, allora per il teorema pag.6 cap.I si ha d = 3s+11t⇔3s+5t = 1. Per trovare s determiniamo con le divisioni successive il M.C.D.(3,11) = 1. Si ha

$$\begin{array}{ccccccccc} 11 & : & 3 & 3 & : & 2 & 2 & : & 1 \\ & & - & & & - & & & - \\ 2 & & 3 & 1 & & 1 & 0 & & 2 \end{array} \quad \text{quindi} \quad \begin{array}{lll} 11 & = & 3 \bullet 3 + 2 \\ 3 & = & 2 \bullet 1 + 1 \\ 2 & = & 1 \bullet 2 + 0 \end{array} \quad \text{da cui} \quad \begin{array}{ll} 2 = & 11 - 3 \bullet 3 \\ 1 = & 3 - 2 \bullet 1 \end{array} \quad \text{e sostituendo } 1 = 3 - (11 - 3 \cdot 3) \cdot 1 \Rightarrow$$

$1 = 3 - 11 + 3 \cdot 3 = 3(1+3) - 11 = 3 \cdot 4 + 11 \Rightarrow s = 4, t = -1 \Rightarrow x_0 = s \cdot c = 4 \cdot 2 = 8 \Rightarrow [8]_{11}$ è la soluzione cercata.

Esercizio: **Gaia telefona ad Ugo una prima volta di domenica ,poi ad intervalli di quattro giorni. Quante telefonate dovrà fare Gaia affinché una sua telefonata cada di martedì? Dimostrare inoltre che si può cambiare l'intervallo di giorni tra una telefonata e la successiva in modo tale che nessuna telefonata cade di martedì e ci sia almeno una telefonata che non cade di domenica.**



Soluzione: Supponiamo di disporre di un orologio di Gauss di 7 ore, ponendo:
0 = Domenica, 1 = Lunedì, 2 = Martedì, 3 =mercoledì, 4 = giovedì, 5 = venerdì, 6 = sabato , poniamo uguale ad x il numero di volte che si muove la lancetta di un ora e con 4x quindi il numero delle volte che si muove la lancetta di quattro ore, cioè il numero di telefonate ad intervalli di quattro giorni. Il problema è quindi risolto dall'equazione congruenziole **4x≡2 (mod 7**). Si ha d = M.C.D.(a,n) = M.C.D.(4,7) = 1, per cui in base al teorema pag.18, vi è una sola classe di congruenza modulo 7, inoltre si ha d|b⇔b = d · c ⇔ 1|2⇔2=1 · c = c. Per il teorema pag.6 cap.I deve essere d = sa+tn, s,t∈ℤ, si ha 4s+7t = 1, equazione diofantea risolvibile in ℤ poiché il M.C.D.(4,7) = 1 divide c = 1. Determiniamo con le divisioni successive il M.C.D.(4,7) = 1 da cui

$$\begin{array}{ccccccccccccc} 7 & : & 4 & 4 & : & 3 & 3 & : & 1 & 4 & : & 3 \\ & & - & & & - & & & - & & & - \\ 3 & & 1 & 1 & & 1 & 0 & & 3 & 1 & & 1 \end{array}$$

$$\begin{array}{lcl} 7 & = & 4 \bullet 1 + 3 \\ 4 & = & 3 \bullet 1 + 1 \\ 3 & = & 3 \bullet 1 + 0 \end{array} \Rightarrow \begin{array}{l} 3 = \quad 7 - 4 \bullet 1 \\ 1 = \quad 4 - 3 \bullet 1 \end{array} \Rightarrow 1 = 4 - (7 - 4 \cdot 1) = 4 - 7 + 4 \cdot 1 = 4(1+1) - 7 = 4 \cdot 2 + 7(-1) \Rightarrow s = 2,\ t = -1 \Rightarrow x_0 = s \cdot c = 2 \cdot 2 =$$

4, per cui la soluzione è $[4]_7 = \{x = 4 + 7h, h \in \mathbb{Z}\}$

Quindi il numero di telefonate ad intervalli di quattro giorni necessario per fare una telefonata di martedì è:

$$\left\{ \begin{array}{lll} 4\ telefonate & per & h = 0 \\ 11\ telefonate & per & h = 1 \\ 18\ telefonate & per & h = 2 \\ 25\ telefonate & per & h = 3 \\ 32\ telefonate & per & h = 4 \\ ecc\ . & ecc\ . & ecc\ . \end{array} \right\}$$

Allo scopo di rispondere all'ultima parte del quesito studiamo la congruenza **ax≡2 (mod 7)** al variare dell'intervallo a∈ℤ delle telefonate.

- **a = 1 ⇒ x≡2 (mod 7)** ⇒d = M.C.D.(a,n) = M.C.D. (1,7) = 1. Vi sono soluzioni se d|b ⇔ b = d · c⇒1|2⇔2 = 1 · 2⇒ c = 2. La soluzione è la classe $[x_0]_7$, con x_0 = s · c = 2s, dove s,t sono le soluzioni intere dell'equazione diofantea d = as + tn ⇒ 1 = s + 7t, che ha soluzioni perché M.C.D.(1,7) = 1|1. E'immediato verificare che una soluzione è la coppia (1,0), per cui s = 1 ⇒ x_0 = 1 · 2 = 2 ⇒ $[2]_7 = \{2 + 7h, h \in \mathbb{Z}\}$, dove il rappresentante 2 della classe indica il numero minimo di telefonate da effettuare. Quindi, se l'intervallo a delle telefonate è di un giorno, la prima telefonata di martedì arriva dopo due telefonate, la seconda dopo nove telefonate, ecc.al variare di h in ℤ.

- **a = 2⇒ 2x≡2 (mod 7)** ⇒d = M.C.D.(a,n) = M.C.D. (2,7) = 1. E' intuitivo osservare che x = 1 soddisfa la congruenza, per cui la soluzione cercata è la classe $[1]_7$ Comunque vi sono soluzioni se d|b ⇔ b = d · c⇒1|2⇔2 = 1 · 2⇒ c = 2. La soluzione è la classe $[x_0]_7$, con x_0 = s · c = 2s, dove s,t sono le soluzioni intere dell'equazione diofantea d = as + tn ⇒ 1 = 2s + 7t, che ha soluzioni perché M.C.D.(2,7) = 1|1 Con l'algoritmo delle divisioni successive si ha $\left\{\begin{array}{l} 7 = 2 \bullet 3 + 1 \\ 2 = 2 \bullet 1 + 0 \end{array}\right\} \Rightarrow$ 1 = 7-2 · 3 = 2(-3) + 7 · 1 ⇒ s = -3, t = 1 ⇒ x_0 = s · c = (-3) · 2 = -6⇒ $[-6]_7 = [1]_7$, essendo -6≡1(mod 7). La soluzione è quindi $[1]_7 = \{1 + 7h, h \in \mathbb{Z}\}$, dove il rappresentante 1 della classe indica il numero minimo di telefonate da effettuare. Quindi, se l'intervallo a delle telefonate è di due giorni, la prima telefonata di martedì arriva dopo una telefonata, la seconda dopo otto telefonate, ecc.al variare di h in ℤ.

- **a = 3⇒ 3x≡2 (mod 7)** ⇒d = M.C.D.(a,n) = M.C.D. (3,7) = 1. Vi sono soluzioni se d|b ⇔ b = d · c⇒1|2⇔2 = 1 · 2⇒ c = 2. La soluzione è la classe $[x_0]_7$, con x_0 = s · c = 2s, dove s,t sono le soluzioni intere dell'equazione diofantea d = as + tn ⇒1 = 3s + 7t, che ha soluzioni perché M.C.D.(3,7) = 1|1 Con l'algoritmo delle divisioni successive si ha $\left\{\begin{array}{l} 7 = 3 \bullet 2 + 1 \\ 3 = 3 \bullet 1 + 0 \end{array}\right\} \Rightarrow$ 1 = 7 - 3 · 2 ⇒ 1 = 3(-2) + 7 · 1 ⇒ s = -2, t = 1⇒ x_0 = s · c = (-2) · 2 = -4⇒ $[-4]_7 = [3]_7$ in quanto rest(4,7) = 3 e quindi 3 ≡ -4(mod 7). La soluzione è allora $[3]_7 = \{3 + 7h, h \in \mathbb{Z}\}$, dove il rappresentante 3 della classe indica il numero minimo di telefonate da effettuare. Quindi, se l'intervallo a delle telefonate è di tre giorni, la prima telefonata di martedì arriva dopo tre telefonate, la seconda dopo dieci telefonate, ecc.al variare di h in ℤ.

- **a = 4⇒ 4x≡2 (mod 7)** l'abbiamo già studiata e sappiamo che la soluzione è $[4]_7 = \{x = 4 + 7h, h \in \mathbb{Z}\}$ Quindi, se l'intervallo a delle telefonate è di quattro giorni, la prima telefonata di martedì arriva dopo quattro telefonate, la seconda dopo undici telefonate, ecc.al variare di h in ℤ.

- **a = 5⇒ 5x≡2 (mod 7)** ⇒d = M.C.D.(a,n) = M.C.D. (5,7) = 1. Vi sono soluzioni se d|b ⇔ b = d·c⇒1|2⇔2 = 1·2⇒ c = 2. La soluzione è la classe $[x_0]_7$, con x_0 = s·c = 2s, dove s,t sono le soluzioni intere dell'equazione diofantea d = as + tn ⇒1 = 5s + 7t, che ha soluzioni perché M.C.D.(5,7) = 1|1 Con l'algoritmo delle divisioni successive si ha
$\begin{cases} 7 = 5 \bullet 1 + 2 \\ 5 = 2 \bullet 2 + 1 \\ 2 = 2 \bullet 1 + 0 \end{cases} \Rightarrow \begin{cases} 1 = 5 - 2 \bullet 2 \\ 2 = 7 - 5 \bullet 1 \end{cases} \Rightarrow 1 = 5 - 2(7 - 5 \bullet 1) = 5 - 2 \bullet 7 + 2 \bullet 5 = 5(1+2) - 2 \bullet 7 = 5 \bullet 3 + 7(-2) \Rightarrow s = 3, t = -2 \Rightarrow x_0 = s \bullet c = 3 \bullet 2 = 6$
$[6]_7 = \{x = 6 + 7h, h \in \mathbb{Z}\}$ è la soluzione cercata, per cui se l'intervallo tra una telefonata e l'altra è di cinque giorni, la prima telefonata di martedì è dopo sei telefonate.

- **a = 6⇒ 6x≡2 (mod 7)** ⇒d = M.C.D.(a,n) = M.C.D. (6,7) = 1. Vi sono soluzioni se d|b ⇔ b = d·c⇒1|2⇔2 = 1·2⇒ c = 2. La soluzione è la classe $[x_0]_7$, con x_0 = s·c = 2s, dove s,t sono le soluzioni intere dell'equazione diofantea d = as + tn ⇒1 = 6s + 7t, che ha soluzioni perché M.C.D.(6,7) = 1|1 Con l'algoritmo delle divisioni successive si ha: 7 = 6·1+1 = 1 = 6(-1)+7·1⇒s = -1, t = 1⇒ x_0 = s·c = -2⇒$[-2]_7 = [5]_7$. Quindi la soluzione è $[5]_7 = \{x = 5 + 7h, h \in \mathbb{Z}\}$, dove 5, rappresentante della classe, indica il numero minimo di telefonate da effettuare affinché una telefonata avvenga di martedì, cioè se l'intervallo delle telefonate è di sei giorni, la prima telefonata di martedì arriva dopo cinque telefonate.

- **a = 7 ⇒ 7x≡2 (mod 7)** ⇒ d = M.C.D.(a,n) = M.C.D. (7,7) = 7≠7, per cui non vi sono soluzioni in quanto, partendo le telefonate di domenica con un intervallo di sette giorni, esse avvengono tutte di domenica.

In generale l'equazione ax ≡ 2 (mod 7) non ha soluzioni quando d = M.C.D.(a,7)≠2. Ora
$d = M.C.D.(a,7) = \begin{cases} 7 \quad se \quad 7/a \\ 1 \quad se \quad a,7 \quad relativamente \quad primi \end{cases}$ per cui, se M.C.D.(a,7)=1⇒1|2, l'equazione ha sempre soluzioni congrue tra loro modulo 7, quindi deduciamo che l'equazione non ha soluzioni se d = M.C.D.(a,7) = 7, perché in tal caso si ha che d = 7≠2. Allora , poiché se a è multiplo di 7 non vi sono soluzioni, come nel caso particolare che a = 7, concludiamo che se l'intervallo è di sette giorni o di multipli di sette giorni, partendo da domenica tutte le telefonate avvengono di domenica e nessuna di martedì. Si osservi che la ricerca di opportuni intervalli a tra le telefonate affinché non vi siano telefonate di domenica, equivale a considerare il caso in cui l'equazione ax≡0 (mod 7) non ha soluzioni, ma d = M.C.D.(a,7) è 1 oppure7 ed in entrambi i casi d|0 per cui si ha che si hanno sempre soluzioni date dalla classe $[0]_7 = \{7h, h \in \mathbb{Z}\}$ in quanto per x = 0 si ha a·0≡0 (mod 7). La conclusione è che vi saranno sempre telefonate di domenica comunque si vari l'intervallo tra le telefonate.

Per risolvere problemi inerenti alla risoluzione di sistemi di congruenze lineari, è fondamentale il seguente teorema dovuto al matematico cinese Sun Tsu Suan-Ching (300 a. C.)

Teorema cinese del resto:

Se n,m∈ℤ, δ = M.C.D.(n,m), il sistema di congruenze lineari $\begin{cases} x \equiv a(\bmod n) \\ x \equiv b(\bmod m) \end{cases}$ ha come soluzione almeno un intero $x_0 \in \mathbb{Z}$ verificante il sistema se e solo se a≡b(mod δ) ovvero se δ è un divisore della differenza dei termini noti.

Si ha inoltre che, se $\delta \neq 1$, allora la soluzione generale è la classe $[x_0]_\delta = \{x_0 + k\delta, k \in \mathbb{Z}\}$,

se invece δ=1, si ha che ∀a,b∈ℤ il sistema è risolvibile ed ha come soluzione la classe

$[x_0]_{nm} = [x_0]_\mu$, dove μ =m.c.m.(n,m)=[n,m]

Dimostrazione:

La condizione è necessaria. Infatti supposto che il sistema ammetta la soluzione $x_0 \in \mathbb{Z}$, deve verificarsi che

$$\begin{cases} x_0 \equiv a \pmod{n} \\ x_0 \equiv b \pmod{m} \end{cases} \Rightarrow \begin{cases} x_0 = a + hn, h \in \mathbb{Z} \\ x_0 = b + kn, k \in \mathbb{Z} \end{cases} \Rightarrow a + hn = b + km \Rightarrow a - b = km - hn$$

Ora δ|n e δ|m per cui, in base alla proposizione8 pag.2 cap.I, divide anche una combinazione lineare di n ed m, quindi δ | km-hn ⇒ δ | a-b ⇒a≡b(mod δ). Viceversa la condizione è sufficiente perché se a≡b(mod δ)⇒ δ | a-b⇒a-b = rδ, r∈ℤ. Allora per l'algoritmo esteso di Euclide (teorema pag.7 cap.I) devono esistere due interi s,t∈ℤ tali che δ = sn + tm, da

cui sostituendo si ha a-b = r(sn+tm) = (rs)n+(rt)m = -hn + km ⇒ x_0 = a + hn = b + km è una soluzione di entrambe le equazioni in quanto a + hn ≡ a (mod n)⇔a + hn – a = hn , b + km ≡ b (mod m) ⇔ b + km – b = km.

Proviamo ora che, detto $\mathcal{S}$ l'insieme delle soluzioni del sistema, con $\mathcal{S}\neq\emptyset$ poiché $x_0 \in\mathcal{S}$, si ha $\mathcal{S} = [x_0]_\delta$ nel caso che $\delta\neq1$. Infatti $\mathcal{S}\subseteq[x_0]_\delta$ perché se $\bar{x}\in\mathcal{S}$ è una soluzione, allora deve aversi

$$\begin{cases} \bar{x} \equiv a \pmod{n} \\ \bar{x} \equiv b \pmod{m} \end{cases} \Rightarrow \begin{cases} \bar{x} = a + h'n, h' \in \mathrm{Z} \\ \bar{x} = b + k'n, k' \in \mathrm{Z} \end{cases} \Rightarrow \bar{x} = a + h'n = b + k'm$$

D'altra parte anche anche x_0 è una soluzione, da

$$\begin{cases} x_0 \equiv a \pmod{n} \\ x_0 \equiv b \pmod{m} \end{cases} \Rightarrow \begin{cases} x_0 = a + hn, h \in \mathrm{Z} \\ x_0 = b + kn, k \in \mathrm{Z} \end{cases} \Rightarrow x_0 = a + hn = b + km$$

Sottraendo membro a membro si ha $\bar{x} - x_0 = (h'-h)n = (k'-k)m$ ⇒ n | $\bar{x} - x_0$, m | $\bar{x} - x_0$ ⇒ δ | $\bar{x} - x_0$ ⇒$\delta\rho$, $\rho\in\mathbb{Z}$⇒ $\bar{x} \equiv x_0 (\mathrm{mod}\, \delta) \Rightarrow \bar{x} \in [x_0]_\delta$.

Si ha pure $[x_0]_\delta \subseteq\mathcal{S}$ poiché se $\bar{x} \in [x_0]_\delta \Rightarrow \bar{x} \equiv x_0 (\mathrm{mod}\ \delta) \Rightarrow \bar{x} = x_0 + h\delta, h \in \mathrm{Z}$, d'altronde essendo x_0 una soluzione del sistema, deve verificare la prima equazione $x_0 \equiv a (\mathrm{mod}\ n)$, inoltre deve essere per un determinato h∈$\mathbb{Z}$ $h\delta \equiv 0 (\mathrm{mod}\ n)$ in quanto n = h'δ⇒ k'n = k'h'δ⇒ hδ = k'n⇒ hδ≡0 (mod n). In base alla compatibilità rispetto alla somma della relazione n$\mathbb{Z}$ (vedi pag.7 cap.II) si ha sommando membro a membro le relazioni

$$\begin{cases} x_0 \equiv a (\mathrm{mod}\ n) \\ h\delta \equiv 0 (\mathrm{mod}\ n) \end{cases} \Rightarrow x_0 + h\delta \equiv a + 0 (\mathrm{mod}\ n) \Rightarrow \bar{x} \equiv a (\mathrm{mod}\ n)$$ per cui $\bar{x}$ è soluzione della prima equazione.

Si ha che $\bar{x}$ è soluzione anche della seconda equazione perché sostituendo $\bar{x} = x_0 + h\delta$ nella seconda equazione si ha $x_0 + h\delta \equiv b (\mathrm{mod}\ m) \Rightarrow \delta h \equiv b - x_0 (\mathrm{mod}\ m)$ equazione nell'incognita h avente soluzioni poiché M.C.D.(δ,m) = δ e $\delta | b - x_0$ in quanto da $x_0 \equiv b (\mathrm{mod}\ m) \Rightarrow b - x_0 (\mathrm{mod}\ m) \Rightarrow b - x_0 = km$ segue che, avendosi δ | km⇔km = $\chi\delta$⇒, sostituendo si ha b - x_0 = $\chi\delta \Rightarrow \delta | b - x_0$. L'equazione $\delta h \equiv b - x_0 (\mathrm{mod}\ m)$ ha come soluzione la classe $[h]_{\frac{m}{\delta}} = \left\{ h + k\frac{m}{\delta}, k \in \mathrm{Z} \right\}$ da cui per k = 0 si ottiene il valore h che nella $\bar{x} = x_0 + h\delta$ verifica la seconda equazione e quindi il sistema. Si conclude quindi che $\mathcal{S} = [x_0]_\delta$.

Nel caso che invece δ=1, si ha che ∀a,b∈$\mathbb{Z}$ il sistema è risolvibile perché, per la prima parte del teorema,ciò si ha se a≡b(mod δ) ⇔ δ|a-b, ed 1|a-b. Detta allora x_0 una soluzione particolare, proviamo che $\mathcal{S} = [x_0]_{nm}$ valendo le relazioni $\mathcal{S}\subseteq[x_0]_{nm}$, $\mathcal{S}\supseteq[x_0]_{nm}$. Si ha $\mathcal{S}\subseteq[x_0]_{nm}$ poiché se $\bar{x} \in \mathcal{S}$

$$\Rightarrow \begin{cases} \bar{x} \equiv a (\mathrm{mod}\ n) \\ \bar{x} \equiv b (\mathrm{mod}\ m) \\ x_0 \equiv a (\mathrm{mod}\ n) \\ x_0 \equiv b (\mathrm{mod}\ m) \end{cases} \Rightarrow \begin{cases} \bar{x} = a + h'n = b + k'm \\ x_0 = a + h''n = b + k''m \end{cases} \Rightarrow \bar{x} - x_0 = (h'-h'')n = (k'-k'')m \Rightarrow$$

n | $\bar{x} - x_0$, m | $\bar{x} - x_0$ ⇒ n·m | $\bar{x} - x_0$ (corollario4 pag.8 capI) ⇒ $\bar{x} - x_0$ = h·nm ⇒ $\bar{x} \equiv x_0 (\mathrm{mod}\ nm) \Rightarrow \bar{x} \in [x_0]_{nm}$.

Viceversa si ha pure $[x_0]_{nm} \subseteq \mathcal{S}$ in quanto $\bar{x} \in [x_0]_{nm} \Rightarrow \bar{x} \equiv x_0 \pmod{nm} \Rightarrow \bar{x} = x_0 + hnm$, $h \in$ Z . Ora ovviamente si ha hnm≡0(mod nm), hnm≡0(mod n), hnm≡0(mod m), da cui

$$\begin{cases} x_0 \equiv a \pmod{n} \\ hnm \equiv 0 \pmod{n} \\ x_0 \equiv b \pmod{m} \\ hnm \equiv 0 \pmod{m} \end{cases} \Rightarrow \begin{cases} x_0 + hnm \equiv a + 0 \pmod{n} \\ x_0 + hnm \equiv b + 0 \pmod{m} \end{cases} \Rightarrow \begin{cases} \bar{x} \equiv a \pmod{n} \\ \bar{x} \equiv b \pmod{m} \end{cases} \Rightarrow \bar{x} \in S$$

Infine si ha $[x_0]_{nm} = [x_0]_\mu$ poiché ricordando che n·m = $\delta \cdot \mu$, si ha

$$x \equiv x_0 \pmod{nm} \Leftrightarrow x = x_0 + hnm = x_0 + h\delta\mu = x_0 + h'\mu \Leftrightarrow x \equiv x_0 \pmod{\mu}.$$

~ § § § ~

Vogliamo ora dare un metodo generale di risoluzione dei sistemi di equazioni congruenziali lineari. Cominciamo con un sistema di due equazioni $\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$ dove supponiamo δ= M.C.D.(n_1, n_2) =1

per cui deve essere μ = m.c.m.$(n_1, n_2) = n_1 \cdot n_2$. In base al teorema precedente la soluzione è la classe $[x_0]_\mu$; ora si ha δ = M.C.D.$(n_i, \frac{\mu}{n_i})$ = M.C.D.$(n_i, \frac{n_i \cdot n_j}{n_i})$ = M.C.D.(n_i, n_j) = 1 ∀i≠j ∈{ 1,2 }, per cui considerati gli interi primi tra loro $n_i, \frac{\mu}{n_i}$,applicando l'algoritmo esteso di Euclide si possono trovare due interi s,t tali che $sn_i + t\frac{\mu}{n_i} = 1$.

Allora posto $e_i = t\frac{\mu}{n_i}$, si ha $sn_i + e_i = 1 \Rightarrow 1 - e_i = sn_i \Rightarrow e_i \equiv 1 \pmod{n_i}$ ed inoltre $e_i \equiv 0 \pmod{n_j}$ per i≠j poiché in tal caso $e_i = tn_j$. Da queste due relazioni segue che $\begin{cases} e_i \equiv 1 \pmod{n_i} \\ e_i \equiv 0 \pmod{n_j} \end{cases} \Rightarrow \begin{cases} a_i e_i \equiv a_i \pmod{n_i} \\ a_i e_i \equiv 0 \pmod{n_j} \end{cases}, i \neq j$

cioè $\begin{cases} a_1 e_1 \equiv a_1 \pmod{n_1} \\ a_1 e_1 \equiv 0 \pmod{n_2} \\ a_2 e_2 \equiv a_2 \pmod{n_2} \\ a_2 e_2 \equiv 0 \pmod{n_1} \end{cases}$ da cui sommando membro a membro la prima con la quarta e la seconda con la terza, si ha :

$\begin{cases} a_1 e_1 + a_2 e_2 \equiv a_1 \pmod{n_1} \\ a_1 e_1 + a_2 e_2 \equiv a_2 \pmod{n_2} \end{cases}$ ovvero la somma $x_0 = \sum_{i=1}^{2} a_i e_i$ soddisfando il sistema è una soluzione particolare dello stesso

. **Esempio:** Sia il sistema $\begin{cases} x \equiv 0 \pmod{7} \\ x \equiv 3 \pmod{5} \end{cases}$ dove, riferendoci alla simbologia precedente, si ha che $n_1 = 7$, $n_2 = 5$.

Poiché δ = M.C.D.(7,5) = 1, il sistema è risolvibile ed ha come soluzione la classe $[x_0]_\mu = [x_0]_{35}$, dove μ = m.c.m.(7,5) = 35.

Applicando l'algoritmo esteso di Euclide dobbiamo trovare due interi s,t tali che $sn_i + t\frac{\mu}{n_i} = 1$ che per i = 1 dà 7s + 5t = 1, quindi con il procedimento delle divisioni successive per determinare il M.C.D.(7,5) = 1 si ha

$$\begin{cases} 7 = 5\cdot 1 + 2 \\ 5 = 2\cdot 2 + 1 \end{cases} \Rightarrow \begin{cases} 2 = 7 - 5\cdot 1 \\ 1 = 5 - 2\cdot 2 \end{cases} \Rightarrow 1 = 5 - 2(7-5) = 5 - 2\cdot 7 + 2\cdot 5 = (1+2)\cdot 5 - 2\cdot 7 = (-2)\cdot 7 + 3\cdot 5 \Rightarrow s = -2,\ t = 3 \Rightarrow$$

$$e_i = t\frac{\mu}{n_i} \Rightarrow \begin{cases} e_1 = t\dfrac{5\cdot 7}{7} = 5t = 15 \\ e_2 = t\dfrac{5\cdot 7}{5} = 7t = 21 \end{cases} \Rightarrow x_0 = a_1e_1 + a_2e_2 = 0\cdot 15 + 3\cdot 21 = 63 \equiv 28 \pmod{35}$$

Quindi la soluzione è la classe $[28]_{35} = \{28 + 35k, k \in Z\}$.

Esempio:
Dato un certo numero di arance ne avanzano 6 se disposte a gruppi di 7, ne avanzano 5 se disposte a gruppi di 9.
Quante sono le arance?
x = 6 (mod 7)
x = 5 (mod 9)

Ora MCD(7,9) = 1 peer cui 6≡5 (mod 1) cioè 1 divide (6-5), quindi la soluzione esiste. x = 7t + 6 = 5 (mod 9), 7t = 5 (mod 9) - 6 = 8 (mod 9). Questo passaggio mi porta ad una unica equazione nell'incognita t alla quale applico la procedura vista sopra: 7t = 8 (mod 9) , MCD(7,9) = 1
1 = 7h +9k; h = 4; k = -38 = p*1; p = 8
t = ph = 32 x = 7t + 6 = 230 . Siccome mcm(7,9) = 63, la soluzione è: x = 230 + 63k = 230 (mod 63) = 41 (mod 63)

Ritorniamo quindi al problema della ricerca delle condizioni secondo le quali in $\mathbb{Z}/n\mathbb{Z}(+,\bullet)$ si hanno elementi invertibili rispetto al prodotto. Mentre in $\mathbb{Z}(\bullet)$ gli unici elementi invertibili sono 1 e -1, in $\mathbb{Z}/n\mathbb{Z}$ vi sono elementi invertibili distinti dall'unità; ci proponiamo quindi di vedere pure quando tutti gli elementi non nulli, ovvero distinti da $[0]_n$, sono invertibili, poiché in tali casi,

essendo $\mathbb{Z}/n\mathbb{Z}(+)$ un gruppo additivo abeliano e $\mathbb{Z}/n\mathbb{Z}$-{$[0]_n$}(•) un gruppo moltiplicativo abeliano, la struttura $\mathbb{Z}/n\mathbb{Z}$-{0}(+,•) risulta un campo. Consideriamo $\mathbb{Z}/n\mathbb{Z}$ con n>1. e $[a]_n \neq [0]_n$, a∈{0,1,…,n-1 }, si ha

Proposizione:

$[a]_n$ è invertibile⇔(a,n)=1

Dimostrazione:

Per semplicità supponiamo inizialmente che a∈{0,1,…,n-1 }.

La condizione è necessaria avendosi $[a]_n$ è invertibile⇒∃ $[a']_n \in \mathbb{Z}/n\mathbb{Z}$ /$[a]_n \bullet [a']_n = [1]_n$ ⇔

$[a\bullet a']_n = [1]_n$ ⇔a a'≡1 (mod n)⇔aa'-1=hn, h∈$\mathbb{Z}$ opportuno.⇔aa'-hn =1.

Se per assurdo d = M.C.D.(a,n)>1,essendo d in particolare un divisore comune di a ed n, deve aversi che d divide qualsiasi loro multiplo per cui d /a ∧ d/n ⇒d/aa'∧ d/hn⇒d/aa'-hn⇒d/1 assurdo, per cui necessariamente M.C.D.(a,n)=1. Viceversa la condizione è sufficiente perché se a ed n sono relativamente primi, cioè M.C.D.(a,n) =1, l'equazione congruenziale ax ≡ 1(mod n) ha come soluzioni la classe $[\bar{x}]_n$ con $\bar{x} \in \mathbb{Z}$ per cui deve verificarsi a$\bar{x}$ ≡ 1(mod n)⟹$[a\bar{x}]_n = [1]_n$ e poichè

$[a\bar{x}]_n = [a]_n \bullet [\bar{x}]_n$, segue $[a]_n \bullet [\bar{x}]_n = [1]_n$, cioè $[a]_n$ è invertibile.

Il teorema sussiste anche nell'<u>ipotesi più generale</u> che $a \in \mathbb{Z}$.

Infatti la condizione è sufficiente perché

se supponiamo che il M.C.D.(a,n) =1, $\forall a \in \mathbb{Z}$,dividendo a per n si ottiene a = bn + rest(a,n),

$0 \leq rest(a,n) < n \Rightarrow [a]_n = [rest(a,n)]_n$ .Ora deve essere M.C.D.(a,n)=1$\Rightarrow$ M.C.D.(rest(a,n),n)=1.

Infatti se per assurdo si avesse M.C.D.(rest(a,n),n) = d >1$\Longrightarrow$d/n $\wedge$ d/rest(a,n)$\Rightarrow$

d/bn,b$\in\mathbb{Z}$ $\wedge$ d/rest(a,n)$\Longrightarrow$d/bn+rest(a,n)$\Rightarrow$d/a. Ma l'aversi simultaneo di d/a e d/n è contro l'ipotesi

che il M.C.D.(a,n) =1. Quindi la classe $[rest(a,n)]_n$ è invertibile per la prima parte del teorema, e

poiché $[a]_n = [rest(a,n)]_n$, anche classe $[a]_n$ è invertibile.

La condizione è necessaria perché, essendo $[a]_n = [rest(a,n)]_n$, se $[a]_n$ è invertibile, lo deve essere

anche $[rest(a,n)]_n$,$0 \leq rest(a,n) < n$, quindi per la prima parte del teorema deve essre

M.C.D.(rest(a,n),n) =1 Si ha infine che M.C.D.(rest(a,n),n)=1$\Longrightarrow$ M.C.D.(a,n)=1

Infatti, se per assurdo a ed n non fossero relativamente primi, posto M.C.D.(a,n)=d >1, deve aversi

d/a $\wedge$ d/n$\Rightarrow$ d/bn, b$\in\mathbb{Z}\Rightarrow$ d/a-bn$\Longrightarrow$ d/rest(a,n). Allora da d/n e d/rest(a,n) segue l'assurdo, essendo

per ipotesi M.C.D.(rest(a,n),n)=1. Quindi deve essere M.C.D.(a,n)=1.

<u>Nota</u>: Quando esiste, indichiamo con $[a]_n^{-1}$ l'inversa di classe $[a]_n$

di modo che

$[a]_n \cdot [a]_n^{-1} = [a]_n \cdot [a^{-1}] = [1]_m$, dove a^{-1} è quell'intero per cui $aa^{-1} \equiv 1 \ (mod\ n)$

L'anello $\mathbb{Z}/6\mathbb{Z}(+,\bullet) = \{[0]_5,[1]_5,[2]_5,[3]_5,[4]_5,[5]_6\}$

Orologio con sei ore

Applicando la proposizione precedente si ha che tutti e soli gli elementi invertibili sono quelli in cui il rappresentante della classe è relativamente primo con 6, cioè 1 e 5 essendo M.C.D.(1,6)=1 e M.C.D.(5,6) = 1. Quindi risultano invertibili solo $[1]_6$ e $[5]_6$.

In generale allora possiamo dire che in $\mathbb{Z}/n\mathbb{Z}$ vi sono sempre elementi invertibili poiché per ogni intero n fissato, vi sono sempre tra gli interi 0,1,…,n-1, numeri che sono relativamente primi con il modulo n della congruenza . Tale numero dei numeri minori di n e primi con n, si indica con $\boldsymbol{\varphi(n)}$ e prende il nome di <u>indicatore di Gauss-Eulero</u>.

<u>Definizione</u>

Dicesi **<u>indicatore di Gauss-Eulero</u>** **,** detta anche **<u>funzione di Eulero</u> o <u>funzione totiente</u>** l'applicazione $\boldsymbol{\varphi:\mathbb{N}\to\mathbb{N}/\forall\ n\in\mathbb{N}\to\varphi(n)\in\mathbb{N}}$**,** con $\varphi(n)$ numero dei numeri primi con n e minori di n nel caso che n>1, mentre se n=1, allora $\varphi(n)=1$, ovvero

$$\phi(n)=\begin{cases} numero\ \ degli\ \ interi\ \ positivi\ \ minori\ \ di\ \ n\ \ e\ \ primi\ \ con\ \ n\ , & n>0 \\ 1\ , & n=1 \end{cases}$$

che risulta essere la cardinalità (numero degli elementi) dell'insieme

$$\varphi(n) = |\{a \in \mathbb{N}\ /1 \leq a \leq n, (a,n) = 1, n \in \mathbb{N}\}|$$

<u>Osservazione</u>: si osservi che i numeri interi a primi con n e minori o uguali ad n sono

necessariamente minori di n, perché per a = n si ha $(a,n) \neq 1$, in quanto n stesso è un fattore comune.

<u>Esempio</u>: $\varphi(2) = 1$, $\varphi(5) = 4$, $\varphi(6) =2$, $\varphi(10) =4$. Infatti ad esempio gli interi positivi minori o uguali a 10 e primi con 10 sono 1, 3, 7, 9.

<u>Esempio</u>: Ricordato che le frazioni proprie sono le frazioni $\frac{m}{n}$, con $1 \leq m \leq n$, tra queste quelle

ridotte ai minimi termini sono quelle per cui $(m,n) = 1$, il cui numero è uguale al numero degli

interi m minori o uguali ad n e primi con n, cioè $\varphi(n)$.

<u>Proposizione</u>:

Se p è primo allora φ(p) = p-1

<u>Dimostrazione</u>: Ovvia, poiché tutti i numeri minori di p sono p-1 e risultano primi con p.

Abbiamo provato a pag.31 che nella struttura moltiplicativa $\mathbb{Z}/n\mathbb{Z}(\cdot)$ delle congruenze modulo n tutte e

sole le classi invertibili $[a]_n$ distinte dalla classe nulla $[0]_n$sono le classi tali che $(a,n) = 1$, cioè tali che sono primi tra loro il rappresentante della classe ed il modulo della congruenza.

Sia $\mathcal{A}_n$ = {[a]$_n$ $\in \mathbb{Z}/n\mathbb{Z}-\{[0]_n\}$/ [a]$_n$ è invertibile} insieme di tutti gli elementi invertibili di $(\mathbb{Z}/n\mathbb{Z}-\{[0]_n\})(\cdot)$. Ora, poiché tutte le classi si riducono alle classi $[a]_n$ con $1 \leq a \leq n-1$, si ha $\mathcal{A}_n$ = {[a]$_n$ $\in \mathbb{Z}/n\mathbb{Z}-\{[0]_n\}$/ $1 \leq a \leq n-1, (a,n) = 1$}, la cui cardinalità è $|\mathcal{A}_n| = \varphi(n)$, numero degli interi minori di n (quindi minori o uguali a n-1) e primi con n.

<u>Un'equazione diofantea</u> <u>lineare</u> è un'equazione del tipo $ax + by = d$, con $a, b, d \in \mathbb{Z}$, nelle incognite intere $x, y \in \mathbb{Z}$.

<u>Proposizione</u>: Se $a, b \in \mathbb{Z}$ sono interi non simultaneamente nulli e $d = (a, b)$, allora $\exists x, y \in \mathbb{Z}$ tali che $ax + by = d$, anzi l'insieme soluzione dell'equazione $\{(x, y) \in \mathbb{Z}^2 / \ ax + by = d\}$ è numerabile.

<u>Dimostrazione</u>: Poiché $ax + by = d \Rightarrow by = d - ax$, le soluzioni cercate per x sono necessariamente quelle per cui $d - ax$ è un multiplo di b. Se x_0 è una di queste, sia y_0 il valore corrispondente di modo che la coppia ordinata (x_0, y_0) risulti una soluzione dell'equazione. Allora da $ax_0 + by_0 = d$ segue sommando e sottraendo $k\frac{ab}{d}$ con $k \in \mathbb{Z}$, $ax_0 - k\frac{ab}{d} + by_0 + k\frac{ab}{d} = d \Rightarrow$

$a\left(x_0 - k\frac{b}{d}\right) + b\left(y_0 + k\frac{a}{d}\right) = d$ (<u>identità di Bezòut</u>), donde $\forall k \in \mathbb{Z}$ $\left(x_0 - k\frac{b}{d}, y_0 + k\frac{a}{d}\right)$ è soluzione dell' equazione.

<u>Corollario</u>: L'equazione diofantea lineare $ax + by = 1$ ha un insieme numerabile di soluzioni se $(a, b) = 1$.

<u>Dimostrazione</u>: Per la proposizione precedente $d = 1 = (a, b)$ è la condizione perché vi siano soluzioni.

Proposizione: La funzione di Eulero $\varphi(n)$ è moltiplicativa, cioè si ha $\forall n, m \in \mathbb{Z}$ primi tra loro per cui $(n,m) = 1$, che $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

Dimostrazione: Consideriamo l'applicazione
$f : [x]_{nm} \in \mathbb{Z}/nm\mathbb{Z} \xrightarrow{f} f([x]_{nm}) = ([x]_n, [x]_m) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, che risulta ben posta perché se due elementi sono uguali nell'insieme di partenza, allora anche le loro rispettive immagini lo sono nell'insieme di arrivo, ossia si ha $[x]_{nm} = [y]_{nm} \Rightarrow f([x]_{nm}) = f([y]_{nm})$.
Infatti

$[x]_{nm} = [y]_{nm} \Rightarrow y \in [x]_{nm} \Rightarrow y - x = k(nm), k \in \mathbb{Z} \Rightarrow y = x + (km)n \Rightarrow [y]_n = [x + (km)n]_n =$
$= [x]_n + [km]_n \cdot [n]_n = [x]_n + [km]_n \cdot [0]_n = [x]_n + [0]_n = [x + 0]_n = [x]_n$ e analogamente

$[x]_{nm} = [y]_{nm} \Rightarrow y \in [x]_{nm} \Rightarrow y = x + k(nm), k \in \mathbb{Z} = x + (kn)m \Rightarrow [y]_m = [x + (kn)m]_m =$
$= [x]_m + [kn]_m \cdot [m]_m = [x]_m + [kn]_m \cdot [0]_m = [x]_m + [0]_m = [x + 0]_m = [x]_m$.
Quindi

$[x]_{nm} = [y]_{nm} \Rightarrow [x]_n = [y]_n, [x]_m = [y]_m \Rightarrow ([x]_n, [x]_m) = ([y]_n, [y]_m) \Rightarrow f([x]_{nm}) = f([y]_{nm})$.
L'applicazione f è biiettiva ovvero al contempo suriettiva e iniettiva. Per provare ciò facciamo vedere che comunque preso un elemento $([a]_n[b]_m)$ dell'insieme di arrivo $\in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, questo è immagine tramite f di uno e un sol elemento $[x]_{nm}$ dell'insieme di partenza $\mathbb{Z}/nm\mathbb{Z}$.
Considerato allora l'elemento $([a]_n[b]_m) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, sia $x \in \mathbb{Z}$ tale che $x \in [a]_n \cap [b]_m$.
Affinché ciò abbia senso deve essere $[a]_n \cap [b]_m \neq \emptyset$ e ciò si ha perché $x \in [a]_n \cap [b]_m \Leftrightarrow \begin{cases} x \in [a]_n \\ x \in [b]_m \end{cases} \Rightarrow \begin{cases} x \equiv a(mod\ n) \\ x \equiv b(mod\ m) \end{cases}$ sistema di congruenze che per il teorema cinese del resto (pag.28) nel caso $\delta = (n,m) = 1$, è risolvibile e ha come unica soluzione la classe $[x]_{nm}$ (essendo
$\mu = m.c.m.(n,m) = nm$).
Avendosi allora che ad ogni fissata coppia ordinata $([a]_n[b]_m) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, corrisponde un'unica classe $[x]_{nm} \in \mathbb{Z}/nm\mathbb{Z}$ avente come immagine tramite f tale coppia, si ha che f è una biiezione tra $\mathbb{Z}/nm\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Vogliamo provare che f induce una corrispondenza biunivoca tra gli insiemi delle classi invertibili $\mathcal{A}_{nm}$ e $\mathcal{A}_n \times \mathcal{A}_m$, dove sappiamo che $\mathcal{A}_n = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} - \{[0]_n\} / [a]_n$ è invertibile$\}$. Se $[c]_{nm} \in \mathcal{A}_{nm}$ è una classe di $\mathcal{A}_{nm}$ invertibile, in base alla proposizione pag..31 deve essere $(c,nm) = 1$ e quindi per la proposizione pag.2 segue $(c,n) = 1$ e $(c,m) = 1$, il che implica l'invertibilità di $[c]_n \in \mathcal{A}_n$ e $[c]_m \in \mathcal{A}_m$. Da ciò segue allora che $f([c]_{nm}) = ([c]_n, [c]_m) \in \mathcal{A}_n \times \mathcal{A}_m$, ossia le immagini degli elementi $[c]_{nm} \in \mathcal{A}_{nm}$ sono gli elementi $([c]_n, [c]_m)$ di $\mathcal{A}_n \times \mathcal{A}_m$che si ottengono considerando la restrizione di f a $\mathcal{A}_{nm} \subset \mathbb{Z}/nm\mathbb{Z}$. Poiché f è iniettiva, lo è anche la sua restrizione
$g: [c]_{nm} \in \mathcal{A}_{nm} \subset \mathbb{Z}/nm\mathbb{Z} \longrightarrow g([c]_{nm}) = f([c]_{nm}) = ([c]_n, [c]_m) \in \mathcal{A}_n \times \mathcal{A}_m \subset \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, che trasforma nello stesso modo di f.
In modo equivalente ciò si può dimostrare osservando che, per essere $[c]_{nm}$una classe invertibile di $\mathbb{Z}/nm\mathbb{Z}$, deve $\exists h \in \mathbb{Z}$ tale che $[h]_{nm} \in \mathbb{Z}/nm\mathbb{Z}$ e $[c]_{nm} \cdot [h]_{nm} = [1]_{nm}$, che implica

$[ch]_{nm} = [1]_{nm} \Rightarrow ch \equiv 1(mod\ nm) \Rightarrow 1 \equiv ch(mod\ nm) \Rightarrow 1 - ch = k(nm), k \in \mathbb{Z}$.
Allora, dall'equazione lineare diofantea $ch + (nm)k = 1$ nelle incognite h e k, avente un insieme numerabile di soluzioni poiché $(c,nm) = 1$, segue che pure hanno soluzioni le equazioni lineari diofantee $ch + (km)n = 1$ e $ch + (kn)m = 1$.
Quindi necessariamente deve essere $(c,n) = 1$ e $(c,m) = 1$, donde l'invertibilità delle classi

$[c]_n \in \mathcal{A}_n$, $[c]_m \in \mathcal{A}_m \Rightarrow ([c]_n, [c]_m) \in \mathcal{A}_n \times \mathcal{A}_m$, ossia $f([c]_{nm}) \in \mathcal{A}_n \times \mathcal{A}_m$.

Proviamo ora che $g: \mathcal{A}_{nm} \longrightarrow \mathcal{A}_n \times \mathcal{A}_m$ è suriettiva, cioè fissato un qualsiasi elemento $([a]_n, [b]_m) \in \mathcal{A}_n \times \mathcal{A}_m$, esiste un unico elemento $[c]_{nm} \in \mathcal{A}_{nm}$, la cui immagine tramite g è $([a]_n, [b]_m) \in \mathcal{A}_n \times \mathcal{A}_m$. Poiché f è biunivoca, fissata la coppia $([a]_n, [b]_m) \in \mathcal{A}_n \times \mathcal{A}_m$, questa è immagine tramite f dell'unico elemento $[c]_{nm} \in \mathbb{Z}/nm\mathbb{Z}$ per cui

$f([c]_{nm}) = ([c]_n, [c]_m) = ([a]_n, [b]_m) \Rightarrow$
$[c]_n = [a]_n$ e $[c]_m = [b]_m$, donde $([c]_n, [c]_m) \in \mathcal{A}_n \times \mathcal{A}_m$. Vogliamo provare che $[c]_{nm} \in \mathcal{A}_{nm}$, avvenendo ciò se e solo se $(c, m) = 1$. Cominciamo a far vedere che $(c, n) = 1$ e $(c, m) = 1$.

Poiché $([a]_n, [b]_m) \in \mathcal{A}_n \times \mathcal{A}_m \Rightarrow [a]_n \in \mathcal{A}_n, [b]_m \in \mathcal{A}_m$, con $(a, n) = 1$ e $(b, m) = 1$, riferendosi inizialmente alla classe $[a]_n$, si ha che $\exists \alpha \in \mathbb{Z} \,/\, [a]_n \cdot [\alpha]_n = [1]_n \Rightarrow [a\,\alpha]_n = [1]_n \Rightarrow$

$1 \equiv a\alpha \pmod{n} \Rightarrow 1 = a\alpha + \beta n, \beta \in \mathbb{Z}$ opportuno. D'altra parte da $[c]_n = [a]_n \Rightarrow a \equiv c \pmod{n} \Rightarrow$

$a = c + kn, k \in \mathbb{Z}$ opportuno, da cui sostituendo segue

$1 = a\alpha + \beta n = \alpha(c + kn) + \beta n = \alpha c + (\alpha k + \beta)n$. Allora l'equazione $c\alpha + n(\alpha k + \beta) = 1$ è un'equazione diofantea lineare nelle incognite intere α e $\alpha k + \beta$ la quale ha soluzione se $(c, n) = 1$.

Ripetendo il ragionamento per la classe $[b]_m \in \mathcal{A}_m$, per cui deve essere $(b, m) = 1$, a causa dell'invertibilità di $[b]_m$ segue che $\exists \alpha' \in \mathbb{Z} \,/\, 1 = b\alpha' + \beta' m, \beta' \in \mathbb{Z}$ e poiché

$[c]_m = [b]_m \Rightarrow b = c + hn, h \in \mathbb{Z}$, segue $1 = \alpha' c + \left(\alpha' h + \beta'\right) m$, donde $(c, m) = 1$. Da ciò segue che necessariamente $(c, nm) = 1$, perché se per assurdo fosse $(c, nm) \neq 1$, allora esisterebbe almeno un intero p primo tale che $p|c$ e $p|nm$, ovvero essendo p primo per il teorema di Euclide pag.2 se $p|nm$ allora $p|n$ oppure $p|m$. In definitiva $p|c$ e $p|n$ oppure $p|m$ implica $(c, n) \neq 1$ oppure $(c, m) \neq 1$, contro l'ipotesi. Ne segue allora che $(c, nm) = 1$, conseguendo da ciò che $[c]_{nm} \in \mathbb{Z}/nm\mathbb{Z}$ è invertibile per cui tale classe deve appartenere a $\mathcal{A}_{nm}$. Allora la funzione g è suriettiva ed essendo iniettiva, risulta una biiezione tra $\mathcal{A}_{nm}$ e $\mathcal{A}_n \times \mathcal{A}_m$; questo implica l'uguaglianza delle cardinalità $\varphi(nm) = |\mathcal{A}_{nm}| = |\mathcal{A}_n \times \mathcal{A}_m| = |\mathcal{A}_n||\mathcal{A}_m| = \varphi(n) \cdot \varphi(m)$. Il teorema è così provato.

<u>Corollario</u>: Se p e q sono numeri primi, allora $\boldsymbol{\varphi(pq) = \varphi(p)\varphi(q)}$.

<u>Dimostrazione</u>: Essendo $\varphi(p) = p - 1$ e $\varphi(q) = q - 1$, si ha l'asserto per il teorema precedente.

Proposizione: Se p è un numero primo, allora $\forall h \in \mathbb{N}$ si ha

$$\varphi(p^h) = p^h - p^{h-1} = p^h\left(1 - \frac{1}{p}\right)$$

Dimostrazione: Se $h = 1$ si ha $\varphi(p^1) = \varphi(p) = p - 1 = p^1 - p^0$. Se $h > 1$, osservato che $\varphi(p^h)$ indica il numero degli interi minori o uguali a p^h e primi con p^h, il numero degli interi minori di p^h e non primi con p^h sono tutti e soli i multipli pk, con $1 \leq k \leq p^{h-1}$, di p minori o uguali a p^h, il cui numero è dato dal numero dei modi con cui si può scegliere k, ossia p^{h-1}. Il numero cercato è allora $\varphi(p^h) = p^h - p^{h-1}$.

Nota: Nella dimostrazione si sfrutta il fatto che un qualsiasi numero (nel nostro caso p^h) si può ottenere facendo la somma di tutti i numeri primi minori di esso (cioè $\varphi(p^h)$) e di tutti i numeri non primi minori di esso (che nel nostro caso è p^{h-1}), per cui il numero dei numeri primi col numero assegnato (cioè $\varphi(p^h)$) è uguale alla differenza tra il numero dato (cioè p^h) e il numero dei numeri non primi con il numero (cioè p^{h-1}).Il numero dei numeri t minori di p^h e non primi con p^h, ovvero per cui $(t, p^h) \neq 1$ è p^{h-1}per il seguente motivo. Un tal numero t ha nella sua scomposizione in fattori o p oppure una potenza di p che al più può essere p^h, per cui è del tipo $t = pk$, dove $k = 1, \dots, p^{h-1}$. Il numero dei numeri t è allora il numero dei numeri k, cioè p^{h-1}.

Poiché per il teorema fondamentale dell'Aritmetica esiste ed è unica la scomposizione in fattori primi di un qualsiasi numero intero, si ha:

Proposizione: Se $n \in \mathbb{N}$ ha la scomposizione in fattori primi $n = p_1^{h_1} p_2^{h_2} \cdot \dots \cdot p_s^{h_s}$, dove $p_i^{h_i}$, con $i = 1, \dots, s$, $s \in \mathbb{N}$, sono numeri interi primi distinti con esponenti $h_i \in \mathbb{N}$, allora si ha

$$\varphi(n) = \varphi\left(p_1^{h_1} p_2^{h_2} \cdot \dots \cdot p_s^{h_s}\right) = \varphi\left(p_1^{h_1}\right) \cdot \varphi\left(p_2^{h_2}\right) \cdot \dots \cdot \varphi\left(p_s^{h_s}\right)$$

Dimostrazione: Dimostriamo per induzione. Se s = 1 (base induttiva) allora

$n = p_1^{h_1} \Rightarrow \varphi(n) = \varphi(p_1^{h_1})$ e la tesi è ovviamente verificata. Supposto che la proposizione sia vera per un qualsiasi intero positivi n avente una fattorizzazione in s fattori primi distinti

$p_i \neq p_j$, $\forall i, j \in \mathbb{N}$ / $1 \leq i \neq j \leq s$ data da $n = p_1^{h_1} p_2^{h_2} \cdot \dots \cdot p_s^{h_s}$, sia m il numero intero

fattorizzabile negli s + 1 primi distinti $m = p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_s^{h_s} p_{s+1}^{h_{s+1}} = n p_{s+1}^{h_{s+1}}$, per cui deve aversi

$\left(n, p_{s+1}^{h_{s+1}}\right) = 1$ essendo relativamente primi n e il fattore $p_{s+1}^{h_{s+1}}$. Sfruttando il fatto che φ è moltiplicativa, stante l'ipotesi induttiva per cui la proposizione è vera per s, si ha che la proposizione è vera anche per s + 1, cioè

$$\varphi(m) = \varphi\left(p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_s^{h_s} p_{s+1}^{h_{s+1}}\right) = \varphi\left((p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_s^{h_s}) p_{s+1}^{h_{s+1}}\right) = \varphi\left(n \cdot p_{s+1}^{h_{s+1}}\right) = \varphi(n) \cdot \varphi\left(p_{s+1}^{h_{s+1}}\right) = \varphi\left(p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_s^{h_s}\right) \cdot \varphi\left(p_{s+1}^{h_{s+1}}\right) = \varphi\left(p_1^{h_1}\right) \varphi\left(p_2^{h_2}\right) \cdot \ldots \cdot \varphi\left(p_s^{h_s}\right) \cdot \varphi\left(p_{s+1}^{h_{s+1}}\right)$$

. In base allora al principio d'induzione, possiamo affermare che la proposizione è vera per ogni numero naturale s.

<u>Osservazione</u>: Che debba essere $\left(n, p_{s+1}^{h_{s+1}}\right) = 1$ risulta dal fatto che, per come si è definito n, nella scomposizione in fattori di quest'ultimo non figura il fattore primo $p_{s+1}^{h_{s+1}}$, ma d'altra parte se per assurdo si avesse $\left(n, p_{s+1}^{h_{s+1}}\right) = d \neq 1$, tale massimo comun divisore dovrebbe contenere nella sua scomposizione in fattori l'intero $p_{s+1}^{h_{s+1}}$ con una certa molteplicità $1 \leq r \leq s+1$, cioè aversi $d = \left(p_{s+1}^{h_{s+1}}\right)^r$, essendo p_{s+1} numero primo. Ma ciò implicherebbe che $\left(p_{s+1}^{h_{s+1}}\right)^r$ divide n e quindi per il teorema di Euclide che p_{s+1} divide $p_i^{h_i}$ per qualche $1 \leq i \leq s$, da cui l'uguaglianza $p_{s+1} = p_i$, assurdo essendo i fattori p_i primi distinti.

Il seguente corollario dà un'espressione di $\varphi(n)$ in funzione dei fattori primi di n indipendentemente dalla loro molteplicità, ovvero dell'esponente con cui compaiono nella fattorizzazione di n.

<u>Corollario</u>: Se $n \in \mathbb{N}$ ha la seguente scomposizione in fattori primi $p_i, (i = 1, \ldots, s)$ distinti

$n = p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_s^{h_s}$, si ha $\quad \varphi(n) = \varphi\left(\prod_{i=1}^{s} p_i^{h_i}\right) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$

<u>Dimostrazione</u>: Per le proposizioni precedenti, sfruttando il fatto che φ è moltiplicativa, si ha:

$$\varphi(n) = \varphi\left(\prod_{i=1}^{s} p_i^{h_i}\right) = \varphi\left(p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_s^{h_s}\right) = \varphi\left(p_1^{h_1}\right)\varphi\left(p_2^{h_2}\right) \cdot \ldots \cdot \varphi\left(p_s^{h_s}\right)$$
$$= p_1^{h_1}\left(1 - \frac{1}{p_1}\right) p_2^{h_2}\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot p_s^{h_s}\left(1 - \frac{1}{p_s}\right)$$
$$= p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_s^{h_s}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right) = n\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right)$$

Esempio: $n = 2^3 \cdot 5^2 \cdot 7 = 8 \cdot 25 \cdot 7 = 1400$; $\varphi(1400) = 1400\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = \frac{33600}{70} = 480$ sono i numeri minori o uguali a 1400 e primi con 1400.

La proposizione di pag.34 che stabilisce che φ è una funzione moltiplicativa, ovvero che $\forall n,m \in \mathbb{Z}$, $(n,m) = 1$, $\varphi(nm) = \varphi(n) \cdot \varphi(m)$, è suscettibile della seguente generalizzazione nel caso $(n,m) = d$, con $d \in \mathbb{N}$ anche se $d \neq 1$.

<u>Proposizione</u>: Se $n,m \in \mathbb{Z}$, hanno come massimo comun divisore $d = (n,m)$, allora si ha:

$$\varphi(nm) = \varphi(n) \cdot \varphi(m)\frac{d}{\varphi(d)}$$

<u>Dimostrazione</u>: Se d = 1, essendo $\varphi(d) = 1$ e $(n,m) = 1$, si ha la proposizione di pag.34 che è vera. Supposto allora che $d \neq 1$, ricordato che il massimo comun divisore di due interi n e m è un divisore comune a n e a m che risulta il più grande dei divisori comuni a n e a m, essendo multiplo di qualsiasi divisore comune a n e a m,si ha che se p è primo, allora $p \mid d \Leftrightarrow p|n \wedge p|m$, inoltre per il teorema di Euclide, $p \mid nm \Rightarrow p|n \vee p|m$ (potendo ovviamente dividere entrambi). Allora, estendendo la produttoria a tutti i numeri primi distinti p che dividono il prodotto nm e osservato che tra questi vi sono quelli che dividono n, quelli che dividono m e quelli che dividono eventualmente entrambi, il numero dei fattori primi distinti che dividono il prodotto nm è dato dal prodotto del numero dei fattori primi che dividono n per il numero dei fattori che dividono m, diviso per il numero dei fattori che dividono entrambi, cioè diviso per il massimo comun divisore di n e m.

Da ciò segue $\prod_{p|nm} = \prod_{p|n} \cdot \prod_{p|m} / \prod_{p|d}$. Si ha:

$$\begin{cases} \varphi(n) = n\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right) = n\prod_{p|n}\left(1-\frac{1}{p}\right) \\ \varphi(m) = m\prod_{j=1}^{u}\left(1-\frac{1}{p_j}\right) = m\prod_{p|m}\left(1-\frac{1}{p}\right) \\ \varphi(d) = d\prod_{r=1}^{v}\left(1-\frac{1}{p_r}\right) = d\prod_{p|d}\left(1-\frac{1}{p}\right) \end{cases} \Longrightarrow \begin{cases} \prod_{p|n}\left(1-\frac{1}{p}\right) = \frac{\varphi(n)}{n} \\ \prod_{p|m}\left(1-\frac{1}{p}\right) = \frac{\varphi(m)}{m} \\ \prod_{p|d}\left(1-\frac{1}{p}\right) = \frac{\varphi(d)}{d} \end{cases}$$, da cui si ottiene:

$$\varphi(nm) = nm\prod_{p|nm}\left(1-\frac{1}{p}\right) = nm\frac{\prod_{p|n}\left(1-\frac{1}{p}\right)\cdot\prod_{p|m}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)} = nm\frac{\frac{\varphi(n)}{n}\cdot\frac{\varphi(m)}{m}}{\frac{\varphi(d)}{d}} = \varphi(n)\cdot\varphi(m)\frac{d}{\varphi(d)}.$$

La funzione di Eulero ha altre interessanti proprietà su cui non ci soffermiamo non essendo strettamente funzionali al nostro discorso. Ritorniamo al problema dell'invertibilità delle calassi di congruenza modulo n.

In quale caso si ha che tutte le classi $[a]_n \neq [0]_n$ sono invertibili? Risponde a ciò la seguente proposizione.

<u>Proposizione</u>:

$\forall [a]_n \in \mathbb{Z}/n\mathbb{Z}-\{0\}$, $[a]_n$ è invertibile $\Leftrightarrow$ n è numero primo

<u>Dimostrazione</u>:

Considerato $n\in\mathbb{N}$ e $0<a<n$, la condizione è sufficiente perché se n è primo allora $n\neq 1$ e gli unici divisori positivi di n sono 1 ed n stesso per cui tutti gli interi positivi minori di n sono relativamente primi con n. In base alla proposizione precedente tutte le classi non nulle di $\mathbb{Z}/n\mathbb{Z}$ sono invertibili. La condizione è poi necessaria perché, se per assurdo n non fosse primo nell' ipotesi che tutte le classi non nulle risultino invertibili, n dovrebbe ammettere divisori non banali ovvero $\exists\, a,b\in\mathbb{Z}, 0<a<n, 0<b<n \,/\, n = ab$. Ora essendo $[a]_n \neq [0]_n$ poiché $1<a<n$, $[b]_n \neq [0]_n$ poiché $1<b<n$, stante la supposta invertibilità, deve aversi $[a]_n = [a]_n \bullet [1]_n = [a]_n ([b]_n \bullet [b']_n) = ([a]_n [b]_n) \bullet [b']_n = [ab]_n \bullet [b']_n = [n]_n \bullet [b']_n = [0]_n \bullet [b']_n = [0]_n$, cioè $[a]_n = [0]_n$, contro l'ipotesi che $[a]_n \neq [0]_n$.

Quindi

Proposizione:

$\mathbb{Z}/n\mathbb{Z}$-{$[0]_n$}(•) è un gruppo abeliano ⇔ n è primo

Dimostrazione:

Essendo verificate le proprietà associativa, commutativa, e l'esistenza dell'l'elemento neutro $[1]_n$, basta dimostrare che in $\mathbb{Z}/n\mathbb{Z}$-{$[0]_n$}(•) tutti gli elementi sono invertibili se e solo se n è primo, il che si ha per la proposizione precedente.

Ancora un po' di teoria

Sia **G(•)** un gruppo moltiplicativo ed H⊆G una sua parte. Consideriamo tutti gli elementi x,y∈H e gli inversi x^{-1} degli elementi non nulli di H, che possono non stare in H in quanto non è detto che H sia sottogruppo, quindi facendo tutti i possibili prodotti che possono non appartenere ad H. ma che appartengono a G, essendo G chiuso rispetto all'operazione. Il sottoinsieme di G che così si ottiene, contenendo i prodotti x x^{-1}=1, contiene l'unità, e per i suoi elementi continuano a valere le proprietà di gruppo, compresa la chiusura rispetto all'operazione, per cui risulta un sottogruppo di G detto <u>sottogruppo generato dalla parte H</u> che indichiamo con **<H>.** Esso risulta il minimo sottogruppo di G contenente H, intersezione di tutti i sottogruppi di G contenenti H. Consideriamo ora il caso che H si riduca ad un solo elemento g∈G, cioè **<H> = <g>.**Il sottogruppo generato dalla parte H = {g}, deve contenere allora i prodotti a due a due gg = g^2, g^{-1}g =1, g g^{-1}=1, g^{-1} g^{-1}= g^{-2}, a tre a tre ggg = g^3, g^{-1} g^{-1} g^{-1}= g^{-3}, altri prodotti a tre a tre danno elementi già trovati, a quattro a quattro gggg = g^4, g^{-1} g^{-1} g^{-1} g^{-1}= g^{-4}, altri prodotti a quattro a quattro danno elementi già trovati ecc. Quindi tali elementi non sono tutti distinti e si vede che **<g> =** { g^n /n∈$\mathbb{Z}$}, minimo sottogruppo di G contenente {g} costituito dalle potenze dell'elemento g∈G.

Definizione

Un gruppo G(•) si dice <u>ciclico</u> se ∃x∈G/<x> = G e l'elemento x dicesi <u>generatore</u> del gruppo G

Osservazione:

Affinché G risulti ciclico è sufficiente che esista almeno un elemento che lo generi e non che ogni elemento di G sia un generatore di G. Si noti che l'unità di G, $1\in G$, genera il sottogruppo identico di G , $<1> = \{1\}(\bullet)$.

Esempio: Il gruppo additivo degli interi $\mathbb{Z}(+)$ è ciclico avendosi $<1> = \mathbb{Z}(+)$. Per questo basta far vedere che l'unico sottogruppo di $\mathbb{Z}(+)$ che contiene 1 è $\mathbb{Z}(+)$.Infatti preso un qualsiasi sottogruppo di $\mathbb{Z}(+)$, allora deve essere $1\in\mathbb{Z}$, ma anche, per definizione di sottogruppo e quindi per la chiusura rispetto all'operazione, $1+1 = 2, 1+2 = 3\in\mathbb{Z}$, ecc..ed anche per l'esistenza dell'opposto di ogni elemento deve contenere $1-1 = 0, -2, -3, \ldots$ecc..,cioè tutto $\mathbb{Z}(+)$. Risultando allora $\mathbb{Z}(+)$ il minimo sottogruppo di $\mathbb{Z}(+)$ che contiene 1, si ha che $\mathbb{Z}(+) = <1>$, cioè che $\mathbb{Z}(+)$ è ciclico. Si vede facilmente che anche $<-1> = \mathbb{Z}(+)$, però si ha che $<2> = 2\mathbb{Z} = \{2n/n\in\mathbb{Z}\} = \mathbb{P}$, sottogruppo dei numeri pari, non è tutto $\mathbb{Z}(+)$, essendo $<t> = t\mathbb{Z}=\{tn/n\in\mathbb{Z}, t\in\mathbb{Z}_0^+\}\subset\mathbb{Z}(+)$ tutti e soli i sottogruppi di $\mathbb{Z}(+)$.

Sia **G(•)** un gruppo moltiplicativo, sappiamo che $\forall x\in$**G,** $x^n = 1$ per n = 0. per definizione. Il problema è ora di stabilire se esistano o meno $n\in\mathbb{N}/x^n = 1$ con $x\in$**G** fissato, per cui consideriamo l'insieme di tutti i numeri naturali che,per un determinato elemento x di G, siano esponenti di potenze uguali a 1, cioè supponiamo che $\{n\in\mathbb{N}/x^n = 1\}\neq\emptyset$.Detto $m = \min\{n\in\mathbb{N}/x^n = 1\}$(assioma del buon ordinamento), deve aversi $m\in\{n\in\mathbb{N}/x^n = 1\}$ per cui $x^m = 1$,con m più piccolo numero naturale per cui ciò accade. Considerato $<x> = \{x^0, x^1, x^2, \ldots, x^{m-1}\}<G$ sottogruppo ciclico generato da $x\in G$, vogliamo provare che tale sottogruppo ha ordine m e a tale scopo diamo le seguenti definizioni.

Definizione

Dicesi ordine o periodo dell'elemento $x\in G(\bullet)$ e si indica con o(x) oppure con |x|, il minimo intero positivo m per cui $x^m = 1$, mentre l'elemento x si dice periodico o di torsione.

Si pone in tal caso $o(x) < \infty$.

Nota:

$\{n\in\mathbb{N}/x^n = 1\}\neq\emptyset.\Longrightarrow\exists$ o(x), cioè il verificarsi di $x^n = 1$ per qualche n>0 , allora l'elemento x è periodico. Si noti pure che in ogni gruppo moltiplicativo l'unità è un elemento periodico di periodo 1 avendosi $1^n = 1$ con n=1 minimo intero positivo per cui ciò si verifica.

Definizione

L'elemento x∈G(•) si dice <u>aperiodico</u> o <u>senza torsione</u> se non è periodico ossia ∀n∈ℕ, $x^n \neq 1$
In tal caso si pone o(x) = ∞

Definizione

Si dice che G(•) è un <u>gruppo</u> <u>periodico</u> o <u>di torsione</u> se ∀x∈G-{1} si ha che x è periodico, cioè se o(x)< ∞.

Definizione

Si dice che G(•) è un <u>gruppo</u> <u>aperiodico</u> o <u>senza</u> <u>torsione</u> se ∀x∈G-{1} si ha che x è aperiodico, cioè se o(x)= ∞.

Definizione

Si dice che G(•) è un gruppo <u>misto</u> se esiste in G-{1} almeno un elemento periodico ed almeno un elemento aperiodico.

Proposizione:

Dato un gruppo moltiplicativo G(•), un elemento x∈G è periodico di ordine m se e solo se il sottogruppo ciclico generato da x ha ordine m, cioè se

$$x \in G, \qquad o(x) = m < \infty \iff |\langle x \rangle| = m$$

Osservazione:

In base a tale proposizione, dire che l'ordine di x è il minimo intero positivo m per cui $x^m = 1$ equivale ad asserire che l'ordine del sottogruppo ciclico generato da x è uguale ad m.

Dimostrazione:

La condizione è necessaria. Infatti se per x∈G si ha o(x) = m, allora deve esistere un intero m, minimo intero positivo per cui si verifica che $x^m = 1$. Il sottogruppo ciclico generato da x è per definizione <x> = { x^n /n∈ℤ}, ora tali potenze sono tutte e sole le m potenze a due a due distinte $x^0, x, x^2, ..., x^{m-1}$. Infatti esse sono tutte a due a due distinte perché se per assurdo esistessero almeno due potenze uguali $x^h = x^k$, con 0≤k<h≤m-1, allora $x^h = x^k \Rightarrow x^h x^{-k} = x^k x^{-k} \Rightarrow x^{h-k} = 1$, con 0<h-k<m ⇒o(x) = h-k<m, contro l'ipotesi o(x) = m, inoltre sono le sole perché se x^n ,n∈ℤ, allora dividendo n per m si ha n = mq + r, 0≤r<m,per cui $x^n = x^{mq+r} = x^{mq} x^r = (x^m)^q x^r = 1^q x^r = x^r \Rightarrow$ $x^n \in \{x^0, x, x^2, ..., x^{m-1}\} \Rightarrow$<x> = { x^n /n∈ℤ} = { $x^0, x, x^2, ..., x^{m-1}$}.⇒
❙ <x> ❙ = ❙ { $x^0, x, x^2, ..., x^{m-1}$} **❙ =** m. Viceversa se **❙ <x> ❙ = ❙**{ x^n /n∈ℤ} **❙** = m, tra tutte le potenze x^n , n∈ℤ, ce ne sono solo m distinte e sono le potenze $x^0, x, x^2, ..., x^{m-1}$. in quanto se per 0≤q<p≤m-1, si avesse $x^p = x^q \Rightarrow x^{p-q} = 1$, 0≤p-q<m⇒ o(x) = p-q < m, assurdo. Allora deve aversi **❙ <x> ❙ = ❙** { $x^0, x, x^2, ..., x^{m-1}$} **❙ =** m, e poiché o(x) = **❙ <x> ❙,** segue che o(x) = m.

La proposizione che segue stabilisce che tra i gruppi periodici ci sono tutti i gruppi finiti

Proposizione:

Se G è un gruppo finito, allora ogni elemento x∈G è periodico, ovvero G è periodico, e se G è un gruppo finito di ordine m per cui si ha |G| =m, allora ∀x∈G, o(x) è un divisore di m.

Dimostrazione:

Fissato x∈G, per la proposizione precedente si ha o(x) = |<x>|<∞, in quanto essendo G finito per ipotesi, deve essere finito anche il sottogruppo <x><G.Per il teorema di Lagrange sui gruppi finiti, l'ordine di ogni sottogruppo di un gruppo finito è un divisore dell'ordine del gruppo, quindi deve aversi |<x>|/|G|⇒o(x)/m, cioè o(x) divide m.

Osservazione:

Il viceversa non vale esistendo gruppi periodici infiniti. Tra i gruppi infiniti vi sono però anche gruppi non periodici come i gruppi ciclici infiniti, che sono tutti isomorfi a ℤ/0ℤ (+) ~ ℤ(+), in quanto ℤ(+) è aperiodico poiché ∀x∈ℤ-{0}, x è aperiodico (se per assurdo x fosse periodico, ∃n∈ℕ/nx = 0, contro la legge di annullamento del prodotto, avendosi n>0, x>0. Si noti che il solo 0 è periodico di periodo 1).

Nota:

Essendo o(x) un divisore di m deve aversi m = o(x)q, q∈ℕ, quindi in particolare
$x^m = x^{o(x)q} = (x^{o(x)})^q = 1^q = 1$

Proposizione:

Se G è G' sono gruppi isomorfi, allora G' è periodico, aperiodico, misto se e solo se lo è G.

Un esempio di gruppo misto è $\mathbb{Q}$-{0}(•). Infatti 2 è aperiodico (se fosse periodico $\exists n\in\mathbb{N}/2^n=1$,assurdo), mentre -1 è periodico in quanto $(-1)^2=1$. Esistendo allora almeno un elemento aperiodico ed uno periodico, il gruppo risulta misto.

Esempio: Il gruppo additivo $\mathbb{Z}/6\mathbb{Z}(+)$ = **{$[0]_5$,$[1]_5$,$[2]_5$,$[3]_5$,$[4]_5$,$[5]_6$}** essendo finito ha tutti gli elementi periodici in base alla seconda proposizione di pag.20, ed inoltre, dovendo il periodo di ogni elemento essere un divisore dell'ordine del gruppo che è 6, possono avere periodo uguale a 1, 2, 3, oppure 6. Ora, in generale si ha o($[x]_6$) = n se $\exists m\in\mathbb{N}$,minimo intero positivo/m$[x]_6$=$[0]_6$, quindi si ottiene che o($[0]_6$) = 1, perché $1[0]_6=[0]_6$con 1 minimo intero positivo affinché ciò sia. .Per trovare o($[1]_6$),osserviamo che essendo l'elemento neutro $[0]_6$ l'unico elemento di periodo 1, o($[1]_6$) può essere 2,3, o 6. Non può essere 2 perché $2[1]_6=[1]_6+[1]_6=[2]_6\neq[0]_6$, né può essere 3 in quanto $3[1]_6=[3]_6\neq[0]_6$, ed è 6 poiché $6[1]_6=[6]_6=[0]_6\Rightarrow$ o($[1]_6$) = 6. Tale fatto però poteva dedursi dalla considerazione che $[1]_6$ è il generatore del gruppo ciclico $\mathbb{Z}/6\mathbb{Z}(+)$, ossia $<[1]_6>=\mathbb{Z}/6\mathbb{Z}(+)$, per cui essendo l'ordine di un elemento uguale all'ordine del sottogruppo da esso generato, ovvero o($[1]_6$) = $|<[1]_6>|$, da $|\mathbb{Z}/6\mathbb{Z}|=6$ *segue* o($[1]_6$) = 6. Per lo stesso motivo si ha o($[5]_6$) = $|<[5]_6>|$ = 6 poiché $<[5]_6>=\mathbb{Z}/6\mathbb{Z}$. Si ha o($[2]_6$) = 3, in quanto $3[2]_6=[6]_6=[0]_6$, con 3 minimo intero positivo per cui accade ciò.In tale modo si calcolano i periodi degli altri elementi.

Arrivati a questo punto ci chiediamo se dato un gruppo moltiplicativo G(•), il sottoinsieme dei suoi elementi periodici(di torsione) costituisca o meno un sottogruppo di G, cioè se

$$T=\{x\in G/\exists n\in\mathbb{N}, x^n=1\}<G(\bullet).$$

La seguente proposizione risponde a tale domanda.

Proposizione:

Il sottoinsieme degli elementi periodici di un gruppo G risulta un sottogruppo di G se G è abeliano.

Nota:

Tale sottogruppo prende il nome di <u>sottogruppo di torsione</u> o massimo sottogruppo di torsione del gruppo G.

Osservazione:

La condizione è solo necessaria esistendo esempi di gruppi G non abeliani aventi un sottogruppo T di torsione.

Dimostrazione:

Sia T = {x∈G/∃n∈ℕ, $x^n = 1$}⊆G, ∀x,y∈T si ha che anche xy∈T, ossia T è parte stabile rispetto all'operazione di G, solo nell'ipotesi che il prodotto sia commutativo, ovvero quando G è abeliano,potendo in tal caso permutare gli elementi nei prodotti seguenti x,y∈T⇒∃n,m∈ℕ/ $x^n = 1, y^m = 1 \Rightarrow (xy)^{mn} = \underbrace{(xy)\ldots(xy)}_{mnvolte} = \underbrace{(x\ldots x)(y\ldots y)}_{mnvolte} = x^{mn}y^{mn} = (x^n)^m(y^m)^n$ $= 1^m 1^n = 1$⇒xy∈T. Si noti che non è detto che mn sia il periodo di xy ovvero il minimo intero per cui $(xy)^{mn} = 1$.

Consideriamo ora l'insieme $\mathcal{A}_n$ = {$[a]_n \in \mathbb{Z}/n\mathbb{Z} - \{[0]_n\}$/$[a]_n$ è invertibile}, dove per la proposizione pag.31, si ha che il numero delle classi invertibili sarà dato dal numero degli interi positivi a>0 minori di n e primi con n, cioè si ha $|\mathcal{A}_n| = \varphi(n)$. Poiché in $\mathcal{A}_n$ vale la proprietà associativa, c'è l'elemento neutro $[1]_n$, ogni classe è invertibile e l'inverso è in $\mathcal{A}_n$, la struttura $\mathcal{A}_n$ (·) è un gruppo moltiplicativo di ordine $\varphi(n)$. A pag. 36 abbiamo dimostrato che se G è un gruppo finito, allora ogni suo elemento x è periodico e quindi, in base alla definizione anche G stesso lo è, per cui se n è l'ordine di G e m quello di x, minimo intero positivo per cui si ha $x^m = 1$, m deve essere un divisore di n, donde posto n = mq , con q intero opportuno, si ricava $x^n = x^{mq} = (x^m)^q = 1^q = 1$.In sintesi : in un gruppo finito di ordine n quindi periodico, si ha che la potenza di ogni elemento, anch'esso periodico, di esponente l'ordine del gruppo è uguale all'unità del gruppo.

Teorema di Eulero – Fermat

Se a∈ℤ, n∈ℕ, (a,n) = 1 si ha $a^{\phi(n)} \equiv 1\,(\boldsymbol{mod\ n})$

Dimostrazione:

Per la proposizione a pag.31 si ha (a,n) = 1⇒$[a]_n$ è invertibile ⇒$[a]_n \in \mathcal{A}_n$= {$[a]_n \in \mathbb{Z}/n\mathbb{Z} - \{[0]_n\}$/ $[a]_n$ è invertibile}, dove $\mathcal{A}_n(\cdot)$ è gruppo moltiplicativo finito di ordine $\varphi(n)$. Per quanto prima detto, si ha che la potenza di un elemento $[a]_n$ del gruppo $\mathcal{A}_n(\cdot)$ di esponente l'ordine $\varphi(n)$ del gruppo deve essere uguale all'unità del gruppo. Deve quindi risultare: $([a]_n)^{\phi(n)} = [1]_n$ e poiché $([a]_n)^{\phi(n)} = \underbrace{[a]_n \ldots [a]_n}_{\phi(n)volte} = [\underbrace{a\ldots a}_{\phi(n)volte}] = [a^{\phi(n)}]_n \Longrightarrow a^{\phi(n)} \equiv 1 (\text{mod } n)$

Nota: Ovviamente il teorema ha la formulazione equivalente

$$[\boldsymbol{a}^{\boldsymbol{\varphi(n)}}]_{\boldsymbol{n}} = [\mathbf{1}]_{\boldsymbol{n}} \text{ se } (\boldsymbol{a}, \boldsymbol{n}) = \mathbf{1}$$

Corollario: $Se\ \ N = pq, con\ p, q\ primi, \quad si\ ha \quad a^{(p-1)(q-1)+1} \equiv a\ (mod\ N)$

Dimostrazione:

Posto N = pq, con p,q primi, se a∈ℤ deve essere M.C.M. (a,N) = 1, per cui in base al teorema di Eulero-Fermat si ha $a^{\phi(N)} \equiv 1(\mathrm{mod}\, N)$. Ora φ(N) = (p-1)(q-1). Infatti, essendo p e q entrambi primi, tutti gli interi minori di p sono primi con p e così tutti gli interi minori di q sono primi con q, e . poiché tutti gli interi minori di p sono p-1 e tutti gli interi minori di q sono q-1, tutti i possibili prodotti che sono (p-1)(q-1), sono primi col prodotto pq = N. Il numero di tutti i numeri interi minori di pq e primi con pq è allora (p-1)(q-1). Possiamo allora scrivere $\mathbf{a}^{(p-1)(q-1)} \equiv 1(\mathrm{mod}\, N)$ $\Rightarrow$**a** $\mathbf{a}^{(p-1)(q-1)} \equiv 1a(\mathrm{mod}\, N)$ $\Rightarrow$ $\mathbf{a}^{(p-1)(q-1)+1} \equiv$ **a** (mod N).

Nota:

Considerato un orologio a numeri primi di Fermat, cioè un orologio sul cui quadrante c'è un numero primo p di ore, L.Eulero nel 1736, cento anni dopo la formulazione di Fermat, scoprì la dimostrazione del teorema, ossia del perché considerata una qualsiasi ora sul quadrante dell'orologio, moltiplicando per se stessa tale ora p volte, la lancetta ritorna al punto di partenza. Anzi **Eulero** estese il teorema al caso che, posto **N = pq**, con p,q primi, si ha :
.

$$\mathbf{a}^{(p-1)(q-1)+1} \equiv \mathbf{a}\ (\mathbf{mod\ N})$$

Tale teorema ha oggi una notevole importanza nella crittografia. Supponete di avere un mazzo di carte da gioco e di disporre una carta in cima al mazzo, quindi di mischiare le carte. Un prestigiatore è in grado, grazie al piccolo teorema di Fermat, di far riapparire la carta da voi scelta in cima al mazzo, dopo una opportuna sequenza di rimescolate. Basta ad esempio dividere il mazzo in due parti uguali, quindi mischiare le due parti in modo di alternare a ciascuna carta di una metà una carta dell'altra metà per otto volte consecutive e, sorpresa, il mazzo ritorna nella sua configurazione iniziale. Allora su di un orologio con N = pq ore sul quadrante, il solo modo per vedere ricomparire il vostro numero sul quadrante (il numero di carta di credito introdotto in un acquisto su Internet) è quello di conoscere i due numeri primi p e q, quindi in base al teorema di Fermat-Eulero il numero appare dopo (p-1)(q-1)+1 rimescolamenti. Quindi per un hacker la difficoltà risiede nel fattorizzare il numero noto N (numero delle cifre possibili di una carta di credito) nel prodotto di due numeri primi di solito molto grandi. Quando un cliente fa un ordine sul sito di un'azienda, l'azienda prende due numeri primi p e q di 60 cifre, li moltiplica tra loro ottenendo un numero N di 120 cifre e tale numero è il numero di ore sul calcolatore ad orologio che ogni cliente userà per cifrare il proprio numero C di carta di credito. Quindi l'azienda fornisce a tutti i clienti uno stesso numero di codifica E (che corrisponde al numero di scozzate effettuate dal prestigiatore del mazzo di carte), allora la cifratura consiste nel calcolare C^E ,tanto l'azienda sa che per il teorema di Fermat-Eulero $C^E \equiv C$ (mod N) . Chiaramente si può risalire al valore di E = (p-1)(q-1) + 1, solo se si conoscono i valori di p e q.

Corollario:

Piccolo teorema di Fermat

Se p è un numero primo, ∀a∈ℤ si ha che $a^p \equiv a \pmod{p}$

Osservazione: Si noti che nell'enunciato non c'è alcuna limitazione sugli elementi a∈ℤ da prendere, mentre nel teorema di Eulero-Fermat gli interi a∈ℤ dovevano essere relativamente primi con n.

Dimostrazione:

Poiché per ipotesi p è primo, per la proposizione a pag.17 si ha φ(p) = p-1 perché tutti i numeri che precedono p non avendo fattori comuni con p risultano primi con p. Fissato ora in modo arbitrario un intero a∈ℤ, vi sono solo due possibilità: a<p oppure a≥p. Se a<p, essendo p primo, deve aversi M.C.D.(a,p) = 1, in quanto a e p risultano relativamente primi. Se invece a≥p, vi sono due eventualità: a è relativamente primo con p per cui M.C.D.(a,p) = 1, a è un multiplo di p ed allora evidentemente deve risultare M.C.D.(a,p) = p, perché l'unico divisore comune di p ed a è p stesso. Dimostriamo il teorema nei due casi possibili M.C.D.(a,p) = 1 e M.C.D.(a,p) = p. Se si verifica M.C.D.(a,p) = 1, per il teorema di Eulero-Fermat (pag.22) si ha $a^{\phi(p)} \equiv 1 (\mathrm{mod} p) \Longrightarrow a^{p-1} \equiv 1 (\mathrm{mod}\ p)$ e poiché la relazione di congruenza è compatibile col prodotto, si può moltiplicare ambo i membri della congruenza per a ottenendo $a^{p-1} \equiv 1 (\mathrm{mod}\ p) \Longrightarrow aa^{p-1} \equiv 1a (\mathrm{mod}\ p) \Rightarrow a^p \equiv a (\mathrm{mod}\ p)$. Se invece risulta M.C.D.(a,p) = p, a essendo multiplo di p deve essere del tipo a = ph, h∈ℤopportuno$\Longrightarrow$ $a^p = \underbrace{a....a}_{p volte} = \underbrace{(ph)...(ph)}_{p volte} = p(p^{p-1}h^p) =$ pk, k∈ℤ, da cui, sottraendo membro a membro, si ha $a^p - a = p(k-h) = pt$, t∈ℤ$\Longrightarrow a^p \equiv a (\mathrm{mod}\ p)$.

Diamo un'altra dimostrazione del teorema che se da una parte ha il pregio di non sfruttare i risultati della teoria dei gruppi per cui risulta per così dire "elementare", dall'altra utilizza gli elementi base del calcolo combinatorio ed è quindi formalmente più pesante. Enunciamo il teorema nel seguente modo equivalente

Piccolo teorema di Fermat

Se p è un numero primo, ∀n∈ℤ si ha che $n^p \equiv n (\mathrm{mod}.p)$

Dimostrazione n.2:

Consideriamo le disposizioni con ripetizione di n elementi $a_1, a_2, ..., a_n$ a p a p, cioè tutte le possibili p-ple $a_{i_1}, a_{i_2}, ..., a_{i_p}$ (i = 1,2,…,n), il cui numero è n^p e notiamo sono in numero di n quelle che hanno tutti gli elementi uguali perché tanti sono gli elementi $a_1, a_2, ..., a_n$.Prese quindi tutte le possibili p-ple in cui non tutti gli elementi sono uguali, il loro numero è $n^p - n = N_p$, fissatone una

in modo arbitrario che indichiamo con $\mathcal{J}_1$, le permutazioni dei suoi p elementi dove a_{i_1} si ripete $r_{a_{i_1}} <$ p volte,…, a_{i_p} si ripete $r_{a_{i_p}} <$ p volte sono date da $P_{J_1} = \dfrac{p!}{r_{a_{i_1}}!\ldots r_{a_{i_p}}!} = p\dfrac{(p-1)!}{r_{a_{i_1}}!\ldots r_{a_{i_p}}!} =$ p k_{J_1}, $k_{J_1} \in \mathbb{Z}$, cioè il numero delle permutazioni con ripetizione P_{J_1} è un multiplo di p. Si noti che P_{J_1} deve essere un numero intero e poiché p è primo, $r_{a_{i_1}}!\ldots r_{a_{i_p}}!$ devono essere divisori di (p-1)! Donde risulta che k_{J_1} è un intero. Sia $\omega_1 = N_p - P_{J_1} \geq 0$ il numero di tutte le p-ple $a_{i_1}, a_{i_2}, \ldots, a_{i_p}$ dove non tutti gli elementi sono uguali detratto del numero di tutte le possibili permutazioni con ripetizione di una generica p-pla $a_{i_1}, a_{i_2}, \ldots, a_{i_p}$ .Se $\omega_1 = 0$ il teorema è dimostrato poiché $\omega_1 = 0 \Rightarrow N_p - P_{J_1} = 0 \Rightarrow N_p = P_{J_1} \Rightarrow n^p - n = pk_{J_1} \Rightarrow n^p \equiv n(\text{mod } .p)$. Se invece $\omega_1 > 0$, scegliamo arbitrariamente una p-pla $a_{j_1}, \ldots, a_{j_p}$ che indichiamo con $\mathcal{J}_2$, distinta da $a_{i_1}, a_{i_2}, \ldots, a_{i_p}$ nell'n-pla $a_1, a_2, \ldots, a_n$ le cui permutazioni con ripetizione sono date da P_{J_2} = p k_{J_2} Consideriamo il numero $\omega_2 = \omega_1 - P_{J_2} = N_p - P_{J_1} - P_{J_2} \geq 0$. Se $\omega_2 = 0$ il teorema è dimostrato perché $\omega_2 = 0 \Rightarrow \omega_1 = P_{J_2} \Rightarrow N_p - P_{J_1} = P_{J_2} \Rightarrow N_p = P_{J_1} + P_{J_2} \Rightarrow$ $n^p - n = pk_{J_1} + pk_{J_2} = p(k_{J_1} + k_{J_2}) \Rightarrow n^p \equiv n(\text{mod } .p)$. Se $\omega_2 > 0$, posto $\omega_3 = \omega_2 - P_{J_3} \geq 0$, il teorema è dimostrato se $\omega_3 = 0$, altrimenti se $\omega_3 > 0$ si continua fino a determinare un intero h∈ℕ per cui $\omega_h = 0 \Rightarrow n^p \equiv n(\text{mod } .p)$ ed il teorema è dimostrato.

Nota:

In altri termini $a^p \equiv a(\text{mod } p) \Rightarrow$ a**p** - a è divisibile per p .per cui a ^{p} ed a hanno lo stesso resto nella divisione per p. in base a quello che abbiamo precedentemente visto. In altre parole, se si prende su un orologio con un numero primo p di ore sul quadrante un numero a e lo si eleva alla potenza p, si ottiene sempre il numero da cui si è partiti.

Ad esempio, se su un orologio con 5 ore sul quadrante, prendiamo il numero 2 e lo eleviamo alla 5, otteniamo 32 che corrisponde a 2 perché il resto della divisione di 32 e 5 è 2.. Procedendo in questo modo, la lancetta dell'orologio dopo 5 passi ritorna al punto di partenza e quindi si ha un andamento ripetitivo come è illustrato dalla seguente tabella in cui la lancetta si ferma su tutte le ore. Si noti però che anche $2^9 \equiv 2(\text{mod}\,5)$ e così per infiniti numeri interi non necessariamente primi, per cui si deduce che in generale l'equazione $a^x \equiv a(\text{mod } p)$ non ha come unica soluzione x = p; il piccolo teorema di Fermat asserisce solo che x = p è certamente una soluzione dell'equazione.

Potenze di 2	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
Calcolo convenzionale	2	4	8	16	32	64	128	256	512	1024
Calcolo su un orologio con 5 ore	2	4	3	1	2	4	3	1	2	4

In un orologio con 13 ore la lancetta ha sempre un andamento ripetitivo ma non si ferma su tutte le ore come si vede dalla seguente tabella

Potenze di 3	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9	3^{10}	3^{11}	3^{12}	3^{13}
Calcolo convenzionale	3	9	27	81	243	729	2187	6561	19683	59049	177147	531441	1594323
Calcolo su un orologio con 13 ore	3	9	1	3	9	1	3	9	1	3	9	1	3

Il piccolo teorema di Fermat si può dimostrare per induzione, prescindendo dal teorema di Fermat – Eulero, anzi esso implicando quest'ultimo è ad esso equivalente. Primo di procedere a questa dimostrazione, premettiamo una proprietà dei numeri primi utile alla stessa dimostrazione.

Definito il coefficiente binomiale $\binom{p}{i}$ (leggi p su i) come l'applicazione

$f: (p, i) \in \mathbb{N} \times \{1, \dots, p-1\} \to f(p,i) = \binom{p}{i} = \frac{p(p-1)\cdot\ldots\cdot(p-i+1)}{i} \in \mathbb{N}$, che associa ad ogni coppia di interi positivi (p,i), con $p \in \mathbb{N}$ e $i \in \{1, \dots, p-1\}$, l'intero $\binom{p}{i} = \frac{p(p-1)\cdot\ldots\cdot(p-i+1)}{i}$. Che si tratti di un intero è dovuto al fatto che i può essere uno dei fattori del numeratore oppure è un divisore di qualcuno di essi se $1 < p < (p-i+1)$.

<u>Proposizione</u>: **p primo** $\Leftrightarrow$ $p \left| \binom{p}{i} \right.$, $\forall i: 0 < i < p$

<u>Dimostrazione</u> :Se p è primo allora, per ogni fissato intero positivo i minore di p, si ha per definizione di coefficiente binomiale $\binom{p}{i} = \frac{p(p-1)\cdot\ldots\cdot(p-i+1)}{i}$, per cui p essendo un fattore del prodotto, deve dividere necessariamente $\binom{p}{i}$. Viceversa se $p \left| \binom{p}{i} \right.$, $\forall i: 0 < i < p$, per ogni fissato i, p divide il prodotto $\frac{p(p-1)\cdot\ldots\cdot(p-i+1)}{i}$, quindi dividendo sé stesso non può dividere gli interi $(p-1), \dots, (p-i+1)$ minori di esso, per cui risulta primo.

Piccolo teorema di Fermat

(dimostrazione indipendente dal teorema di Eulero-Fermat)

Se p è un numero primo, $\forall a \in \mathbb{Z}$ si ha che $\boxed{a^p \equiv a \pmod{p}}$

<u>Dimostrazione</u>:

Supponiamo inizialmente $a \geq o$ e dimostriamo per induzione su a.

Se $a = 0 \Rightarrow 0^p = 0$, d'altra parte $0 \equiv 0 \ (mod\ p)$, quindi $0^p \equiv 0 \ (mod\ p), \forall p \in \mathbb{Z}$ e quindi in particolare per p primo. Se $a > 0$, supponiamo che sia vero per ipotesi induttiva $a^p \equiv a (mod\ p)$ e dimostriamo che ciò vale anche per $a + 1$.

Infatti, per la formula del binomio di Newton si ha $(a+1)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} 1^i =$

$$\sum_{i=0}^{p} \binom{p}{i} a^{p-i} = \binom{p}{0} a^p + \binom{p}{1} a^{p-1} + \dots + \binom{p}{p-1} a + \binom{p}{p} a^0 = a^p + pa^{p-1} + \dots + pa + 1 =$$

$\sum_{i=1}^{p-1}\binom{p}{i}a^{p-i}+a^p+1$. Ora per la proposizione precedente si ha, per ogni fissato indice i tale che $0<i<p$, che p divide i coefficienti binomiali $\binom{p}{i}$ per cui si ha $\binom{p}{i}=pk_i$, con $k_i\in\mathbb{Z}$ opportuno. Allora

$$(a+1)^p-(a^p+1)=\sum_{i=1}^{p-1}\binom{p}{i}a^{p-i}=\sum_{i=1}^{p-1}pk_i\,a^{p-i}=p\sum_{i=1}^{p-1}k_i\,a^{p-i}=ph$$

, dove $h=\sum_{i=1}^{p-1}k_i\,a^{p-i}\in\mathbb{Z}$.

Segue $(a+1)^p-(a^p+1)=ph\Rightarrow(a+1)^p\equiv a^p+1\ (mod\ p)$, quindi valendo l'ipotesi induttiva $a^p\equiv a(mod\ p)$, si ha $a^p+1\equiv a+18mod\ p)$, donde $(a+1)^p\equiv a+1\ (mod\ p)$. Per il principio d'induzione allora $\forall n\in\mathbb{N}$ si ha $a^p\equiv a(mod\ p)$.

Nel caso che $a<0$ si ha $-a>0\Rightarrow(-a)^p\equiv(-a)\ (mod\ p)$ ed inoltre

$$[a+(-a)]^p=\sum_{i=0}^{p}\binom{p}{i}a^{p-i}(-a)^i=\sum_{i=1}^{p-1}\binom{p}{i}a^{p-i}(-a)^i+a^p+(-a)^p\Rightarrow$$

$$[a+(-a)]^p-[a^p+(-a)^p]=\sum_{i=1}^{p-1}\binom{p}{i}a^{p-i}(-a)^i=$$

$$p\sum_{i=1}^{p-1}k_i\,a^{p-i}(-a)^i=ph\Rightarrow[a+(-a)]^p\equiv a^p+(-a)^p(mod\ p)\Rightarrow$$

$$a+[a+(-a)]^p\equiv a+a^p+(-a)^p(mod\ p).$$

Allora

$$a=a+0=a+0^p=a+[a+(-a)]^p\equiv a+a^p+(-a)^p\equiv a+a^p+(-a)=a^p\ (mod\ p)$$

, cioè $a^p\equiv a(mod\ p)$ ed il teorema è così completamente provato.

Corollario:

Se $(a,p)=1$, cioè l'intero a è relativamente primo con il modulo p della congruenza, si ha

$$\boxed{a^{p-1}\equiv 1\ (mod\ p)}$$

Dimostrazione: Per la proposizione pag. 34, essendo $(a,p)=1$, $[a]_p$ è invertibile, per cui esiste la classe inversa $[a]_p^{-1}$ tale che

$[a]_p\cdot[a]_p^{-1}=[1]_p\Rightarrow[a]_p\cdot[a^{-1}]=[1]_p\Rightarrow aa^{-1}\equiv 1\ (mod\ p)$. Per il piccolo teorema di Fermat si ha

$a^p \equiv a(mod\ p) \Rightarrow a^p a^{-1} \equiv aa^{-1}(mod\ p) \Rightarrow a^{p-1} \equiv aa^{-1}(mod\ p)$, quindi avendosi

$a^p a^{-1} \equiv 1\ (mod\ p)$, per la transitività della congruenza segue $a^{p-1} \equiv 1\ (mod\ p)$.
Facciamo vedere ora la dimostrazione del teorema di Fermat- Eulero noto il Piccolo teorema di Fermat.

Teorema di Fermat – Eulero

Se a e n sono due interi primi tra loro, allora

$$\boldsymbol{a^{\varphi(n)} \equiv 1\ (mod\ n)}$$

<u>Dimostrazione</u>:

Per il teorema fondamentale dell'Aritmetica si ha che esiste ed è unica la scomposizione in fattori primi dell'intero n, cioè si ha: $n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}$, $s \in \mathbb{N}$ Cominciamo a provare il teorema nel caso che s = 1, cioè che $n = p_1^{h_1} = p^h$, con p primo per induzione si h.

Se h = 1, si ha $\varphi(n) = \varphi(p^h) = \varphi(p) = p - 1 \Rightarrow a^{\varphi(p)} = a^{p-1}$, quindi per il corollario del piccolo teorema di Fermat $a^{p-1} \equiv 1(mod\ p)$, segue $a^{\varphi(n)} \equiv 1\ (mod\ n)$, donde è vera la base induzione. Supposto ora che il teorema valga per un qualsiasi intero fissato $h \geq 1$, per cui $n = p^h$, cioè che

$a^{\varphi(n)} \equiv 1\ (mod\ n) \Rightarrow a^{p^h} \equiv 1(mod\ n)$, proviamo che il teorema vale pure per h + 1 e che cioè si abbia
$a^{\varphi(p^{h+1})} \equiv 1\ (mod\ p^{h+1})$.
Per la proposizione pag.36 si ha $\varphi(p^{h+1}) = p^{h+1} - p^h = p(p^h - p^{h-1}) = p\varphi(p^h)$. Ora essendo

$1 \leq h \Rightarrow$
$h + 1 \leq 2h \leq ih\,, i \geq 2$, inoltre per definizione di congruenza si ha $a^{\varphi(p^h)} \equiv 1\ (mod\ p^h)$
$\Leftrightarrow \exists k \in \mathbb{Z}\ /\ a^{\varphi(p^h)} - 1 = kp^h \Leftrightarrow a^{\varphi(p^h)} = 1 + kp^h$. Allora per quanto detto, applicando la formula del binomio di Newton, segue $a^{\varphi(p^{h+1})} = a^{p\varphi(p^h)} = \left(a^{\varphi(p^h)}\right)^p = (1 + kp^h)^p =$
$\sum_{i=0}^{p} \binom{p}{i} (kp^h)^i =$
$\sum_{i=0}^{p} \binom{p}{i} k^i p^{ih} = \sum_{i=0}^{p} \binom{p}{i} k^i p^{ih-(h+1)+(h+1)} = \sum_{i=0}^{p} \binom{p}{i} k^i p^{ih-(h+1)} p^{h+1} =$
$p^{h+1} \sum_{i=0}^{p} \binom{p}{i} k^i\, p^{ih-(h+1)} = p^{h+1} \binom{p}{0} p^{-(h+1)} + p^{h+1} \binom{p}{1} kp^{h-(h+1)} + p^{h+1} \sum_{i=2}^{p} \binom{p}{i} k^i\, p^{ih-(h+1)}$
$= 1 + kpp^h + p^{h+1} \sum_{i=2}^{p} \binom{p}{i} k^i\, p^{ih-(h+1)} = 1 + p^{h+1}\left(k + k \sum_{i=2}^{p} \binom{p}{i} k^{i-1}\, p^{ih-(h+1)}\right) =$
$1 + p^{h+1} k \left(1 + \sum_{i=2}^{p} \binom{p}{i} k^{i-1}\, p^{ih-(h+1)}\right) = 1 + p^{h+1} kt$, dove l'intero t è il termine in parentesi.

Quindi posto $u = kt$, si ha $a^{\varphi(p^{h+1})} = 1 + up^{h+1} \Rightarrow a^{\varphi(p^{h+1})} \equiv 1\ (mod\ p^{h+1})$, per cui in base al principio d'induzione segue che $\forall h \in \mathbb{N}$ è vero che $a^{\varphi(p^h)} \equiv 1(mod\ p^h)$.

Nel caso generale che n sia scomponibile in un numero fissato s di fattori potenze di numeri primi per cui $n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}$, osservato che si è provato prima che $\forall i \in \{1,2,\ldots,s\}$ $a^{\varphi\left(p_i^{h_i}\right)} \equiv 1(mod\ p_i^{h_i})$ e che $\varphi\left(p_i^{h_i}\right)$ è un divisore di $\varphi(n)$ in quanto, essendo φ moltiplicativa, si ha $\varphi(n) = \varphi\left(\prod_{i=0}^{s} p_i^{h_i}\right) = \prod_{i=0}^{s} \varphi\left(p_i^{h_i}\right) \Rightarrow \varphi\left(p_i^{h_i}\right) \Big| \varphi(n) \Rightarrow \frac{\varphi(n)}{\varphi\left(p_i^{h_i}\right)} \in \mathbb{Z}$ e si ha pure

$a^{\varphi(n)} \equiv 1\ (mod\ p_i^{h_i})$ poché $a^{\varphi(n)} = a^{\varphi\left(p_i^{h_i}\right)\cdot\frac{\varphi(n)}{\varphi\left(p_i^{h_i}\right)}} = \left(a^{\varphi\left(p_i^{h_i}\right)}\right)^{\frac{\varphi(n)}{\varphi\left(p_i^{h_i}\right)}} \equiv 1\ (mod\ p_i^{h_i})$,

applicando la proposizione 4, pag.6.
Allora applicando la proposizione 8 pag.7 si ha
$a^{\varphi(n)} \equiv 1(mod\ p_1^{h_1}) \wedge \ldots \wedge a^{\varphi(n)} \equiv 1\left(mod\ p_s^{h_s}\right) \Rightarrow a^{\varphi(n)} \equiv 1\left(mod\ p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}\right) \Rightarrow a^{\varphi(n)} \equiv 1(mod\ n)$ e il teorema è provato.

<u>Nota</u>:

Il teorema di Eulero – Fermat permette di semplificare potenze del tipo $a^m\ (mod\ n)$ con $(a,n) = 1$, nel senso che assegnata una congruenza modulo n e la potenza $a^m, m \in \mathbb{N}$, dove la base a della potenza e il modulo n della congruenza sono relativamente primi, si chiede di trovare un rappresentante x della classe $[a^m]_n$ più piccolo di a^m , ossia tale che $x \equiv a^m\ (mod\ n)$. Il teorema di Eulero – Fermat assicura che $a^{\varphi(n)} \equiv 1(mod\ n)$ se $(a,n) = 1$, cioè che $\left[a^{\varphi(n)}\right]_n = [1]_n$.
Allora, verificato che $(a,n) = 1$, ovvero che a e n sono primi tra loro, si calcola $\varphi(n)$, poi si divide m per $\varphi(n)$, ottenendo $m = \varphi(n)$q+r, dove q è il quoziente e $0 \leq r < \varphi(n)$ è il resto, quindi si ottiene $a^m = a^{\varphi(n)\mathrm{q+r}} = \left(a^{\varphi(n)}\right)^q \cdot a^r$. Ora, per la proprietà 4 pag. 6 e il Teorema di Fermat - Eulero, si ha $a^{\varphi(n)} \equiv 1(mod\ n) \Leftrightarrow \left(a^{\varphi(n)}\right)^q \equiv 1^q = 1(mod\ n)$, ottenendo che $\left(a^{\varphi(n)}\right)^q \equiv 1\ (mod\ n)$.
Applicando la proposizione 1 pag.6, moltiplicando ambo i membri della congruenza per a^r, si ha $\left(a^{\varphi(n)}\right)^q a^r \equiv 1 \cdot a^r = a^r(mod\ n)$, per cui alla fine si ottiene $a^m \equiv a^r(mod\ n)$, con $r < m$, cioè $[a^m]_n = [a^r]_n$.
<u>Esempio 1</u>:
Trovare il più piccolo rappresentante della classe $\left[13^{163}\right]_{27}$.
Notato che la base della potenza e il modulo della congruenza sono relativamente primi essendo $(13,27) = 1$, tramite la funzione di Eulero calcoliamo $\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 18$, quindi dividiamo 163 per 18 ottenendo $163 = 18 \cdot 9 + 1$, per cui il resto è $r = 1$.
Applicando la formula $a^m \equiv a^r(mod\ n)$, si ha $13^{163} \equiv 13\ (mod\ 27) \Rightarrow \left[13^{163}\right]_{27} = [13]_{27}$.
<u>Esempio 2</u>:
Vogliamo ridurre $\left[2^{2012}\right]_{136}$. Si ha $(2,3) = 1$ e $136 = 2^3 \cdot 17$. Allora, ricordando che se n ha la scomposizione in fattori primi $n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}$, applicando la formula $\varphi(n) = n \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right)$, si ha che $S = 2, h_1 = 3, p_1 = 2, p_2 = 17 \Rightarrow \varphi(136) = 136\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{17}\right) = 68 \cdot \frac{16}{17} = 16 \cdot 4 = 64$. Quindi dividendo 2012 per 64 si ottiene $21 = 64 \cdot 31 + 28 \Rightarrow [2^{2012}]_{136} = [2^{28}]_{136}$.

Le considerazioni che seguono sono utili per comprendere una dimostrazione del Piccolo Teorema di Fermat più semplice ed intuitiva delle precedenti.
Sempre ad esempio in un orologio a 5 ore, non considerando l'ora zero, le ore possibili sono 1, 2, 3, 4, corrispondenti rispettivamente alle classi di equivalenza modulo 5, $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$.
Considerato un intero, per esempio $a = 8$, moltiplichiamo a per i numeri della lista delle ore 1, 2, 3, 4, ottenendo $8 \times 1 = 8 \equiv 3(mod5)$, perché 8 diviso 5 ha quoziente 1 e resto 3, per cui $8 \times 1 \in [3]_5$, $8 \times 2 = 16 \equiv 1(mod5)$, perché 16 diviso 5 ha quoziente 3 e resto 1, per cui $8 \times 2 \in [1]_5$,
$8 \times 3 = 24 \equiv 4(mod5)$, perché 24 diviso 5 ha quoziente 4 e resto 4, per cui $8 \times 3 \in [4]_5$,
$8 \times 4 = 32 \equiv 2(mod5)$, perché 32 diviso 5 ha quoziente 6 e resto 2, per cui $8 \times 4 \in [2]_5$. Questo significa che le ore possibili 1, 2, 3, 4, rappresentanti le classi di congruenza modulo 5, moltiplicate per il numero a = 8, danno i numeri 8, 16, 24, 32, che sono congrui rispettivamente ai numeri 3, 1, 4, 2, la quale è una permutazione di 1, 2, 3, 4. Notiamo che il prodotto $1 \times 2 \times 3 \times 4 = 4! = 24$ diviso per 5 dà quoziente 4 e resto 4, per cui $24 \equiv 4(mod5)$, quindi $24 \in [4]_5$, inoltre $8 \times 16 \times 24 \times 32 = 98304$ diviso per 5 dà quoziente 19660 e resto 4, per cui $19660 \equiv 4(\mathrm{mod}5)$ e quindi $19660 \in [4]_5$. Similmente se moltiplichiamo per a = 2 la serie 1, 2, 3, 4, otteniamo 2, 4, 6, 8, equivalente a 2, 4, 1, 3, mentre se moltiplichiamo per 5 otteniamo 5, 10, 15, 20, equivalente a 0, 0, 0, 0, e così per un qualsiasi multiplo di 5.
Ora per dimostrare il piccolo teorema di Fermat, se p è un numero primo, ∀a∈ℤ si ha che $a^p \equiv a \pmod p$, è sufficiente dimostrare che $a^{p-1} \equiv 1(mod\ p)$, implicando ciò che $a \cdot a^{p-1} \equiv a \cdot 1(modp)$, ossia $a^p \equiv a \pmod p$. Osservato che il teorema è banalmente vero se a = 0, supponiamo che $a \neq 0$ e a sia primo con p, cioè $M.C.D.(a,p) = 1$. La serie 1, 2,…, p -1 dei resti delle divisioni per p si ottiene nuovamente con un diverso ordine quando i numeri di questa vengono moltiplicati per a. Infatti se $i \in \{1,2,\dots,p-1\}$ è uno dei numeri della serie, considerato il prodotto $a \times i$, deve esistere un intero $m_i \in \{1,2,\dots,p-1\}$, dove lo zero è escluso per le ipotesi su a, tale che $a \times i \equiv m_i\ (mod\ p)$, dovendo $a \times i$ necessariamente appartenere ad una ed una sola delle classi $[m_i]_p$.
Allora se nella nuova serie scriviamo al posto di $a \times i$ il numero m_i, si ha che la p-pla $m_1, m_2, \dots, m_{p-1}$ è una permutazione semplice della p-pla 1, 2,…, p -1, ove si sostituisca ad ogni termine $a \times i$ il suo rispettivo intero m_i congruo modulo p.
Da ciò si ricava che il prodotto $1 \times 2 \times \cdots \times (p-1) = (p-1)!$ e il prodotto $m_1 \times m_2 \times \dots \times m_{p-1}$ congruo modulo p al prodotto $(a \times 1) \times (a \times 2) \times \cdots \times (a \times (p-1)) = (p-1)!\,a^{p-1}$ sono uguali , cioè $(p-1)! = m_1 \times m_2 \times \dots \times m_{p-1}$, da cui essendo (*) $m_1 \times m_2 \times \dots \times m_{p-1} \equiv (p-1)!\,a^{p-1}\ (mod\ p)$, segue $(p-1)! \equiv (p-1)!\,a^{p-1}(mod\ p)$. Ora poiché $(p-1)!$ è primo con p in quanto p è primo con tutti i fattori del prodotto $1 \times 2 \times \cdots \times (p-1)$, in base alla proposizione 2 pag.4 si ha l'asserto $a^{p-1} \equiv 1(mod\ p)$ dividendo ambo i membri della congruenza precedente per $(p-1)!$.
Nel caso invece che $M.C.D.(a,p) \neq 1$, a è un multiplo di p, potendo in particolare essere anche uguale a p, non potendo essere minore di p altrimenti d = 1, posto $a = hp, h \in \mathbb{Z}$ opportuno, si ha $a^p = (hp)^p = p(h^p p^{p-1}) = pk$, dove $k = h^p p^{p-1} \in \mathbb{Z}$, donde $a^p - a = pk - a = pk - hp = p(k-h) = pt$, con $t = k - h \in \mathbb{Z}$, e quindi in base alla definizione segue $a^p \equiv a(mod\ p)$.

(*) Poiché $a \equiv b, c \equiv d \Rightarrow ac \equiv bd$ in quanto $a \equiv b \Rightarrow ac \equiv bc$, $c \equiv d \Rightarrow bc \equiv bd \Rightarrow ac \equiv bd$, si ha $m_i \equiv a \times i, m_j \equiv a \times j \Rightarrow m_i\ m_j \equiv (a \times i)(a \times j)$.