1 Congruenze

Definizione 1.1. $a, b, n \in \mathbb{Z} \quad n \geq 2$, allora definiamo $a \equiv b \pmod{n}$ se $n \mid a - b$.

Proposizione 1.2. $\forall n \geq 2$ la congruenza $\bmod n$ è una relazione di equivalenza su $\mathbb{Z}$.

Dimostrazione.

- $a \equiv a \ (n)$ perché $n \mid a - a$
- $a \equiv b \ (n) \quad \Rightarrow \quad b \equiv a \ (n)$
- $a \equiv b \ (n) \quad b \equiv c \ (n) \quad \Rightarrow \quad n \mid a - b \qquad n \mid b - c$
  $\Rightarrow \ n \mid a - c = (a - b) + (b - c)$
  $\Rightarrow \ a \equiv c \ (n)$

▲

Proposizione 1.3. $a, b \in \mathbb{Z} \ \ n \geq 2$. Sono fatti equivalenti:

1. $n \mid a - b$
2. $\exists k_0 \in \mathbb{Z}$ tale che $a = b + k_0 n$
3. $\{nk + a\}_{k \in \mathbb{Z}} = \{nk + b\}_{k \in \mathbb{Z}}$
4. a e b hanno lo stesso resto nella divisione euclidea per n

Dimostrazione.

$1 \Rightarrow 2$ Ovvio

$2 \Rightarrow 3$ $\{nk + a\}_{k \in \mathbb{Z}} = \{n(k + k_0) + b\}_{k \in \mathbb{Z}} = \{nk + b\}_{k \in \mathbb{Z}}$

$3 \Rightarrow 4$ $a = q_1 n + r_1 \quad 0 \leq r_1 < n$
$\Rightarrow \quad r_1 \in \{nk + a\}_{k \in \mathbb{Z}} = \{nk + b\}_{k \in \mathbb{Z}} \quad \Rightarrow$
$\Rightarrow \quad r_1 = nq + b \quad \Rightarrow$
$\Rightarrow \quad b = n(-q) + r_1 \qquad 0 \leq r_1 < n$
quindi r_1 è il resto della divisione di b per n .

$4 \Rightarrow 1$ $a = q_1 n + r \qquad b = q_2 n + r \quad \Rightarrow \quad n \mid a - b$

▲

Osservazione 1.4. La Proposizione 1.3 dice che ognuna delle condizioni $1, \ldots, 4$ può essere presa come definizione di CONGRUENZA

Classi di Congruenza:

$$[a]_n := \{b \in \mathbb{Z} \mid a \equiv b \ (n)\} = \{a + kn \mid k \in \mathbb{Z}\}$$

$$\downarrow$$

progres. aritmetica di ragione n e punto iniziale a

Le classi di congruenza danno una partizione di $\mathbb{Z}$

$$\mathbb{Z} = \overset{\circ}{\bigcup_{a \in X}} [a]$$

dove X è insieme di rappresentanti.

Corollario 1.5. (della Proposizione 1.3)

- $\forall a \in \mathbb{Z} \ \exists$ un unico $0 \leq r < n$ tale che $a \equiv r \ (n)$ (il resto di a diviso n)
- Le classi di congruenza modulo n sono esattamente n e possono essere rappresentate da

$$[0]_n, [1]_n, \ldots, [n-1]_n$$

Definizione 1.6.

$$\mathbb{Z}/n\mathbb{Z} := \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

$\mathbb{Z}/n\mathbb{Z}$ è l'insieme quoziente di $\mathbb{Z}$ rispetto alla relazione di congruenza $\bmod n$

Esempio 1.7. 1. $1239 \equiv 9 \ (10)$

2. $\mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\} == \{[36], [-5], [8], [-3], [604], [-1]\}$.

Osservazione 1.8. n interi consecutivi sono sempre un insieme completo di rappresentanti delle classi modulo n

Proposizione 1.9. Se $d \mid n$ le classi di congruenza modulo n danno una partizione più fine di quelle modulo d. Più precisamente

$$[a]_d = \overset{\circ}{\bigcup_{i=0,\ldots,\frac{n}{d}-1}} [a + id]_n$$

DIMOSTRAZIONE.

Ovviamente $[a]_n \subset [a]_d \quad \forall a \in \mathbb{Z}$.

Poiché $[a+id]_d = [a]_d$ si ha

$$\bigcup_{i=0}^{\frac{n}{d}-1} [a+id]_n \subset [a]_d$$

Viceversa $\forall k \in \mathbb{Z}$ sia $k = q\frac{n}{d} + i$ con $0 \leq i < \frac{n}{d}$

allora $a + kd \equiv a + id \ (n)$

$$\Rightarrow \quad [a]_d = \bigcup_{i=0}^{\frac{n}{d}-1} [a+id]_n$$

e l'unione è sicuramente disgiunta perché si tratta di classi diverse modulo n ▲

Proprietà delle congruenze: Siano $a, b \in \mathbb{Z}$ e sia $n \in \mathbb{N}$ con $n \geq 2$.

1. $a \equiv b \ (n) \ \Rightarrow \ \forall h \in \mathbb{Z}$ si ha $ha \equiv hb \ (n)$
2. $a \equiv b \ (n)$ e $a' \equiv b' \ (n) \ \Rightarrow \ a + a' \equiv b + b' \ (n)$ e $aa' \equiv bb' \ (n)$
3. se $a \equiv b \ (n)$ e $d \mid n \ \Rightarrow \ a \equiv b \ (d)$
4. $a \equiv b \ (n)$ e $a \equiv b \ (m) \ \Rightarrow \ a \equiv b \ ([n, m])$
5. $a \equiv b \ (n) \ \Rightarrow \ (a, n) = (b, n)$
6. $ra \equiv rb \ (n)$ con $r \neq 0 \ \Rightarrow \ a \equiv b \ \left(\frac{n}{(n,r)}\right)$.

   In particolare se $(n, r) = 1$ vale $a \equiv b \ (n) \iff ra \equiv rb \pmod{n}$.

DIMOSTRAZIONE.

1. $n \mid a - b \ \Rightarrow \ n \mid h(a-b) = ha - hb$
2. $a = b+kn$ e $a' = b'+k'n$ da cui sommando le equazioni si ottiene $a+a' = b+b'+(k+k')n$ e moltiplicandole si ottiene $aa' = bb' + (bk' + b'k)n$
3. ovvio
4. $n \mid a-b$ e $m \mid a-b$, quindi per definizione di minimo comune multiplo si ha $[m, n] \mid a-b$
5. $a = b + kn$, quindi $(a, n) = (b + kn, n) = (b, n)$
6. Dalla relazione $n \mid ra - rb = r(a-b)$ dividendo per (n, r) si ottiene

$$\frac{n}{(n,r)} \,\Big|\, \frac{r}{(n,r)}(a-b)$$

   Poiché $\left(\frac{n}{(n,r)}, \frac{r}{(n,r)}\right) = 1$ si ha $\frac{n}{(n,r)} \,\Big|\, a - b$

▲

Osservazione 1.10. Per la relazione di congruenza **NON VALE** la legge di cancellazione. Ad esempio

$$6 \equiv 2 \ (4) \quad \text{ma} \quad 3 \not\equiv 1 \ (4)$$

Usando la proprietà 5 si ha

$$3 \equiv 1 \ (2)$$

Applicazioni:

Criteri di divisibilità per 3 : "Un numero è divisibile per 3 se e soltanto se la somma delle sue cifre (in base 10) è divisibile per 3 ".

Infatti sia $n \in \mathbb{N}$ un numero naturale la cui scrittura posizionale sia $a_k a_{k-1} \dots a_0$, con $0 \leq a_i \leq 9$. Allora

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

quindi, poiché $10 \equiv 1 \ (3)$,

$$n \equiv 0 \ (3) \iff a_k 10^k + \cdots + a_1 10 + a_0 \equiv a_k + \cdots + a_1 + a_0 \equiv 0 \ (3)$$

Nello stesso modo si possono dimostrare i criteri di divisibilità per $2, 5, 9, 10, 11$. Si possono anche derivare criteri di divisibilità per altri numeri, ma in genere non hanno una formulazione elegante.

Proposizione 1.11. Siano $a, b \in \mathbb{Z}$ e sia $n \geq 2$. Allora

$$ax \equiv b \ (n)$$

ha soluzione se e solo se $d = (a, n) \mid b$.

In tal caso la congruenza ha esattamente d soluzioni modulo n .

In particolare, $ax \equiv 1 \pmod{n}$ ha soluzione se e solo se $(a, n) = 1$ e in tal caso ha un'unica soluzione modulo n .

Dimostrazione.

$ax \equiv b \pmod{n}$ ha soluzione se e solo se $\exists x_0 \in \mathbb{Z}$ tale che $ax_0 \equiv b \pmod{n}$, quindi se e solo se $\exists y_0 \in \mathbb{Z}$ tale che $ax_0 = b + ny_0$. Ne segue che la congruenza $ax \equiv b \pmod{n}$ ha soluzione se e solo se ha soluzione l'equazione $ax - ny = b$.

Sappiamo che questa equazione diofantea è risolubile se e solo se $d = (a, n) \mid b$ e in tal caso l'insieme delle soluzioni è

$$\begin{cases} x = x_1 + \frac{n}{d} \, t \\ \\ y = y_1 + \frac{a}{d} \, t \end{cases} \qquad t \in \mathbb{Z}$$

dove $(x_1, y_1) \in \mathbb{Z}^2$ è una qualsiasi soluzione dell'equazione. Abbiamo ottenuto che

$$ax \equiv b \ (n) \iff x \equiv x_1 \ \left(\frac{n}{d}\right)$$

Volendo esprimere la soluzione in termini di congruenza modulo n, otteniamo

$$x \equiv x_1 \ (n), \quad x \equiv x_1 + \frac{n}{d} \ (n), \ \ldots\ldots, x \equiv x_1 + \frac{n}{d}\,(d-1) \ \ (n)$$

▲

Il TEOREMA CINESE

Consideriamo il seguente sistema di congruenze

$$\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases} \qquad (1)$$

Tale sistema equivale a

$$\begin{cases} x = a + mu \\ x = b + nv \end{cases}$$

che ha come equazione risolvente $mu - nv = b - a$. Tale equazione ha soluzione se e solo se $(m, n) \mid b - a$.

In tal caso le soluzioni sono

$$\begin{cases} u = u_1 + \frac{n}{(n,m)}\, t \\ \qquad\qquad\quad t \in \mathbb{Z} \\ v = v_1 + \frac{m}{(n,m)}\, t \end{cases}$$

(dove (u_1, v_1) è una soluzione qualsiasi dell'equazione risolvente).

Sostituendo si ha $x = a + mu_1 + \frac{mn}{(m,n)}\, t = x_1 + [m, n]t$, dove $x_1 := a + mu_1$. Possiamo quindi concludere che

IL SISTEMA (1) HA SOLUZIONI $\iff$ $(m, n) \mid b - a$.

In tal caso la soluzione è del tipo $x \equiv x_1 \ ([m, n])$.

In particolare se $\underline{(m, n) = 1}$ il sistema (1) ha sempre un'unica soluzione modulo $m \cdot n$,

cioè $\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$ è equivalente a $x \equiv x_1 \ (mn)$.

Teorema 1.12. (Teorema Cinese)

Siano $m_1, \ldots, m_r \in \mathbb{N}$ tali che siano a due a due coprimi e $m_i \geq 2$. Consideriamo $a_1, \ldots, a_r \in \mathbb{Z}$. Allora il sistema

$$\begin{cases} x \equiv a_1 \ (m_1) \\ \vdots \\ x \equiv a_r \ (m_r) \end{cases}$$

ammette un'unica soluzione modulo $m_1 \cdots m_r$.

DIMOSTRAZIONE.

Per induzione su r . Il caso $r = 2$ è stato appena visto. Se abbiamo r equazioni ci si può ricondurre al caso $r - 1$ equazioni sostituendo le prime due equazioni con il risultato del sottosistema da loro formato. ▲

Esempio 1.13.

$$\begin{cases} x \equiv 7 \ (9) \\ x \equiv 4 \ (13) \\ x \equiv 11 \ (317) \end{cases}$$

ha un'unica soluzione modulo $9 \cdot 13 \cdot 317$

Esercizio 1.14. Contare le soluzioni del sistema modulo 90

$$\begin{cases} 4x \equiv 6 \ (18) \\ 3x \equiv 4 \ (5) \end{cases}$$

Poiché $(4, 18) = 2 \mid 6$, la prima equazione ha esattamente 2 soluzioni modulo 18 , ossia $x \equiv a_1 \ (18)$ e $x \equiv a_2 \ (18)$

Inoltre $(3, 5) = 1 \mid 4$, quindi la seconda equazione ha soluzione $x \equiv b \ (5)$.

Quindi le soluzioni del sistema sono le soluzioni di

$$\begin{cases} x \equiv a_1 \ (18) \\ x \equiv b \ (5) \end{cases} \qquad \text{e} \qquad \begin{cases} x \equiv a_2 \ (18) \\ x \equiv b \ (5) \end{cases}$$

Tali soluzioni $x \equiv x_1 \ (90)$ e $x \equiv x_2 \ (90)$ sono tra loro diverse perché $x_1 \equiv a_1 \ (18)$ e $x_2 \equiv a_2 \ (18)$

Operazioni su $\mathbb{Z}/n\mathbb{Z}$

Le proprietà delle congruenze possono essere lette come propietà delle classi di congruenza. Questo ci permette di definire operazioni di somma e prodotto di classi di congruenza.

Siano $a, b \in \mathbb{Z}$ e sia $n \geq 2$

DEF: SOMMA $[a]_n + [b]_n := [a+b]_n$

PRODOTTO $[a]_n[b]_n := [ab]_n$

Verifichiamo che le definizioni sono ben poste, ossia che non dipendono dai rappresentanti delle classi. Vogliamo dunque provare che

$$[a] = [a'],\ [b] = [b'] \ \Rightarrow\ [a+b] = [a'+b'],\ [ab] = [a'b']$$

Questo è vero e segue dalla Proprietà 2 delle congruenze.

Proprietà di somma e prodotto in $\mathbb{Z}/n\mathbb{Z}$

1. $+, \cdot$ sono <u>associative</u>
2. $+, \cdot$; sono <u>commutative</u>
3. Esiste l'<u>elemento neutro:</u> $+ : [a] + [0] = [a]\ \forall a \in \mathbb{Z}$
   $\cdot : [a] \cdot [1] = [a]\ \forall a \in \mathbb{Z}$.
4. Esiste l' <u>inverso</u> per $+ : [a] + [-a] = [0]\ \forall a \in \mathbb{Z}$
5. Legge distributiva: $\forall [a], [b], [c] \in \mathbb{Z}$ vale $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$

Queste proprietà si verificano partendo dalle definizioni e usando il fatto che sono vere per i numeri interi.

Def: $[a] \in \mathbb{Z}/n\mathbb{Z}$ si dice *invertibile* se è invertibile rispetto al prodotto, cioè se $\exists [x] \in \mathbb{Z}/n\mathbb{Z}$ tale che $[a][x] = [1]$.
Poniamo $\mathbb{Z}/n\mathbb{Z}^* := \{[a] \in \mathbb{Z}/n\mathbb{Z} \,|\, [a] \text{ è invertibile}\}$

Esempio 1.15. In $\mathbb{Z}/n\mathbb{Z}$ non tutti gli elementi sono invertibili rispetto al prodotto, ad esempio $[0]$ non è invertibile modulo n per nessun n . In $\mathbb{Z}/4\mathbb{Z}$ le classi invertibili invertibili $[1]$ e $[3]$, mentre in $\mathbb{Z}/5\mathbb{Z}$ sono invertibili $[1], [2], [3], [4]$.

Proposizione 1.16. 1. Il prodotto è un'operazione su $\mathbb{Z}/n\mathbb{Z}^*$.

2. $[a] \in \mathbb{Z}/m\mathbb{Z}^* \iff (a, m) = 1$.
3. Se p è un numero primo allora $\mathbb{Z}/p\mathbb{Z}^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$.

DIMOSTRAZIONE.

1) Siano $[a], [b] in \mathbb{Z}/n\mathbb{Z}^*$ e siano $[u], [v]$ i loro inversi. Allora $[a][b]$ ha come inverso $[uv]$, infatti $[a][b][uv] = [abuv] = [aubv] = [1]$.

2) $[a] \in \mathbb{Z}/n\mathbb{Z}^*$ se e solo se ha soluzione la congruenza $ax \equiv 1 \pmod{n}$; per la Proposizione 1.11 questo vale se e solo se $(a, m) = 1$.

3) Segue dal punto (2).

Il Teorema cinese si può enunciare anche per le classi di resto

Teorema 1.17. (Teorema Cinese, seconda forma)

Siano $m, n \geq 2$ due interi tali che $(m, n) = 1$. La funzione

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

definita da $\varphi([a]_{mn}) = ([a]_m, [a]_n)$ è bigettiva.

DIMOSTRAZIONE.

φ <u>è ben definita</u>: infatti, sia $[a]_{mn} = [a']_{mn}$ cioè $a \equiv a' \pmod{m}$, allora per le proprietà dimostrate si ha $a \equiv a' \pmod{n}$ e $a \equiv a' \pmod{n}$, quindi $([a]_m, [a]_n) = ([a']_m, [a']_n)$.

φ <u>è surgettiva</u>: occorre verificare che $\forall([a]_m, [b]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ esiste $[x]_{mn}$ tale che $\varphi([x]_{mn}) = ([x]_m, [x]_n) = ([a]_m, [b]_n)$.
Questo equivale a dire che esiste $x \in \mathbb{Z}$ tale che

$$\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$$

e questo è vero per il teorema cinese.

φ <u>è iniettiva</u>: poiché φ è surgettiva e tra insiemi finiti della stessa cardinalità, allora è anche iniettiva. ▲

Lemma 1.18. 1. $(a, mn) = 1 \iff (a, m) = 1$ e $(a, n) = 1$

2. $(m, n) = 1 \Rightarrow (a, mn) = (a, m)(a, n)$

DIMOSTRAZIONE.

1. " $\Rightarrow$ " $ax_0 + mny_0 = 1 \Rightarrow (a, m) = 1$ e $(a, n) = 1$

   " $\Leftarrow$ " $ax_0 + my_0 = 1$ e $a\alpha_0 + n\beta_0 = 1$ da cui moltiplicando le equazione si ha $a(.....) + mny_0\beta_0 = 1$, da cui $(a, mn) = 1$

2. Si dimostra facilmente usando la caratterizzazione del massimo comune divisore in termini di fattorizzazione.

▲

Corollario 1.19. $(m,n)=1$. Sia $[x]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$.

$$[x]_{mn} \in \mathbb{Z}/mn\mathbb{Z}^* \iff \varphi([x]_{mn}) \in \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$$

Corollario 1.20. Siano $m,n \geq 2$ tali che $(m,n)=1$ e sia φ^* la restrizione di φ a $\mathbb{Z}/mn\mathbb{Z}^*$. Allora

$$\varphi^* : \mathbb{Z}/mn\mathbb{Z}^* \longrightarrow \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$$

è bigettiva.

Dimostrazione.

È ben definita per il precedente corollario

È surgettiva perché φ è surgettiva e per il precedente corollario.

È iniettiva perché restrizione di un'applicazione iniettiva

▲

Funzione Φ di Eulero

$$\begin{array}{rccll} \Phi: & \mathbb{N} & \longrightarrow & \mathbb{N} & \\ & n & \mapsto & \Phi(n) & = \sharp\{x \mid 1 \leq x \leq n,\ \ (x,n)=1\} \\ & & & & = \sharp\mathbb{Z}/n\mathbb{Z}^* \end{array}$$

Vogliamo dare una formula per calcolare $\Phi(n)$. Per il Corollario 1.20 si ha che

$\forall m,n, \quad (m,n)=1 \ \Rightarrow \ \Phi(mn)=\Phi(m)\Phi(n)$, ossia Φ è moltiplicativa.

Quindi per calcolare $\Phi(n)$ basta calcolare $\Phi(p^k)$ per p primo (sappiamo già che $\Phi(p)=p-1$).

Sia $1 \leq a \leq p^k$. Chiaramente

$$(a,p^k) \neq 1 \iff p \mid a \iff a = p\alpha$$

quindi

$\Phi(p^k) = p^k - \sharp\{p\alpha \mid 1 \leq \alpha \leq p^{k-1}\} = p^k - p^{k-1} = p^{k-1}(p-1)$

Dalla moltiplicatività della Φ otteniamo che se

$n = p^{e_1} \cdots p^{e_r} \qquad$ con $\quad p_i \neq p_j$

$$\Rightarrow \quad \Phi(n) = \prod_{i=1}^{n} p_i^{e_i-1}(p_i-1)$$

Teorema 1.21. Sia p primo. Allora $\forall x, y \in \mathbb{Z}$ si ha

$$(x+y)^p \equiv x^p + y^p \ (p).$$

DIMOSTRAZIONE.

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} + y^p$$

Devo far vedere che $\sum_{i=1}^{p-1} \binom{p}{i}$ è un multiplo di p.
Osservo che $\forall i = 1, \ldots, p-1$ si ha che $p \mid \binom{p}{i}$. Infatti

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

ha numeratore divisibile per p ma il denominatore non lo è. ▲

Teorema 1.22. (Teorema di Fermat)

Sia p un primo. Allora
$\forall x \in \mathbb{Z}$ si ha $x^p \equiv x \ (p)$.

DIMOSTRAZIONE.

Lo dimostriamo prima per $x \in \mathbb{N}$, per induzione:

$x = 0$ OK

$x \Rightarrow x+1 \qquad (x+1)^p \equiv x^p + 1^p \equiv x+1 \ (p)$

Se $x < 0 \quad \Rightarrow \quad -x > 0$ quindi $(-x)^p \equiv (-x) \ (p)$

$$(-1)^p x^p \equiv -x \ (p)$$

se $p \neq 2$ si ha $x^p \equiv x \ (p)$

se $p = 2$ si ha $x^2 \equiv -x \ (2)$
ma modulo 2 si ha che $1 \equiv -1$

Corollario 1.23. Sia p un primo. Allora $\forall x \in \mathbb{Z}$ tale che $(x,p) = 1$ si ha

$$x^{p-1} \equiv 1 \ (p).$$

DIMOSTRAZIONE.

Sappiamo che $x^p \equiv x \ (p)$ e che se $(x,p) = 1$ allora $[x]_p$ è invertibile.
Dunque moltiplicando per l'inverso di $[x]_p$ otteniamo $x^{p-1} \equiv 1 \ (p)$.

▲

Osservazione 1.24. Il corollario appena visto dice che

$$\forall [x]_p \in \mathbb{Z}/p\mathbb{Z}^* \quad [x]_p[x^{p-2}]_p = [1]_p$$

cioè che $[x^{p-2}]_p$ è l'inverso di $[x]_p$.

Teorema 1.25. (Teorema di Eulero)

Sia $m \geq 2$ e sia $x \in \mathbb{Z}$ tale che $(x, m) = 1$. Allora

$$x^{\Phi(m)} \equiv 1 \pmod{m}.$$

Dimostrazione.

Sia $x \in \mathbb{Z}$ tale che $(x, m) = 1$; allora $[x] \in \mathbb{Z}/m\mathbb{Z}^*$. Sia $f : \mathbb{Z}/m\mathbb{Z}^* \to \mathbb{Z}/m\mathbb{Z}^*$ la funzione definita da $f([a]) = [a][x]$; si ha:
f è ben definita perché $\mathbb{Z}/m\mathbb{Z}^*$ è chiuso rispetto al prodotto;
f è iniettiva: infatti, $f([a]) = f([b]) \iff [a][x] = [b][x] \iff [a] = [b]$ perché $[x]$ è invertibile;
f è surgettiva perchè è una funzione iniettiva da un insieme finito in sé.
Da questo segue che $f(\mathbb{Z}/m\mathbb{Z}^*) = \mathbb{Z}/m\mathbb{Z}^*$ e quindi

$$[c] = \prod_{[a]\in\mathbb{Z}/m\mathbb{Z}^*} [a] = \prod_{[a][x]\in f(\mathbb{Z}/m\mathbb{Z}^*)} ([a][x]) = [x]^{\Phi(m)}[c].$$

Poiché $[c] \in \mathbb{Z}/m\mathbb{Z}^*$, moltiplicando per $[c]^{-1}$ entrambi i membri dell'equazione $[c] = [x]^{\Phi(m)}[c]$, otteniamo $[x]^{\Phi(m)} = [1]$. ▲