5. Equazioni congruenziali lineari

Definizione 1. *Si chiama equazione congruenziale lineare modulo n un'equazione del tipo*

$$aX \equiv b \ (mod\ n) \quad \text{[ovvero, più brevemente,} \quad aX \equiv b\ (n)\,\text{]},$$

con $a, b \in \boldsymbol{Z}$, $n \geq 2$ ed $a \notin n\boldsymbol{Z}$. Una sua soluzione [se esiste] è un intero x tale che $ax \equiv b\ (mod\ n)$. Un'equazione congruenziale lineare è detta compatibile se ammette una soluzione; altrimenti è detta incompatibile. È evidente che se x è una soluzione, anche $x + nh$ $(\ \forall\, h \in \boldsymbol{Z})$ è una soluzione della stessa equazione.

Si noti che ogni equazione congruenziale lineare $aX \equiv b\ (mod\ n)$ si trasforma in modo naturale nell'equazione lineare $\overline{a}X = \overline{b}$, con coefficienti in $\boldsymbol{Z}_n$. Ovviamente, x è soluzione dell'equazione $aX \equiv b\ (mod\ n) \iff \overline{x}$ è soluzione dell'equazione $\overline{a}X = \overline{b}$.

Proposizione 1. *L'equazione $aX \equiv b\ (mod\ n)$ è compatibile $\iff (a, n) \,\big|\, b$.*

Dim. $aX \equiv b\ (mod\ n)$ è compatibile $\iff \exists\, x \in \boldsymbol{Z}$ tale che $ax \equiv b\ (n) \iff \exists\, x, y \in \boldsymbol{Z}$ tali che $ax - b = ny \iff$ l'equazione $aX - nY = b$ ammette una soluzione intera (cioè in $\boldsymbol{Z}\times\boldsymbol{Z}$).

Per concludere basta allora dimostrare il seguente lemma.

Lemma 1. *L'equazione $aX - nY = b$ ammette soluzioni in $\boldsymbol{Z}\times\boldsymbol{Z} \iff (a, n) \,\big|\, b$.*

Dim. (**Lemma 1**). Si ponga $d := (a, n)$.

$(\Longrightarrow)$. Sia $(x, y) \in \boldsymbol{Z}\times\boldsymbol{Z}$ tale che $ax - ny = b$. Da $d \left|\begin{matrix} a \\ n \end{matrix}\right.$ segue che $d \,\big|\, ax - ny = b$.

$(\Longleftarrow)$. Supponiamo che $d = (a, n) \overset{Bez}{=} ar + ns$. Per ipotesi $d \,\big|\, b$, cioè $b = db_1$, $\exists\, b_1 \in \boldsymbol{Z}$. Allora $b = db_1 = arb_1 + nsb_1$. Ne segue che $(rb_1, -sb_1)$ è una soluzione intera di $aX - nY = b$.

Osservazione 1. Sia $aX \equiv b\ (n)$, con $d := (a, n) \,\big|\, b$. Tale equazione è compatibile (in base a **Prop. 1**). Una sua soluzione si ottiene schematicamente con questa procedura:

$$\begin{aligned} & d = (a, n) \overset{Bez}{=} ar + ns; \\ & d \,\big|\, b \implies b = db_1; \\ & b = db_1 = ab_1r + nb_1s \equiv a(b_1r)\ (mod\ n). \end{aligned}$$

Dunque $x = b_1r$ è una soluzione dell'equazione.

Definizione 2. *Siano $aX \equiv b\ (mod\ n)$ e $a_1X \equiv b_1\ (mod\ n_1)$ due equazioni congruenziali lineari. Tali equazioni sono dette equivalenti $\iff$ hanno le stesse soluzioni $\iff$ $\big[\ \forall\, x \in \boldsymbol{Z}$, risulta: $n \,\big|\, ax - b \iff n_1 \,\big|\, a_1x - b_1\big]$.*

Proposizione 2. *(i) Se $(a, n) = 1$, l'equazione $aX \equiv b\ (mod\ n)$ è equivalente a $X \equiv ba'\ (mod\ n)$, con a' inverso aritmetico di a $(mod\ n)$.*

(ii) Se l'equazione $aX \equiv b\ (mod\ n)$ è compatibile, essa è equivalente a $\frac{a}{d}X \equiv \frac{b}{d}\ (mod\ \frac{n}{d})$, con $d = (a, n)$.

Dim. (i) Essendo $aa' \equiv 1\ (mod\ n)$, risulta $1 = aa' + nr$, $\exists\, r \in \boldsymbol{Z}$. Bisogna verificare che $n \,\big|\, ax - b \iff n \,\big|\, x - ba'$, $\forall\, x \in \boldsymbol{Z}$.

$(\Longrightarrow)$. $n \,\big|\, ax - b \implies ax - b = ns \implies aa'x - ba' = a'ns \implies (1 - nr)x - ba' = a'ns \implies$
$\implies x - ba' = n(rx + a's) \implies n \,\big|\, x - ba'$.

$(\Longleftarrow)$. $n \,\big|\, x - ba' \implies x - ba' = nt \implies ax - aba' = ant \implies ax - (1 - nr)b = ant \implies$

$\Longrightarrow\ ax-b=n(at-rb)\ \Longrightarrow\ n\,\big|\,ax-b.$

(*ii*) Se $n\,|\,ax-b$, allora $\frac{n}{d}\,\big|\,\frac{a}{d}x-\frac{b}{d}$ (essendo $\frac{n}{d},\ \frac{a}{d},\ \frac{b}{d}\in\boldsymbol{Z}$). Viceversa, se $\frac{n}{d}\,\big|\,\frac{a}{d}x-\frac{b}{d}$, moltiplicando per d si ottiene $n\,|\,ax-b$.

Proposizione 3. *(i) Sia $aX\equiv b\ (mod\ n)$ un'equazione congruenziale lineare compatibile (e quindi $d:=(a,n)\,|\,b$) e sia x_0 una sua soluzione. Si ha:*

(1) $x_0+\frac{n}{d}h$ è una soluzione, $\forall\,h\in\boldsymbol{Z}$.

(2) Ogni soluzione è del tipo $x_0+\frac{n}{d}h$ (per un opportuno $h\in\boldsymbol{Z}$).

(3) Se $h_1,\ h_2\in\boldsymbol{Z}$ sono tali che $0\le h_1\ne h_2<d$, le due soluzioni $x_0+\frac{n}{d}h_1$ e $x_0+\frac{n}{d}h_2$ non sono congruenti $(mod\ n)$.

(4) Per ogni $h\in\boldsymbol{Z}$, $\exists!\,r$ tale che $0\le r<d$ e $x_0+\frac{n}{d}h\equiv x_0+\frac{n}{d}r\ (mod\ n)$.

Dai punti precedenti segue che un insieme "massimale" (cioè non estendibile) di soluzioni a due a due non congruenti dell'equazione $aX\equiv b\ (mod\ n)$ è dato da:

$$\left\{x_0,\ x_0+\tfrac{n}{d},\ x_0+2\tfrac{n}{d},\ \dots,\ x_0+(d-1)\tfrac{n}{d}\right\}.$$

Un tale insieme di soluzioni è detto sistema completo di soluzioni *dell'equazione $aX\equiv b\ (mod\ n)$.*

Le corrispondenti classi resto forniscono l'insieme di tutte le d soluzioni (a due a due distinte) dell'equazione lineare $\overline{a}X=\overline{b}$ in $\boldsymbol{Z}_n$.

Dim. (*1*) Osservato che $\frac{a}{d}\in\boldsymbol{Z}$, $a(x_0+\frac{n}{d}h)=ax_0+a\frac{n}{d}h=ax_0+\frac{a}{d}\,nh\equiv ax_0\equiv b\ (mod\ n)$. Dunque $x_0+\frac{n}{d}h$ è una soluzione di $aX\equiv b\ (mod\ n)$.

(*2*) Sia x una soluzione: $ax\equiv b\ (mod\ n)$. Allora $a(x-x_0)\equiv b-b\equiv 0\ (mod\ n)$. Quindi: $n\,|\,a(x-x_0)$, da cui $\frac{n}{d}\,\big|\,\frac{a}{d}(x-x_0)$. Poiché $\left(\frac{n}{d},\ \frac{a}{d}\right)=1$, dal Lemma di Euclide $\frac{n}{d}\,\big|\,x-x_0$. Allora $x-x_0=\frac{n}{d}h$, $\exists\,h\in\boldsymbol{Z}$, da cui $x=x_0+\frac{n}{d}h$.

(*3*) Essendo $0\le h_1\ne h_2<d$, allora: $0\le h_1<d$, $-d<-h_2\le 0$ e quindi, sommando membro a membro, $-d<h_1-h_2<d$. Poiché inoltre $h_1-h_2\ne 0$, allora $d\nmid h_1-h_2$.

Se per assurdo $x_0+\frac{n}{d}h_1\equiv x_0+\frac{n}{d}h_2\ (mod\ n)$, allora $n\,\big|\,\frac{n}{d}(h_1-h_2)$, cioè $n(h_1-h_2)=nds$, da cui $h_1-h_2=ds$, cioè $d\,|\,h_1-h_2$: assurdo.

(*4*) Sia $h=dq+r$, con $0\le r<d$. Allora: $x_0+\frac{n}{d}h=x_0+\frac{n}{d}(dq+r)=x_0+nq+\frac{n}{d}r\equiv x_0+\frac{n}{d}r\ (mod\ n)$. L'unicità di r discende da (*3*).

Osservazione 2. Per risolvere un'equazione congruenziale lineare compatibile $aX\equiv b\ (mod\ n)$, si può procedere seguendo due vie diverse:

(*A*): utilizzando i due risultati della **Prop. 2**. In tal modo l'equazione assegnata viene trasformata in un'equazione del tipo $X\equiv b'\ (mod\ n')$, la cui generica soluzione è data dall'insieme $b'+n'\boldsymbol{Z}$.

(*B*): utilizzando l'**Osserv. 1** per determinare una soluzione. Si usa poi la formula di **Prop. 3** per scrivere un sistema completo di soluzioni.

Come messo in luce dall'esempio che segue, le soluzioni ottenute con i due procedimenti possono presentarsi in forma diversa, ma in realtà "globalmente" si tratta delle stesse soluzioni.

Esempio 1. Risolvere l'equazione $15X\equiv 12\ (mod\ 21)$.

Poiché $3=(15,21)\,|\,12$, l'equazione è compatibile. Ne otterremo le soluzioni seguendo i due metodi (*A*) e (*B*).

(*A*) L'equazione data è equivalente a $5X\equiv 4\ (mod\ 7)$. Un inverso aritmetico di 5 $(mod\ 7)$ è 3 [infatti $5\cdot 3\equiv 1\ (mod\ 7)$]. Allora $5X\equiv 4\ (mod\ 7)$ è equivalente a $X\equiv 4\cdot 3\ (mod\ 7)$, cioè $X\equiv 5\ (mod\ 7)$ Pertanto le soluzioni sono date dall'insieme

$$5+7\boldsymbol{Z}=\{5+7h,\ \ \forall\,h\in\boldsymbol{Z}\}.$$

(*B*) Risulta:

$$3=(15,21)\overset{Bez}{=}15\cdot 3+21\cdot(-2),$$
$$3\,|\,12\quad[12=3\cdot 4],$$

$$12 = 15{\cdot}12 + 21{\cdot}(-8) \equiv 15{\cdot}12 \ (mod\ 21).$$

Una soluzione è quindi $x_0 = 12$. Un sistema completo di soluzioni è quindi

$$\{12,\ 12 + \tfrac{21}{3},\ 12 + 2\tfrac{21}{3}\} = \{12,\ 19,\ 26\}_{\equiv_{21}} = \{12,\ 19,\ 5\}.$$

Le soluzioni sono pertanto date dall'unione dei tre insiemi:

$$(5 + 21\boldsymbol{Z}) \cup (12 + 21\boldsymbol{Z}) \cup (19 + 21\boldsymbol{Z}) \qquad [= 5 + 7\boldsymbol{Z}\,].$$

Veniamo ora allo studio di *sistemi* di equazioni congruenziali lineari, della forma:

$$(*) \qquad \begin{cases} a_1X \equiv b_1 \ (mod\ n_1) \\ a_2X \equiv b_2 \ (mod\ n_2) \\ : \\ a_sX \equiv b_s \ (mod\ n_s). \end{cases}$$

Un tale sistema è detto *compatibile* se esiste $x \in \boldsymbol{Z}$ tale che $\begin{cases} a_ix \equiv b_i \ (mod\ n_i) \\ \forall\, i = 1, \dots, s\,. \end{cases}$

Osservazione 3. Se il sistema $(*)$ è compatibile, ogni singola equazione deve esserlo. Allora $(a_i, n_i) \,\big|\, b_i$, $\forall\, i = 1, \dots, s$. Il viceversa è però falso: ad esempio il sistema

$$\begin{cases} 2X \equiv 4 \ (mod\ 6) \\ 2X \equiv 2 \ (mod\ 6) \end{cases}$$

è formato da due equazioni compatibili ma non è compatibile [altrimenti si avrebbe, per transitività, $4 \equiv 2 \ (mod\ 6)$]. Dimostreremo che se le singole equazioni sono compatibili e se i moduli n_i sono a due a due coprimi, allora il sistema è compatibile. Ma prima di dimostrare tale risultato (cfr. **Teor. 2**), dobbiamo introdurre e risolvere sistemi di equazioni congruenziali particolari, detti *sistemi "cinesi"*.

Definizione 3. *Un sistema cinese di s equazioni congruenziali lineari è un sistema del tipo:*

$$(**) \qquad \begin{cases} X \equiv c_1 \ (mod\ r_1) \\ X \equiv c_2 \ (mod\ r_2) \\ : \\ X \equiv c_s \ (mod\ r_s), \end{cases} \qquad \text{con } r_1, \dots, r_s \text{ a due a due coprimi.}$$

Teorema 1. (*Teorema Cinese del resto* - 1^a **formulazione**). *Ogni sistema cinese $(**)$ è compatibile ed ha un'unica soluzione $(mod\ r_1r_2 \dots r_s)$.*

Dim. (*Unicità della soluzione*). Siano x, y due soluzioni del sistema $(**)$: va dimostrato che $x \equiv y \ (mod\ r_1r_2 \dots r_s)$.

Da $\begin{cases} x \equiv c_i \equiv y \ (r_i) \\ \forall\, i = 1, \dots, s, \end{cases}$ segue che $r_i \,\big|\, x - y$, $\forall\, i = 1, \dots, s$. In particolare, $r_1 \,\big|\, x - y$ e dunque $x - y = r_1t_1$. In base a *EU*, da $r_2 \,\big|\, x - y = r_1t_1$ e $(r_1, r_2) = 1$, segue: $r_2 \,\big|\, t_1 \implies t_1 = r_2t_2 \implies x - y = r_1r_2t_2$.
Ancora in base a *EU*, da $r_3 \,\big|\, x - y = r_1r_2t_2$ e $(r_1r_2, r_3) = 1$ [cfr. **Eserc. 2.1**], segue: $r_3 \,\big|\, t_2 \implies t_2 = r_3t_3 \implies x - y = r_1r_2r_3t_3$.
Proseguendo in questo modo si conclude che $x - y = r_1r_2 \dots r_s\, t_s$, cioè $x \equiv y \ (mod\ r_1r_2 \dots r_s)$.

(*Esistenza della soluzione*). Non è restrittivo assumere che risulti $0 \le c_i < r_i$, $\forall\, i = 1, \dots, s$. In tal caso la s-pla $(c_1, \dots, c_s)$ appartiene ad un insieme di cardinalità $n := \prod_{i=1}^{s} r_i$.

Per ogni intero k tale che $0 \le k < n$, $\exists!\, k_i \in \boldsymbol{Z}$ tale che $k_i \equiv k \ (mod\ r_i)$ e $0 \le k_i < r_i$. L'intero k definisce quindi la s-pla $\tilde{k} = (k_1, \dots, k_s)$. Si verifica subito che se $\tilde{k} = \tilde{k}'$, allora $k = k'$. Infatti, essendo $k \equiv k_i = k'_i \equiv k' \ (mod\ r_i)$, allora [con la stessa dimostrazione svolta per l'unicità] $k \equiv k' \ (mod\ n)$ e dunque [essendo $0 \le k, k' < n$] $k = k'$.

Le s-ple $\tilde{k}$ sono quindi a due a due distinte e sono complessivamente n. Tra esse c'è anche la s-pla $(c_1, \dots, c_s)$. Dunque k è soluzione del sistema $(**)$, se $\tilde{k} = (c_1, \dots, c_s)$.

La precedente dimostrazione non è costruttiva. Vogliamo quindi fornire un metodo per il calcolo della soluzione per sistemi cinesi. Per semplicità ci limitiamo però ad illustrare il procedimento per sistemi di 2 o 3 equazioni.

(a) È assegnato il sistema cinese di due equazioni

$$(\bullet) \qquad \begin{cases} X \equiv c_1 \ (mod\ r_1) \\ X \equiv c_2 \ (mod\ r_2), \end{cases} \qquad \text{con} \quad (r_1, r_2) = 1.$$

Associamo a $(\bullet)$ i due seguenti sistemi cinesi:

$$(\circ) \quad \begin{cases} X \equiv 1 \ (mod\ r_1) \\ X \equiv 0 \ (mod\ r_2), \end{cases} \qquad\qquad (\circ\,\circ) \quad \begin{cases} X \equiv 0 \ (mod\ r_1) \\ X \equiv 1 \ (mod\ r_2). \end{cases}$$

Da $1 = (r_1, r_2) \overset{Bez}{=} ar_1 + br_2$, segue subito che:

- br_2 è una soluzione di $(\circ)$: infatti $\begin{cases} br_2 \equiv 1 \ (mod\ r_1) \\ br_2 \equiv 0 \ (mod\ r_2), \end{cases}$
- ar_1 è una soluzione di $(\circ\,\circ)$: infatti $\begin{cases} ar_1 \equiv 0 \ (mod\ r_1) \\ ar_1 \equiv 1 \ (mod\ r_2). \end{cases}$

Consideriamo ora l'intero $x = c_1(br_2) + c_2(ar_1)$. Verifichiamo che x è soluzione di $(\bullet)$. Infatti:

$$\begin{cases} x \equiv c_1 br_2 \equiv c_1 \cdot 1 = c_1 \ (mod\ r_1) \\ x \equiv c_2 ar_1 \equiv c_2 \cdot 1 = c_2 \ (mod\ r_2). \end{cases}$$

Abbiamo così dimostrato che $(\bullet)$ ammette una soluzione.

(b) È assegnato il sistema cinese di tre equazioni

$$(\bullet\bullet) \qquad \begin{cases} X \equiv c_1 \ (mod\ r_1) \\ X \equiv c_2 \ (mod\ r_2) \\ X \equiv c_3 \ (mod\ r_3), \end{cases} \qquad \text{con} \quad (r_1, r_2) = (r_1, r_3) = (r_2, r_3) = 1.$$

Gli associamo i tre seguenti sistemi cinesi:

$$(\circ) \ \begin{cases} X \equiv 1 \ (mod\ r_1) \\ X \equiv 0 \ (mod\ r_2) \\ X \equiv 0 \ (mod\ r_3), \end{cases} \quad (\circ\,\circ) \ \begin{cases} X \equiv 0 \ (mod\ r_1) \\ X \equiv 1 \ (mod\ r_2) \\ X \equiv 0 \ (mod\ r_3), \end{cases} \quad (\circ\,\circ\,\circ) \ \begin{cases} X \equiv 0 \ (mod\ r_1) \\ X \equiv 0 \ (mod\ r_2) \\ X \equiv 1 \ (mod\ r_3). \end{cases}$$

Da $1 = (r_1, r_2 r_3) \overset{Bez}{=} r_1 \cdot a_1 + r_2 r_3 \cdot b_1$, segue che $b_1 r_2 r_3$ è soluzione di $(\circ)$.
Da $1 = (r_2, r_1 r_3) \overset{Bez}{=} r_2 \cdot a_2 + r_1 r_3 \cdot b_2$, segue che $b_2 r_1 r_3$ è soluzione di $(\circ\,\circ)$.
Da $1 = (r_3, r_1 r_2) \overset{Bez}{=} r_3 \cdot a_3 + r_1 r_2 \cdot b_3$, segue che $b_3 r_1 r_2$ è soluzione di $(\circ\,\circ\,\circ)$.
Posto allora $x = c_1 b_1 r_2 r_3 + c_2 b_2 r_1 r_3 + c_3 b_3 r_1 r_2$, si verifica che x è una soluzione del sistema $(\bullet\bullet)$.

Osservazione 4. Per risolvere il sistema cinese $(**)$ si può procedere seguendo due vie diverse.

(A) Si segue l'idea sviluppata nei precedenti algoritmi: calcolate le identità di Bézout

$$\begin{aligned} &1 = (r_1, r_2 r_3 \dots r_s) = a_1 \cdot r_1 + b_1 \cdot r_2 r_3 \dots r_s, \\ &1 = (r_2, r_1 r_3 \dots r_s) = a_2 \cdot r_2 + b_2 \cdot r_1 r_3 \dots r_s, \\ &\vdots \\ &1 = (r_s, r_1 r_2 \dots r_{s-1}) = a_s \cdot r_s + b_s \cdot r_1 r_3 \dots r_{s-1}, \end{aligned}$$

allora $x := \sum_{i=1}^{s} c_i b_i r_1 \dots \cancel{r_i} \dots r_s$ è l'unica soluzione di (**).

(B) Si consideri la generica soluzione della prima equazione: $x = c_1 + r_1 t_1$, $\forall t_1 \in \boldsymbol{Z}$. La si sostituisce nella seconda equazione, ottenendo l'equazione $c_1 + r_1 t_1 \equiv c_2 \ (r_2)$ [nell'incognita t_1]. Si risolve tale congruenza, ottenendo $t_1 = d_1 + r_2 t_2$, $\forall t_2 \in \boldsymbol{Z}$. La si inserisce nella precedente espressione di x, ottenendo $x = c_1 + r_1 d_1 + r_1 r_2 t_2$.

Si sostituisce tale espressione nella terza equazione del sistema, si risolve l'equazione [in t_2] e si inserisce la generica soluzione $t_2 = d_2 + t_3 r_3$ nell'ultima espressione di x, ottenendo $x = c_1 + r_1 d_1 + r_1 r_2 t_2 + r_1 r_2 r_3 t_3$.

Procedendo in tal modo, dopo un numero finito di passi si ottiene l'unica soluzione del sistema.

Esempio 2. Risolvere il seguente sistema cinese:

$$\begin{cases} X \equiv 3\ (5) \\ X \equiv 4\ (7) \\ X \equiv 4\ (11). \end{cases}$$

Si noti che $(5,7) = (5,11) = (7,11) = 1$. Dunque i moduli sono a due a due coprimi e quindi il sistema è compatibile. Ne otterremo le soluzioni seguendo i due metodi (A) e (B).

(A) Si ha:

$$1 = (5,77) \overset{Bez}{=} 5{\cdot}31 + 77{\cdot}(-2) = 5{\cdot}31 + (-154),$$
$$1 = (7,55) \overset{Bez}{=} 7{\cdot}8 + 55{\cdot}(-1) = 7{\cdot}8 + (-55),$$
$$1 = (11,35) \overset{Bez}{=} 11{\cdot}16 + 35{\cdot}(-5) = 11{\cdot}16 + (-175).$$

Allora: $x = 3(-154)+4(-55)+4(-175) = -1382$. Poiché $-1382 \equiv 158\ (mod\ 385)$, l'unica soluzione del sistema è $x = 158\ (mod\ 385)$.

(B) La prima equazione ha generica soluzione $x = 3 + 5t_1$. Inserendo tale valore nella seconda equazione: $3 + 5t_1 \equiv 4\ (7) \implies 5t_1 \equiv 1\ (7) \implies t_1 \equiv 3\ (7) \implies t_1 = 3 + 7t_2$. Allora

$$x = 3 + 5(3 + 7t_2) = 18 + 35t_2.$$

Inserendo tale valore nella terza equazione: $18 + 35t_2 \equiv 4\ (11) \implies 7 + 2t_2 \equiv 4\ (11) \implies 2t_2 \equiv 8\ (11) \implies t_2 \equiv 48\ (11) \implies t_2 \equiv 4\ (11) \implies t_2 = 4 + 11t_3$. Allora

$$x = 18 + 35t_2 = 18 + 35(4 + 11t_3) = 158 + 385t_3.$$

L'unica soluzione del sistema è quindi, come prima, $x = 158\ (mod\ 385)$.

Torniamo ora al più generale problema della risoluzione di un sistema di tipo (*), con moduli a due a due coprimi (cfr. **Osserv. 3**).

Teorema 2. *Assegnato il sistema di equazioni congruenziali lineari*

$$(*) \qquad \begin{cases} a_1 X \equiv b_1\ (mod\ n_1) \\ \vdots \\ a_s X \equiv b_s\ (mod\ n_s), \end{cases}$$

con $d_i := (a_i, b_i) \mid b_i$, $\forall\, i = 1, \ldots s$, *e con* $(n_i, n_j) = 1$, $\forall\, i \neq j$, *tale sistema è equivalente ad un sistema cinese del tipo:*

$$(**) \qquad \begin{cases} X \equiv c_1\ (mod\ n_1') \\ \vdots \\ X \equiv c_s\ (mod\ n_s'), \end{cases}$$

con $n_i' := \frac{n_i}{d_i}$, $\forall\, i = 1, \ldots s$. *Ne segue che* $(*)$ *ha un'unica soluzione* $mod\ \prod_{i=1}^{s} n_i'$.

Dim. Dalla **Prop. 2**(ii) segue che $a_i X \equiv b_i\ (n_i)$ è equivalente a $\frac{a_i}{d_i}X \equiv \frac{b_i}{d_i}\ \left(mod\ \frac{n_i}{d_i}\right)$. Dunque $(*)$ è equivalente al sistema

$$(\bullet) \qquad \begin{cases} \frac{a_i}{d_i}X \equiv \frac{b_i}{d_i}\ \left(mod\ \frac{n_i}{d_i}\right) \\ \forall\, i = 1, \ldots s. \end{cases}$$

Poiché $\left(\frac{a_i}{d_i}, \frac{n_i}{d_i}\right) = 1$, esiste un inverso aritmetico di $\frac{a_i}{d_i}\ mod\ \frac{n_i}{d_i}$, che denotiamo α_i. Dalla **Prop. 2**(i) segue che $(\bullet)$ è equivalente al sistema

$$(\bullet\bullet) \qquad \begin{cases} X \equiv \frac{b_i}{d_i}\,\alpha_i\ (mod\ n_i') \\ \forall\, i = 1, \ldots s, \end{cases}$$

che è il sistema cinese $(**)$ cercato.

Esempio 3. Risolvere il seguente sistema di equazioni congruenziali lineari:

$$\begin{cases} 6X \equiv 8\ (10) \\ 9X \equiv 15\ (21) \\ 2X \equiv 8\ (11). \end{cases}$$

Si noti che $(10,21) = (10,11) = (21,11) = 1$ e che $(6,10) \,|\, 8$, $(9,21) \,|\, 1$, $(2,11) \,|\, 8$. Pertanto il sistema assegnato è compatibile ed è equivalente ad un sistema cinese. Si ha:

$6X \equiv 8\ (10)$ è equivalente a $3X \equiv 4\ (5)$ e $9X \equiv 15\ (21)$ è equivalente a $3X \equiv 5\ (7)$. Dunque il sistema assegnato è equivalente a

$$\begin{cases} 3X \equiv 4\ (5) \\ 3X \equiv 5\ (7) \\ 2X \equiv 8\ (11). \end{cases}$$

Poiché $3{\cdot}2 \equiv 1\ (5)$, $3{\cdot}5 \equiv 1\ (7)$, $2{\cdot}6 \equiv 1\ (11)$, allora il sistema diventa equivalente al sistema cinese

$$\begin{cases} X \equiv 8\ (5) \\ X \equiv 4\ (7) \\ X \equiv 4\ (11). \end{cases}$$

A questo punto va risolto il sistema. Ma lo abbiamo già fatto nel precedente **Esempio 2**. L'unica soluzione del sistema asegnato è quindi $x = 158\ (mod\ 385)$.

Cosa si può dire sulla compatibilità di un sistema a moduli non coprimi? In generale non è compatibile. Vale il seguente risultato relativo ad un sistema "di tipo cinese" di due equazioni.

Proposizione 4. *Dato il sistema di due equazioni*

$$(\bullet) \qquad \begin{cases} X \equiv a\ (mod\ n) \\ X \equiv b\ (mod\ m), \end{cases} \qquad con\ \ d := (m,n),$$

risulta: $(\bullet)$ *è compatibile* $\iff d \,|\, a-b$.

In tal caso ha un'unica soluzione modulo $mcm(m,n)$.

Dim. $(\bullet)$ è compatibile $\iff \exists\, x \in \boldsymbol{Z} : \begin{cases} n \,|\, x-a, \\ m \,|\, x-b \end{cases} \iff \exists\, x,t,s \in \boldsymbol{Z} : \begin{cases} x-a = tn, \\ x-b = ms \end{cases} \iff$

$\iff \exists\, t,s \in \boldsymbol{Z} : a-b = sm-tn \iff$ l'equazione $mX - nY = a-b$ ha una soluzione in $\boldsymbol{Z}\times\boldsymbol{Z} \iff$

$\iff$ [cfr. **Lemma 1**] $(m,n) \,|\, a-b \iff d \,|\, a-b$.

Sia ora $(\bullet)$ compatibile e siano x, y due sue soluzioni. Allora

$$\begin{cases} x \equiv a\ (n) \\ x \equiv b\ (m), \end{cases} \quad \begin{cases} y \equiv a\ (n) \\ y \equiv b\ (m), \end{cases} \quad \text{da cui} \quad \begin{cases} x \equiv y\ (n) \\ x \equiv y\ (m), \end{cases}$$

cioè $\begin{matrix} n \\ m \end{matrix} \Big|\, x-y$. Allora $mcm(m,n) \,|\, x-y$, cioè $x \equiv y\ \big(mod\ mcm(m,n)\big)$.

Esempio 4. Verificare che il sistema $\begin{cases} X \equiv 3\ (mod\ 10) \\ X \equiv 5\ (mod\ 6) \end{cases}$ è compatibile e calcolarne l'unica soluzione $(mod\ 30)$.

Si ha: $(10,6) = 2 \,|\, 3-5$. Dunque il sistema è compatibile. Dalla prima equazione: $x = 3+10t$. Sostituendo nella seconda: $3 + 10t \equiv 5\ (6) \implies 4t \equiv 2\ (6) \implies 2t \equiv 1\ (3) \implies t \equiv 2\ (3) \implies t = 2+3s$. Allora $x = 3 + 10(2+3s) = 23 + 30s$. L'unica soluzione è $x = 23\ (mod\ 30)$.

Veniamo ora ad una diversa formulazione del teorema cinese del resto. Occorre premettere una definizione.

Definizione 4. *Siano $(A, +, \cdot)$ e $(B, +, \cdot)$ due anelli [c. u.]. Sul prodotto cartesiano $A\times B$ si introduce una struttura di anello [c. u.], con le seguenti operazioni:*

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \quad (a_1, b_1)\cdot(a_2, b_2) = (a_1\cdot a_2, b_1\cdot b_2).$$

Si verifica facilmente che $(A\times B, +, \cdot)$ è un anello [c. u.], detto prodotto diretto *di A, B. In modo analogo si definisce il prodotto diretto $A_1\times A_2\times \dots \times A_n$ di n anelli $A_1, A_2, \dots, A_n$.*

Teorema 3. (*Teorema Cinese del resto* - 2^a **formulazione**). *Se r, s sono interi relativamente primi, sussiste l'isomorfismo di anelli*

$$\boldsymbol{Z}_{rs} \cong \boldsymbol{Z}_r\times\boldsymbol{Z}_s .$$

<u>Tale risultato può essere formulato in modo più completo, in questo modo</u>:

Siano $r, s \geq 2$. Risulta:

(1) L'applicazione $F : \boldsymbol{Z}_{rs} \to \boldsymbol{Z}_r\times\boldsymbol{Z}_s$ tale che $F(\overline{x}) = (\overline{x}_r, \overline{x}_s)$, $\forall\, \overline{x} \in \boldsymbol{Z}_{rs}$, è un omomorfismo di anelli [con $\overline{x}_r$ (rispett. $\overline{x}_s$) si è denotata la classe resto di x (mod r) (rispett. (mod s))].

(2) Sono condizioni equivalenti:

- *(i) F è biiettiva (cioè un isomorfismo di anelli).*
- *(ii) $(r, s) = 1$.*
- *(iii) ogni sistema di equazioni congruenziali del tipo*

$$\begin{cases} X \equiv a \ (mod\ r) \\ X \equiv b \ (mod\ s) \end{cases}$$

ammette una ed una sola soluzione (mod rs).

Dim. (*1*) Verifichiamo che F è ben definita, cioè che: $\overline{x} = \overline{y}$ (in $\boldsymbol{Z}_{rs}$) $\Longrightarrow$ $F(\overline{x}) = F(\overline{y})$.

Infatti, se $rs \mid x - y$, allora $\begin{matrix} r \\ s \end{matrix} \Big| \, x - y$ e quindi $\overline{x}_r = \overline{y}_r$, $\overline{x}_s = \overline{y}_s$, cioè $F(\overline{x}) = F(\overline{y})$.

Verifichiamo ora che F è un omomorfismo di anelli. Si ha infatti:

$$F(\overline{x} + \overline{y}) = F(\overline{x+y}) = (\overline{x+y}_r, \overline{x+y}_s) = (\overline{x}_r + \overline{y}_r, \overline{x}_s + \overline{y}_s) = F(\overline{x}) + F(\overline{y})$$

ed in modo analogo si verifica che $F(\overline{x}\cdot\overline{y}) = F(\overline{x})\cdot F(\overline{y})$.

(*2*) Osserviamo preliminarmente che $|\boldsymbol{Z}_{rs}| = rs = |\boldsymbol{Z}_r\times\boldsymbol{Z}_s|$. Ne segue che F è biiettiva $\Longleftrightarrow$ F è iniettiva $\Longleftrightarrow$ F è suriettiva.

(*i*) $\Longrightarrow$ (*ii*). Per assurdo, sia $d := (r, s) > 1$. Posto $h := mcm(r, s)$, allora $h = \frac{rs}{d}$ e $1 \leq h < rs$. Ne segue che $\overline{h} \neq \overline{0}$, in $\boldsymbol{Z}_{rs}$. Poiché $\begin{matrix} r \\ s \end{matrix} \Big| \, h$, allora $\overline{h}_r = \overline{0}_r$, $\overline{h}_s = \overline{0}_s$ e quindi $F(\overline{h}) = (\overline{0}_r, \overline{0}_s)$. Poiché ovviamente anche $F(\overline{0}) = (\overline{0}_r, \overline{0}_s)$, allora F non è iniettiva: assurdo.

(*ii*) $\Longrightarrow$ (*iii*). È il teorema cinese del resto nella 1^a formulazione, relativo a sistemi di due equazioni.

(*iii*) $\Longrightarrow$ (*i*). Basta dimostrare che F è suriettiva. Per ogni $(\overline{a}_r, \overline{b}_s) \in \boldsymbol{Z}_r\times\boldsymbol{Z}_s$, si consideri il sistema

$$\begin{cases} X \equiv a \ (mod\ r) \\ X \equiv b \ (mod\ s). \end{cases}$$

Per ipotesi tale sistema ammette una soluzione x (*mod* rs). Si ha: $F(\overline{x}) = (\overline{x}_r, \overline{x}_s) = (\overline{a}_r, \overline{b}_s)$. Dunque F è suriettiva.

Corollario 1. *Se $r_1, \dots, r_t$, sono interi a due a due coprimi, risulta:*

$$\boldsymbol{Z}_{r_1 \cdots r_t} \cong \boldsymbol{Z}_{r_1}\times \dots \times\boldsymbol{Z}_{r_t} .$$

<u>Tale risultato viene riformulato in questo modo</u>:

Siano $r_1, \dots, r_t \geq 2$. Risulta:

(1) L'applicazione $F : \boldsymbol{Z}_{r_1 \cdots r_t} \to \boldsymbol{Z}_{r_1}\times \dots \times\boldsymbol{Z}_{r_t}$ tale che $F(\overline{x}) = (\overline{x}_{r_1}, \dots, \overline{x}_{r_t})$, $\forall\, \overline{x} \in \boldsymbol{Z}_{r_1 \cdots r_t}$, è un omomorfismo di anelli.

(2) *Sono condizioni equivalenti:*

(i) F *è biiettiva (cioè un isomorfismo di anelli).*

(ii) $r_1, \dots, r_t$, *sono a due a due coprimi.*

(iii) *ogni sistema di equazioni congruenziali del tipo*

$$\begin{cases} X \equiv a_i \ (mod\ r_i) \\ \forall\, i = 1, \dots t \end{cases}$$

ammette una ed una sola soluzione $(mod\ \prod_{i=1}^{t} r_i)$.

Dim. La dimostrazione di (*1*) è esattamente la stessa del **Teorema 3**. Le implicazioni (*ii*) $\Longrightarrow$ (*iii*) e (*iii*) $\Longrightarrow$ (*i*) sono del tutto analoghe a quelle dimostrate nello stesso teorema.

(*i*) $\Longrightarrow$ (*ii*). Assumiamo, per assurdo, che, ad esempio, $d := (r_1, r_2) > 1$. Allora $h := mcm(r_1, r_2) < r_1 r_2$. Ne segue che, posto $x := h\, r_3 \dots r_t$, risulta $\overline{x} \neq \overline{0}$ in $\boldsymbol{Z}_{r_1 \cdots r_t}$ e $r_i \,\big|\, x$, $\forall\, i = 1, \dots, t$. Allora $\overline{x}_{r_i} = \overline{0}$ in $\boldsymbol{Z}_{r_i}$ e dunque $F(\overline{x}) = F\overline{0})$. Ciò contraddice l'iniettività di F.

Osservazione 6. Il teorema cinese del resto, nella sua formulazione $\boldsymbol{Z}_{rs} \cong \boldsymbol{Z}_r \times \boldsymbol{Z}_s$, se $(r, s) = 1$, si presta a semplificare vari calcoli aritmetici.

Ad esempio, vogliamo calcolare le ultime due cifre di $n = 827^7$.

Poiché le ultime due cifre di n sono il resto della divisione di n per 100, basta calcolare una soluzione in $[0, 99]$ della congruenza $X \equiv 827^7\ (mod\ 100)$.

Sussiste un isomorfismo $F : \boldsymbol{Z}_{100} \longrightarrow \boldsymbol{Z}_4 \times \boldsymbol{Z}_{25}$. Allora

$F(\overline{827}) = (\overline{827}_4, \overline{827}_{25}) = (\overline{3}_4, \overline{2}_{25})$ e quindi $F(\overline{827^7}) = F(\overline{827}^{\,7}) = (\overline{827}_4, \overline{827}_{25})^7 = (\overline{3}_4^{\,7}, \overline{2}_{25}^{\,7})$.

Si ha:

$$3^7 = 3{\cdot}3^3{\cdot}3^3 = 3{\cdot}27{\cdot}27 \equiv 3{\cdot}3{\cdot}3 \equiv 3\ (mod\ 4), \quad 2^7 = 4{\cdot}32 \equiv 4{\cdot}7 = 28 \equiv 3\ (mod\ 25)$$

e dunque $F(\overline{827}^{\,7}) = (\overline{3}_4, \overline{3}_{25})$.

Sia ora $\overline{x} \in \boldsymbol{Z}_{100}$ tale che $F(\overline{x}) = (\overline{3}_4, \overline{3}_{25})$. Per ottenere $\overline{x}$ basta risolvere il sistema cinese

$$\begin{cases} X \equiv 3\ (mod\ 4) \\ X \equiv 3\ (mod\ 25). \end{cases}$$

Si ha: $x = 3 + 25t \implies 3 + 25t \equiv 3\ (4) \implies 25t \equiv 0\ (4) \implies t \equiv 0\ (4) \implies t = 4s$. Allora $x = 3 + 100s$. Pertanto $827^7 \equiv 3\ (mod\ 100)$. Le ultime due cifre di 827^7 sono $0, 3$.

6. Piccolo teorema di Fermat. Il teorema di Eulero-Fermat

Teorema 1. *(Piccolo Teorema di Fermat (1640) - 1^a* **formulazione***) [abbr. PTF_1]. Sia p un numero primo. Risulta, per ogni $a \in \boldsymbol{Z}$,*

$$a^p \equiv a \ (mod\, p).$$

La dimostrazione fa uso del seguente lemma.

Lemma 1. *Sia p un numero primo. Per ogni $x, y \in \boldsymbol{Z}$:*

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

Dim. (Lemma 1). Si noti che, se p è primo, $p \,\big|\, \binom{p}{k}$, $\forall\, k = 1, \dots, p-1$. Si ha quindi:

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p = x^p + y^p + p(\ \dots\ ) \equiv x^p + y^p \ (mod\, p).$$

Dim. (PTF_1). Distinguiamo due casi: $a \geq 0$, $a < 0$.

$\boldsymbol{a \geq 0}$. Per induzione su a.

Base induttiva: sia $a = 0$. $0^p \equiv 0 \ (mod\, p)$ è ovvio.

Passo induttivo: sia $a \geq 0$ ed assumiamo che $a^p \equiv a \ (mod\, p)$. Dimostriamo che $(a+1)^p \equiv a+1 \ (mod\, p)$. Si ha, per il lemma e l'ipotesi induttiva: $(a+1)^p \equiv a^p + 1^p \equiv a+1 \ (mod\, p)$.

$\boldsymbol{a < 0}$. Poiché $-a > 0$, $(-a)^p \equiv -a \ (mod\, p)$. Si ha (dal lemma e dal caso precedente):

$$0 = 0^p = \big(a + (-a)\big)^p \equiv a^p + (-a)^p \equiv a^p + (-a) \ (mod\, p), \text{ cioè } a \equiv a^p \ (mod\, p).$$

Corollario 1. (*Piccolo Teorema di Fermat* - 2^a **formulazione**) [abbr. PTF_2]. *Siano $a, p \in \boldsymbol{Z}$, con $(a,p) = 1$. Se p è primo, risulta:*

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

[Dunque $\overline{a}^{\,p-1} = \overline{1}$, $\forall\, \overline{a} \in \boldsymbol{Z}_p^{\bullet}$].

Dim. Dal PTF_1, $a^p \equiv a \ (mod\, p)$, cioè $p \,\big|\, a^p - a = a(a^{p-1} - 1)$. Poiché $(p, a) = 1$, segue da EU che $p \,\big|\, a^{p-1} - 1$, cioè $a^{p-1} \equiv 1 \ (mod\, p)$.

Osservazione 1. Se p non è primo, la conclusione del PTF (in entrambe le formulazioni) è in generale falsa. Ad esempio, se $p = 4$ ed $a = 3$, risulta: $a^{p-1} \not\equiv 1$, $a^p \not\equiv a \ (mod\, 4)$.

Anche il viceversa del PTF è falso: ad esempio risulta: $5^{4-1} \equiv 1 \ (mod\, 4)$, ma 4 non è primo.

Osservazione 2. In forma contrappositiva, il PTF_2 può enunciarsi in questo modo:

Siano $a, n \in \boldsymbol{Z}$, con $(a,n) = 1$. Se $a^{n-1} \not\equiv 1 \ (mod\, n)$, allora n non è primo.

Questa formulazione è utile come "*test di non primalità*". Supponiamo infatti di voler sapere se un naturale n è o non è primo. Si può ovviamente assumere n dispari e $n \geq 3$.

Si può scegliere come base $a = 2$. Se $2^{n-1} \not\equiv 1 \ (mod\ n)$, allora n non è primo; se invece $2^{n-1} \equiv 1 \ (mod\, n)$, non si può decidere nulla.

Si scelga in tal caso come base il più piccolo numero primo successivo a 2 e relativamente primo con n: dunque $a = 3$ (se $(3,n) = 1$). Se $3^{n-1} \not\equiv 1 \ (mod\ n)$, n non è primo. Se invece $3^{n-1} \equiv 1 \ (mod\, n)$, non si può concludere nulla, ma si può scegliere $a = 5$ (se $(5,n) = 1$) e verificare se $5^{n-1} \equiv 1 \ (mod\, n)$.

[Si noti che è inutile verificare se $4^{n-1} \equiv 1 \ (mod\ n)$. Infatti $4^{n-1} = 2^{n-1} \cdot 2^{n-1}$ ed, essendo $2^{n-1} \equiv 1 \ (mod\ n)$, allora $4^{n-1} \equiv 1 \ (mod\ n)$. Da ciò segue che è inutile scegliere come base a un numero non primo].

Il procedimento sopra descritto ovviamente non può aver termine se n è primo.

Si noti infine che per calcolare a^{n-1} $(mod\, n)$ conviene procedere in questo modo:

- si scrive l'intero $n-1$ come somma di potenze decrescenti di 2 (cfr. **Osserv. 2.8**):

$$n-1=2^{k_1}+2^{k_2}+\ \dots\ +2^{k_s},\ \text{con}\ \ k_1>k_2>\ \dots\ >k_s\geq 1\ \ \text{[si osservi che } n-1 \text{ è pari]}.$$

- si calcolano $(mod\, n)$ le potenze $a=a^{2^0},\ a^{2^1},\ a^{2^2},\ \dots\ ,\ a^{2^{k_1}}$, nell'ordine indicato, tenendo conto del fatto che $a^{2^i}\equiv (a^{2^{i-1}})^2\ (mod\, n)$.

A questo punto, si utilizza il fatto che $a^{n-1}=\big(a^{2^{k_1}}\big)\cdot\big(a^{2^{k_2}}\big)\cdot\ \dots\ \cdot\big(a^{2^{k_s}}\big)$ e si riduce tale uguaglianza *modulo n*.

Esempio 1. Vogliamo verificare che $n=341$ non è primo.

Risulta: $n-1=340=2^8+2^6+2^4+2^2$. Scelta come base $a=2$, si ha:

$$\begin{aligned}
&2^{2^0}=2\equiv 2\ (mod\, 341),\\
&2^{2^1}\equiv (2)^2\equiv 4\ (mod\, 341),\\
&2^{2^2}\equiv (4)^2\equiv 16\ (mod\, 341),\\
&2^{2^3}\equiv (16)^2\equiv 256\ (mod\, 341),\\
&2^{2^4}\equiv (256)^2\equiv 64\ (mod\, 341),\\
&2^{2^5}\equiv (64)^2\equiv 4\ (mod\, 341),\\
&2^{2^6}\equiv (4)^2\equiv 16\ (mod\, 341),\\
&2^{2^7}\equiv (16)^2\equiv 256\ (mod\, 341),\\
&2^{2^8}\equiv (256)^2\equiv 64\ (mod\, 341).
\end{aligned}$$

Ne segue che $2^{340}=2^{2^8}\cdot 2^{2^6}\cdot 2^{2^4}\cdot 2^{2^2}\equiv 64\cdot 16\cdot 64\cdot 16=16^2\cdot 64^2\equiv 256\cdot 4=1024\equiv 1\ (mod\, 341)$.

Nulla si può quindi decidere sulla "non primalità" di 341, ma si può passare alla base $a=3$. Si ha:

$$\begin{aligned}
&3^{2^0}=3\equiv 3\ (mod\, 341),\\
&3^{2^1}\equiv (3)^2\equiv 9\ (mod\, 341),\\
&3^{2^2}\equiv (9)^2\equiv 81\ (mod\, 341),\\
&3^{2^3}\equiv (81)^2\equiv 82\ (mod\, 341),\\
&3^{2^4}\equiv (82)^2\equiv 245\ (mod\, 341),\\
&3^{2^5}\equiv (245)^2\equiv 9\ (mod\, 341),\\
&3^{2^6}\equiv (9)^2\equiv 81\ (mod\, 341),\\
&3^{2^7}\equiv (81)^2\equiv 82\ (mod\, 341),\\
&3^{2^8}\equiv (82)^2\equiv 245\ (mod\, 341).
\end{aligned}$$

Ne segue che $3^{340}=3^{2^8}\cdot 3^{2^6}\cdot 3^{2^4}\cdot 3^{2^2}\equiv 245\cdot 81\cdot 245\cdot 81\equiv 56\ (mod\, 341)$. Poiché $3^{340}\not\equiv 1\ (mod\, 341)$, allora 341 non è primo. [In effetti sappiamo che $11\,\big|\,343$. Dunque $341=11\cdot 31$].

Ora descriveremo un risultato analogo al PTF_2, ma valido *modulo* un naturale n non necessariamente primo: è il *teorema di Eulero-Fermat* (cfr. **Teorema 2**). Premettiamo la definizione di *funzione di Eulero* ed una formula per il suo calcolo.

Definizione 1. *Per ogni $n\geq 1$, si denota con $\boldsymbol{U}_n$ l'insieme*

$$\boldsymbol{U}_n=\{k\in\boldsymbol{Z}\ :\ 1\leq k\leq n\ \ e\ \ (k,n)=1\}.$$

Si chiama funzione di Eulero l'applicazione $\varphi:\boldsymbol{N}^{\cdot}\to\boldsymbol{N}^{\cdot}$ tale che $\varphi(n)=|\boldsymbol{U}_n|$, $\forall\, n\in\boldsymbol{N}^{\cdot}$. [Dunque $\varphi(n)$ è il numero dei naturali $\leq n$ e primi con n.]

Osservazione 3. Per ogni $n\geq 2$, risulta: $\varphi(n)=\big|\mathcal{U}(\boldsymbol{Z}_n)\big|$. Infatti è noto che

$$\mathcal{U}(\boldsymbol{Z}_n)=\big\{\overline{a}\in\boldsymbol{Z}_n\ :\ 1\leq a<n\ \ \text{e}\ \ (a,n)=1\big\}.$$

Si noti che: $\varphi(1)=1$ (perché $\boldsymbol{U}_1=\{1\}$); $\varphi(2)=1$ (perché $\boldsymbol{U}_2=\{1\}$); $\varphi(3)=2$ (perché $\boldsymbol{U}_3=\{1,2\}$); per ogni primo p, $\varphi(p)=p-1$ (perché $\boldsymbol{U}_p=\{1,2,\dots,p-1\}$). Si tratta ora di calcolare $\varphi(n)$, $\forall\, n \geq 1$.

Proposizione 1. *Se* $n = p_1^{r_1} \dots p_s^{r_s}$, *risulta:*
$$\varphi(n) = \left(p_1^{r_1} - p_1^{r_1-1}\right)\cdot \dots \cdot\left(p_s^{r_s} - p_s^{r_s-1}\right).$$

Dim. Basterà dimostrare i due seguenti risultati:

(A) Se $(r,s)=1$, $\varphi(rs) = \varphi(r)\cdot\varphi(s)$.

(B) Se p è primo, $\varphi(p^r) = p^r - p^{r-1}$ $(\forall\, r \geq 1)$.

Per dimostrare (A) abbiamo bisogno del seguente lemma.

Lemma 2. *Sia* $f : A \to B$ *un isomorfismo di anelli commutativi unitari. Allora* $f\big(\mathcal{U}(A)\big) = \mathcal{U}(B)$.

Dim. Lemma 2. Osserviamo che $f(1_A) = 1_B$. Infatti, essendo f suriettiva, $\forall\, b \in B$, $\exists\, a \in A$ tale che $f(a) = b$. Allora $b = f(a) = f(a\cdot 1_A) = f(a)\cdot f(1_A) = b\cdot f(1_A) = f(1_A)\cdot b$, cioè $b\cdot f(1_A) = b = f(1_A)\cdot b$. Dunque $f(1_A)$ è l'unico elemento neutro in B (rispetto al prodotto), cioè $f(1_A) = 1_B$.

Verifichiamo che $f\big(\mathcal{U}(A)\big) \subseteq \mathcal{U}(B)$. Per ogni $a \in \mathcal{U}(A)$ [con $aa' = 1_A$] si ha: $1_B = f(1_A) = f(aa') = f(a)f(a')$. Dunque $f(a) \in \mathcal{U}(B)$.

Verifichiamo che $\mathcal{U}(B) \subseteq f\big(\mathcal{U}(A)\big)$. Per ogni $b \in \mathcal{U}(B)$ [con $bb' = 1_B$] si ha: se $b = f(a)$ e $b' = f(a')$, allora $f(1_A) = 1_B = bb' = f(a)f(a') = f(aa')$: ne segue che (essendo f iniettiva) $1_A = aa'$. Quindi $a \in \mathcal{U}(A)$ e $b \in f\big(\mathcal{U}(A)\big)$

Dim. (A). Sia $(r,s) = 1$. Dal teorema Cinese del Resto (cfr. **Teor. 5.3**), $F : \boldsymbol{Z}_{rs} \to \boldsymbol{Z}_r \times \boldsymbol{Z}_s$ è un isomorfismo di anelli. Dal precedente **Lemma 2**, F trasforma $\mathcal{U}(\boldsymbol{Z}_{rs})$ in $\mathcal{U}(\boldsymbol{Z}_r \times \boldsymbol{Z}_s)$. Ora verifichiamo che $\mathcal{U}(\boldsymbol{Z}_r \times \boldsymbol{Z}_s) = \mathcal{U}(\boldsymbol{Z}_r) \times \mathcal{U}(\boldsymbol{Z}_s)$. Infatti:

$$(\overline{a},\overline{b}) \in \mathcal{U}(\boldsymbol{Z}_r \times \boldsymbol{Z}_s) \iff (\overline{a},\overline{b})\cdot(\overline{c},\overline{d}) = (\overline{1}_r, \overline{1}_s),\ \exists\, c,d \in \boldsymbol{Z} \iff \overline{a}\cdot\overline{c} = \overline{1}_r \text{ e } \overline{b}\cdot\overline{d} = \overline{1}_s \iff$$
$$\iff \overline{a} \in \mathcal{U}(\boldsymbol{Z}_r) \text{ e } \overline{b} \in \mathcal{U}(\boldsymbol{Z}_s) \iff (\overline{a},\overline{b}) \in \mathcal{U}(\boldsymbol{Z}_r) \times \mathcal{U}(\boldsymbol{Z}_s).$$

Ne segue: $\varphi(rs) = \big|\mathcal{U}(\boldsymbol{Z}_{rs})\big| = \big|\mathcal{U}(\boldsymbol{Z}_r \times \boldsymbol{Z}_s)\big| = \big|\mathcal{U}(\boldsymbol{Z}_r) \times \mathcal{U}(\boldsymbol{Z}_s)\big| = \big|\mathcal{U}(\boldsymbol{Z}_r)\big|\cdot\big|\mathcal{U}(\boldsymbol{Z}_s)\big| = \varphi(r)\cdot\varphi(s)$.

Nota. Se $r_1, \dots r_s$ sono a due a due coprimi, risulta: $\varphi(r_1\cdot \dots \cdot r_s) = \prod_{i=1}^{s} \varphi(r_i)$.

Dim. (B). Per definizione, $\varphi(p^r) = \big|\boldsymbol{U}_{p^r}\big|$. Si ha:
$$\boldsymbol{U}_{p^r} = \left\{k \in \boldsymbol{Z} \text{ tali che } 1 \leq k \leq p^r,\ (k,p^r) = 1\right\}.$$
Si ha: $(k,p^r) = 1 \iff (k,p) = 1$. Ne segue: $(k,p^r) \neq 1 \iff (k,p) \neq 1 \iff (k,p) = p \iff k \in p\boldsymbol{Z}$. Pertanto:
$$\boldsymbol{U}_{p^r} = \left\{k \in \boldsymbol{Z} \,:\, 1 \leq k \leq p^r,\ k \notin p\boldsymbol{Z}\right\} = \left\{1, 2, \dots, p^r\right\} - \left\{ph,\ \ \forall\, h = 1, \dots, p^{r-1}\right\}.$$
Allora $\varphi(p^r) = \big|\boldsymbol{U}_{p^r}\big| = p^r - p^{r-1}$.

Teorema 2. *(Teorema di Eulero-Fermat). Sia* $n \geq 2$ *e sia* $a \in \boldsymbol{Z}$ *tale che* $(a,n) = 1$. *Risulta:,*
$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$
[Dunque $\overline{a}^{\,\varphi(n)} = \overline{1}$, $\forall\, \overline{a} \in \mathcal{U}(\boldsymbol{Z}_n)$*].*

Dim. (*J. Ivory, 1806*). Denotiamo con $t_1, \dots, t_{\varphi(n)}$ i naturali compresi tra 1 ed n, relativamente primi con n. Poiché $(a,n) = 1$, anche $at_1, \dots, at_{\varphi(n)}$ sono relativamente primi con n. Inoltre sono a due a due non congruenti $mod\, n$. Se infatti $at_i \equiv at_j$ $(mod\, n)$, allora $n \,\big|\, t_i - t_j$ (da *EU*) e dunque $t_i - t_j = 0$. Ne segue che
$$\left\{\overline{t_1}, \dots, \overline{t_{\varphi(n)}}\right\} = \mathcal{U}(\boldsymbol{Z}_n) = \left\{\overline{at_1}, \dots, \overline{at_{\varphi(n)}}\right\}.$$
Pertanto, moltiplicando gli elementi dei due insiemi,
$$\overline{t_1}\cdot \dots \cdot \overline{t_{\varphi(n)}} = \overline{at_1}\cdot \dots \cdot \overline{at_{\varphi(n)}} = \overline{a}^{\,\varphi(n)}\,\overline{t_1}\cdot \dots \cdot \overline{t_{\varphi(n)}}$$

e, semplificando i fattori $\overline{t}_i$, si ottiene $\overline{1} = \overline{a}^{\varphi(n)}$, cioè $a^{\varphi(n)} \equiv 1 \ (mod\, n)$.

Osservazione 4. Si noti che con la stessa dimostrazione si può dimostrare anche il PTF_2.

Corollario 2. *Sia $n \geq 2$ e sia $a \in \boldsymbol{Z}$ tale che $(a,n) = 1$. Un inverso aritmetico a' di a modulo n è dato da $a^{\varphi(n)-1}$.*

Dim. Infatti $a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} \equiv 1 \ (mod\, n)$.

Il teorema di Eulero-Fermat è un utile strumento per risolvere problemi aritmetici, come negli esempi che seguono. Si noti che, utilizzando soltanto il teorema Cinese del Resto (come fatto in **Osserv. 5.6**) i calcoli sarebbero molto più laboriosi.

Esempio 2. Usando il teorema di Eulero-Fermat, calcolare le ultime due cifre di $n = 81^{82}$.

Si tratta di risolvere la congruenza $81^{82} \equiv X \ (mod\, 100)$.

Si ha: $(81, 100) = 1$ e $\varphi(100) = \varphi(4) \cdot \varphi(25) = 2 \cdot 20 = 40$. Allora, in base al teorema di Eulero-Fermat, $81^{40} = 81^{\varphi(100)} \equiv 1 \ (mod\, 100)$. Dunque

$$81^{82} = \left(81^{40}\right)^2 \cdot 81^2 \equiv 1^2 \cdot 81^2 = 6561 \equiv 61 \ (mod\, 100).$$

Le ultime due cifre di 81^{82} sono $6, 1$.

Esempio 3. Usando il teorema di Eulero-Fermat, calcolare le ultime tre cifre di $n = 7^{827}$.

Si tratta di risolvere la congruenza $7^{827} \equiv X \ (mod\, 1000)$.

Si ha: $(7, 1000) = 1$ e $\varphi(1000) = \varphi(8) \cdot \varphi(125) = 4 \cdot 100 = 400$. Allora, in base al teorema di Eulero-Fermat, $7^{400} \equiv 1 \ (mod\, 1000)$. Allora $7^{827} = (7^{400})^2 \cdot 7^{27} \equiv 1^2 \cdot 7^{27} \ (mod\, 1000)$. Si tratta quindi di calcolare $7^{27} \ (mod\, 1000)$.

Essendo $27 = 2^4 + 2^3 + 2 + 1$, allora $7^{27} \equiv 7^{16} \cdot 7^8 \cdot 7^2 \cdot 7 \ (mod\, 1000)$. Si ha:

$$\begin{aligned}
&7 \equiv 7 \ (mod\, 1000),\\
&7^2 \equiv 49 \ (mod\, 1000),\\
&7^4 \equiv 401 \ (mod\, 1000),\\
&7^8 \equiv (401)^2 \equiv 801 \ (mod\, 1000),\\
&7^{16} \equiv (801)^2 \equiv 601 \ (mod\, 1000).
\end{aligned}$$

Poiché $601 \cdot 801 \equiv 401 \ (mod\, 1000)$ e $49 \cdot 7 \equiv 343 \ (mod\, 1000)$, allora $7^{27} \equiv 401 \cdot 343 \equiv 543 \ (mod\, 1000)$.
Si conclude che le ultime tre cifre di 7^{827} sono $5, 4, 3$.

7. Esercizi del Capitolo II

2.1. (i) Estendere la definizione di MCD al caso di un numero finito di interi $a_1, \dots, a_n$, con $n \geq 2$.
(ii) Assegnati tre interi non nulli a, b, c, verificare che $MCD(a, b, c) = MCD(a, MCD(b, c))$.
(iii) Verificare che se gli interi a, b, c sono a due a due coprimi, allora $MCD(ab, ac, bc) = 1$.
(iv) Se $MCD(a, b, c) = 1$, è vero che $MCD(ab, ac, bc) = 1$?
(v) Se $MCD(a, b, c) = 1$, determinare un'identità di Bézout, del tipo $1 = ax+by+cz$, con $x, y, z \in \boldsymbol{Z}$.

* * * * * * * * *

2.2. (i) Sia p un numero primo. Sia $a \in \boldsymbol{N}$ tale che $1 \leq a < p^2$. Quali a sono privi di inverso aritmetico $mod\, p^2$?
(ii) Siano n, m interi ≥ 2, tali che $n \mid m$. Sia $a \in \boldsymbol{N}$ tale che $1 \leq a < n$. Verificare che se a ha inverso aritmetico $mod\, m$ lo ha anche $mod\, n$. È vero che se a ha inverso aritmetico $mod\, n$ lo ha anche $mod\, m$?

* * * * * * * * *

2.3. Risolvere l'equazione congruenziale lineare $121\, X \equiv 22 \ (mod\ 33)$, indicandone un sistema completo di soluzioni $mod\ 33$.

* * * * * * * * *

2.4. Posto $n = 9, 10, 11, 12, 13, 14, 15, 16$, risolvere l'equazione congruenziale lineare

$$6\, X \equiv 9 \ (mod\ n),$$

indicandone, se compatibile, la totalità delle soluzioni ed un sistema completo di soluzioni $mod\ n$.

* * * * * * * * *

2.5. Risolvere il seguente sistema 'cinese' di equazioni congruenziali lineari

$$\begin{cases} X \equiv 2 \ (mod\ 5) \\ X \equiv 1 \ (mod\ 3) \\ X \equiv 6 \ (mod\ 14) \\ X \equiv 5 \ (mod\ 11). \end{cases}$$

* * * * * * * * *

2.6. Risolvere il seguente sistema di equazioni congruenziali lineari

$$\begin{cases} 18\, X \equiv 12 \ (mod\ 30) \\ 7\, X \equiv 4 \ (mod\ 9) \\ 28\, X \equiv 14 \ (mod\ 98). \end{cases}$$

* * * * * * * * *

2.7. Verificare se il seguente sistema di equazioni congruenziali lineari è compatibile:

$$\begin{cases} 2\, X \equiv 8 \ (mod\ 9) \\ 2\, X \equiv 6 \ (mod\ 15). \end{cases}$$

* * * * * * * * *

2.8. [*Esonero 8/4/03*] Determinare, se esistono, i valori $a \in \boldsymbol{Z}$ per cui il seguente sistema ammette soluzione:

$$\begin{cases} 6425\, X \equiv 7 \ \ mod\ 12 \\ 8614\, X \equiv 3 \ \ mod\ 7 \\ 3\, X \equiv a \ \ mod\ 8. \end{cases}$$

Per tali valori calcolare le soluzioni stesse.

* * * * * * * * *

2.9. [*Esame 1/7/03*] Al variare di $a \in \boldsymbol{N}$, $0 \leq a < 15$, sono assegnati i seguenti sistemi di congruenze:

$$\begin{cases} 2X \equiv 5 \ (mod\ 7) \\ X \equiv 4 \ (mod\ 9) \\ 4X \equiv a \ (mod\ 15). \end{cases}$$

Determinare gli eventuali a per cui il sistema è compatibile e scriverne la generica soluzione.

* * * * * * * * *

2.10. [*Esame 15/6/04*] È assegnato il seguente sistema di equazioni congruenziali lineari, dipendente da due parametri $a, b \in \boldsymbol{Z}$:

$$\begin{cases} aX \equiv 3 \ (mod\ 5) \\ 3X \equiv b \ (mod\ 8). \end{cases}$$

(i) Determinare per quali $a, b \in \boldsymbol{Z}$ il sistema è compatibile.

(ii) Per siffatti valori scrivere la generica soluzione del sistema, in funzione dei parametri a, b ed eventualmente di loro inversi aritmetici a', b'.

* * * * * * * * *

2.11. [*Esonero 8/4/03*] Sia $f : \boldsymbol{Z}_{18} \to \boldsymbol{Z}_6 \times \boldsymbol{Z}_3$ l'applicazione così definita:

$f(\overline{x}_{18}) = (\overline{x}_6, \overline{x}_3)$, $\forall\, \overline{x}_{18} \in \boldsymbol{Z}_{18}$ [dove $\overline{x}_k$ denota la classe resto $\overline{x}$ in $\boldsymbol{Z}_k$, $\forall\, k \geq 2$].

(i) Verificare che f è ben definita.

(ii) Determinare $Im(f)$ e calcolare $f^{-1}((\overline{0}_6, \overline{0}_3))$, $f^{-1}((\overline{1}_6, \overline{2}_3))$.

(iii) Sia $g : \boldsymbol{Z}_6 \to \boldsymbol{Z}_{18}$ tale che: $g(\overline{x}_6) = \overline{x}_{18}$, $\forall\, \overline{x}_6 \in \boldsymbol{Z}_6$. g è ben definita? g è iniettiva?

* * * * * * * * *

2.12. Utilizzando il teorema Cinese del Resto, verificare che le ultime tre cifre di $n = 46^{14}$ sono $6, 5, 6$.

* * * * * * * * *

2.13. Determinare, se esiste, il minimo intero $n > 0$ tale che 7123^n abbia come ultima cifra 1.

* * * * * * * * *

2.14. Considerati i numeri naturali 734^h, $\forall\, h \geq 2$, determinare le possibili ultime due cifre di tali numeri.

* * * * * * * * *

2.15. È assegnato il numero naturale $n = 133^{42}$.

(i) Usando il teorema di Eulero-Fermat, calcolare le ultime due cifre di n.

(ii) Usando il teorema Cinese del Resto, calcolare le ultime tre cifre di n.

* * * * * * * * *

2.16. Sia $n \geq 2$. Verificare che ogni elemento non nullo di $\boldsymbol{Z}_n$ è o un elemento invertibile o uno zero-divisore di $\boldsymbol{Z}_n$.

* * * * * * * * *

2.17. Utilizzando opportunamente la relazione di congruenza $mod\ 3$, verificare che esiste un'unica terna di numeri primi della forma

$$(n,\ n-2,\ n-4), \ \text{ con } \ n \in \boldsymbol{N}.$$

* * * * * * * * *

2.18. Dimostrare che esistono infiniti primi congruenti a $3\ mod\ 4$.

Suggerimento. Per assurdo, l'insieme A dei primi congruenti a $3\ mod\ 4$ sia finito. Poniamo

$$A = \{p_1 = 3,\ p_2 = 7,\ p_3,\ \dots,\ p_n\}.$$

Posto inoltre $P = \prod_{i=1}^{n} p_i$, $Q = 4P - 1$, verificare preliminarmente che:

$$(a)\ \ Q \text{ non è primo}; \qquad (b)\ \ \exists\, p_k \in A \text{ tale che } p_k \,\big|\, Q.$$

* * * * * * * * *

Appendice 2

Metodi di fattorizzazione in prodotti di primi

Ci proponiamo di determinare la fattorizzazione in primi di un naturale n, che assumeremo dispari e ≥ 3. Descriveremo due algoritmi. Il primo è attribuito a Fermat.

Definizione 1. *Poniamo,* $\forall\, n \geq 3$*:*

$$\mathcal{A}_n := \{(a,b) \in \boldsymbol{N} \times \boldsymbol{N} \ \ \textit{tali che} \ \ ab = n,\ 1 \leq a \leq b\}.$$

Osservazione 1. (i) Risulta: $\mathcal{A}_n \neq \emptyset$ [infatti $(1,n) \in \mathcal{A}_n$].
(ii) Risulta: $\mathcal{A}_n = \{(1,n)\} \iff n$ è primo [ovvio].
(iii) $\mathcal{A}_n$ è un insieme finito [infatti, $\forall\,(a,b) \in \mathcal{A}_n,\ 1 \leq a, b \leq n$].
(iv) $\mathcal{A}_n$ è un insieme totalmente ordinato rispetto alla seguente relazione:

$$(a,b) \leq (a_1,b_1) \iff b - a \leq b_1 - a_1, \quad \forall\,(a,b),\,(a_1,b_1) \in \mathcal{A}_n$$

[Verifichiamo che $\leq$ è una relazione d'ordine totale su $\mathcal{A}_n$:

- la riflessività e la transitività di $\leq$ sono ovvie.
- $\leq$ è *antisimmetrica*: sia infatti $(a,b) \leq (a_1,b_1)$ e $(a_1,b_1) \leq (a,b)$. Allora $b-a = b_1-a_1$. Se per assurdo fosse $a < a_1$, si avrebbe $\frac{n}{a} > \frac{n}{a_1}$, cioè $b > b_1$. Allora $b_1-a_1 < b-a$: assurdo. Analogamente si esclude che sia $a_1 < a$. Dunque $a_1 = a$ e quindi $b_1 = b$, cioè $(a,b) = (a_1,b_1)$.
- $\leq$ è *totale*: se infatti $(a,b) \not\leq (a_1,b_1)$, allora $b-a \not\leq b_1-a_1$ e quindi $b_1-a_1 < b-a$, da cui $(a_1,b_1) \leq (a,b)$.

Si noti che $(a,b) \leq (1,n)$, $\forall\,(a,b) \in \mathcal{A}_n$: dunque $(1,n)$ è l'ultimo elemento di $\mathcal{A}_n$.]

Assumiamo per il momento di saper calcolare il primo elemento di $\mathcal{A}_n$, che denoteremo $(\tilde{a},\tilde{b})$. Con lo stesso procedimento potremo poi calcolare il primo elemento di $\mathcal{A}_{\tilde{a}}$ e di $\mathcal{A}_{\tilde{b}}$ e così via, finché ci ridurremo ad insiemi di tipo $\mathcal{A}_{p_i}$, con p_i primo. Tutti i primi p_i ottenuti forniranno la fattorizzazione richiesta di n.

Allo scopo di calcolare gli elementi di $\mathcal{A}_n$ (ed in particolare il primo elemento), introduciamo la seguente definizione.

Definizione 2. *Poniamo,* $\forall\, n \geq 3$*:*

$$\mathcal{B}_n := \{(x,y) \in \boldsymbol{N} \times \boldsymbol{N} \ \ \textit{tali che} \ \ 0 \leq y < x \ \ \text{e} \ \ x^2 - y^2 = n\}.$$

Osservazione 2. (i) Verifichiamo che gli insiemi $\mathcal{A}_n$, $\mathcal{B}_n$ sono in corrispondenza biunivoca. Allo scopo definiamo le due applicazioni:

$$\varphi : \mathcal{A}_n \to \mathcal{B}_n \ \text{ tale che } \ \varphi((a,b)) = \big(\tfrac{b+a}{2},\ \tfrac{b-a}{2}\big), \quad \forall\,(a,b) \in \mathcal{A}_n$$

[si noti che, essendo n dispari, anche a, b lo sono e dunque $\frac{b+a}{2}, \frac{b-a}{2} \in \boldsymbol{N}$. Inoltre si ha: $0 \leq \frac{b-a}{2} < \frac{b+a}{2}$ e $(\frac{b+a}{2})^2 - (\frac{b-a}{2})^2 = ab = n$. Dunque $\varphi((a,b)) \in \mathcal{B}_n$];

$$\psi : \mathcal{B}_n \to \mathcal{A}_n \ \text{ tale che } \ \psi((x,y)) = \big(x-y,\ x+y\big), \quad \forall\,(x,y) \in \mathcal{B}_n$$

[si noti che $1 \leq x-y \leq x+y$; inoltre $(x+y)(x-y) = x^2 - y^2 = n$. Dunque $\psi((x,y)) \in \mathcal{A}_n$].

Lasciamo per esercizio la verifica che φ, ψ sono l'una inversa dell'altra.

(*ii*) L'ordinamento totale di $\boldsymbol{\mathcal{A}}_n$ si trasforma tramite φ in un ordinamento totale di $\boldsymbol{\mathcal{B}}_n$, che è così definito:

$$(x,y) \le (x_1,y_1) \iff x \le x_1 \iff y \le y_1.$$

Infatti: $(x,y) \le (x_1,y_1) \iff \psi((x,y)) \le \psi((x_1,y_1)) \iff (x-y, x+y) \le (x_1-y_1, x_1+y_1) \iff x+y-(x-y) \le x_1+y_1-(x_1-y_1) \iff 2y \le 2y_1 \iff y \le y_1 \iff y^2 \le y_1^2 \iff y^2+n \le y_1^2+n \iff x^2 \le x_1^2 \iff x \le x_1$.

Per ottenere gli elementi di $\boldsymbol{\mathcal{A}}_n$ (ed in particolare il primo, che denoteremo $(\tilde{a}, \tilde{b})$), basterà calcolare gli elementi di $\boldsymbol{\mathcal{B}}_n$ (ed in particolare il primo elemento $(\tilde{x}, \tilde{y})$) e poi trasformarli nei corrispondenti di $\boldsymbol{\mathcal{A}}_n$.

Proposizione 1. *Sia* $x_0 :=$ *minimo intero* $\ge \sqrt{n}$. *Per ogni* $(x,y) \in \boldsymbol{N} \times \boldsymbol{N}$, *risulta:*

$$(x,y) \in \boldsymbol{\mathcal{B}}_n \iff y = \sqrt{x^2-n} \text{ e } x_0 \le x \le \tfrac{n+1}{2}.$$

Dim. $(\Longrightarrow)$. Sia $(x,y) \in \boldsymbol{\mathcal{B}}_n$. Allora

$(*)$ $y^2 = x^2 - n > 0 \Rightarrow y = \sqrt{x^2-n}$;

$(**)$ essendo $(a,b) \le (1,n)$, $\forall (a,b) \in \boldsymbol{\mathcal{A}}_n$, allora $(x,y) = \varphi((a,b)) \le \varphi((1,n)) = (\frac{n+1}{2}, \frac{n-1}{2})$ e quindi $x \le \frac{n+1}{2}$.

$(***)$ $x^2 = n + y^2 \ge n$ e quindi $x \ge \sqrt{n}$. Allora $x \ge x_0$.

Da $(*)$, $(**)$ e $(***)$ segue l'implicazione $(\Longrightarrow)$.

$(\Longleftarrow)$. Sia $(x,y) \in \boldsymbol{N} \times \boldsymbol{N}$ tale che $y = \sqrt{x^2-n}$ e $x_0 \le x \le \frac{n+1}{2}$. Allora

$(*)$ $y^2 = x^2 - n \Rightarrow x^2 - y^2 = n$.

$(**)$ $0 \le y$ è ovvio.

$(***)$ $y = \sqrt{x^2-n} < \sqrt{x^2} = x$: dunque $y < x$.

Da $(*)$, $(**)$ e $(***)$ segue che $(x,y) \in \boldsymbol{\mathcal{B}}_n$.

La **Prop. 1** consente di determinare $\boldsymbol{\mathcal{B}}_n$: tra gli interi $x = x_0 + h \in [x_0, \frac{n+1}{2}]$, si scelgono quelli per cui $(x_0+h)^2 - n$ è un quadrato. Allora $\boldsymbol{\mathcal{B}}_n$ è formato dalle coppie $\big(x_0+h, \sqrt{(x_0+h)^2-n}\big)$, per ogni x_0+h scelto. In particolare, la prima coppia ottenuta (corrispondente al valore minimo possibile di h) è il primo elemento di $\boldsymbol{\mathcal{B}}_n$ [che poi corrisponde al primo elemento $(\tilde{a}, \tilde{b})$ di $\boldsymbol{\mathcal{A}}_n$].

Osservazione 3. Si noti che il metodo di fattorizzazione di Fermat è più efficiente rispetto al metodo di fattorizzazione standard (cfr. **Cap. II.2**). Ciò dipende dal fatto che i due fattori $\tilde{a}$ e $\tilde{b}$ sono sensibilmente inferiori a $n_1 = \frac{n}{k_1}$ e portano quindi ad una semplificazione più rapida del problema.

Esempio 1. Fattorizzare $n = 375$ con il metodo di Fermat.

Si ha: $x_0 =$ minimo intero $\ge \sqrt{375} = 19,...$ e dunque $x_0 = 20$.

Si considerano gli interi compresi tra 20 e $\frac{376}{2} = 188$ e si cerca il primo $h \ge 0$ tale che $(20+h)^2 - 375$ è un quadrato.

Sia $h = 0$. $(20+0)^2 - 375 = 25 = 5^2$: è un quadrato. Dunque $(20,5)$ è il primo elemento di $\boldsymbol{\mathcal{B}}_{375}$. Ad esso corrisponde $(15,25) \in \boldsymbol{\mathcal{A}}_{375}$. Dunque $375 = 15 \cdot 25$.

Ora bisogna calcolare i primi elementi di $\boldsymbol{\mathcal{A}}_{15}$ ed $\boldsymbol{\mathcal{A}}_{25}$.

Consideriamo $\boldsymbol{\mathcal{A}}_{15}$. Risulta: $\sqrt{15} = 4,...$ e quindi $x_0 = 4$. Cerchiamo il primo $h \ge 0$ tale che $(4+h)^2 - 15$ è un quadrato. Per $h = 0$, $(4+0)^2 - 15 = 1 = 1^2$: è un quadrato. Allora $(4,1)$ è il primo elemento di $\boldsymbol{\mathcal{B}}_{15}$ e ad esso corrisponde $(3,5) \in \boldsymbol{\mathcal{A}}_{15}$ [infatti $15 = 3 \cdot 5$].

Consideriamo $\boldsymbol{\mathcal{A}}_{25}$. Risulta: $\sqrt{25} = 5$ e quindi $x_0 = 5$; inoltre $(5+0)^2 - 25 = 0 = 0^2$: è un quadrato. Allora il primo elemento di $\boldsymbol{\mathcal{B}}_{25}$ è $(5,0)$ e ad esso corrisponde $(5,5)$, primo elemento di $\boldsymbol{\mathcal{A}}_{25}$ [infatti $25 = 5 \cdot 5$].

Poiché $(3,5)$ e $(5,5)$ sono coppie di primi, il procedimento è terminato e si ha

$$375 = 15\cdot 25 = (3\cdot 5)\cdot(5\cdot 5) = 3\cdot 5\cdot 5\cdot 5.$$

Esempio 2. Fattorizzare $n = 85$ con il metodo di Fermat.

Si ha: $\sqrt{85} = 9,...$ e dunque $x_0 = 10$.

Si ha: $10^2 - 85 = 15$ (non quadrato); $11^2 - 85 = 36 = 6^2$ (quadrato). Allora $(11,6) \in \boldsymbol{\mathcal{B}}_{85}$ e quindi $(5,17) \in \boldsymbol{\mathcal{A}}_{85}$.

5, 17 sono primi e quindi il procedimento termina: $85 = 5\cdot 17$.

Esempio 3. Fattorizzare $n = 13485$ con il metodo di Fermat.

Si ha: $\sqrt{13485} = 116,...$ e dunque $x_0 = 117$.

Si ha: $117^2 - n$ non quadrato; $118^2 - n$ non quadrato; $119^2 - n = 26^2$ (quadrato). Allora $(119,26) \in \boldsymbol{\mathcal{B}}_n$ e quindi $(93,145) \in \boldsymbol{\mathcal{A}}_n$.

Si può verificare con il metodo di Fermat (o, ovviamente, direttamente) che $93 = 3\cdot 31$ e $145 = 5\cdot 29$. Si conclude che

$$n = 13485 = 93\cdot 145 = (3\cdot 31)\cdot(5\cdot 29) = 3\cdot 5\cdot 29\cdot 31.$$

Un altro algoritmo per la fattorizzazione di un naturale in primi è dovuto a N.A.Draim ($\sim$ 1950). Draim [capitano della marina statunitense] non ha mai pubblicato il suo algoritmo, che invece è stato divulgato da J.H.Davenport [cfr. *The Higher Arithmetic*, Cambridge Univ. Press (1982)].

Sia n un naturale dispari e ≥ 3. Si ponga $n_1 = m_1 = n$. L'algoritmo consiste nel creare due successioni di naturali $\{n_k\}$, $\{m_k\}$ così definite: denotati con q_k ed r_k rispettivamente il quoziente ed il resto della divisione euclidea di n_k per $2k+1$, cioè

$$(*) \qquad n_k = (2k+1)\, q_k + r_k\,, \ \forall\, k \geq 1,$$

si ponga, $\forall\, k \geq 2$:

$$m_k = m_{k-1} - 2q_{k-1}\,, \quad n_k = m_k + r_{k-1}\,.$$

Da tali definizioni segue facilmente che, $\forall\, k \geq 2$:

$$(**) \qquad n_k = k\,n - (2k+1) \sum_{t=1}^{k-1} q_t\,,$$

$$(*\,*\,*) \qquad m_k = n - 2 \sum_{t=1}^{k-1} q_t\,.$$

Da $(*)$, $(**)$ e dal fatto che $MCD(k, 2k+1) = 1$, segue subito che

$$r_k = 0 \iff 2k+1 \,\big|\, n.$$

Se quindi $r_k = 0$ e $r_1, ..., r_{k-1} > 0$, allora $2k+1$ è il minimo fattore (necessariamente primo) di n. In tal caso da $(**)$ segue che

$$k\,n = (2k+1) \sum_{t=1}^{k} q_t\,.$$

Tenuto conto di tale uguaglianza e dell'espressione di m_{k+1} [dedotta da $(*\,*\,*)$], si ottiene

$$m_{k+1} = n - 2 \sum_{t=1}^{k} q_t = n - 2\tfrac{kn}{2k+1} = \tfrac{n}{2k+1}\,.$$

Dunque n è prodotto dei due fattori $2k+1$, m_{k+1} (di cui il secondo non è necessariamente primo). Si applica ora l'algoritmo sopra esposto ad m_{k+1} e, dopo un numero finito di passi, si perverrà ad una completa fattorizzazione di n.

Tenuto conto del **Lemma 3.2** (cioè del fatto che ogni non primo $n \geq 4$ ammette un fattore $\leq [\sqrt{n}\,]$), le successioni $\{n_k\}$, $\{m_k\}$ andranno al più calcolate fino al massimo indice k tale che $2k+1 \leq [\sqrt{n}]$ ovvero fino al minimo indice k tale che $r_k = 0$, mentre $r_1, ..., r_{k-1} > 0$.

Esempio 4. Fattorizzare $n = 85$ con il metodo di Draim.

Risulta:

$$n_1 = 85 = 3\cdot 28 + 1, \quad q_1 = 28, \quad r_1 = 1.$$

Ne segue:

$$m_2 = 85 - 2q_1 = 29, \quad n_2 = m_2 + r_1 = 30.$$

Risulta:

$$n_2 = 30 = 5\cdot 6 + 0, \quad q_2 = 6, \quad r_2 = 0.$$

Essendo $r_2 = 0$, il fattore minimo di $n = 85$ è 5 e l'altro fattore è $m_3 = m_2 - 2q_2 = 17$ (anch'esso primo). Il procedimento quindi termina con $85 = 5\cdot 17$.

Esempio 5. Fattorizzare $n = 13485$ con il metodo di Draim.

Risulta:

$$n_1 = 13485 = 3\cdot 4495 + 0, \quad q_1 = 4495, \quad r_1 = 0$$

e si conclude che n è fattorizzato da 3, 4495.

Riapplichiamo il procedimento a $n_1 = 4495$ Risulta:

$$n_1 = 4495 = 3\cdot 1498 + 1, \quad q_1 = 1498, \quad r_1 = 1$$

e quindi

$$m_2 = 4495 - 2q_1 = 1499, \quad n_2 = m_2 + r_1 = 1500.$$

Risulta:

$$n_2 = 1500 = 5\cdot 300 + 0, \quad q_2 = 300, \quad r_2 = 0.$$

Allora $m_3 = m_2 - 2q_2 = 899$ e pertanto n è fattorizzato da 3, 5, 899.

Riapplichiamo ora il procedimento a $n_1 = 899$. In questo caso i calcoli si rivelano piuttosto laboriosi, ma sappiamo che le successioni $\{n_k\}$, $\{m_k\}$ andranno al più calcolate per $2k+1 \leq [\sqrt{899}\,] = 29$, cioè per $k \leq 14$. Si può verificare che:

$$\begin{aligned}
\{m_k\}_{k\geq 1} &= \{899, 301, 181, 129, 101, 83, 71, 61, 53, 49, 43, 41, 37, 35, 31\},\\
\{n_k\}_{k\geq 1} &= \{899, 303, 184, 131, 106, 90, 83, 69, 54, 65, 45, 63, 50, 58\},\\
\{r_k\}_{k\geq 1} &= \{2, 3, 2, 5, 7, 12, 8, 1, 16, 2, 22, 13, 23, 0\}.
\end{aligned}$$

Poiché r_{14} è il primo resto nullo, si può concludere che 899 è fattorizzato da $2\cdot 14+1 = 29$, $m_{15} = 31$ (primo). Pertanto $13485 = 3\cdot 5\cdot 29\cdot 31$.