Corso di Algebra I - esercizi e complementi n. 3

Problemi di divisione (da varie gare matematiche)

Le notazioni sono quelle in vigore nelle dispense. In particolare, $\mathbb{Z}$ è l'insieme dei numeri interi, $\mathbb{N}$ quello dei numeri naturali e $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$; gli elementi di $\mathbb{N}^*$ sono i numeri interi *positivi*. Per evitare confusione con le coppie ordinate, se $a, b \in \mathbb{Z}$ denotiamo $mcd(a, b)$ il loro massimo comun divisore positivo.

I due strumenti principali per la soluzione del primo gruppo di problemi sono la *Formula di Bezout* (Teorema 2.3 delle dispense, la sua dimostrazione e il corollario) e quello che possiamo chiamare il *Lemma di Euclide* (ovvero, la proprietà fondamentale dei numeri primi: Lemma 2.4 delle dispense):

1. **Formula di Bezout**: *siano a, b interi non entrambi nulli, allora $mcd(a, b)$ è il minimo $d \in \mathbb{N}^*$ per cui esistono $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha a + \beta b$; in particolare a, b sono coprimi se e solo se esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b 1$.*
2. **Lemma di Euclide**: *siano $a, b \in \mathbb{Z}$ e $d \geq 1$; se $d \mid ab$ e $mcd(d, a) = 1$ allora $d \mid b$; in particolare, se p è un numero primo e $p \mid ab$, allora $p \mid a$ o $p \mid b$.*

Il primo problema che propongo è tratto dalla prima edizione delle Olimpiadi Matematiche Internazionali (nel seguito abbreviato IMO, *International Mathematical Olympiad*) che si tenne in Romania nel 1959. Oggi, problemi così semplici (le soluzioni si trovano tutte alla fine) non sono presi in considerazione dagli organizzatori di nessuna gara matematica.

Problema 1 (IMO, Bucarest 1959). *Provare che per ogni $n \in \mathbb{N}^*$, la frazione*

$$\frac{21n + 4}{14n + 3}$$

è ridotta (cioè numeratore e denominatore sono numeri coprimi).

La formula di Bezout è la chiave anche per la soluzione del prossimo problema, che è semplice ma non banale.

Problema 2 (Putnam[1], 2000). *Si provi, che per ogni coppia di interi $n \geq m \geq 1$, l'espressione*

$$\frac{mcd(m, n)}{n} \binom{n}{m}$$

è un numero intero.

Il prossimo problema comincia a essere più impegnativo: la soluzione richiede tecnicamente poco più che la definizione di massimo comun divisore (in questo caso di un insieme infinito di interi positivi), ma poi occorre qualche piccola idea.

[1] La *William Lowell Putnam mathematical competition* è un gara matematica per studenti dei primi anni dell'Università che si disputa annualmente tra Canada e Stati Uniti dal 1938 (con l'interruzione negli anni della seconda guerra mondiale).

PROBLEMA 3 (Italia[2] 2014). *Per ogni intero positivo n, sia d_n il massimo comune divisore di tutti i numeri della forma $a^n + (a+1)^n + (a+2)^n$ al variare di $a \in \mathbb{N}^*$. Dimostrare che per ogni n, $d_n = 3^k$ per qualche $k \in \mathbb{N}$.*

Per risolvere il prossimo problema applicate in modo astuto il Lemma di Euclide, ed il fatto banale che se un numero divide due altri numeri, allora ne divide la somma (e la differenza).

PROBLEMA 4 (Iberoamericana[3], 2006). *Determinare tutte le coppie (a, b) di numeri interi positivi tali che $2a - 1$ e $2b + 1$ sono coprimi e $a + b$ divide $4ab + 1$.*

Un trucchetto spesso utile nell'affrontare problemi di divisione è l'osservazione che garantisce l'efficacia dell'algoritmo di Euclide (Esercizio 2.10 delle dispense), e che in sostanza discende da quanto detto sopra sulla somma o differenza di multipli di uno stesso numero.

3. **Euclide II**: *Siano a e b interi non nulli; allora, per ogni $q \in \mathbb{Z}$, $mcd(a, b) = mcd(b, a + qb)$.*

Il problema che segue si risolve utilizzando questo ad un livello molto essenziale, ma l'aspetto difficile è farsi la corretta idea di cosa sta succedendo (per avere un aiuto, potete andare alla soluzione e leggere solo la prima riga, dove trovate la risposta).

PROBLEMA 5 (Germania[4] 1996). *Una pietra si muove sui punti a coordinate intere del piano secondo le regole seguenti:*

(i) *Da ogni punto (a, b) la pietra può spostarsi in $(2a, b)$ oppure $(a, 2b)$.*
(ii) *Da ogni punto (a, b) la pietra può muovere in $(a-b, b)$ se $a > b$, oppure in $(a, b-a)$ se $a < b$.*

Si dica quali punti (x, y) può raggiungere la pietra partendo dal punto $(1, 1)$.

Un altro aspetto da tener sempre presente è l'eventualità di usare le diseguaglianze: perché se a, b sono interi positivi e $a \mid b$ allora anche $a \leq b$. Vediamo prima la soluzione di un caso un poco laborioso, e poi un problema per voi (che non sarà proprio facile).

PROBLEMA 6 (IMO, Mosca 1992). *Si determinino tutte le terne di numeri interi a, b, c con $1 < a < b < c$ tali che $(a-1)(b-1)(c-1)$ divide $abc - 1$.*

SOLUZIONE. Siano a, b, c come nelle ipotesi e supponiamo esista un $x \in \mathbb{N}^*$ tale che

$$(*) \qquad x \cdot (a-1)(b-1)(c-1) = abc - 1.$$

Chiaramente $x \geq 2$. Osserviamo poi che se uno tra i numeri a, b, c è dispari, allora il membro di sinistra in $(*)$ è pari, dunque abc deve essere dispari e quindi a, b, c sono tutti dispari. Pertanto, a, b, c sono tutti pari oppure tutti dispari.

---

[2] Le *Olimpiadi di Matematica* italiane si svolgono annualmente dal 1983; la gara finale (da cui sono i problemi) si tiene a Cesenatico.

[3] *Olimpiada Iberoamericana de Matematicas*, si disputa dal 1985.

[4] Quando compare solo l'indicazione di una nazione, si intende che il problema è stato proposto nelle olimpiadi matematiche nazionali di quella.

Inoltre, tenendo conto che la funzione $n \to \frac{n}{n-1}$ è decrescente, da $(*)$ segue

$$(**) \qquad x < \frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1} \leq \frac{a}{a-1} \cdot \frac{a+2}{a+1} \cdot \frac{a+4}{a+3} \leq \frac{2}{1} \cdot \frac{4}{3} \cdot \frac{6}{5} = \frac{16}{5},$$

quindi $x \in \{2, 3\}$.

Siano a, b, c pari. Allora il termine di destra in $(*)$ è dispari e dunque anche x è dispari; quindi, $x = 3$. Se $a \geq 4$, allora, dalla $(**)$,

$$x < \frac{4}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} = \frac{64}{35} < 2$$

che è assurdo. Dunque $a = 2$, $x = 3$; sostituendo nella $(*)$ si ottiene $3(b-1)(c-1) = 2bc - 1$, da cui

$$bc + 4 = 3b + 3c \leq 3(c-2) + 3c = 6c - 6,$$

e, poiché $b > 2$ è pari, $b = 4$. Sostituendo nella $(*)$, si ha $9(c-1) = 8c - 1$, da cui $c = 8$.
Siano a, b, c dispari. Dalla $(**)$ si ricava

$$x < \frac{3}{2} \cdot \frac{5}{4} \cdot \frac{7}{6} = \frac{35}{16} < 3$$

e quindi $x = 2$. Ragionando poi come nel caso pari, se $a \geq 5$, sempre dalla $(**)$ si ha

$$x < \frac{5}{4} \cdot \frac{7}{6} \cdot \frac{9}{8} = \frac{105}{64} < 2$$

che è assurdo. Dunque $a = 3$, $x = 2$; sostituendo nella $(*)$ si ottiene $4(b-1)(c-1) = 3bc - 1$, da cui

$$bc + 5 = 4b + 4c \leq 4(c-2) + 4c = 8c - 8.$$

Dunque $b = 5, 7$. Sostituendo in $(*)$ si trova che il solo caso possibile e $b = 5$, che dà $c = 15$.

In conclusione, le soluzioni sono $(a, b, c) = (2, 4, 8), (3, 5, 15)$. ∎

Problema 7 (IMO, Taiwan 1998). *Determinare tutte le coppie (a, b) di interi positivi tali che*

$$ab^2 + b + 7 \mid a^2b + a + b.$$

E ancora un altro problema con una diseguaglianza, questa volta nell'enunciato.

Problema 8 (San Pietroburgo[5], 2008). *Siano a, b e c interi positivi distinti; si provi che*

$$mcd(ab + 1, ac + 1, bc + 1) < \frac{a + b + c}{3}.$$

Infine, segnalo un'altra ben nota identità che interviene molto spesso nei calcoli legati a questo tipo di problemi:

4. **Serie geometrica.** *Siano a, b, numeri reali e n un intero positivo; allora*

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1});$$

in particolare, $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1)$.

Il prossimo problema è un esercizio standard, ma anche un'osservazione molto utile.

[5]Le *Olimpiadi Matematiche di San Pietroburgo* si svolgono annualmente dal 1934 (naturalmente, fino al 1991 si sono chiamate Olimpiadi Matematiche di Leningrado).

PROBLEMA 9. *Siano a, m, n interi positivi, con $a \geq 2$. Si provi che*

$$mcd(a^m - 1, a^n - 1) = a^{mcd(m,n)} - 1.$$

A partire da questo, non dovrebbe essere troppo difficile risolvere il prossimo quesito.

PROBLEMA 10 (Baltic Way[6], 2014). *Siano m, n interi positivi coprimi. Determinare tutti i possibili valori di*

$$mcd(2^m - 2^n, 2^{m^2+mn+n^2} - 1).$$

* * *

Tre problemi tosti. Il primo dei problemi tosti è piuttosto impegnativo e anche laborioso; non richiede alcun strumento tecnico particolarmente sofisticato (nulla che non abbiamo già utilizzato in queste pagine), ma necessita di una certa padronanza nella manipolazione algebrica, l'intuizione della risposta corretta, e la capacità di condurre in modo efficace un argomento per induzione.

PROBLEMA 11 (Giappone 1996). *Siano n, m interi positivi coprimi. Si determini*

$$(5^m + 7^m, 5^n + 7^n).$$

[Un suggerimento per iniziare è la seguente identità elementare

$$5^n + 7^n = (5^m + 7^m)(5^{n-m} + 7^{n-m}) - (7^m 5^{n-m} + 5^m 7^{n-m}).\ ]$$

Le soluzioni degli ultimi due problemi sono, se condotte nel modo migliore, molto più brevi; tuttavia si differenziano abbastanza negli argomenti (che rimangono pur sempre elementari dal punto di vista tecnico) da quelle dei problemi precedenti, perché richiedono dei ragionamenti ad hoc non proprio ovvi. Il primo di questi problema riguarda la nozione di massimo comun divisore, ed è di natura piuttosto astratta; per la soluzione, suggerirei di fare qualche esperimento per capire cosa sta succedendo.

PROBLEMA 12 (Putnam, 1999). *Sia S un insieme finito di numeri interi strettamente maggiori di 1. Si assuma che per ogni intero positivo n esista almeno un $s \in S$ tale che o $mcd(s, n) = 1$ oppure $mcd(s, n) = s$. Si provi che esistono $s, t \in S$ tali che $mcd(s, t)$ è un numero primo.*

Infine, l'ultimo esercizio riguarda un argomento fatto a lezione ma non ancora toccato in queste pagine supplementari, ovvero la fattorizzazione in primi.

PROBLEMA 13 (San Pietroburgo, 1987). *Rappresentare il numero $n = 989 \cdot 1001 \cdot 1007 + 320$ come un prodotto di primi.*

Naturalmente, dovete cercare di rispondere a quest'ultimo quesito senza ricorrere ad ausili di calcolo meccanico (che non sarebbe bello); avviso però che la soluzione (o, almeno, quella che ho trovato io) richiede di passare per un polinomio ed il Teorema di Ruffini, argomenti che nel corso si studieranno più avanti, ma che forse qualcuno conosce già abbastanza da poterli applicare (il polinimio è di terzo grado): ho deciso di inserire ugualmente questo problema perché mi sembra molto bellino.

[6] I giochi di matematica denominati *Baltic Way* si svolgono dal 1990 ed hanno la caratteristica di essere una competizione autenticamente tra squadre.

SOLUZIONI

PROBLEMA 1. Per ogni $n \in \mathbb{N}^*$ si ha

$$(-2) \cdot (21n+4) + 3 \cdot (14n+3) = -42n - 8 + 42n + 9 = 1,$$

e quindi $mcd(21n+4, 14n+3) = 1$. ∎

PROBLEMA 2. Sia $d = \mathrm{m}cd(m,n)$. Per la formula di Bezout, esistono due numeri interi a, b tali che $d = an + bm$. Dunque

$$\frac{d}{n}\binom{n}{m} = \frac{an+bm}{n}\binom{n}{m} = a \cdot \binom{n}{m} + b \cdot \frac{m}{n}\binom{n}{m} = a \cdot \binom{n}{m} + b \cdot \binom{n-1}{m-1},$$

che è un numero intero. ∎

PROBLEMA 3. Sia $n \in \mathbb{N}^*$ e sia d_n il massimo comun divisore di tutti i numeri del tipo

$$a^n + (a+1)^n + (a+2)^n$$

con $a \geq 1$. Sostituendo d_n e $d_n + 1$ per a si trova che d_n divide sia $d_n^n + (d_n+1)^n + (d_n+2)^n$ che $(d_n+1)^n + (d_n+2)^n + (d_n+3)^n$, dunque divide la loro differenza $(d_n+3)^n - d_n^3$, e quindi

$$d_n | (d_n+3)^n.$$

Se $d_n = 1 = 3^0$ siamo a posto. Altrimenti, sia p un divisore primo di d_n; allora p divide $(d_n+3)^n$ e quindi, essendo un primo, p divide $d_n + 3$. Dunque, p divide $d_n + 3 - d_n$ e quindi $p = 3$, così provando che d_n è una potenza di 3. ∎

PROBLEMA 4. Sia (a,b) una delle coppie cercate. Allora

$$(*) \qquad a+b \mid 4a(a+b) - (4ab+1) = 4a^2 - 1 = (2a+1)(2a-1),$$

e similmente

$$(**) \qquad a+b \mid 4b(a+b) - (4ab+1) = 4b^2 - 1 = (2b+1)(2b-1).$$

Sia $d = mcd(a+b, 2b+1)$. Poiché d e $2a-1$ sono coprimi per ipotesi, da $(*)$ e il Lemma di Euclide segue che d divide $2a+1$, quindi d divide $(2b+1) + (2a+1) - 2(a+b) = 2$, e pertanto, poiché $2b+1$ è dispari, $d = 1$. Dunque, $a+b$ e $2b+1$ sono coprimi e da $(**)$ (e ancora i Lemma di Euclide) si deduce che $a+b$ divide $2b-1$. In particolare, $a+b \leq 2b-1$ e pertanto $a+1 \leq b$. Similmente si dimostra che $a+b$ divide $2a+1$, quindi $a+b \leq 2a+1$ e dunque $b \leq a+1$.
In conclusione $b = a+1$. La verifica che tutte le coppie del tipo $(a, a+1)$ con $a \geq 1$ soddisfano la condizione assegnata è immediata. ∎

PROBLEMA 5. La risposta è che (x,y) è raggiungibile da $(1,1)$ se e soltanto se $mcd(x,y)$ è una potenza di 2.

Vediamo la dimostrazione. Siano a, b interi positivi e $d = mcd(a,b)$; allora $mcd(a-b, b) = mcd(a, b-a) = d$, mentre $mcd(2a, b) = 2^\epsilon d$ e $mcd(2a, b) = 2^\mu d$, dove $\epsilon, \mu \in \{0, 1\}$.

Quindi, nel gioco descritto dal Problema, ogni mossa lecita della pietra sposta questa da un punto (a, b) a coordinate intere in un punto il cui massimo comun divisore delle coordinate è uguale oppure il doppio di $mcd(a, b)$. Da ciò segue immediatamente che se il punto (x, y) si può raggiungere da $(1, 1)$ allora $mcd(x, y) = 2^t$ per qualche $t \geq 0$.
Viceversa, proviamo che ogni punto (x, y), con $x, y \in \mathbb{N}^*$ e tale che $mcd(x, y) = 2^t$ per qualche $t \in \mathbb{N}$, è raggiungibile da $(1, 1)$ in un numero finito di mosse. Per induzione su $x+y$. Se $x+y = 2$, $(x, y) = (1, 1)$ e non c'è altro da aggiungere. Sia $x + y > 2$. Se $x = 2a$ è pari allora $mcd(a, y)$ è una potenza di due, (a, y) è raggiungibile da $(1, 1)$ per ipotesi induttiva e quindi (x, y) è raggiungibile dato che ci si arriva da (a, y) con una mossa di tipo (i); lo stesso argomento si applica se y è pari. Rimane il caso in cui sia x che y sono dispari, quindi $mcd(x, y) = 1$ e in particolare $x \neq y$; sia $x > y$, allora

$$mcd\Big(\frac{x+y}{2}, y\Big) = 1 \quad \text{e} \quad \frac{x+y}{2} + y < x + y,$$

dunque $(\frac{x+y}{2}, y)$ è raggiungibile da $(1, 1)$ per ipotesi induttiva, e quindi (x, y) è raggiungibile:

$$(1, 1) \to \Big(\frac{x+y}{2}, y\Big) \xrightarrow{\text{(i)}} (x + y, y) \xrightarrow{\text{(ii)}} (x, y).$$

La stessa cosa, nella seconda componente, si fa se $y > x$.
Quindi (x, y) è raggiungibile da $(1, 1)$ se e soltanto se $mcd(x, y)$ è una potenza di 2. ∎

Problema 7. Se $ab^2 + b + 7$ divide $a^2b + a + b$ allora divide

$$b(a^2b + a + b) - a(ab^2 + b + 7) = b^2 - 7a. \tag{$*$}$$

Se $b^2 = 7a$ si ha $a = 7x^2$, $b = 7x$ (con $x \in \mathbb{N}^*$) che sono delle soluzioni.
Se $b^2 - 7a > 0$, allora $0 < ab^2 + b + 7 \leq b^2 - 7a \leq b^2$ che è una contraddizione.
Sia $b^2 - 7a < 0$, allora $ab^2 < ab^2 + b + 7 \leq 7a - b^2 < 7a$, da cui $b^2 < 7$ e quindi $b = 1, 2$.
Se $b = 2$, sostituendo in $(*)$ si deduce che $4a + 9$ divide $7a - 4$, il che si vede subito non sussiste per $a \in \mathbb{N}^*$. Rimane il caso $b = 1$. Allora da $(*)$ si deduce che $a + 8$ divide $7a - 1$; quindi $a + 8$ divide $7(a + 8) - (7a - 1) = 57 = 19 \cdot 3$. Poiché $a \geq 1$ si hanno le due possibilità $a + 8 = 19$ e $a + 8 = 57$, che danno, rispettivamente, $a = 11$ e $a = 19$.
In conclusione, le coppie (a, b) cercate sono $(11, 1), (49, 1)$ e $(7x^2, 7x)$ con $x \in \mathbb{N}^*$. ∎

Problema 8. Siano a, b, c interi positivi con $a < b < c$ e sia $d = mcd(ab + 1, ac + 1, bc + 1)$. Allora,

$$d \mid (ab + 1)c - a(bc + 1) = c - a,$$

e similmente si prova $d|b-a$. Quindi esistono due numeri interi m, n con $1 \leq m < n$ (perché $a < b < c$, si osservi anche $m + n \geq 3$) tali che

$$b = a + md$$
$$c = a + nd.$$

Dunque

$$\frac{a+b+c}{3} = \frac{a + (a + md) + (a + nd)}{3} = \frac{3a + (m + n)d}{3} \geq \frac{3a + 3d}{3} = a + d > d,$$

come si voleva. ∎

PROBLEMA 9. Siano a, m, n come nelle ipotesi; scriviamo $D = mcd(a^m - 1, a^n - 1)$ e $d = mcd(m, n)$. Procediamo per induzione su $m + n$ (che è almeno 2). Se $m + n = 2$, allora $d = m = n = 1 = d$ e l'asserto è ovvio. Sia quindi $m + n > 2$, e assumiamo, come certo possiamo, $n \geq m$. Se $m = n$, allora $d = m = n$ e ancora l'asserto è banale. Si quindi $n > m$; allora per Euclide II, $d = (m, n - m)$. Ora, a^m e $a^m - 1$ sono coprimi, quindi, per il Lemma di Euclide,

$$D = mcd(a^m(a^{n-m} - 1), a^m - 1) = mcd(a^{n-m} - 1, a^m - 1),$$

da cui si conclude, per quanto osservato sopra e l'ipotesi induttiva, $D = a^d - 1$. (Anche verificare direttamente che D soddisfa la definizione di massimo comun divisore, non è difficile.) ∎

PROBLEMA 10. Siano m, n interi positivi coprimi, e poniamo $D = mcd(2^m - 2^n, 2^{m^2+mn+n^2} - 1)$. Poiché n, m sono coprimi, il solo caso in cui sono uguali è quando sono entrambi 1, e in quel caso

$$D = mcd(0, 2^3 - 1) = 7.$$

Sia ora $m \neq n$; dato che il segno dei termini non influisce sul massimo comun divisore, possiamo supporre $m > n$. Allora, poiché il termine $2^{m^2+mn+n^2} - 1$ è dispari e per il Problema precedente,

$$(*) \qquad D = mcd(2^n(2^{m-n} - 1), 2^{m^2+mn+n^2} - 1) = mcd(2^{m-1} - 1, 2^{m^2+mn+n^2} - 1) = 2^d - 1,$$

dove $d = mcd(m - n, m^2 + mn + n^2)$. Ora, poiché $mcd(m, n) = 1$, si ha $mcd(m - n, mn) = 1$; quindi, applicando Euclide II,

$$d = mcd(m - n, (m - n)^2 + 3mn) = mcd(m - n, 3mn) = mcd(m - n, 3) \in \{1, 3\},$$

che sostituito in $(*)$, dà $D \in \{1, 7\}$ (entrambi i casi si verificano, ad esempio

$$mcd(2^4 - 2, 2^{4^2+4+1} - 1) = mcd(14, 2^{21} - 1) = 7\ ).$$

La risposta è quindi che D può essere 1 oppure 7. ∎

PROBLEMA 11. Possiamo porre $1 \leq m < n$. Come detto, il gioco si sviluppa a partire dall'identità

$$5^n + 7^n = (5^m + 7^m)(5^{n-m} + 7^{n-m}) - (7^m 5^{n-m} + 5^m 7^{n-m});$$

dalla quale segue, per Euclide II,

$$(\dagger) \qquad (5^m + 7^m, 5^n + 7^n) = (5^m + 7^m, 7^m 5^{n-m} + 5^m 7^{n-m})$$

(si osservi che questo non richiede la coprimità di m e n).
Sia $n \geq 2m$; allora $n - m \geq m$ e $7^m 5^{n-m} + 5^m 7^{n-m} = 5^m 7^m (5^{n-2m} + 7^{n-2m})$; poiché né 5 né 7 dividono $5^m + 7^m$, dalla $(\dagger)$ segue

$$(*) \qquad (5^m + 7^m, 5^n + 7^n) = (5^m + 7^m, 5^{n-2m} + 7^{n-2m}).$$

Se invece $n < 2m$, allora $n - m < m$ e, ragionando in modo analogo a sopra, si ottiene

$$(**) \qquad (5^m + 7^m, 5^n + 7^n) = (5^m + 7^m, 5^{2m-n} + 7^{2m-n}).$$

Queste due identità suggeriscono chiaramente la possibilità di ragionare per induzione, ed osservando che un aspetto che si mantiene nella relazione tra i due diversi esponenti nelle riduzioni $(*)$ e $(**)$ è la

parità della loro somma ($n+m$ inizialmente), si capisce sarà opportuno distinguere i due casi $n+m$ pari e $n+m$ dispari.
Un punto essenziale è poter propriamente operare un passo induttivo; cioè che passando dalla coppia m, n alla coppia $m, 2n-m$ oppure $m, 2m-n$, secondo i casi, la somma dei termini effettivamente diminuisca. Nel primo caso si ha sempre $m+(n-2m) = n-m < m+m$ e non dà problemi, nel secondo caso $m+(2m-n)$ è uguale a $m+n$ se $m = n$. Dobbiamo quindi escludere che in qualche passo della riduzione induttiva capiti che i due esponenti in ballo siano uguali (se non al termine, quando sono 1). Da qui la richiesta che n, m siano coprimi; questo infatti assicura che anche le coppie $m, n-2m$ e $m, 2m-n$ sono coprime, e così via. Supponiamo quindi che m, n siano coprimi
Sia $n+m$ pari (dunque, in quanto coprimi, n e m sono entrambi dispari); poiché il caso più piccolo si ha per $n = 1 = m$ e in questo caso il MCD è $5+7 = 12$, formuliamo un primo enunciato:

(i) *se $n+m$ è pari, allora* $(5^m+7^m, 5^n+7^n) = 12$.

La dimostrazione è per induzione su $n+m$; il caso iniziale essendo stato osservato prima. Siano quindi n, m dispari con $n+m \geq 4$. Se $n > 2m$, applicando $(*)$ e l'ipotesi induttiva (dato che $n-2m$ è dispari e $m+(n-2m) < n+m$),

$$(5^m+7^m, 5^n+7^n) = (5^m+7^m, 5^{n-2m}+7^{n-2m}) = 12.$$

Se $n < 2m$, similmente si applica $(**)$ e l'ipotesi induttiva, ottenendo

$$(5^m+7^m, 5^n+7^n) = (5^m+7^m, 5^{2m-n}+7^{2m-n}) = 12.$$

Veniamo al caso $n+m$ dispari, il cui minimo si ha per $m = 1, n = 2$, per il quale si ha $(5+7, 5^2+7^2) = (12, 74) = 2$. In questo caso proviamo allora

(ii) *se $n+m$ è dispari, allora* $(5^m+7^m, 5^n+7^n) = 2$.

La dimostrazione è però del tutto analoga a quella del caso precedente e non la ripetiamo. ∎

Problema 12. Poiché l'insieme S è finito, esistono interi positivi che non sono coprimi con alcun elemento di S (ad esempio, il minimo comune multiplo di tutti gli elementi di S): sia n il minimo di tali numeri. Per ipotesi, esiste $s \in S$ tale che $s \mid n$. Se s è un numero primo abbiamo finito prendendo $t = s$. Altrimenti, sia p un divisore primo di s; posto $n' = n/p$, abbiamo $1 < n' < n$, e dunque per la scelta di n esiste $t \in S$ tale che $mcd(t, n') = 1$. Da ciò segue $mcd(t, n) = p$, in particolare $p \mid t$ e dunque $p \mid mcd(s, t)$. D'altra parte, $s \mid n$ e quindi $mcd(s, t) \mid mcd(n, t) = p$. Dunque, $mcd(s, t) = p$. ∎

Problema 13. Poniamo $a = 1001$; allora $n = (a-12) \cdot a \cdot (a+6) + 320$, da cui

$$n = a^3 - 6a^2 - 72a + 320.$$

Trattiamo il termine di destra come un polinomio a coefficienti interi nell'indeterminata a; esaminando i divisori del termine noto, si scopre che 4 ne è una radice, e che quindi, per il Teorema di Ruffini, il polinomio è diviso da $a-4$. Svolgendo la divisione si trova

$$\begin{aligned} n &= (a-4)(a^2-2a-80) = (a-4)((a-1)^2-81) = (a-4)((a-1)^2-9^2) = \\ &= (a-10)(a-4)(a+8) = 991 \cdot 997 \cdot 1009, \end{aligned}$$

che è la fattorizzazione di n in prodotto di primi.