Divisibilità e aritmetica modulare

Davide Borra

Indice

v. 2.0

davide.borra@studenti.unitn.it - davideborra.github.io

Sommario

Obiettivo di queste lezioni sarà fornire qualche strumento dell'aritmetica modulare e dell'algebra per ricolvere problemi delle Olimpiadi di Matematica. Inoltre si cercherà, ove possibile, di dimostrare quanto si afferma, in modo da presentare anche alcuni processi utili nello svolgimento di esercizi dimostrativi. Per la maggior parte dei risultati, faccio riferimento alle note del prof. W.A. De Graaf [Gra], disponibili gratuitamente sul suo sito web.

1 Principio di induzione e principio del buon ordinamento

Prima di iniziare a parlare di algebra, dobbiamo introdurre uno strumento di fondamentale importanza nelle dimostrazioni. Il perchè questo principio funzioni è abbastanza intuivivo: immaginiamo di dover costruire una scala un gradino alla volta, allora ci basta trovare un modo per mettere il primo gradino e poi, preso un qualsiasi gradino di aggiungerci il successivo. In questo modo, avendo costruito il primo gradino, possiamo costruire tutti gli altri.

Teorema 1.1 (Principio di induzione)**.** *Sia $\mathcal{P}(n)$ una proprietà che dipende da un intero n. Se valgono le seguenti due condizioni:*

i) $\mathcal{P}(n_0)$ *è vera;*

ii) se $\mathcal{P}(n)$ *è vera, allora* $\mathcal{P}(n+1)$ *è vera;*

allora $\mathcal{P}(n)$ *è vera per ogni* $n \in \mathbb{N}_{\geq n_0}$.

Vediamo ora un esempio dell'applicazione del principio di induzione ad un caso semplice

Esempio 1.1.

Dimostrare che $1+2+3+...+n = \frac{n(n+1)}{2}$ procedendo per induzione su n.

Chiamiamo $\mathcal{P}(n) = \text{«}\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\text{»}$ e sia $n_0 = 1$. Allora:

i) $P(n_0)$ è vera: $\sum_{i=1}^{1} i = \frac{1(1+1)}{2} = 1$ è banalmente vera.

ii) Se $P(n)$ è vera, allora $P(n+1)$ è vera: assumiamo che $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ e vogliamo dimostrare che $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$.

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$$

Per induzione, segue quindi la tesi. □

Un altro principio intuitivo ma non scontato e che ci servirà nelle dimostrazioni che vedremo è il seguente:

Teorema 1.2 (Principio del buon ordinamento)**.** *Ogni sottoinsieme non vuoto di* $\mathbb{N}$ *ammette minimo.*

Si può provare che i due enunciati sono equivalenti, ovvero che è sufficiente la veridicità di uno qualsiasi dei due per provare l'altro. Per maggiori dettagli riguardo insiemi ordinati, induzione e buon ordinamento rimando a [Hal74].

2 I numeri interi

Rapidamente, ricordiamo alcune proprietà dell'insieme dei numeri interi $\mathbb{Z}$:

DEF 2.1 (Numeri interi)**.** L'insieme dei numeri interi è l'insieme $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ che comprende i numeri naturali e loro opposti. Esso ha due operazioni, che rispettivamente godono delle seguenti proprietà:

$+$ Somma

- $[A]$ Associativa: $(a+b)+c = a+(b+c)$
- $[N]$ Neutro: $a+0 = 0+a = a$
- $[I]$ Inverso: $\forall a \in \mathbb{Z} \exists -a \in \mathbb{Z}$ tale che $a+(-a) = (-a)+a = 0$
- $[C]$ Commutativa: $a+b = b+a$

· Prodotto

[A] Associativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

[N] Neutro: $a \cdot 1 = 1 \cdot a = a$

[C] Commutativa: $a \cdot b = b \cdot a$

E le quali distribuiscono:

[D] $a \cdot (b + c) = a \cdot b + a \cdot c$

Si dice quindi che $\mathbb{Z}$ è un anello commutativo con unità.

2.1 Divisibilità

DEF 2.2 (Divisibilità)**.** Siano $a, b \in \mathbb{Z}$, allora si dice che a divide b (e si indica $a|b$) se $\exists c \in \mathbb{Z}$ tale che

$$b = a \cdot c.$$

Osservazione 2.3.

i) $\forall a, a|0$;

ii) $0|a \implies a = 0$;

iii) $a|b$ e $b|a \implies a = \pm b$;

Lemma 2.4 (Divisione con resto)**.** *Siano $a, b \in \mathbb{Z}$, $b \neq 0$, allora $\exists! q, r \in \mathbb{Z}$ tali che*

$$a = bq + r \quad e \quad 0 \leq r < |b|.$$

Dimostrazione.

- **Esistenza** Sia $M = \{a - qb \,|\, q \in \mathbb{Z}\} \cap \mathbb{N} \subset \mathbb{N}$. Allora $M \neq \varnothing$, per cui per il principio del buon ordinamento M ammette minimo r. Ora, se $r \geq |b|$, anche $r - |b| \in M$, per cui esso sarebbe il minimo, ma non può essere per scelta di r, quindi $r < |b|$. Inoltre, siccome $r \in M$, esiste un q tale che $r = a - qb$.
- **Unicità** Supponiamo esistano due q e due r distinti che verifichino il lemma, ovvero

  $$a = q_1 b + r_1 = q_2 b + r_2 \qquad \text{con } 0 \leq r_1, r_2 < |b|$$

  Allora $(q_1 - q_3)b = r_2 - r_1$, da cui $b|r_2 - r_1$. Ma $|r_2 - r_1| < |b|$, per cui $r_2 - r_1 = 0$, da cui $r_1 = r_2$ e $q_1 = q_2$.

QED

2.2 Massimo comun divisore e minimo comune multiplo

2.2.1 Massimo comun divisore

Daremo una definizione inusiale di MCD che è quasi equivalente a quella classica, me che è molto più comoda per le dimostrazioni. Dimostreremo che in questo modo il MCD risulterà unico a meno del segno.

DEF 2.5 (Massimo comun divisore)**.** Siano $a, b \in \mathbb{Z}$. Si dice massimo comun divisore di a e b un numero $d \in \mathbb{Z}$ tale che:

i) $d|a$ e $d|b$;

ii) se $c|a$ e $c|b$, allora $c|d$.

In particolare se $d = 1$, a e b si dicono coprimi.

Prima di tutto dimostriamo che un tale d esiste sempre. Per farlo dimostreremo una proprietà leggermente più forte perché alcune sue implicazioni ci torneranno utili più avanti.

Teorema 2.6 (Esistenza del MCD - Bézout)**.** *Siano $a, b \in \mathbb{Z}$. Allora essi hanno un massimo comun divisore d ed esistono $s, t \in \mathbb{Z}$ tali che $d = as + bt$. Inoltre d è unico a meno del segno.*

Dimostrazione. Se $a = b = 0$, non c'è niente da dimostrare. Si ha $d = 0$ e s, t qualsiasi. Altrimenti possiamo definire un insieme

$$I = \{xa + yb \,|\, x, y \in \mathbb{Z}\}$$

osserviamo che $0 \in I$ (basta porre $x = y = 0$) e che

$$\alpha, \beta \in I \implies \alpha + \beta \in I$$

$$\alpha \in I, \lambda \in \mathbb{Z} \implies \lambda\alpha \in I$$

(un insieme con queste proprietà si dice ideale di $\mathbb{Z}$) Ora, per il principio del buon ordinamento l'insieme $I \cap \mathbb{N}_{>0}$ ammette minimo (infatti $I \cap \mathbb{N}_{>0} \ni |a|, |b|$). Chiamiamo questo valore d. Siccome $d \in I$ esistono s, t tali che $d = sa + tb$. Ora dimostriamo che esso è effettivamente il MCD di a e b.

i) $d|a$ e $d|b$
dalla divisione con resto, segue che $\exists! q, r \ : \ a = qd + r$ con $0 \leq r < d$

$$\left.\begin{array}{rcl} d \in I & \implies & qd \in I \\ a \in I & \implies & a - qd \in I \end{array}\right\} \implies r \in I$$

Ma siccome $0 \leq r < d$, r non può essere che 0, da cui $d|a$. Analogamente si dimostra che $d|b$.

ii) Sia $c \in \mathbb{Z}$ tale che $c|a$ e $c|b$, ovvero tale che esistono a', b' tali che $a = ca'$ e $b = cb'$. Ora

$$d = sa + tb = s(ca') + t(cb') = c(sa' + tb') \quad \implies \quad c|d$$

In conclusione dimostriamo che d è unico a meno del segno: siano d, d' due MCD di a e b. Allora $d|d'$ e $d'|d$, da cui $d = \pm d'$. QED

2.2.2 Algoritmo di Euclide

Lemma 2.7 (Euclide)**.** *Siano $a, b \in \mathbb{Z}$ tali che $a = qb + r$. Allora d è un massimo comun divisore di a e b se e solo se è un massimo comun divisore di b e r.*

Per dimostrare la doppia implicazione proviamo separatamente le due direzioni.

Dimostrazione.

- Se d è un MCD di a e b, allora è un MCD di b e r.
  - *i)* Allora per definizione $d|a$ e $d|b$, equivalentemente $a = da'$ e $b = db'$ per qualche $a', b' \in \mathbb{Z}$. Ma allora $r = a - qb = d(a' - qb')$, da cui $d|r$.
  - *ii)* Sia $c \in \mathbb{Z}$ tale che $c|b$ e $c|r$. Allora $b = c\hat{b}$ e $r = c\hat{r}$ per qualche $\hat{b}, \hat{r} \in \mathbb{Z}$. Ma allora $a = qb + r = qc\hat{b} + c\hat{r} = c(q\hat{b} + \hat{r})$, da cui $c|a$. Siccome $c \mid a$ e $c \mid b$, allora anche $c \mid d$.
- Se d è un MCD di b e r, allora è un MCD di a e b.
  - *i)* Allora per definizione $d|b$ e $d|r$, equivalentemente $b = db'$ e $r = dr'$ per qualche $b', r' \in \mathbb{Z}$. Ma allora $a = qb + r = d(qb' + r')$, da cui $d|a$.
  - *ii)* Sia $c \in \mathbb{Z}$ tale che $c|a$ e $c|b$. Allora $a = c\hat{a}$ e $b = c\hat{b}$ per qualche $\hat{a}, \hat{b} \in \mathbb{Z}$. Ma allora $r = a - qb = c\hat{a} - qc\hat{b} = c(\hat{a} - q\hat{b})$, da cui $c|r$. Siccome $c \mid b$ e $c \mid r$, allora anche $c \mid d$.

QED

Algoritmo di Euclide Siano $a, b \in \mathbb{Z}$, $a > b > 0$. Allora calcoliamo il resto r_0 della divisione tra a e b. Per il lemma precedente, $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_0)$, per cui possiamo sostituire a con b e b con r_0. Iterando questo procedimento otteniamo una successione di resti $r_0, r_1, \ldots, r_n$ tali che $r_{n+1} = 0$. Allora r_n è il MCD di a e b.

Esiste anche una variante, presentata nell'esempio seguente, che permette di calcolare anche s, t tali che $d = as + bt$.

Esempio 2.1.

Calcolare il massimo comun divisore d di 665 e 273 e due interi s, t tali che $665s + 273t = d$

$$\begin{array}{rcl} 665 & = & 1 \cdot 665 \ + \ 0 \cdot 273 \\ 273 & = & 0 \cdot 665 \ + \ 1 \cdot 273 \end{array}$$

Ora facciamo la divisione con resto tra 665 e 273:

$$\begin{array}{l} 665 : 273 = 2 \\ 119 \end{array}$$

per cui abbiamo che $665 = 2 \cdot 273 + 119$, quindi

$$119 \quad = \quad 1 \cdot 665 \quad + \quad (-2) \cdot 273$$

Ora facciamo la divisione con resto tra 273 e 119:

$$\begin{array}{l} 273 : 119 = 2 \\ 35 \end{array}$$

per cui abbiamo che $273 = 2 \cdot 119 + 35$, quindi

$$35 \quad = \quad (-2) \cdot 665 \quad + \quad 5 \cdot 273$$

Ora facciamo la divisione con resto tra 119 e 35:

$$\begin{array}{r} 119 : 35 = 3 \\ 14 \end{array}$$

per cui abbiamo che $119 = 3 \cdot 35 + 14$, quindi

$$14 \quad = \quad 7 \cdot 665 \quad + \quad (-17) \cdot 273$$

Ora facciamo la divisione con resto tra 35 e 14:

$$\begin{array}{r} 35 : 14 = 2 \\ 7 \end{array}$$

per cui abbiamo che $35 = 2 \cdot 14 + 7$, quindi

$$7 \quad = \quad (-16) \cdot 665 \quad + \quad 39 \cdot 273$$

Ora facciamo la divisione con resto tra 14 e 7:

$$\begin{array}{r} 14 : 7 = 2. \\ 0 \end{array}$$

Dunque il MCD di 665 e 273 è 7. Inoltre possiamo scrivere

$$7 \quad = \quad (-16) \cdot 665 \quad + \quad 39 \cdot 273 \quad \Longrightarrow \; s = -16, \; t = 39$$

2.2.3 Minimo comune multiplo

DEF 2.8 (Minimo comune multiplo)**.** Siano $a, b \in \mathbb{Z}$. Si dice minimo comune multiplo di a e b un numero $m \in \mathbb{Z}$ tale che:

i) $a|m$ e $b|m$;

ii) se $a|m$ e $b|c$, allora $m|c$.

Su questo argomento ci soffermiamo solo brevemente per dimostrare la seguente

Proposizione 2.9. *Siano $a, b \in \mathbb{Z}_{>0}$ e $d, m \in \mathbb{Z}_{>0}$ rispettivamente un loro massimo comun divisore e un loro minimo comune multiplo. Allora $dm = ab$.*

Dimostrazione. Equivalentemente, possiamo dire che esistono $a', b', m_a, m_b \in \mathbb{Z}_{>0}$ tali che

$$\begin{array}{ll} a = a'd & b = b'd \\ m = am_a & m = bm_b \end{array} \qquad (\star)$$

Dimostriamo prima di tutto che a' e b' sono coprimi. Supponiamo per assurdo che non lo siano ma abbianno un fattore in comune c, allora

$$\left.\begin{array}{lll} a = a'd = \hat{a}cd & \Longrightarrow & cd|a \\ b = b'd = \hat{b}cd & \Longrightarrow & cd|b \end{array}\right\} \underset{(ii)}{\Longrightarrow} cd|d \Longrightarrow c = 1$$

Analogamente si priva che m_a e m_b sono coprimi. Ora da $(\star)$ segue che $a'm_a = b'm_b$. Di conseguenza

$$\left.\begin{array}{lll} a'|b'm_b & \Longrightarrow & (a', b' \text{ coprimi}) \quad a'|m_b \\ m_b|a'm_a & \Longrightarrow & (m_a, m_b \text{ coprimi}) \quad m_b|a' \end{array}\right\} \Longrightarrow a' = m_b$$

Analogamente si prova che $b' = m_a$. Allora da $(\star)$ segue che

$$md = (am_a)d = a(b'd) = ab$$

QED

Esercizio 2.1. *Dimostrare che se $a, b \in \mathbb{Z}$ sono coprimi e $a|bc$, allora $a|c$.* *Soluzione a pag. 15*

2.3 Numeri primi

DEF 2.10 (Primo)**.** Un $p \in \mathbb{Z}_{>1}$ si dice primo se i suoi unici divisori sono 1 e p. **Equivalentemente** p è primo se e solo se per ogni $a, b \in \mathbb{Z}$ tale che $p|ab$ allora $p|a$ o $p|b$.

Osservazione 2.11. Notiamo che per la definizione che abbiamo dato prima di mcd *non* serve alcuna nozione di primalità, a differenza di quella data in precedenza.

Esercizio 2.2. *Verificare che la definizione classica di MCD coincide con quella data.* *Soluzione a pag. 15*

Lemma 2.12 (Euclide, ~ 300 a.C.)**.** *I numeri primi sono infiniti.*

Dimostrazione. Supponiamo per assurdo che esistano un numero finito di primi $p_1, \dots, p_n$. Sia allora

$$a = p_1 \cdot \ldots \cdot p_n,$$

osserviamo che $\forall 1 \leq i \leq n,\ p_i \nmid a$, infatti siccome p_i divide a, non può dividere $a+1$. Di conseguenza anche $a+1$ è primo, il che conduce ad una contraddizione. Segue quindi che i numeri primi devono essere infiniti. QED

3 Relazioni di equivalenza

Per comprendere appieno da un punto di vista formale il concetto di congruenza, è necessario introdurre il concetto di relazione, di relazione di equivalenza e di insieme quoziente. Cominciamo dalle basi:

DEF 3.1 (Relazione)**.** Sia A un insieme non vuoto. Una relazione su A è un sottoinsieme $R \in \mathcal{P}(A \times A)$.

A seconda dei casi scriveremo $(x, y) \in R$ oppure xRy per indicare che x e y sono in relazione R. A noi tuttavia interessano un particolare tipo di relazioni, dette di equivalenza:

DEF 3.2 (Relazione di equivalenza)**.** Una relazione R è detta di equivalenza se è:

[R] riflessiva: $\forall x \in A,\ xRx$;

[S] simmetrica: $\forall x, y \in A,\ xRy \implies yRx$;

[T] transitiva: $\forall x, y, z \in A,\ xRy$ e $yRz \implies xRz$.

Generalmente per le relazioni di equivalenza si usano i simboli $\sim, \simeq, \cong, \equiv$ a seconda del contesto.

Un esempio di relazione di equivalenza sono la similitudine e la congruenza viste in geometria.
Le relazioni di equivalenza permettono di definire inoltre un'altra serie di concetti:

DEF 3.3 (Classi di equivalenza)**.** Sia $\sim \in \mathcal{P}(A^2)$ una relazione di equivalenza su A. Allora per ogni $x \in A$ si definisce la classe di equivalenza di x come

$$[x]_\sim = [x] = \{y \in A \mid y \sim x\}.$$

Segue inoltre direttamente il seguente teorema che non dimostreremo.

Teorema 3.4. *Siano $\sim \in \mathcal{P}(A^2)$ una relazione di equivalenza su A e $a, b \in A$. Allora le seguenti affermazioni sono equivalenti*

i) $a \sim b$ *ii)* $a \in [b]$ *iii)* $[a] \subseteq [b]$

iv) $[a] = [b]$ *v)* $[a] \cap [b] \neq \varnothing$

Inoltre si ha che A è l'unione disgiunta di tutte le classi, per cui esse costituiscono una partizione di A. Si può infine definire l'insieme quoziente come segue:

DEF 3.5 (Insieme quoziente)**.** Sia $\sim \in \mathcal{P}(A^2)$ una relazione di equivalenza su A. Allora l'insieme quoziente di A rispetto a $\sim$ è l'insieme

$$A/_\sim = \{[x] \mid x \in A\}.$$

4 Congruenze

DEF 4.1 (Congruenza)**.** Sia $n \in \mathbb{Z}$. Definiamo una relazione di equivalenza $\equiv \in \mathcal{P}(\mathbb{Z}^2)$ tale che

$$x \equiv y \mod n \iff n \mid b - a$$

Ovvero se il resto della divisione di a per n è uguale a quello della divisione di b per n. $\equiv$ è detta

congruenza modulo n.

La dimostrazione del fatto che questa sia una relazione di equivalenza è banale e pertanto è lasciata al lettore.

Esercizio 4.1. *Dimostrare che la congruenza è una relazione di equivalenza.* *Soluzione a pag. 15*

Osserviamo prima di tutto che la congruenza modulo n e la congruenza modulo $-n$ sono equivalenti, per cui possiamo assumere $n > 0$. Per un qualsiasi $a \in \mathbb{Z}$ si definisce la classe di equivalenza di a come

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

infatti se $b \equiv a \mod n$ allora $n \mid b - a$ e quindi $b - a = kn$ per un qualche $k \in \mathbb{Z}$, da cui segue che $b = a + kn$. Queste classi sono dette anche classi di congruenze o classi di resto modulo n.

Una prima proprietà che ci interessa studiare è quante e quali sono queste classi

Proposizione 4.2. *Le classi di congruenza modulo n sono n e sono $[0]_n, [1]_n, \dots, [n-1]_n$.*

Dimostrazione. La dimostrazione è banale e non è di nostro interesse, quindi la saltiamo. QED

Indichiamo con $\mathbb{Z}/n\mathbb{Z}$ l'insieme quoziente di $\mathbb{Z}$ rispetto alla congruenza modulo n. Ovvero

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

a volte si trovano anche altre notazioni, ad esempio $\mathbb{Z}_n$ o $\mathbb{F}_p$ (nel caso in cui p sia un primo).

Rimane solo da definire le operazioni di somma e prodotto tra classi di congruenza.

DEF 4.3 (Operazioni in $\mathbb{Z}/n\mathbb{Z}$)**.** Siano $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$. Allora definiamo

- $[a]_n + [b]_n = [a + b]_n$;
- $[a]_n \cdot [b]_n = [a \cdot b]_n$.

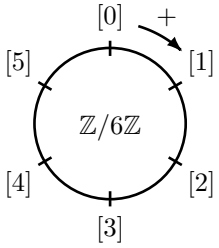
Questa definizione ha però un problema: non abbiamo la garanzia che sia ben definita, ovvero che non dipenda dalla scelta dei rappresentanti delle classi. Per esempio, se $[a]_n = [a']_n$ e $[b]_n = [b']_n$ allora dobbiamo dimostrare che $[a + b]_n = [a' + b']_n$. Per fare questo ci basta ricordare che $a' = a + hn$ e $b' = b + kn$ per qualche $h, k \in \mathbb{Z}$, per cui

$$[a' + b'] = [a + hn + b + kn] = [a + b + (h + k)n] = [a + b]$$
$$[a'b'] = [(a + hn)(b + kn)] = [ab + n(ak + bh + hkn)] = [ab]$$

e quindi le operazioni sono ben definite. Con queste operazioni $\mathbb{Z}/n\mathbb{Z}$ è un anello commutativo con unità, ovvero come $\mathbb{Z}$ la somma è a le proprietà [A], [N], [I], [C] mentre il prodotto ha le proprietà [A], [N], [C].

4.1 Visualizziamo $\mathbb{Z}/n\mathbb{Z}$

Abbiamo definito tutto in modo molto formale, ma abbiamo davvero un'idea di cosa stiamo facendo? Per capire meglio cosa stiamo facendo possiamo pensare a $\mathbb{Z}/n\mathbb{Z}$ come a un cerchio su cui vengono disposti n punti, ognuno dei quali è una classe di congruenza. In questo modo sommare equivale a percorrere questo cerchio in senso antiorario.



$$\begin{aligned}
[0] &= \{\dots, -12, -6, 0, 6, 12, \dots\} \\
[1] &= \{\dots, -11, -5, 1, 7, 13, \dots\} \\
[2] &= \{\dots, -10, -4, 2, 8, 14, \dots\} \\
[3] &= \{\dots, -9, -3, 3, 9, 15, \dots\} \\
[4] &= \{\dots, -8, -2, 4, 10, 16, \dots\} \\
[5] &= \{\dots, -7, -1, 5, 11, 17, \dots\}
\end{aligned}$$

Figura 4.1: Rappresentazione grafica di $\mathbb{Z}/6\mathbb{Z}$

Guardando questa immagine ci giustifichiamo in qualche modo anche la scelta del termine *anello* per descrivere queste strutture.

4.2 Criteri di divisibilità

Vediamo una prima applicazione delle congruenze nella determinazione dei criteri di divisibilità: qui vedremo solo i principali, ma mediante lo stesso procedimento è possibile determinare criteri di divisibilità per qualsiasi numero. Ricordiamo prima di tutto che dalla definizione di congruenze segue che

$$a \mid b \quad \iff \quad b \equiv 0 \mod a$$

Tralasciamo il criterio di divisibilità per 2, che è banale, e passiamo a quello per 3. Ricordiamo inoltre che $a \mid b \Leftrightarrow a \mid -b$.

Proposizione 4.4 (Criterio di divisibilità per 3)**.** *Un numero è divisibile per 3 se e solo se la sua somma delle cifre lo è.*

Dimostrazione. Sia $a \in \mathbb{Z}$ qualsiasi (possiamo assumere $a > 0$), allora lo scriviamo in forma polinomiale:

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots + a_n x^n$$

Ora osserviamo che $10 \equiv 1 \mod 3$, quindi $10^k \equiv 1 \mod 3$ per ogni $k \in \mathbb{N}$. Dunque possiamo riscrivere a come

$$a \equiv a_0 + a_1 + a_2 + \cdots + a_n \mod 3$$ QED

Esercizio 4.2. *Dimostrare che un numero è divisibile per 9 se e solo se la somma delle sue cifre lo è.* *Soluzione a pag. 15*

Proposizione 4.5 (Criterio di divisibilità per 4)**.** *Un numero è divisibile per 4 se e solo se le sue ultime due cifre lo sono.*

Dimostrazione. Sia $a \in \mathbb{Z}$ qualsiasi (possiamo assumere $a > 0$), allora lo scriviamo in forma polinomiale:

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots + a_n x^n$$

Ora osserviamo che $4 \mid 10^k$ se e solo se $k \geq 2$, dunque possiamo riscrivere a come

$$a \equiv a_0 + 10a_1 \mod 4$$ QED

Esercizio 4.3. *Dimostrare che un numero è divisibile per 8 se e solo se le sue ultime tre cifre lo sono.* *Soluzione a pag. 15*

Proposizione 4.6 (Criterio di divisibilità per 11)**.** *Un numero è divisibile per 11 se e solo se la differenza tra la somma delle cifre di posto pari e la somma delle cifre di posto dispari è divisibile per 11.*

Dimostrazione. Sia $a \in \mathbb{Z}$ qualsiasi (possiamo assumere $a > 0$), allora lo scriviamo in forma polinomiale:

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots + a_n x^n$$

Ora osserviamo che $10 \equiv -1 \mod 11$, quindi $10^k \equiv (-1)^k \mod 11$ per ogni $k \in \mathbb{N}$. Dunque possiamo riscrivere a come

$$a \equiv a_0 - a_1 + a_2 - \cdots + (-1)^n a_n \mod 11$$

ovvero

$$a \equiv (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots) \mod 11$$ QED

4.3 Invertibilità in $\mathbb{Z}/n\mathbb{Z}$

DEF 4.7 (Invertibilità)**.** Sia R un anello e sia $a \in R$. Allora a si dice *invertibile* se esiste $b \in R$ tale che

$$ab = ba = 1.$$

DEF 4.8 (Divisori dello zero)**.** Sia R un anello e sia $a \in R \setminus \{0\}$. Allora a si dice *divisore dello zero* se esiste $b \in R \setminus \{0\}$ tale che

$$ab = ba = 0.$$

Ora dimostriamo alcune proprietà su gli invertibili e sui divisori dello zeroin $\mathbb{Z}/n\mathbb{Z}$.

Lemma 4.9. *Sia $n \in \mathbb{N}$ e sia $[a] \in \mathbb{Z}/n\mathbb{Z}$. Allora $[a]$ è invertibile se e solo se* $\mathrm{mcd}(a, n) = 1$.

Dimostrazione.

"$\Leftarrow$" Per il Teorema di esistenza del massimo comun divisore (2.6) sappiamo che esistono $x, y \in \mathbb{Z}$ tali che

$$1 = \mathrm{mcd}(a, n) = ax + ny \Leftrightarrow ax = 1 - ny \equiv 1 \mod n$$

"$\Rightarrow$" Sia $b \in \mathbb{Z}/n\mathbb{Z}$ tale che $ab \equiv 1 \mod n$. Allora esiste $k \in \mathbb{Z}$ tale che $ab = 1 + kn$, ovvero $ab - kn = 1$. Dunque $\mathrm{mcd}(a, n) = 1$ per il Teorema di esistenza del massimo comun divisore (2.6).

QED

Lemma 4.10. *Sia $n \in \mathbb{N}$ e sia $[a] \in \mathbb{Z}/n\mathbb{Z}$. Allora $[a]$ è un divisore dello zero se e solo se* $\mathrm{mcd}(a, n) \neq 1$.

Dimostrazione. È lecito supporre $0 < a < n$ come rappresentante della classe, per cui $\mathrm{mcd}(a, n) \neq 1 \Leftrightarrow a \mid n$.

"⇐" Supponiamo $a \mid n$. Allora esiste $k \in \mathbb{Z} \setminus \{0\}$ tale che $n = ak$, ovvero $ak \equiv 0 \mod n$. Dunque

$$[a][k] = [ak] = [0]$$

.

"⇒" Supponiamo $[a][b] = [0]$ e $[a], [b] \neq [0]$. Allora si ha che per qualche $k \in \mathbb{Z}$, $ab = nk$. Ora supponiamo per assurdo che $\mathrm{mcd}(a, n) = 1$, allora abbiamo che $n \mid ab$ per cui $n \mid b$. Ma allora $[b] = [0]$, per cui deve essere $\mathrm{mcd}(a, n) \neq 1$.

QED

Possiamo quindi mettere insieme tutti i risultati che abbiamo appena dimostrato nel seguente

Teorema 4.11 (Elementi di $\mathbb{Z}/n\mathbb{Z}$)**.** *Sia $n \in \mathbb{N}$. Allora un $[a] \in \mathbb{Z}/n\mathbb{Z}$ è:*

- $[0]$
- *Invertibile, se* $\mathrm{mcd}(a, n) = 1$
- *Divisore dello zero, se* $\mathrm{mcd}(a, n) \neq 1$

Dimostrazione. Segue dai lemmi precedenti. QED

Osserviamo quindi che se $n =: p$ è un primo, allora $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ è formato solo dallo zero e dagli invertibili. Una struttura di questo tipo si dice campo. Altri esempi di campi sono $\mathbb{R}, \mathbb{Q}$ e $\mathbb{C}$.

4.4 Teoremi notevoli

4.4.1 Piccolo Teorema di Fermat

Teorema 4.12 (Fermat - piccolo)**.** *Sia p un primo e sia $a \in \mathbb{Z}$. Allora*

$$a^p \equiv a \mod p$$

Dimostrazione. Separiamo i casi $a \geq 0$ e $a < 0$.

- Sia $a \geq 0$. Dimostriamo il teorema per induzione su a:
  - **Caso base:** $a = 0$. Allora $0^p \equiv 0 \mod p$.
  - **Passo induttivo:** supponiamo vero il teorema per a e dimostriamolo per $a + 1$. Allora per il binomio di Newton
  $$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1.$$
  Ricordando che
  $$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$
  osserviamo che, siccome p è primo, $p \nmid i!$ e $p \nmid (p-i)!$ per ogni $i \in \{1, \ldots, p-1\}$. Dunque $p \mid \binom{p}{i}$ per ogni $i \in \{1, \ldots, p-1\}$. Ma allora
  $$(a+1)^p \equiv a^p + 1$$
  infine, per ipotesi induttiva,
  $$a^p \equiv a \mod p$$
- Sia $a < 0$. Allora sia $b := -a > 0$ e per quanto dimostrato sopra
  $$b^p \equiv b \mod p$$
  ovvero
  $$a^p = (-1)^p b^p \equiv (-1)^p b = \begin{cases} b & p \text{ dispari} \\ -b & p = 2 \end{cases} \mod p$$
  Se p è dispari, abbiamo la tesi ($b = -a$). Altrimenti se $p = 2$, allora $-a \equiv a \mod 2$ e abbiamo la tesi.

QED

Corollario 4.13. Sia p un primo e sia $a \in \mathbb{Z}$ tale che $p \nmid a$. Allora

$$a^{p-1} \equiv 1 \mod p$$

Dimostrazione. Per il Piccolo Teorema di Fermat, $a^p \equiv a \mod p$, ovvero $p \mid a^p - a \Leftrightarrow p \mid a(a^{p-1} - 1)$. Di conseguenza, siccome $p \nmid a$, deve essere $p \mid a^{p-1} - 1 \Leftrightarrow a^{p-1} \equiv 1 \mod p$. QED

Corollario 4.14. Siano $x, y \in \mathbb{Z}$, p un primo e $p \nmid x$. Allora

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

4.4.2 Funzione e Teorema di Eulero

Di questa parte vedremo solo enunciati e proprietà, tralasciando le dimostrazioni.

DEF 4.15 (Funzione di Eulero)**.** Definiamo la funzione $\varphi : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ data da

$$\varphi(n) = \#\{k \in \mathbb{N}_{>0} \mid k < n \text{ e } \mathrm{mcd}(n,k) = 1\},$$

ovvero che conta il numero di interi positivi minori di n e "coprimi" con n. Equivalentemente, conta il numero di elementi invertibili in $\mathbb{Z}/n\mathbb{Z}$.

Lemma 4.16. *Siano $p \in \mathbb{N}$ rispettivamente un primo e $\alpha \in \mathbb{N}_{>0}$. Allora $\varphi(\pi^\alpha) = p^\alpha - p^{\alpha-1}$.*

Dimostrazione. Calcoliamo $\varphi(p^\alpha)$ per differenza rispetto al complementare:

$$\begin{aligned}
\varphi(p^\alpha) &= \#\{n \in \mathbb{N}_{>0} \mid n < p^\alpha \text{ e } \mathrm{mcd}(n, p^\alpha) = 1\} = \\
&= p^\alpha - \#\{n \in \mathbb{N}_{>0} \mid n < p^\alpha \text{ e } \mathrm{mcd}(n, p^\alpha) \neq 1\} = \\
&= p^\alpha - \#\#\{n \in \mathbb{N}_{>0} \mid n < p^\alpha \text{ e } p \mid n \neq 1\} = \\
&= p^\alpha - \#\{pk \mid pk < p^\alpha\} = \\
&= p^\alpha - \#\{p^k \mid k < p^{\alpha-1}\} = \\
&= p^\alpha - p^{\alpha-1}.
\end{aligned}$$

QED

Lemma 4.17. *Siano $n, m \in \mathbb{N}$ due interi coprimi. Allora $\varphi(nm) = \varphi(n)\varphi(m)$.*

Dimostrazione. Scriviamo tutti gli interi positivi tra 1 e mn in una tabella

$$\begin{bmatrix}
1 & 2 & 3 & \cdots & m \\
m+1 & m+2 & m+3 & \cdots & 2m \\
2m+1 & 2m+2 & 2m+3 & \cdots & 3m \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & nm
\end{bmatrix}$$

allora un elemento a della tabella è coprimo con n e m se e solo se è coprimo sia con n che con m. In particolare, è coprimo con m se e solo se è in una colonna coprima con m: queste colonne sono esattamente $\varphi(m)$. Inoltre, se guardiamo i resti modulo n di ogni elemento, osserviamo che l'ultima colonna contiene tutti i possibili prodotti di m con un elemento di $\mathbb{Z}/n\mathbb{Z}$ che, siccome m è coprimo con n, non sono altro che tutti gli elementi di $\mathbb{Z}/n\mathbb{Z}$. Lo stesso vale per le altre colonne, che si ottengono sottraendo lo stesso numero a tutti gli elementi dell'ultima: di conseguenza ogni colonna contiene esattamente $\varphi(n)$ elementi coprimi con n. Mettendo tutto assieme, abbiamo selezionato $\varphi(m)$ colonne e da ciascuna di esse $\varphi(n)$ elementi, per cui $\varphi(nm) = \varphi(n)\varphi(m)$. QED

Conscio che la dimostrazione può non essere molto chiara, riporto un esempio.

Esempio 4.1.

Proviamo a ripetere quanto fatto nella dimostrazione con $n = 5$ e $m = 6$. La tabella ha la forma

$$\begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
7 & 8 & 9 & 10 & 11 & 12 \\
13 & 14 & 15 & 16 & 17 & 18 \\
19 & 20 & 21 & 22 & 23 & 24 \\
25 & 26 & 27 & 28 & 29 & 30
\end{bmatrix}$$

osserviamo che tutti gli elementi delle colonne non coprime con 6 sono a loro volta non coprimi con 6, quindi quelle vanno escluse. Osserviamo ora cosa succede prendendo le classi modulo 5:

$$\begin{bmatrix}
1 & 2 & 3 & 4 & 0 & 1 \\
2 & 3 & 4 & 0 & 1 & 2 \\
3 & 4 & 0 & 1 & 2 & 3 \\
4 & 0 & 1 & 2 & 3 & 4 \\
0 & 1 & 2 & 3 & 4 & 0
\end{bmatrix}$$

ogni colonna contiene tutti i rappresentanti delle classi di resto modulo 5. Limitandoci alle colonne selezionate in precedenza, prendiamo quindi gli elementi coprimi.

$$\begin{bmatrix} \boxed{1} & 2 & 3 & 4 & 0 & 1 \\ \boxed{2} & 3 & 4 & 0 & \boxed{1} & 2 \\ \boxed{3} & 4 & 0 & 1 & \boxed{2} & 3 \\ \boxed{4} & 0 & 1 & 2 & \boxed{3} & 4 \\ 0 & 1 & 2 & 3 & \boxed{4} & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} \boxed{1} & 2 & 3 & 4 & 5 & 6 \\ \boxed{7} & 8 & 9 & 10 & \boxed{11} & 12 \\ \boxed{13} & 14 & 15 & 16 & \boxed{17} & 18 \\ \boxed{19} & 20 & 21 & 22 & \boxed{23} & 24 \\ 25 & 26 & 27 & 28 & \boxed{29} & 30 \end{bmatrix}$$

Ritornando alla tabella originale, è facile notare come abbiamo selezionato esattamente gli elementi coprimi con sia 6 che 5, e quindi con $6 \cdot 5$.

Teorema 4.18 (Formula moltiplicativa di Eulero)**.** *Dato un intero $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, con p_i primi distinti e $\alpha_i \in \mathbb{N}_{>0}$, allora*

$$\varphi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Dimostrazione. Procediamo per induzione sul numero di fattori primi:

$\boxed{k = 1}$ In questo caso, $n = p_1^{\alpha_1}$, quindi la tesi segue dal Lemma 4.16.

$\boxed{k > 1}$ Osserviamo che $p_1^{\alpha_1}$ e $p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ sono coprimi. Per il Lemma 4.16 $\varphi\left(p_1^{\alpha_1}\right) = p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$, mentre per ipotesi induttiva, $\varphi(p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = \prod_{i=2}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$. Di conseguenza per Lemma 4.16,

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \prod_{i=2}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) \quad \text{QED}$$

Teorema 4.19 (Eulero)**.** *Siano $a, n \in \mathbb{Z}$ tali che $\mathrm{mcd}(a, n) = 1$. Allora*

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

Dimostrazione. Consideriamo l'insieme $B = \{[b]_n \mid \mathrm{mcd}(b, n) = 1\}$: osserviamo che moltiplicando ogni elemento di B per $[a]_n$, siccome $\mathrm{mcd}(a, n) = 1$, otteniamo nuovamente B. Di conseguenza, siccome $\#B = \varphi(n)$,

$$\prod_{[b] \in B} [b] = \prod_{[b] \in B} [ab] = [a]^{\varphi(n)} \prod_{[b] \in B} [b].$$

Poiché il prodotto di invertibili è ancora invertibile, concludiamo che $[a^{\varphi(n)}] = [1]$. QED

Osserviamo che il Corollario 4.13 segue naturalmente anche da questo Teorema.

5 Equazioni con le congruenze

5.1 Equazioni in una variabile

Un'equazione nelle congruenze è un'equazione del tipo

$$ax \equiv b \mod n$$

dove $a, b, n \in \mathbb{Z}$ e x è l'incognita. Osserviamo che se x_0 è una soluzione di questa equazione, allora anche $x_0 + kn$ è una soluzione per ogni $k \in \mathbb{Z}$. Inoltre il Teorema 2.6 ci da una condizione di risolubilità per l'equazione, ovvero che $\mathrm{mcd}(a, n) \mid b$. Infatti otteniamo che esistono $s, t, k \in \mathbb{Z}$ tali che

$$as + nt = k \quad \text{e} \quad b = kb'$$

quindi

$$ax \equiv b = kb' = b'(as + nt) = b'as + b'nt \equiv a(b's) \mod n$$

da cui segue che $x_0 = b's$ è una soluzione dell'equazione.

Esempio 5.1.

Calcolare le soluzioni di $273x \equiv 21 \mod 665$

Nell'esempio 2.1 abbiamo trovato che

$$\mathrm{mcd}(273, 665) = 7 = (-16) \cdot 665 + 39 \cdot 273$$

per cui l'equazione ammette soluzione $(7 \mid 21)$ inoltre sappiamo che

$$39 \cdot 273 \equiv 7 \mod 665$$

quindi

$$117 \cdot 273 = 39 \cdot 3 \cdot 273 \equiv 7 \cdot 3 = 21 \mod 665 \quad \rightsquigarrow \quad x = 39 + k665$$

5.2 Sistemi di equazioni e Teorema Cinese del Resto

Lo stesso ragionamento del paragrafo precedente può essere applicato ai sistemi di congruenze, per i quali dobbiamo tuttavia discutere la compatibilità, la quale è garantita nelle ipotesi del

Teorema 5.1 (Cinese del Resto)**.** *Siano $m, n \in \mathbb{Z}$ coprimi, allora esiste un isomorfismo di anelli*

$$\begin{array}{rccc} \sigma: & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & [a]_{mn} & \longmapsto & ([a]_m, [a]_n) \end{array}$$

il quale in questa formulazione non ci dice molto, ma ci permette di dimostrare un corollario

Corollario 5.2 (Compatibilità di sistemi lineari di equazioni di congruenze)**.** Siano $m_1, \dots, m_n \in \mathbb{Z}$ coprimi a due a due e siano $a_1, \dots, a_n \in \mathbb{Z}$. Allora il sistema

$$\begin{cases} x \equiv a_1 \mod m_1 \\ \vdots \\ x \equiv a_n \mod m_n \end{cases}$$

è compatibile e ammette una soluzione unica modulo $m_1 \cdot \ldots \cdot m_n$.

Esempio 5.2.

Risolvere il sistema $\begin{cases} x \equiv 2 \mod 11 \\ x \equiv 18 \mod 19 \end{cases}$

Osserviamo che 11 e 19 sono coprimi, per cui una soluzione esiste.

$$\begin{cases} x \equiv 2 \mod 11 \\ x \equiv 18 \mod 19 \end{cases} \rightsquigarrow x = 18 + 19\lambda$$

$$\rightsquigarrow 19\lambda \equiv 2 - 18 \equiv 6 \mod 11$$

Calcoliamo ora il reciproco di $8 \mod 11$ con l'algoritmo di Euclide esteso:

$$\begin{array}{rcrcr} 11 & = & 11 & + & 0 \\ 8 & = & 0 & + & 8 \\ 3 & = & 11 & + & (-1) \cdot 8 \\ 2 & = & (-2) \cdot 11 & + & (3) \cdot 8 \\ 1 & = & (3) \cdot 11 & + & (-4) \cdot 8 \end{array}$$

da cui $-4 \cdot 8 \equiv 7 \cdot 8 \equiv 1 \mod 11$. Segue quindi che $\lambda \equiv 6 \cdot 7 \equiv 42 \equiv 9 \mod 11$, quindi

$$x = 18 + 19 \cdot 9 + 209k = 189 + 209k.$$

Esempio 5.3.

Una contadina porta delle uova al mercato. Sa che contandole a 2 a 2 ne avanza 1, contandole a 3 a 3 ne avanza 1, a 4 a 4 ne avanza 1, a 5 a 5 ne avanza 1, a 6 a 6 ne avanza sempre 1, mentre contandole a 7 a 7 non ne avanza alcuna. Quante uova ha la contadina? (L. Fibonacci, *Liber Abbaci*, 1202)

Riscriviamo il problema in termini di congruenze:

$$\begin{cases} x \equiv 1 \mod 2 & \leftarrow \\ x \equiv 1 \mod 3 & \leftarrow \\ x \equiv 1 \mod 4 & \leftarrow \\ x \equiv 1 \mod 5 & \\ x \equiv 1 \mod 6 & \leftarrow \\ x \equiv 0 \mod 7 & \end{cases}$$

ora, osserviamo che $2, 3, 4, 6$ non sono coprimi a due a due, infatti le righe segnate sono ridondanti o

incompatibili. Verifichiamo che non cono incompatibili: osserviamo infatti che possiamo tenere solo

$$\begin{cases} x \equiv 1 \mod 4 \\ x \equiv 1 \mod 3 \end{cases}$$

Infatti $x \equiv 1 \mod 4 \implies x \equiv 1 \mod 2$ e

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 1 \mod 3 \end{cases} \implies x \equiv 1 \mod 6$$

Per cui riscriviamo il sistema come

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 1 \mod 4 \\ x \equiv 1 \mod 5 \\ x \equiv 0 \mod 7 \quad \leftarrow \end{cases}$$

Ora cominciamo a risolvere il sistema: la riga segnata può essere riscritta come $\boxed{x = 7\alpha}$, per cui sostituiamo questo nel sistema

$$\begin{cases} 7\alpha \equiv \alpha \equiv 1 \mod 3 \quad \leftarrow \\ 7\alpha \equiv -\alpha \equiv 1 \mod 4 \\ 7\alpha \equiv 2\alpha \equiv 1 \mod 5 \end{cases}$$

da cui abbiamo $\boxed{\alpha = 1 + 3\beta}$

$$\begin{cases} -(1+3\beta) \equiv -1 - 3\beta \equiv 1 \mod 4 \\ 2(1+3\beta) \equiv 2 + 6\beta \equiv 1 \mod 5 \end{cases} \rightsquigarrow \begin{cases} \beta \equiv 2 \mod 4 \quad \leftarrow \\ \beta \equiv -1 \mod 5 \end{cases}$$

ora poniamo $\boxed{\beta = 2 + 4\gamma}$

$$2 + 4\gamma \equiv -1 \mod 5 \rightsquigarrow \gamma \equiv 3 \mod 5 \rightsquigarrow \boxed{\gamma = 3 + 5\lambda}$$

Infine riscriviamo tutte le sostituzioni che abbiamo fatto:

$$\begin{cases} x = 7\alpha \\ \alpha = 1 + 3\beta \\ \beta = 2 + 4\gamma \\ \gamma = 1 + 5\lambda \end{cases} \rightsquigarrow \begin{aligned} x &= 7\alpha = 7(1+3\beta) = 7(1+3(2+4\gamma)) = 7(1+3(2+4(3+5\lambda))) = \\ &= 7(1+3(2+12+20\lambda)) = 7(1+42+60\lambda) = \boxed{301 + 420\lambda} \end{aligned}$$

6 Bonus: la costruzione di $\mathbb{Z}$ e $\mathbb{Q}$

L'idea che abbiamo usato di definire delle operazioni su classi di equivalenza, è un procedimento estremamente comune in matematica. Vediamo ora qualche altra sua applicazione, in particolare alla costruzione dei numeri interi e dei numeri razionali a partire dai numeri naturali.

6.1 $\mathbb{Z}$

Quando ci sono stati spiegati per la prima volta i numeri interi, ci è stato spiegato che i numeri negativi servono per rendere sempre possibile la sottrazione. Qui vogliamo spiegare in che modo questo funziona a livello teorico. Cominciamo considerando tutte le possibili differenze di numeri naturali, anche quelle che in $\mathbb{N}$ non si possono fare: esse corrispondono a tutte le coppie $(a, b) \in \mathbb{N}^2$ di naturali. A questo punto introduciamo una relazione di equivalenza: due coppie di numeri naturali sono equivalenti se e solo se hanno la stessa differenza, ovvero

$$(a, b) \sim (c, d) : \iff (a - b = c - d) \iff a + d = b + c$$

a questo punto possiamo definire la somma su $\mathbb{N}^2/\sim$ come (indico $[(a, b)] = [a, b]$)

$$[a, b] + [c, d] := [a + c, b + d] \qquad \text{e} \qquad -[a, b] := [b, a]$$

Si verifica facilmente che questa operazione è ben definita, e che, chiamando $[0, 0] = 0, [a, 0] = a$ e $[0, b] = -b$ otteniamo proprio $\mathbb{Z}$

6.2 $\mathbb{Q}$

Torniamo alla costruzione delle frazioni vista alle elementari: una frazione è una coppia di numeri interi, il secondo nonzero, $\frac{a}{b}$, e due frazioni $\frac{a}{b}$ e $\frac{c}{d}$ sono uguali se e solo se esiste un $k \in \mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ tale che $a = kc$ e $b = kd$. Queste informazioni sono sufficienti per definire $\mathbb{Q}$: come prima consideriamo le coppie di interi $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ e definiamo la relazione di equivalenza che abbiamo appena descritto:

$$(a, b) \sim (c, d) : \iff \left[\exists k \in \mathbb{Z} : \begin{cases} a = kc \\ b = kd \end{cases} \right].$$

Consideriamo ora l'insieme $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$, dove indichiamo $(a, b) := \frac{a}{b}$, allora possiamo definire

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{e} \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd},$$

ed è facile verificare che queste operazioni sono ben definite e che $(\mathbb{Q}, \cdot, +)$ è un campo.

7 Soluzioni degli esercizi

Esercizio 2.1

Dimostrazione. Poiché $\mathrm{mcd}(a,b) = 1$, esistono $s,t \in \mathbb{Z}$ tali che $as + bt = 1$, ovvero $asc + btc = c$. Poiché $a|bc$, esiste $\lambda \in \mathbb{Z}$ tale che $bc = a\lambda$. Allora $asc + btc = asc + at\lambda = a(sc + t\lambda) = c$, ovvero $a|c$. □

Esercizio 2.2

Dimostrazione. Per ogni $a, b \in \mathbb{Z}$, scriviamo $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \cdot q_1^{\gamma_1} \cdot \ldots \cdot q_m^{\gamma_m}$ e $b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n} r_1^{\delta_1} \cdot \ldots \cdot r_k^{\delta_k}$, allora con la definizione usuale, $d =: \mathrm{mcd}(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot \ldots \cdot p_n^{\min\{\alpha_n,\beta_n\}}$. Proviamo che d soddisfa la gli assiomi di Definizione 2.5:

- banalmente, $d \mid a$ e $d \mid b$;
- supponiamo che $c \mid a$ e $c \mid b$ e scriviamo $c = s_1^{\varepsilon_1} \cdot \ldots \cdot s_1^{\varepsilon_\ell}$. In particolare per ogni i, $s_i \mid a$ e $s_i \mid b$, quindi in particolare s_i deve dividere un primo comune, ovvero uno dei p_j e $\epsilon_i \leq \alpha_i$, $\epsilon_i \leq \beta_i$. Iterando questo ragionamento concludiamo che per costruzione $c \mid d$.

□

Esercizio 4.1

Dimostrazione. Fissato $n \in \mathbb{N}^*$, verifichiamo gli assiomi di relazione di equivalenza:

[R] $\forall a \in \mathbb{Z}$, $a - a = 0$ e $n|0$, quindi $a \equiv a \mod n$.

[S] $\forall a, b \in \mathbb{Z}$, se $a \equiv b \mod n$ allora $a - b = kn$ per qualche $k \in \mathbb{Z}$, ovvero $b - a = -kn$ per qualche $k \in \mathbb{Z}$, ovvero $b \equiv a \mod n$.

[T] $\forall a, b, c \in \mathbb{Z}$, se $a \equiv b \mod n$ e $b \equiv c \mod n$ allora $a - b = kn$ e $b - c = ln$ per qualche $k, l \in \mathbb{Z}$, ovvero $a - c = (a - b) + (b - c) = kn + ln = (k + l)n$, ovvero $a \equiv c \mod n$.

□

Esercizio 4.2

Dimostrazione. Sia $a \in \mathbb{Z}$ qualsiasi (possiamo assumere $a > 0$), allora lo scriviamo in forma polinomiale:

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots + a_n x^n$$

Ora osserviamo che $10 \equiv 1 \mod 9$, quindi $10^k \equiv 1 \mod 9$ per ogni $k \in \mathbb{N}$. Dunque possiamo riscrivere a come

$$a \equiv a_0 + a_1 + a_2 + \cdots + a_n \mod 9$$ □

Esercizio 4.3

Dimostrazione. Sia $a \in \mathbb{Z}$ qualsiasi (possiamo assumere $a > 0$), allora lo scriviamo in forma polinomiale:

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots + a_n x^n$$

Ora osserviamo che $8 \mid 10^k$ se e solo se $k \geq 3$, dunque possiamo riscrivere a come

$$a \equiv a_0 + 10a_1 + 100a_2 \mod 8$$ □

Riferimenti bibliografici

[Gra] Willem Adriaan de Graaf. *Algebra*. eng. URL: https://degraaf.maths.unitn.it/algnotes/algebranotes.pdf.

[Hal74] Paul Richard Halmos. *Naive set theory*. eng. 1st ed. 1974. Undergraduate texts in mathematics. New York: Springer, 1974. ISBN: 1-4757-1645-1.