Teorema: I numeri primi sono infiniti.

Dim: Sia $S=\{p_1,p_2,\dots,p_n\}$ un insieme finito di numeri primi.
Vogliamo mostrare che esiste un numero primo diverso dai precedenti (o dai loro opposti).
Consideriamo $\alpha = p_1\cdot p_2\cdot\ldots\cdot p_n+1$ Se α è primo abbiamo finito.
Se α non è primo $\Rightarrow$ α è riducibile $\Rightarrow$ $\exists q$ numero primo t.c. $q\mid\alpha$.
Se $q\notin S$ allora abbiamo finito. Se $q\in S \Rightarrow \exists i$ t.c. $q=p_i$, ma allora $\exists k\in\mathbb{Z}$ t.c. $\alpha=p_i\cdot k$

$$p_i k = \alpha = p_1\cdot p_2 \cdots \overset{p_i}{|} \cdots p_n + 1 \quad\Rightarrow\quad -1 = p_1\cdot p_2 \cdot \overset{p_i}{|}\cdots p_n - p_i\cdot k = p_i\cdot\underbrace{\left(\frac{p_1p_2\cdots p_n}{p_i}-k\right)}_{\text{intero}}$$

$\Rightarrow$ p_i è invertibile ASSURDO perché p_i primo. $\Rightarrow q\notin S$. $\boxtimes$

ARITMETICA MODULARE (I PARTE)

Sono le 9:31. Che ore saranno fra 6 ore? Saranno le 3:31.

Implicitamente pensiamo: $9+6=3$ l'aritmetica dell'orologio è "speciale".

Dove sarà la lancetta dei minuti fra 1000 minuti?

$(1000+31):60=17$ col resto di 11 minuti $\Rightarrow$ la lancetta è sull'11.

Idea: quello che conta è il resto della divisione euclidea.

Fissiamo $N\in\mathbb{N}\setminus\{0\}$, che chiamiamo modulo, e consideriamo i seguenti sottoinsiemi di $\mathbb{Z}$:

$A_0=\{n\in\mathbb{Z}\mid \exists q\in\mathbb{Z} \text{ t.c. } n=q\cdot N\}$ numeri divisibili per N

$A_1=\{n\in\mathbb{Z}\mid \exists q\in\mathbb{Z} \text{ t.c. } n=q\cdot N+1\}$ numeri che divisi per N danno resto 1

$\vdots$

$A_{N-1}=\{n\in\mathbb{Z}\mid \exists q\in\mathbb{Z} \text{ t.c. } n=q\cdot N+(N-1)\}$ " " " " $N-1$

Prop: $A_0, A_1, \dots A_{N-1}$ formano una partizione di $\mathbb{Z}$.

Dim: Non sono vuoti perché $\forall i,\ 0\le i\le N-1,\ i\in A_i$.

Sono disgiunti perché il resto della divisione è unico.

Coprono tutto $\mathbb{Z}$ perché $\forall n\in\mathbb{Z}\ \exists! q,r$ t.c. $n=q\cdot N+r \quad 0\le r<N$.

<u>Def</u>: L'insieme quoziente della partizione appena vista si chiama "insieme delle classi di resto modulo N" e si denota $\mathbb{Z}_N$

$$\mathbb{Z}_N = \{A_0, A_1, \dots, A_{N-1}\}$$

Useremo anche la scrittura in termini di rappresentanti delle classi:

$$\mathbb{Z}_N = \{[0]_N, [1]_N, \dots, [N-1]_N\} \quad \text{dove} \quad [i]_N = A_i = \{n \in \mathbb{Z} \mid \exists q \in \mathbb{Z} \text{ t.c. } n = q \cdot N + i\}$$

i fa parte di questa classe, è un rappresentante.

<u>Esempio</u>: $N = 3$ $\quad \mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

$[0]_3 = A_0 = \{n \in \mathbb{Z} \mid \exists q \in \mathbb{Z} \text{ t.c. } n = q \cdot 3\} = \{\dots, -6, -3, 0, 3, 6, 9, \dots\}$ classe 0 modulo 3

$[1]_3 = A_1 = \{n \in \mathbb{Z} \mid \exists q \in \mathbb{Z} \text{ t.c. } n = q \cdot 3 + 1\} = \{\dots, -5, -2, 1, 4, 7, \dots, 19, \dots\}$ classe 1 mod 3

$$-5 = \underbrace{(-2)}_{q} \cdot 3 + \underbrace{1}_{r}$$

$[2]_3 = A_2 = \{n \in \mathbb{Z} \mid \exists q \in \mathbb{Z} \text{ t.c } n = q \cdot 3 + 2\}$

$= \{\dots, -4, -1, 2, 5, 8, \dots\}$ classe 2 mod 3

<u>Notazione</u>: A volte le classi si indicano con una barra: $\bar{0} = [0]_N$ (usata soprattutto se è chiaro quale sia N)

Come stabilire se $[x]_N = [y]_N$?

Es: $[3]_7 \overset{?}{=} [10]_7$ Sì, perché $10 = 1 \cdot 7 + \underbrace{3}_{r}$

$[111]_{34} = [5702]_{34}$?

Lemma: Fissato $N \in \mathbb{N} \setminus \{0\}$, $[x]_N = [y]_N \Longleftrightarrow N \mid (x-y)$ (ovvero $\exists q \in \mathbb{Z}$ t.c. $x-y = q \cdot N$)

In tal caso diciamo che "x è congruo a y modulo N" e scriviamo $x \equiv y \mod N$.

Dim: "$\Longrightarrow$" Supponiamo che $[x]_N = [y]_N$. Allora $\exists q, q', r \in \mathbb{Z}$, $0 \le r < N$ t.c.

$x = qN + r$ e $y = q' \cdot N + r$. Ma allora $x - y = qN + r - q'N - r = N \cdot (q - q')$

Cioè $N \mid (x-y)$.

"$\Longleftarrow$" Supponiamo che $N \mid (x-y)$. Allora $\exists q \in \mathbb{Z}$ t.c. $x - y = N \cdot q$.

Di conseguenza $x = N \cdot q + y$. Ora, grazie alla divisione euclidea $\exists q', r \in \mathbb{Z}$

tali che $y = q' \cdot N + r$ e $0 \le r < N$, cioè $y \in [r]_N$. Inoltre, sostituendo:

$x = N \cdot q + y = N \cdot q + q'N + r = (q + q') \cdot N + r \Longrightarrow x \in [r]_N$

Ma anche $y \in [r]_N \Rightarrow [x]_N = [y]_N$.

Es: $5702 - 111 = 5591$ poiché $34 \nmid 5591 \Rightarrow [111]_{34} \neq [5702]_{34}$

Operazioni in $\mathbb{Z}_N$

Addizione: $\mathbb{Z}_N \times \mathbb{Z}_N \xrightarrow{+} \mathbb{Z}_N$

$$(\bar a, \bar b) \longmapsto \bar a + \bar b := \overline{a+b}$$

è una notazione — è una classe ben determinata

rappresentano cose diverse

$$\bar a \oplus \bar b := \overline{a \oplus b}$$

è l'operazione che stiamo definendo — è l'addizione in $\mathbb{Z}$

Dobbiamo dimostrare che l'operazione così definita è "ben posta".
Ovvero: dobbiamo assicurarci che cambiando rappresentanti degli addendi, la classe somma non cambi.

Sia $[a']_N = [a]_N$ e $[b']_N = [b]_N$. Vuol dire che $\exists h \in \mathbb{Z}$ t.c. $a' - a = h \cdot N \Rightarrow a' = h \cdot N + a$
$\exists k \in \mathbb{Z}$ t.c. $b' - b = k \cdot N \Rightarrow b' = k \cdot N + b$

Ora $a' + b' = hN + a + kN + b = (h+k) \cdot N + a + b$

Sposto $a+b$ a sinistra: $(a'+b') - (a+b) = (h+k) \cdot N \overset{\text{Lemma}}{\Rightarrow} [a'+b']_N = [a+b]_N$

Es: $N = 5$ $\quad \mathbb{Z}_5 = \{\bar 0, \bar 1, \bar 2, \bar 3, \bar 4\}$

$$\bar 2 + \bar 1 = \overline{2+1} = \bar 3 \quad , \quad \bar 2 + \bar 4 = \overline{2+4} = \bar 6 = \bar 1 \quad \text{perché} \quad 6 \equiv 1 \bmod 5$$

$$\bar 3 + \bar 4 + \bar 2 + \bar 4 = \overline{3+4+2+4} = \overline{13} = \bar 3$$

Tornando all'orologio... $N = 12$ $\quad \bar 9 + \bar 6 = \overline{15} = \bar 3$ perché $15 \equiv 3 \bmod 12$