Lezione 7

Prerequisiti: L'insieme dei numeri interi. Lezione 6.

Numeri primi.
Teorema Fondamentale dell'Aritmetica.

Definizione 7.1 Un numero intero *p*, diverso da 0, 1 e –1 si dice *primo* se, per ogni $a, b \in \mathbb{Z}$

$$p \mid ab \Rightarrow p \mid a \quad \text{oppure} \quad p \mid b.$$

Altrimenti *p* si dice *composto.*

Definizione 7.2 Un numero intero *p*, diverso da 0, 1 e –1 si dice *irriducibile* se, per ogni $a, b \in \mathbb{Z}$

$$p = ab \Rightarrow a \text{ è invertibile oppure } b \text{ è invertibile.}$$

Altrimenti *p* si dice *riducibile.*

Queste due nozioni sono, in realtà, equivalenti, come risulta dal seguente

Lemma 7.3 Sia *p* un numero intero diverso da 0, 1 e –1. Allora sono equivalenti le seguenti condizioni.

(i) *p* è primo;
(ii) *p* è irriducibile;
(iii) i divisori di *p* sono 1, –1, *p*, –*p*.

Dimostrazione: (i) $\Rightarrow$ (ii) Sia *p* primo, e siano $a, b \in \mathbb{Z}$ tali che $p = ab$. Essendo *p* non nullo, anche *a* e *b* sono non nulli. Inoltre, in particolare, $p \mid ab$, quindi, in base alla Definizione 7.1, $p \mid a$ oppure $p \mid b$. Nel primo caso $a = pq$, per qualche $q \in \mathbb{Z}$, perciò si ha $a = abq$, da cui, essendo *a* cancellabile (in quanto elemento non nullo di un dominio di integrità), si deduce che $bq = 1$. Pertanto *b* è invertibile. Analogamente si deduce che, nel secondo caso, *a* è invertibile. Ciò prova che *p* è irriducibile.
(ii) $\Rightarrow$ (iii) Sia *p* irriducibile, e sia *a* un divisore di *p*. Allora si ha che $p = ab$ per qualche $b \in \mathbb{Z}$. Segue, in base alla Definizione 7.2, che *a* è invertibile oppure *b* è invertibile. Nel primo caso, $a \in \{1, -1\}$. Nel secondo caso, ciò vale per *b* e, di conseguenza, $a \in \{p, -p\}$. Dunque i divisori di *p* sono 1, -1, *p*, -*p*.
(iii) $\Rightarrow$ (i) Supponiamo che *p* verifichi (iii), e siano $a, b \in \mathbb{Z}$ tali che $p \mid ab$. Sia *d* un massimo comune divisore di *a* e *p*. Allora *d* è un divisore di *p*, e quindi $d \in \{1, -1\}$ oppure $d \in \{p, -p\}$. Nel secondo caso *p* divide *a*. Nel primo caso *p* ed *a* sono coprimi e quindi, per la Proposizione 6.24, segue che *p* divide *b*. Ciò prova che *p* è primo. □

Esempio 7.4 Sono numeri primi 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ... Il più grande numero primo finora conosciuto è $2^{136279841} - 1$, scoperto nel 2024. Tale numero ha 41024320 cifre decimali.

Il prossimo risultato si deduce, con un facile ragionamento induttivo, dalla Definizione 7.2.

Lemma 7.5* Sia p un numero primo e siano $a_1,...,a_r \in \mathbb{Z}$ tali che $p \mid a_1 \cdots a_r$. Allora $p \mid a_i$ per qualche $i \in \{1,...,r\}$.

Siamo ora in grado di provare il

Teorema 7.6 *(Teorema Fondamentale dell'Aritmetica* o *Teorema di fattorizzazione unica)* Sia n un numero intero maggiore di 1. Allora esistono, per qualche intero positivo s, s interi positivi primi $p_1, p_2,..., p_s$ tali che

$$n = p_1 p_2 \cdots p_s. \tag{1}$$

Inoltre, il numero s ed i numeri primi $p_1, p_2,..., p_s$ sono univocamente determinati.

<u>Dimostrazione</u>: Supponiamo per assurdo che esista un numero intero maggiore di 1 per il quale non esiste una decomposizione del tipo (1). Allora l'insieme X di tali numeri è un sottoinsieme non vuoto di $\mathbb{N}$ ed in quanto tale, per il principio del minimo (assioma di buon ordinamento), ammette un minimo m. In particolare m non è allora un numero primo. Quindi, in virtù del Lemma 7.3, m è un numero riducibile. Pertanto esistono $a, b \in \mathbb{Z}$ non invertibili tali che $m = ab.$ Essendo m positivo possiamo supporre, a meno di moltiplicare eventualmente entrambi i fattori per -1, che a e b siano entrambi positivi. Allora essi sono entrambi maggiori di 1. In particolare, da $a > 1$ segue che $b = \frac{m}{a} < m$. Quindi $b \notin X$, e pertanto b si scrive come prodotto di interi positivi primi. Ma, per simmetria, si ha anche che $a \notin X$, e quindi anche a si scrive come prodotto di interi positivi primi. Segue che lo stesso vale per m, contro l'ipotesi. Ciò prova che ogni numero intero maggiore di 1 ammette una decomposizione del tipo (1). Supponiamo ora che il numero intero positivo n ammetta, oltre ad (1), la seguente decomposizione, dove t è un intero positivo e $q_1, q_2,..., q_t$ sono interi positivi primi:

$$n = q_1 q_2 \cdots q_t. \tag{2}$$

Proviamo allora che $s = t$ e che, a meno di riordinare i fattori in (1) e in (2), si ha $p_i = q_i$ per ogni $i = 1,..., s.$ Procediamo per induzione su s. Se $s = 1$, allora $n = p_1$ è primo. Dalla (2) segue allora che $t = 1.$ Non può essere, infatti, $t \geq 2,$ perché altrimenti n sarebbe il prodotto di q_1 e $q_2 \cdots q_t$, che sono numeri naturali maggiori di 1 e quindi non invertibili, e quindi n sarebbe riducibile e dunque, per il Lemma 7.3, non sarebbe primo. Quindi $n = q_1$, e dunque, in particolare, $p_1 = q_1$. Ciò prova la base dell'induzione. Supponiamo ora che sia $s > 1$ e che la tesi sia vera per $s - 1.$ Dalla (1) e dalla (2) segue che

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{3}$$

Poiché p_1 divide il prodotto a secondo membro, in virtù del Lemma 7.5, a meno di riordinare i fattori, si ha che $p_1 \mid q_1.$ Ma, in base al Lemma 7.3, i divisori di q_1 sono $1, -1, q_1, -q_1.$ Essendo p_1 positivo e diverso da 1 e –1, segue che $p_1 = q_1$. Allora, essendo p_1, q_1 non nulli e quindi cancellabili, dalla (3) segue che $p_2 \cdots p_s = q_2 \cdots q_t$. Il numero di fattori a primo membro è $s - 1,$

mentre i fattori a secondo membro sono $t-1$, quindi, per l'ipotesi induttiva, si ha $s-1=t-1$, cioè $s=t$, e, a meno di riordinare i fattori, per ogni $i=2,...,s,\ p_i=q_i$.
Ciò conclude il passo induttivo e completa la dimostrazione. □

Nota L'uguaglianza (1) si dice *fattorizzazione* o *decomposizione in fattori primi* del numero naturale *n*. I numeri p_i si dicono i *fattori primi* di *n*.
Raccogliendo, nella (1), i fattori primi uguali, si ottiene una scrittura più compatta:

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}, \tag{4}$$

ove i primi p_i sono a due a due distinti, e gli esponenti α_i sono interi positivi (precisamente, per ogni indice *i*, α_i è il numero di volte che il fattore primo p_i compare nella fattorizzazione di *n*).

Esempio 7.7 La fattorizzazione di 1500 è $2^2\cdot 3\cdot 5^3$, la fattorizzazione di 26094 è $2\cdot 3\cdot 4349$.

Vediamo ora alcune applicazioni del Teorema Fondamentale dell'Aritmetica.
Il prossimo risultato sfrutta l'esistenza della decomposizione in fattori primi.

Teorema 7.8 *(Infinità dei numeri primi)* Esistono infiniti numeri primi.

<u>Dimostrazione</u>: Dimostriamo che sono infiniti i numeri primi positivi. Supponiamo per assurdo che ciò non sia vero. Allora i numeri primi positivi formano un insieme finito, diciamo $\{p_1, p_2..., p_k\}$. Sia $N=p_1p_2\cdots p_k+1$. Allora *N* è un intero e $N>1$, quindi, in virtù del Teorema Fondamentale dell'Aritmetica, ammette una decomposizione in fattori primi. In particolare, *N* è divisibile per un numero primo, quindi esiste un indice $i\in\{1,2,...,k\}$ tale che p_i divide *N*. Ma allora, in virtù della Proposizione 6.9 (b), segue che p_i divide 1, il che è impossibile. Ciò produce la contraddizione desiderata e prova la tesi. □

Nei prossimi esercizi utilizzeremo l'unicità della decomposizione in fattori primi, che riformuliamo nella forma seguente. Sia *a* un intero positivo, e siano $p_1, p_2, ..., p_u$ numeri primi positivi tali che si abbia $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_u^{\alpha_u}$, ove gli esponenti α_i sono interi non negativi. Allora questi esponenti sono univocamente determinati. Ciò è banalmente vero se $a=1$. Se, invece, $a>1$, i fattori primi di *a* sono univocamente determinati, quindi sono univocamente determinati gli indici *i* per i quali p_i non è un fattore primo di *a*, ossia per i quali $\alpha_i=0$. Eliminando i fattori corrispondenti a questi indici (che sono $p_i^{\alpha_i}=p_i^0=1$), si ottiene l'espressione di *a* come prodotto dei suoi fattori primi, ossia la (4), nella quale gli esponenti sono univocamente determinati.

Esercizio 7.9 Siano $p_1, p_2, ..., p_u$ numeri primi positivi, e sia $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_u^{\alpha_u}$, ove gli esponenti α_i sono interi non negativi. Sia *b* un intero positivo. Provare che allora *b* divide *a* se e solo se $b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_u^{\beta_u}$, ove gli esponenti β_i sono interi non negativi tali che $\beta_i\le\alpha_i$ per ogni indice *i*.

<u>Svolgimento</u>: Supponiamo che *b* divida *a*. Allora esiste un intero (positivo) *q* tale che $a=bq$. Se $q=1$, allora $a=b$ e quindi la tesi è banalmente vera. Se $b=1$, allora si ha la decomposizione voluta per *b* con $\beta_i=0$ per ogni indice *i*. Supponiamo allora che $b>1$ e $q>1$. Poiché *b* e *q*

dividono a, i loro fattori primi sono anche fattori primi di a (in virtù della transitività della relazione di divisibilità). Quindi le loro fattorizzazioni sono della forma seguente:

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_u}$$
$$q = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_u^{\gamma_u}$$

per opportuni esponenti interi non negativi β_i e γ_i. Segue allora che

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_u^{\alpha_u} = bq = (p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_u})(p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_u^{\gamma_u}),$$

da cui

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_u^{\alpha_u} = p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \cdots p_u^{\beta_u+\gamma_u}. \tag{5}$$

Da ciò, per l'unicità della fattorizzazione, si deduce che, per ogni indice i, si ha $\alpha_i = \beta_i + \gamma_i$, da cui $\beta_i \le \alpha_i$, come volevasi. Viceversa, se $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_u}$ e valgono queste disuguaglianze, allora vale la (5) con $\gamma_i = \alpha_i - \beta_i$ (intero non negativo) per ogni indice i, e quindi $a = bq$, con q come sopra. Pertanto b divide a.

Esercizio 7.10* Siano a, b interi maggiori di 1. Determinare un massimo comune divisore ed un minimo comune multiplo di a, b a partire dalle loro fattorizzazioni.

<u>Svolgimento</u>: Siano $p_1, p_2, ..., p_u$ i numeri primi (a due a due distinti) che sono fattori primi di a o di b. Allora le fattorizzazioni di a, b si scrivono nella forma

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_u^{\alpha_u},$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_u},$$

ove gli esponenti α_i, β_i sono interi non negativi (se p_i non compare nella fattorizzazione di a, allora $\alpha_i = 0$, se p_i non compare nella fattorizzazione di b, allora $\beta_i = 0$). Allora

$$\text{MCD}(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_u^{\min(\alpha_u,\beta_u)}.$$

Proviamo che il prodotto a secondo membro (certamente positivo) verifica le condizioni (a) e (b) della Definizione 6.13. Per semplicità di notazione, poniamo, per ogni indice i, $\gamma_i = \min(\alpha_i, \beta_i)$, e $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_u^{\gamma_u}$. Allora, essendo, per ogni indice i, $\gamma_i \le \alpha_i$ e $\gamma_i \le \beta_i$, in virtù dell'Esercizio 7.9 si ha che d divide a e d divide b. Supponiamo ora che l'intero e divida a e b. Possiamo supporre, a meno di cambiare il segno, che e sia positivo. Allora, in base all'Esercizio 7.9, si decompone in un prodotto della forma

$$e = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_u^{\varepsilon_u},$$

ove gli esponenti ε_i sono tutti interi non negativi e, per ogni indice i, si ha $\varepsilon_i \le \alpha_i$ e $\varepsilon_i \le \beta_i$. Segue che, per ogni indice i, $\varepsilon_i \le \gamma_i$. Ciò, in base all'Esercizio 7.9, implica che e divide d. Ciò prova che d è un massimo comune divisore di a e b.
La parte relativa al minimo comune multiplo è lasciata al lettore.

Esercizio 7.11* Siano a, b interi maggiori di 1. Provare che a, b sono coprimi se e solo se non hanno fattori primi in comune.

Esercizio 7.12* Siano $a_1, ..., a_r$ numeri interi non nulli. Provare che

(a) un intero b è un multiplo comune di $a_1, ..., a_r$ se e solo se $\mathrm{mcm}(a_1, ..., a_r) \mid b$;

(b) se $a_1, ..., a_r$ sono a due a due coprimi, allora $\mathrm{mcm}(a_1, ..., a_r) = |a_1| \cdots |a_r|$.