Considerazioni iniziali.

L'aritmetica è stata nel corso della storia uno dei capitoli fondamentali per l'insegnamento della Matematica (Elementi di Euclide libri VII VIII e IX)
L'aritmetica è insegnata fin dalle scuole elementari ed è l'argomento che almeno nella sua parte applicativa è abbastanza conosciuto dai ragazzi che arrivano in prima superiore.

Nella scuola di oggi:
elementari : algoritmi di calcolo manuale delle 4 operazioni sfruttando la posizione delle cifre
medie: Numeri primi, Teorema fondamentale dell'aritmetica, mcm, MCD, operazioni con le frazioni, potenze, radice quadrata, basi numeriche.
Superiori: ripasso, spesso superficiale delle conoscenze delle scuole medie. (le conoscenze delle medie non vengono integrate con l'algebra studiate alle superiori)

NOTA: spesso i ragazzi che abbiamo in classe ragionano per compartimenti stagni. Per fortuna che i ragazzi coinvolti nelle gare di matematica non sono così.

Alcuni esercizi sulla notazione posizionale e sulle scritture in base diversa da 10.

TEOREMA FONDAMENTALE DELL'ARITMETICA
Ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi. Tale fattorizzazione è unica.

Dimostrazione.

- esistenza
Dimostrazione per induzione
Sia $P(n)$ = { i numeri naturali compresi tra 2 ed n sono fattorizzabili in numeri primi }

Base dell'induzione:
Ovviamente $P(2)$ è vera visto che 2 è un numero primo.

Passo dell'induzione:
Supponiamo vera $P(n)$
Consideriamo $n+1$, se $n+1$ è primo, allora è già scomposto in fattori primi,
altrimenti $n+1$ è divisibile per un numero primo, quindi $n+1 = p \cdot m$. Ora m è scomponibile in fattori primi (per l'ipotesi induttiva) e quindi $n+1$ è scomponibile in fattori primi.

- unicità
Supponiamo per assurdo esistano dei numeri naturali che possiedano due scomposizioni in fattori primi diverse, e sia n il più piccolo di tutti (esiste per il principio del buon ordinamento)
e siano le due fattorizzazioni diverse:

$n = p_1 p_2 p_3 \dots p_s$ (supponiamo $p_1 \le p_2 \le p_3 \le \dots \le p_s$)
$n = q_1 q_2 q_3 \dots q_t$ (supponiamo $q_1 \le q_2 \le q_3 \le \dots \le q_t$)

Osserviamo che $p_1 \neq q_1$,

infatti se fosse $p_1 = q_1$, avrei che $n' = \frac{n}{p_1} = p_2 p_3 \dots p_s = q_2 q_3 \dots q_t < n$ contro l'ipotesi che n sia il più piccolo intero ad essere fattorizzabile in più di un modo.

Supponiamo sia $p_1 < q_1$:

considero il numero
$m = n - p_1 q_2 q_3 \dots q_t = q_1 q_2 q_3 \dots q_t - p_1 q_2 q_3 \dots q_t = (q_1 - p_1) q_2 q_3 \dots q_t < n$

Ora $q_1 - p_1$ potrebbe non essere primo e quindi avrà una sua fattorizzazione (visto che è più piccolo di n sarà unica) dove p_1 non vi potrà comparire: infatti se $q_1 - p_1 = a \cdot p_1$, sarebbe $q_1 = a \cdot p_1 + p_1 = (a+1) p_1$ e q_1 non sarebbe un fattore primo.
Quindi p_1 non potendo essere nessuno tra q_2, q_3, … , q_t non compare nella fattorizzazione di m.

Riprendiamo in mano m:
$m = n - p_1 q_2 q_3 \dots q_t = p_1 p_2 p_3 \dots p_s - p_1 q_2 q_3 \dots q_t = p_1 (p_2 p_3 \dots p_s - q_2 q_3 \dots q_t)$

Qualunque sia la fattorizzazione di $p_2 p_3 \dots p_s - q_2 q_3 \dots q_t$, abbiamo trovato una fattorizzazione di m che contiene p_1. Abbiamo dunque due fattorizzazioni diverse per $m < n$, ma questo è assurdo.

2 esercizi sulla fattorizzazione di un numero.

CONSIDERAZIONI SULLA FATTORIZZAZIONE DI UN NUMERO

Assegnato un numero k, la cui scomposizione in fattori primi sia:
$k = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$

Calcolare i divisori di k:

Un qualunque divisore dovrà essere nella forma: $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}$ con $0 \le \beta_i \le \alpha_i$.

Per ciascun β_i avremo $\alpha_i + 1$ possibili scelte, quindi in totale ci saranno:

$d(k) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_n + 1)$ divisori.

Esercizi sui divisori.

Alle scuole medie viene spiegato un modo per calcolare il MCD, i ragazzi ne imparano “da soli” un altro. L’algoritmo di Euclide per il calcolo del MCD spesso rimane sconosciuto.

Ancora sulla divisione: la divisione intera (cioè quella con resto zero)

Due numeri di dicono primi tra loro (o co-primi) se il MCD tra i due numeri è 1.

LA FUNZIONE DI EULERO
Definiamo per ogni $n \in N$
$\varphi(n) =$ numero di interi $< n$ coprimi con n

Si osserva che $\varphi(1) = 1$
se p è primo $\varphi(p) = p - 1$
se $MCD(a,b) = 1$ allora $\varphi(ab) = \varphi(a)\varphi(b)$

Osserviamo che un numero è coprimo con ab se e solo se è coprimo sia con a che con b.
Infatti, dato un x coprimo con ab, questo non ha fattori in comune con ab, e quindi non ha fattori in comune né con a né con b;
viceversa, se x è coprimo con a e con b, ed esistesse un primo p che divide sia ab che x, p dovrebbe dividere, per il lemma di Euclide, almeno uno tra a e b, e quindi x non può esser coprimo con entrambi.

Si dimostra che $\varphi(p^k) = (p-1)p^{k-1}$
Infatti, immaginiamo di scrivere tutti i numero da 1 a p^k, ne abbiamo scritti p^k. Ora tutti i multipli di p sono da togliere:
$1,2,3...,p,.....2p.....3p.....p^{k-1} \cdot p$
Ne abbiamo da togliere p^{k-1}.
$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Si può quindi calcolare $\varphi(n)$ conoscendo la fattorizzazione di n:
infatti:

se $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_n}$

$\varphi(n) = (p_1 - 1)p_1^{k-1}(p_2 - 1)p_2^{k-1}....$

Che può essere riscritta:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...$$

1 esercizio sulla funzione di Eulero