La funzione φ di Eulero

Sia n un numero naturale e sia $\mathbf{Z}_n$ l'anello degli interi modulo n. Scriviamo $\overline{a}$ per la classe di congruenza modulo n di a. Se vogliamo enfatizzare il modulo n, indichiamo $\overline{a}$ anche con $a \pmod n$. Abbiamo che

$$\mathbf{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Sia $\mathbf{Z}_n^*$ il sottoinsieme di $\mathbf{Z}_n$ formato dalle classi $\bar{a} \in \mathbf{Z}_n$ *invertibili* rispetto al prodotto, cioè

$$\exists \bar{a}^{-1} \in \mathbf{Z}_n \quad : \quad \bar{a} \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot \bar{a} = \overline{1}.$$

Ciò accade se e solo se $\mathrm{mcd}(a, n) = 1$, per cui

$$\mathbf{Z}_n^* = \{\overline{a} \in \mathbf{Z}_n : \mathrm{mcd}(a, n) = 1\}.$$

La funzione di Eulero $\varphi\colon \mathbf{N} \to \mathbf{N}$ è per definizione la funzione il cui valore su un intero positivo n è la cardinalità dell'insieme $\mathbf{Z}_n^*$:

$$\varphi(n) = \#\mathbf{Z}_n^*.$$

Il risultato principale di questa nota è la seguente formula per $\varphi(n)$.

Teorema. *Sia n un numero naturale. Allora si ha che*

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}),$$

dove p varia fra i divisori primi p di n.

Ad esempio, se $n = 7020 = 2^2 \cdot 3^3 \cdot 5 \cdot 13$, vale

$$\varphi(7020) = 7020(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{13}) = 1728.$$

Dim. Distinguiamo diversi casi:

• Sia p un numero primo. Allora $\varphi(p) = p - 1$.
Per ogni $a \in \mathbf{Z}$, si ha infatti che $\mathrm{mcd}(a, p) \neq 1$ se e solo se p divide a e quindi se e solo se $a \equiv 0 \pmod p$. In altre parole, l'insieme $\mathbf{Z}_p^*$ è uguale a $\mathbf{Z}_p$ privato dell'elemento $\overline{0}$.

• Sia p un numero primo e sia m un numero naturale. Allora

$$\varphi(p^m) = p^m(1 - \frac{1}{p}).$$

Un numero $a \in \mathbf{Z}$ soddisfa $\mathrm{mcd}(a, p^m) = 1$ se e solo se p non divide a. Un elemento $\overline{a} \in \mathbf{Z}_{p^m}$ è quindi invertibile se e solo se p non divide a. Siccome esattamente uno ogni p elementi di

$$\mathbf{Z}_{p^m} = \{\overline{1}, \ldots, \overline{p}, \ldots, \overline{2p}, \ldots, \overline{3p}, \ldots\ldots, \overline{p^m - 1}, \overline{p^m} = \overline{0}\}$$

è divisibile per p, vediamo che $\frac{1}{p}p^m$ elementi di $\mathbf{Z}_{p^m}$ *non* sono invertibili. Il numero di elementi invertibili è quindi uguale a $p^m - \frac{1}{p}p^m$.

• Siano $l, m \in \mathbf{Z}$ due interi che soddisfano $\mathrm{mcd}(l, m) = 1$. Allora si ha che

$$\varphi(lm) = \varphi(l)\varphi(m).$$

Questo fatto segue dal Teorema Cinese del Resto e verrà dimostrato a parte nella Proposizione qui di seguito.

Facciamo vedere ora che le tre proprietà suddette ci permettono di calcolare $\varphi(n)$ per ogni numero naturale n. Scriviamo

$$n = p_1^{k_1} p_2^{k_2} \dots p_\alpha^{k_\alpha},$$

dove $p_1, p_2, \dots, p_\alpha$ sono numeri primi distinti a gli esponenti $k_1, k_2, \dots, k_\alpha$ sono interi positivi. Si ha quindi che $p_i^{k_i}$ divide n, mentre $p_i^{k_i+1}$ non divide n. Poiché le potenze $p_i^{k_i}$ e $p_j^{k_j}$ non hanno fattori comuni per $i \neq j$, vale

$$\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_\alpha^{k_\alpha}).$$

Per ogni $i = 1, \dots, \alpha$ vale

$$\varphi(p_i^{k_i}) = p_i^{k_i}(1 - \frac{1}{p_i}),$$

da cui segue che

$$\varphi(n) = p_1^{k_1}(1 - \frac{1}{p_1}) \cdot p_2^{k_2}(1 - \frac{1}{p_2}) \cdot \dots \cdot p_\alpha^{k_\alpha}(1 - \frac{1}{p_\alpha}) = n \prod_{p|n}(1 - \frac{1}{p}),$$

dove p varia fra i divisori *primi* distinti di n, come richiesto.

Lemma. *Siano $n, m \in \mathbf{Z}$ due interi che soddisfano* $\mathrm{mcd}(n, m) = 1$. *Allora per ogni $a \in \mathbf{Z}$ abbiamo che n e m dividono a se e solo se il prodotto nm divide a.*

Dim. Se nm divide a, allora è chiaro che sia n che m dividono a. Supponiamo adesso che n e m dividano a. Esistono quindi $r, s \in \mathbf{Z}$ tali che $a = nr$ e $a = ms$. Siccome $\mathrm{mcd}(n, m) = 1$, per il Teorema di Bézout esistono due interi $x, y \in \mathbf{Z}$ tali che $xn + ym = 1$. Vediamo che

$$a = a(xn + ym) = ms(xn) + nr(ym) = (sx + yr)nm,$$

da cui nm divide a, come richiesto.

Proposizione. *Siano $n, m \in \mathbf{Z}$ due interi che soddisfano* $\mathrm{mcd}(n, m) = 1$. *Allora valgono i seguenti fatti:*
(a) l'applicazione $f : \mathbf{Z}_{nm} \longrightarrow \mathbf{Z}_n \times \mathbf{Z}_m$, data da $\bar{x} \pmod{nm} \mapsto (\bar{x} \pmod{n}, \bar{x} \pmod{m})$, è una biiezione.
(b) l'applicazione $f : \mathbf{Z}^*_{nm} \longrightarrow \mathbf{Z}^*_n \times \mathbf{Z}^*_m$ data da $(\bar{x} \pmod{nm} \mapsto (\bar{x} \pmod{n}, \bar{x} \pmod{m}))$, è una biiezione. In particolare

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Dim. (a) Poiché gli insiemi $\mathbf{Z}_{nm}$ e $\mathbf{Z}_n \times \mathbf{Z}_m$ hanno la stessa cardinalità (vale a dire nm), basta dimostrare che f è iniettiva. Siano quindi $\bar{x} \pmod{nm}$ e $\bar{y} \pmod{nm}$ due elementi di $\mathbf{Z}_{nm}$ e supponiamo che $f(\bar{x} \pmod{nm}) = f(\bar{y} \pmod{nm})$. Questo vuol dire che

$$(\bar{x} \pmod{n}, \bar{x} \pmod{m}) = (\bar{y} \pmod{n}, \bar{y} \pmod{m})$$

e quindi

$$\bar{x} \equiv \bar{y} \pmod{n}, \quad \text{e} \quad \bar{x} \equiv \bar{y} \pmod{m}.$$

Dunque, sia n che m dividono $x - y$ e, poiché $\mathrm{mcd}(n, m) = 1$, per il Lemma anche nm divide $x - y$. In altre parole, abbiamo che $\bar{x} \equiv \bar{y} \pmod{nm}$ e da ciò segue l'iniettività di f. *Questo è anche il contenuto del Teorema Cinese del Resto.*

(b) Consideriamo adesso la restrizione dell'applicazione f al sottoinsieme $\mathbf{Z}^*_{nm}$ di $\mathbf{Z}_{nm}$. Se la classe $\bar{x} \pmod{nm}$ sta in $\mathbf{Z}^*_{nm}$, allora si ha che $\mathrm{mcd}(x, nm) = 1$. Questo implica che $\mathrm{mcd}(x, n) = 1$ e che $\mathrm{mcd}(x, m) = 1$. Per ogni elemento $\bar{x} \pmod{nm}$ in $\mathbf{Z}^*_{nm}$, abbiamo quindi che $\bar{x} \pmod{n}$ sta nel sottoinsieme $\mathbf{Z}^*_n$ di $\mathbf{Z}_n$ e $\bar{x} \pmod{m}$

sta nel sottoinsieme $\mathbf{Z}_m^*$ di $\mathbf{Z}_m$. In altre parole, l'immagine della *restrizione di f a $\mathbf{Z}_{nm}^*$* è contenuta nel sottoinsieme $\mathbf{Z}_n^* \times \mathbf{Z}_m^*$ di $\mathbf{Z}_n \times \mathbf{Z}_m$.
Dal punto (a) abbiamo che f è iniettiva ed in particolare *restrizione di f a $\mathbf{Z}_{nm}^*$* è iniettiva. Dimostriamo ora che tale restrizione è anche suriettiva su $\mathbf{Z}_n^* \times \mathbf{Z}_m^*$. Consideriamo un elemento arbitrario di $\mathbf{Z}_n^* \times \mathbf{Z}_m^*$. Per il punto (a) sappiamo che esso è della forma $(\bar{x} \pmod n, \bar{x} \pmod n)$, per qualche $\bar{x} \pmod{nm}$ in $\mathbf{Z}_{nm}$. Resta da far vedere che in realtà la classe $\bar{x} \pmod{nm}$ appartiene a $\mathbf{Z}_{nm}^*$, ossia che vale $\mathrm{mcd}(x, mn) = 1$. Il fatto che che $\mathrm{mcd}(x, n) = 1$ e $\mathrm{mcd}(x, m) = 1$ implica che anche $\mathrm{mcd}(x, mn) = 1$. Dunque $\bar{x} \pmod{nm}$ è contenuto in $\mathbf{Z}_{nm}^*$ ed $f : \mathbf{Z}_{nm}^* \longrightarrow \mathbf{Z}_n^* \times \mathbf{Z}_m^*$ è suriettiva.

Poiché i due insiemi $\mathbf{Z}_{nm}^*$ e $\mathbf{Z}_n^* \times \mathbf{Z}_m^*$ hanno lo stesso numero di elementi, abbiamo che $\#\mathbf{Z}_{nm}^* = \varphi(nm)$ e $\#(\mathbf{Z}_n^* \times \mathbf{Z}_m^*) = \#\mathbf{Z}_n^* \cdot \#\mathbf{Z}_m^* = \varphi(n)\varphi(m)$, come richiesto.

Esercizi.

1. Calcolare $\varphi(150)$ e $\varphi(2^8 \cdot 3^5 \cdot 7^{10})$.
   Sol. Poiché $150 = 2 \cdot 3 \cdot 5^2$, abbiamo
   $$\varphi(150) = 150(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 40.$$
   Analogamente
   $$\varphi(2^8 \cdot 3^5 \cdot 7^{10}) = 2^8 \cdot 3^5 \cdot 7^{10}(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7}) = 3^5 \cdot 2^9 \cdot 7^9.$$
2. *Formula di Gauss.* Sia n un numero naturale. Dimostrare che $\sum_{d|n} \varphi(d) = n$, dove d varia fra i divisori positivi di n.
   Dim. Scriviamo
   $$\mathbf{Z}_n = \bigcup_{d|n} \{\bar{x} \in \mathbf{Z}_n \mid gcd(x, n) = d\}$$
   e calcoliamo la cardinalità dell'insieme $\{\bar{x} \in \mathbf{Z}_n \mid gcd(x, n) = d\}$. Sia $0 < x < n$. Abbiamo che
   $$gcd(x, n) = d \;\Leftrightarrow\; gcd(\frac{x}{d}, \frac{n}{d}) = 1 \;\Leftrightarrow\; \frac{\bar{x}}{d} \in \mathbf{Z}_{\frac{n}{d}}^*.$$
   Dunque la cardinalità cercata è $\varphi(\frac{n}{d})$, da cui segue che
   $$n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d).$$
3. Calcolare $\varphi(10!)$ e $\varphi(10001)$.
4. Sia n un numero naturale e sia p un primo tale che p divide n, ma p^2 non divide n.
   (a) Verificare che $\varphi(p)$ divide $\varphi(n)$;
   (b) Verificare che $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$.
5. Determinare gli interi positivi n per cui si ha $\varphi(n) = 1$. Stessa domanda per $\varphi(n) = 2$.