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, scriviamo anche $a \pmod{n}$ per la classe di congruenza $\overline{a}$. Abbiamo che

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

Sia $\mathbf{Z}_n^*$ il sottoinsieme di $\mathbf{Z}_n$ degli elementi *invertibili*. Abbiamo quindi che

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

Definiamo la funzione φ di Eulero come $\varphi(n) = \#\mathbf{Z}_n^*$. In altre parole, abbiamo che

$$\varphi(n) = \#\{a \in \mathbf{Z} : 0 < a \leq n \text{ e } \mathrm{mcd}(a, n) = 1\}.$$

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.

Per esempio, se prendiamo $7020 = 2^2 \cdot 3^3 \cdot 5 \cdot 13$, vale

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

È facile calcolare $\varphi(p)$, quando p è un numero primo. Per ogni $a \in \mathbf{Z}$, si ha infatti che $\mathrm{mcd}(a, p) = 1$ 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 $\overline{0}$. Ne segue che $\varphi(p) = p-1$. Dimostriamo adesso un risultato simile per una *potenza* di un numero primo.

Proposizione 1. *Sia p un numero primo e sia m un numero naturale. Allora si ha che*

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

Dimostrazione. 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 su ogni p elementi di

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

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

Lemma 2. *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.*

Dimostrazione. 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 3. *Siano $n, m \in \mathbf{Z}$ due interi che soddisfano* $\mathrm{mcd}(n, m) = 1$. *Allora l'applicazione*

$$f : \mathbf{Z}_{nm} \quad \longrightarrow \quad \mathbf{Z}_n \times \mathbf{Z}_m,$$

data da $x \pmod{nm} \mapsto (x \pmod{n}, x \pmod{m})$, *è una biezione.*

Dimostrazione. Siccome 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 una iniezione. Siano quindi $x \pmod{nm}$ e $y \pmod{nm}$ due elementi di $\mathbf{Z}_{nm}$ e supponiamo che $f(x \pmod{nm}) = f(y \pmod{nm})$. Questo vuol dire che $(x \pmod{n}, x \pmod{m}) = (y \pmod{n}, y \pmod{m})$ e quindi

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

In altre parole, abbiamo che sia n che m dividono $x - y$. Siccome si ha che $\mathrm{mcd}(n, m) = 1$, il Lemma 2 implica che nm divide $x - y$. In altre parole, abbiamo che $x \equiv y \pmod{nm}$ e questo dimostra l'iniettività di f.

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

Proposizione 4. *Siano $n, m \in \mathbf{Z}$ due interi che soddisfano* $\mathrm{mcd}(n, m) = 1$. *Allora l'applicazione*

$$f : \mathbf{Z}_{nm}^* \quad \longrightarrow \quad \mathbf{Z}_n^* \times \mathbf{Z}_m^*$$

data da $(x \pmod{nm} \mapsto (x \pmod{n}, x \pmod{m})$, *è una biiezione.*

Dimostrazione. Dalla Prop. 3 segue subito che f è iniettiva. Basta quindi dimostrare che f è suriettiva. Consideriamo quindi un elemento arbitrario di $\mathbf{Z}_n^* \times \mathbf{Z}_m^*$. Per la Prop. 3 sappiamo che esso è della forma $(x \pmod{n}, x \pmod{n})$, per qualche $x \pmod{nm}$ in $\mathbf{Z}_{nm}$. Resta da far vedere che in realtà $x \pmod{nm}$ in $\mathbf{Z}_{nm}^*$. Si ha che $\mathrm{mcd}(x, n) = 1$ e $\mathrm{mcd}(x, m) = 1$. Questo implica banalmente che anche $\mathrm{mcd}(x, mn) = 1$. Dunque $x \pmod{nm}$ è contenuto in $\mathbf{Z}_{nm}^*$ ed f è suriettiva.

Corollario 5. *Siano $n, m \in \mathbf{Z}$ due interi che soddisfano* $\mathrm{mcd}(n, m) = 1$. *Allora si ha che*

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

Dimostrazione. Siccome l'applicazione f della Prop. 4 è una biiezione, 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 $\#(\mathbf{Z}_n^* \times \mathbf{Z}_m^*) = \#\mathbf{Z}_n^* \cdot \#\mathbf{Z}_m^* = \varphi(n)\varphi(m)$.

Dimostrazione del Teorema. Sia n un numero naturale e sia

$$n \quad = \quad \prod_{p|n} p^{a(p)}$$

la fattorizzazione di n come prodotto di potenze di numeri primi distinti. Si ha quindi che $p^{a(p)}$ divide n, mentre $p^{a(p)+1}$ non divide n. Poiché le potenze $p^{a(p)}$ non hanno fattori comuni, il Cor. 5 implica che

$$\varphi(n) \quad = \quad \prod_{p|n} \varphi(p^{a(p)}).$$

Per la Prop. 1 abbiamo che $\varphi(p^{a(p)}) = p^{a(p)}(1 - \frac{1}{p})$ e quindi

$$\begin{aligned} \varphi(n) &= \prod_{p|n} p^{a(p)}(1 - \frac{1}{p}), \\ &= \prod_{p|n} p^{a(p)} \cdot \prod_{p|n}(1 - \frac{1}{p}), \\ &= n \prod_{p|n}(1 - \frac{1}{p}), \end{aligned}$$

come richiesto.

Esercizi.

1. Calcolare $\varphi(10!)$ e $\varphi(10001)$.
2. Dimostrare che $\sum_{d|n} \varphi(d) = n$. (nella sommatoria d varia fra i divisori positivi di n).
3. Determinare gli interi positivi n per cui si ha $\varphi(n) = 1$. Stessa domanda per $\varphi(n) = 2$.
4. Dimostrare che l'insieme $\{\frac{\varphi(n)}{n} : n \in \mathbf{Z}_{>0}\}$ è *denso* nell'intervallo $[0, 1]$.