

Part A: More properties of $\varphi(n)$.Thm 2.4

$$\varphi(n) = \begin{cases} n \prod_{p|n} (1 - 1/p) & \text{if } n > 1, \\ 1 & \text{if } n = 1. \end{cases}$$

Proof

It's clear for $n=1$, so assume $n > 1$. Write

$$n = \prod_{i=1}^r p_i^{a_i} \text{ with } a_i > 0 \text{ for } 1 \leq i \leq r.$$

By expanding the product,

$$\prod_{p|n} (1 - 1/p) = \prod_{i=1}^r (1 - 1/p_i)$$

$$= 1 - \sum_{i=1}^r \frac{1}{p_i} + \sum_{\substack{i,j=1 \\ i \neq j}}^r \frac{1}{p_i p_j} - \sum_{\substack{i,j,k=1 \\ i \neq j \neq k \neq i}}^r \frac{1}{p_i p_j p_k} + \dots + \frac{(-1)^r}{p_1 p_2 \dots p_r}$$

$$= \sum_{\substack{d|n \\ d \text{ is square-free}}} \frac{(-1)^{\# \text{ of factors of } d}}{d}$$

$$= \sum_{d|n} \mu(d)/d.$$

Now multiply both sides by n , and use Thm. 2.3, which says

$$\sum_{d|n} \mu(d) n/d = \varphi(n). \quad \square$$

Next, we have

(2)

Thm. 2.5. Let $m, n, \alpha, a, b \in \mathbb{Z}_+$.

(a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for p prime.

(b) $\varphi(mn) = \varphi(m)\varphi(n) \cdot \frac{(m,n)}{\varphi((m,n))}$.

(c) If $(m,n)=1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

(d) $a|b \Rightarrow \varphi(a)|\varphi(b)$.

(e) (i) $\varphi(n)$ is even for $n \geq 3$.

(ii) If r distinct odd primes divide n , for some $r \geq 0$, then $2^r | \varphi(n)$.

Proof.

(a) Thm. 2.4 with $n = p^\alpha$.

(b) Note that $p|mn \Rightarrow p|m$ or $p|n$. Also,
 $p|m$ and $p|n \Leftrightarrow p|(m,n)$.
 Then by Thm. 2.4,

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

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

$$= \frac{[\varphi(m)/m] \cdot [\varphi(n)/n]}{\varphi((m,n))/(m,n)}.$$

→ The numerator counts those p with $p|m$ and $p|n$ twice, so cancel once

Now multiply through by mn .

(c) By (b) with $(m, n) = 1$.

(d) We use induction on b . If $b = 1$, then $a|b \Rightarrow a = 1$, and the desired result is clear.

Now assume that the result is true for $1 \leq b \leq k-1$. We wish to deduce that $a|k \Rightarrow \phi(a) | \phi(k)$.

This is clear if $a = 1$. So assume $a > 1$, and $a|k$. Write $k = ac$. By part (b) above,

$$\phi(k) = \phi(ac) = \phi(a)\phi(c) \cdot \frac{(a, c)}{\phi((a, c))}. \quad (*)$$

Now since $a > 1$, we have $c < k$; also, $(a, c) | c$, so by induction, $\phi((a, c)) | \phi(c)$. So by (*),

$$\phi(k) = \phi(a) \cdot (a, c) \cdot l \text{ for some } l \in \mathbb{Z}_+.$$

So $\phi(a) | \phi(k)$ as required. \square

(e) First assume $n = 2^\alpha$ for some $\alpha \in \mathbb{Z}_+$. Then by (a), $\phi(n) = 2^\alpha - 2^{\alpha-1} = 2^{\alpha-1}$. So (e)(i) holds (since $2^\alpha \geq 3 \Rightarrow \alpha \geq 2$), and (e)(ii) holds with $r = 0$.

Next, suppose $n = 2^\alpha \prod_{i=1}^r p_i^{a_i}$ where each p_i is odd, and $\alpha \geq 0$, $a_i \geq 0$ for $1 \leq i \leq r$. By parts (a) and (c) above,

$$\phi(n) = (2^\alpha - 2^{\alpha-1}) \prod_{i=1}^r (p_i^{a_i} - p_i^{a_i-1}).$$

Each term $p_i^{a_i} - p_i^{a_i-1}$ is even. \square

Part B: Dirichlet products (a.k.a. "splat").

Definition: If f and g are arithmetic functions, we define the Dirichlet product $f * g$ ("f splat g") by

$$f * g(n) = \sum_{d|n} f(d) g(n/d).$$

For example, if we define the unit function u by $u(n) = 1 \ \forall n$, the identity function $I(n)$ by $I(n) = \lfloor 1/n \rfloor \ \forall n$, and the function N by $N(n) = n \ \forall n$, then we have

- (i) $\mu * u = I$ (Thm. 2.1),
- (ii) $\varphi * u = N$ (Thm. 2.2)
- (iii) $\mu * N = \varphi$ (Thm. 2.3)

Parts (ii) and (iii) exemplify Möbius inversion; see Thm. 2.9 below.