ARITHMETIC FUNCTIONS

M. ATIF ZAHEER

Contents

1. Basic examples

An *arithmetic function* is a complex-valued function defined on $\mathbb{N}$, i.e., a sequence of complex numbers. While the class of arithmetic functions is broad, namely $\mathbb{C}^{\mathbb{N}}$, we will restrict our attention to only those of number-theoretic significance

Below are some commonly occurring arithmetic functions.

- The *identity function* e is defined as $e(n) = \lfloor 1/n \rfloor$, i.e., $e(1) = 1$ and $e(n) = 0$ for $n > 1$. It is called so because, as we will see later, it acts as the identity element in a group of arithmetic functions.
- For any $\alpha \in \mathbb{C}$, the *power function* N^α is defined as $N^\alpha(n) = n^\alpha$. We denote N^0 by 1 and call it the *unit function*
- For $n \in \mathbb{N}$, $\Omega(n)$ is defined to be the total number of prime factors of n counted with multiplicity. We can write this in summation notation as
$$\Omega(n) = \sum_{p^k \mid n} 1 = \sum_{p^k \| n} k.$$
It is sometimes called *big omega* function.
- For $n \in \mathbb{N}$, $\omega(n)$ is defined to be the number of prime factors of n. We can write it in summation notation as
$$\omega(n) = \sum_{p \mid n} 1.$$
It is usually called *small omega* function.
- The *Liouville function*, denoted λ, is defined as $\lambda(n) = (-1)^{\Omega(n)}$.

We now turn our attention to some more interesting arithmetic functions that occur frequently in (analytic) number theory.

The *Möbius function*, denoted μ, is defined as follows
$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 \dots p_k, \text{ where } p_1, \dots, p_k \text{ are distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

Note that μ is the signed characteristic function of squarefree positive integers. The definition of μ may seem unmotivated at this point but later we will see later that μ is the inverse of the unit function 1 in some group of arithmetic functions. Given that such an inverse exists one can easily recover this definition.

The Möbius function μ has an intimate connection with one of the most important function in (analytic) number theory, namely Riemann zeta function $\zeta(s)$. For instance, the estimate $M(x) = \sum_{n \leqslant x} \mu(n) \ll x^{1/2+\epsilon}$ implies the Riemann Hypothesis (RH), one of the most notoriously difficult problem in all of mathematics. In fact, the convergence of the Dirichlet series $\sum_{n=1}^{\infty} \mu(n) n^{-s}$ for every s with $\mathrm{Re}(s) > 1/2$ also implies RH. We begin a simple result about the divisor sum of μ.

Proposition 1.1. *If $n \geqslant 1$, then*

$$\sum_{d \mid n} \mu(d) = e(n).$$

Proof. If $n = 1$, then the formula clearly holds as $\mu(1) = 1$. Now suppose that $n = \prod_{i=1}^{k} p_i^{a_i}$. Because $\mu(d)$ is nonzero if and only if d is squarefree, we can restrict the sum to divisors of the form $\prod_{i \in I} p_i$, where I is a subset of $\{1, \ldots, k\}$. Hence, we get

$$\sum_{d \mid n} \mu(d) = \sum_{I \subset \{1, \ldots, n\}} \mu\left(\prod_{i \in I} p_i\right) = \sum_{I \subset \{1, \ldots, n\}} (-1)^{|I|}.$$

Since for each $0 \leqslant r \leqslant k$ there are precisely $\binom{k}{r}$ subsets of $\{1, \ldots, k\}$ containing r elements, we therefore deduce that

$$\sum_{d \mid n} \mu(d) = \sum_{r=0}^{k} \binom{k}{r} (-1)^r = (-1+1)^k = 0. \qquad \square$$

$\square$

The *Euler's totient function* φ is defined at n to be the number of positive integers not exceeding n that are relatively prime to n, i.e.,

$$\varphi(n) = |\{1 \leqslant k \leqslant n : (k, n) = 1\}|.$$

We can rewrite $\varphi(n)$ in the summation notation as

$$\varphi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1.$$

Proposition 1.2. *If $n \geqslant 1$, then*

$$\sum_{d \mid n} \varphi(d) = n.$$

Proof. The key idea behind the proof is to partition the set $\{1, \ldots, n\}$ into subsets $A_d = \{1 \leqslant k \leqslant n : (k, n) = d\}$, where d is a divisor of n, and to note that there is a one-to-one bijection between elements of A_d and integers $1 \leqslant r \leqslant n/d$ satisfying $(r, n/d) = 1$. This then implies that

$$n = \sum_{d \mid n} |A_d| = \sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d). \qquad \square$$

$\square$

The next result provides us with a relationship between μ and φ.

PROPOSITION 1.3. *If $n \geqslant 1$, then we have*

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}. \tag{1.1}$$

PROOF. We use the formula for the divisor sum of μ to obtain

$$\varphi(n) = \sum_{k=1}^{n} e((k,n)) = \sum_{k=1}^{n} \sum_{d|(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d)$$

Changing the order of summation we obtain

$$\varphi(n) = \sum_{d|n} \sum_{\substack{k=1 \\ d|k}}^{n} \mu(d) = \sum_{d|n} \mu(d) \sum_{\substack{k=1 \\ d|k}}^{n} 1 = \sum_{d|n} \mu(d) \frac{n}{d}. \qquad \square$$

$\square$

Next we obtain a nice product formula for $\varphi(n)$.

PROPOSITION 1.4. *For $n \geqslant 1$ we have*

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

PROOF. If $n = 1$, then the product on the right hand side is empty and so the formula trivially holds. Now let $p_1, \ldots, p_k$ be the prime divisors of n let $[k] := \{1, \ldots, k\}$. Then expanding the product, we get

$$\begin{aligned} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) &= \sum_{I \subset [k]} \prod_{i \in I} \left(-\frac{1}{p_i}\right) = \sum_{I \subset [k]} \frac{(-1)^{|I|}}{\prod_{i \in I} p_i} \\ &= \sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}. \qquad \square \end{aligned}$$

$\square$

PROPOSITION 1.5. *The Euler's totient function has the following properties:*

(a) $\varphi(p^a) = p^a - p^{a-1}$ *for prime p and $a \geqslant 1$.*
(b) $\varphi(mn) = \varphi(m)\varphi(n)(d/\varphi(d))$*, where $d = (m,n)$.*
(c) $\varphi(mn) = \varphi(m)\varphi(n)$ *if $(m,n) = 1$.*
(d) $n|m$ *implies* $\varphi(n)|\varphi(m)$.
(e) $\varphi(n)$ *is even for $n \geqslant 3$. Moreover, if n has r distinct odd prime factors, then* $2^r|\varphi(n)$.

Proof. Part (a) follows immediately from the product formula. As for part (b) note that

$$
\begin{aligned}
\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1-\frac{1}{p}\right) &= \prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{\substack{p|n\\ p\nmid m}}\left(1-\frac{1}{p}\right) \\
&= \prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)\prod_{\substack{p|n\\ p|m}}\left(1-\frac{1}{p}\right)^{-1} \\
&= \frac{\varphi(m)}{m}\frac{\varphi(n)}{n}\prod_{p|(n,m)}\left(1-\frac{1}{p}\right)^{-1} \\
&= \frac{\varphi(m)}{m}\frac{\varphi(n)}{n}\frac{d}{\varphi(d)},
\end{aligned}
$$

where $d = (m, n)$.

Part (c) follows immediately from part (b).

For part (d) let $n = p_1^{a_1} \cdots p_k^{a_k}$ and $m = p_1^{b_1} \cdots p_k^{b_k}$, where a_i are nonnegative. Because $a_i \leqslant b_i$, we have $\varphi(p_i^{a_i})|\varphi(p_i^{b_i})$ due to part (a). This coupled with the fact that φ is multiplicative (due to part (c)) gives us the desired result.

Finally for part (e) observe that if $n \geqslant 3$ and $n = 2^a$ for some positive integer a then a must be at least 2 and so $\varphi(2^a) = 2^a - 2^{a-1} = 2(2^{a-1} - 2^{a-2})$ is even. Now note that

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

where the factor $n(\prod_{p|n} p)^{-1}$ is an integer. If n is not of the form 2^a, then an odd prime p divides n, and so the factor on the right must be even which implies that $\varphi(n)$ is even. Finally, if n has r distinct odd prime factors then $2^r | \prod_{p|n}(p-1)$ and hence $2^r|\varphi(n)$. $\square$

The *von-Mangoldt function* (usually referred to as simply Mangoldt function), denoted Λ, is defined as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^a \text{ for some prime } p \text{ and integer } a \geqslant 1, \\ 0 & \text{otherwise.} \end{cases}$$

The von-Mangoldt function Λ plays an important role in prime number theory.

2. Dirichlet product

If f and g are two arithmetic functions we define their *Dirichlet product* (or *Dirichlet convolution*) to be the arithmetic function $f * g$ defined as

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

It is easily seen that Dirichlet multiplication is both commutative and associative, i.e., for any arithmetic functions f, g, h we have

$$f * g = g * f \quad \text{and} \quad (f * g) * h = f * (g * h).$$

Moreover, we have $e * f = f$ for any arithmetic function f. Thus the set of all arithmetic functions is a commutative monoid. The next result allows us to characterize arithmetic functions that are invertible under Dirichlet multiplication.

PROPOSITION 2.1. *If f is an arithmetic function with $f(1) \neq 0$, then there is a unique arithmetic function g such that*

$$g * f = f * g = e.$$

The function g is given by

$$g(1) = \frac{1}{f(1)}, \qquad g(n) = -\frac{1}{f(1)} \sum_{\substack{d \mid n \\ d<n}} g(d) f(n/d) \quad \text{for } n > 1.$$

The above result show that the set of all arithmetic functions f satisfying $f(1) \neq 0$ form an abelian group under Dirichlet multiplication.

The Dirichlet multiplication provides a convenient notation to write some of our earlier results in a compact fashion;

$$\mu * 1 = e, \quad \varphi * 1 = N, \quad \varphi = \mu * N.$$

PROPOSITION 2.2 (Möbius inversion formula). *Let f and g be arithmetic functions. Then*

$$f(n) = \sum_{d \mid n} g(d)$$

for every $n \in \mathbb{N}$ if and only if

$$g(n) = \sum_{d \mid n} f(d) \mu(n/d)$$

for every $n \in \mathbb{N}$.

PROOF. Follow immediately by noting that $f = g * 1$ if and only if $g = f * \mu$ which is seen by multiplying by μ (or 1) and using the identity $\mu * 1 = e$. □

3. MULTIPLICATIVE FUNCTIONS

An arithmetic function f is called *multiplicative* if f is not identically zero and

$$f(mn) = f(m) f(n) \quad \text{whenever } (m, n) = 1.$$

A multiplicative function f is called *completely multiplicative* (or *totally multiplicative*) if f is not identically zero and

$$f(mn) = f(m) f(n) \quad \text{for all } m, n.$$

EXAMPLE 3.1. We note some common examples of multiplicative functions.

(a) The power function N^α is completely multiplicative.
(b) The identity function e is completely multiplicative.
(c) The Möbius function μ is multiplicative. However, it is not completely multiplicative as $\mu(4) = 0 \neq 1 = \mu(2)^2$.
(d) The Euler totient function φ is multiplicative. However, it is not completely multiplicative as $\varphi(4) = 2 \neq 1 = \varphi(2)^2$.

PROPOSITION 3.2. *If f is multiplicative, then $f(1) = 1$.*

From this it immediately follows that Λ is not multiplicative as $\Lambda(1) = 0$.

PROPOSITION 3.3. *Let f be an arithmetic function with $f(1) = 1$.*

(a) f is multiplicative if and only if

$$f(p_1^{a_1} \cdots p_k^{a_k}) = f(p_1^{a_1}) \cdots f(p_k^{a_k}),$$

where $p_1, \ldots, p_k$ are distinct primes.

(b) If f is multiplicative, then f is completely multiplicative if and only if

$$f(p^a) = f(p)^a$$

for all primes p and all integers $a \geqslant 1$.

The above result shows that a multiplicative function is uniquely determined by its values on prime powers, and a completely multiplicative function is uniquely determined by its values on primes.

PROPOSITION 3.4. *If f and g are multiplicative, then so is their Dirichlet product $f * g$.*

PROOF. Let m and n be relatively prime integers. Then observe that

$$(f * g)(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right)$$

as every divisor of mn can be uniquely written as ab, where $a|m$ and $b|n$. Using the multiplicativity of f and g we obtain

$$\begin{aligned}(f * g)(mn) &= \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) = \sum_{a|m}\sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right) = (f * g)(m)(f * g)(n). \qquad \square\end{aligned}$$

$\square$

The Dirichlet product of two completely multiplicative functions need not be completely multiplicative. For instance, the divisor function $d = 1 * 1$ is not completely multiplicative as $d(4) = 3 \neq 4 = d(2)^2$ whereas 1 clearly is.

PROPOSITION 3.5. *If f is multiplicative, then so is it's Dirichlet inverse f^{-1}.*

PROOF. Suppose for the sake of contradiction that f^{-1} is not multiplicative. Then there exist positive integers m and n with $(m, n) = 1$ such that

$$f^{-1}(mn) \neq f^{-1}(m)f^{-1}(n).$$

We choose such a pair m and n for which the product mn is the smallest. Since f is multiplicative therefore $f^{-1}(1) = 1/f(1) = 1$ and hence neither m nor n can be 1. In particular, $mn > 1$. By the construction of the product mn, $f(ab) = f(a)f(b)$ for all positive integers a and b with $(a, b) = 1$ and $ab < mn$. It now follows that

$$f^{-1}(mn) = -\sum_{\substack{a|m \\ b|n \\ ab<mn}} f^{-1}(ab)f\left(\frac{mn}{ab}\right) = -\sum_{\substack{a|m \\ b|n \\ ab<mn}} f^{-1}(a)f^{-1}(b)f\left(\frac{m}{a}\right)f\left(\frac{n}{b}\right)$$

Splitting the sum we obtain

$$\begin{aligned}
f^{-1}(mn) &= -f^{-1}(n)\sum_{\substack{a\mid m\\ a<m}} f^{-1}(a)f\left(\frac{m}{a}\right) - f^{-1}(m)\sum_{\substack{b\mid n\\ b<n}} f^{-1}(b)f\left(\frac{n}{b}\right)\\
&\quad - \sum_{\substack{a\mid m\\ a<m}}\sum_{\substack{b\mid n\\ b<n}} f^{-1}(a)f^{-1}(b)f\left(\frac{m}{a}\right)f\left(\frac{n}{b}\right)\\
&= f^{-1}(n)f^{-1}(m) + f^{-1}(m)f^{-1}(n) - f^{-1}(m)f^{-1}(n)\\
&= f^{-1}(m)f^{-1}(n).
\end{aligned}$$

This contradiction proves the result.

Second Proof. Let g be an arithmetic function defined as

$$g(n) = \prod_{p^a\,\|\,n} f^{-1}(p^a).$$

Then g is a multiplicative function by definition and so it suffices to show that $f^{-1} = g$. Note that

$$\begin{aligned}
(g*f)(p^k) &= \sum_{d\mid p^k} g(d)f(p^k/d) = \sum_{i=0}^{k} g(p^i)f(p^{k-i})\\
&= \sum_{i=0}^{k} f^{-1}(p^i)f(p^{k-i}) = \sum_{d\mid p^k} f^{-1}(d)f(p^k/d) = (f^{-1}*f)(p^k) = e(p^k).
\end{aligned}$$

Because $g*f$ and e are both multiplicative functions and agree on prime powers, it follows that $g*f = e$ and so $g = f^{-1}$. □

PROPOSITION 3.6. *Let f be multiplicative. Then f is completely multiplicative if and only if $f^{-1} = \mu f$.*

PROOF. Suppose f is completely multiplicative. Then observe that

$$(f*\mu f)(n) = \sum_{d\mid n} \mu(d)f(d)f\left(\frac{n}{d}\right) = f(n)\sum_{d\mid n}\mu(d) = f(n)e(n) = e(n).$$

Conversely, assume that $f^{-1} = \mu f$. Then observe that

$$\sum_{d\mid n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0$$

for $n > 1$. Let $n = p^a$, where $a \geqslant 1$. Then, we get

$$\mu(1)f(1)f(p^a) + \mu(p)f(p)f(p^{a-1}) = 0.$$

It then follows that

$$f(p^a) = f(p)f(p^{a-1}).$$

This implies that $f(p^a) = f(p)^a$. Thus f is completely multiplicative. □

PROPOSITION 3.7. *If f is a multiplicative arithmetic function then*

$$\sum_{d\mid n} \mu(d)f(d) = \prod_{p\mid n}(1 - f(p)).$$

PROOF. Let $g = 1 * \mu f$. Then g is a multiplicative function. Thus, it suffices to know the value of g at prime powers. We observe that

$$g(p^a) = \sum_{d \mid p^a} \mu(d) f(d) = \mu(1) f(1) + \mu(p) f(p) = 1 - f(p).$$

Hence, we obtain

$$g(n) = \prod_{p \mid n} g(p^a) = \prod_{p \mid n} (1 - f(p)). \qquad \square$$

$\square$

EXERCISES

EXERCISE 1. Show that for every $k \in \mathbb{N}$ there are infinitely many n such that

$$\mu(n+1) = \cdots = \mu(n+k).$$

(Hint: Use Chinese Remainder Theorem.)

EXERCISE 2. Prove that

$$\frac{n}{\varphi(n)} = \sum_{d \mid n} \frac{\mu^2(d)}{\varphi(d)}.$$

EXERCISE 3. Prove that $\varphi(n) \to \infty$ as $n \to \infty$.

EXERCISE 4. Show that $\sigma(n) \leqslant n(\log n + 1)$ for every $n \in \mathbb{N}$.

EXERCISE 5. Show that

$$\frac{n^2}{\zeta(2)} \leqslant \sigma(n)\varphi(n) \leqslant n^2$$

for every $n \in \mathbb{N}$. Conclude that

$$\varphi(n) \geqslant \frac{n}{\zeta(2)(\log n + 1)}$$

EXERCISE 6. Show that $d(n) \ll n^\epsilon$ for every $\epsilon > 0$.

EXERCISE 7. Prove that $\varphi(n) \gg n^{1-\epsilon}$ for every $\epsilon > 0$.

EXERCISE 8. Let us denote $e^{2\pi i \alpha}$ by $e(\alpha)$.

(a) Prove that

$$\frac{1}{q} \sum_{a=1}^{q} e(an/q) = \begin{cases} 1 & \text{when } q \mid n, \\ 0 & \text{when } q \nmid n. \end{cases}$$

(b) The *Ramanujan's sum* $c_q(n)$ is defined as

$$c_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(an/q).$$

Prove that

$$c_q(n) = \sum_{d \mid (q,n)} d\mu(q/d)$$

and conclude that $c_q(n) = O_n(1)$.

(c) Prove that
$$\sigma(n) = \frac{\pi^2 n}{6} \sum_{q=1}^{\infty} \frac{c_q(n)}{q^2}.$$

EXERCISE 9. For a prime p let $\mathcal{A}_p$ denote the set of all positive integers n such that either $n+1 \equiv 0 \pmod{p^2}$ or $n-1 \equiv 0 \pmod{p^2}$.

(a) If $[N]$ denotes the set of positive integers up to N, then show that
$$\left| [N] \cap \bigcup_p \mathcal{A}_p \right| \leqslant 2N \sum_{p \leqslant N} \frac{1}{p^2} + 2\pi(N),$$
where $\pi(x)$ denotes the number of primes up to x (you can assume that $\pi(x)/x \to 0$ as $x \to \infty$).

(b) Prove that
$$\sum_p \frac{1}{p^2} < \frac{1}{4}$$
and conclude that the set of twin squarefree integers have positive density.

EXERCISE 10. Let $Q(x)$ denote the number of squarefree integers up to x.

(a) Show that
$$Q(N) \geqslant N - \sum_p \left\lfloor \frac{N}{p^2} \right\rfloor$$
for every positive integer n.

(b) Justify the relations
$$\sum_p \frac{1}{p^2} < \frac{1}{4} + \sum_{k=1}^{\infty} \frac{1}{(2k+1)^2} < \frac{1}{4} + \frac{1}{4} \sum_{k=1}^{\infty} \frac{1}{k(k+1)} = \frac{1}{2}.$$

(c) Show that $Q(N) > N/2$ for all positive integers N.

(d) Show that every positive integer $n > 1$ can be written as a sum of two squarefree numbers.

SOLUTIONS

SOLUTION 1. Let $p_1, \ldots, p_k$ be distinct primes. Then by the Chinese Remainder Theorem there exist infinitely many positive integers n such that $n \equiv -j \mod p_j^2$ for every $1 \leqslant j \leqslant k$. Thus $p_j^2 | (n+j)$ for every $1 \leqslant j \leqslant k$ and so $n+j$ is not squarefree, i.e., $\mu(n+1) = \cdots = \mu(n+k) = 0$.

SOLUTION 2. Note that
$$\frac{n}{\varphi(n)} = \prod_{p|n} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p|n} \frac{p}{p-1} = \prod_{p|n} \left(1 + \frac{1}{p-1}\right).$$

Expanding the product we get
$$\frac{n}{\varphi(n)} = \sum_{I \subset \{p|n\}} \prod_{p \in I} \frac{1}{p-1} = \sum_{I \subset \{p|n\}} \prod_{p \in I} \frac{1}{\varphi(p)} = \sum_{I \subset \{p|n\}} \frac{1}{\varphi(\prod_{p \in I} p)}.$$

Thus we obtain

$$\frac{n}{\varphi(n)} = \sum_{\substack{d \mid n \\ d \text{ sq. free}}} \frac{1}{\varphi(d)} = \sum_{d \mid n} \frac{\mu(d)^2}{\varphi(d)}.$$

We now present another solution. Let $f = \mu/\varphi$. Note that f is multiplicative and so we have

$$\sum_{d \mid n} \frac{\mu(d)^2}{\varphi(d)} = \sum_{d \mid n} \mu(d) f(d) = \prod_{p \mid n} (1 - f(p)) = \prod_{p \mid n} \left(1 - \frac{\mu(p)}{f(p)}\right) = \prod_{p \mid n} \frac{p}{p-1}$$

due to Proposition 3.7. Since $p^a/\varphi(p^a) = p/(p-1)$ we conclude that

$$\sum_{d \mid n} \frac{\mu(d)^2}{\varphi(d)} = \frac{n}{\varphi(n)}.$$

Solution 3. Let $M > 0$ and let $\varphi(n) \leqslant M$. Take $n = \prod_{i=1}^{k} p_i^{a_i}$. Then we have $\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1) \leqslant M$. This shows that $p_i - 1 \leqslant M$ and $2^{a_i - 1} \leqslant M$ for every i. Hence we have $p_i < M$ and $2^{a_i} \leqslant 2M$ for every i. Thus the exponents a_i are bounded by $\log_2(2M)$. This shows that there are only finitely many positive integers n with $\varphi(n) \leqslant M$. Hence we have $\varphi(n) \to \infty$ as $n \to \infty$.

Solution 4. Note that

$$\sigma(n) = \sum_{d \mid n} d = n \sum_{d \mid n} \frac{1}{d} \leqslant n \sum_{d \leqslant n} \frac{1}{d} \leqslant n \left(\int_1^n \frac{dt}{t} + 1 \right) = n(\log n + 1).$$

Solution 5. Observe that

$$\begin{aligned} \sigma(n)\varphi(n) &= \prod_{p^\alpha \| n} \sigma(p^\alpha)\varphi(p^\alpha) = \prod_{p^\alpha \| n} \left(\frac{p^{\alpha+1} - 1}{p - 1} \right) p^{\alpha - 1}(p - 1) \\ &= \prod_{p^\alpha \| n} (p^{2\alpha} - p^{\alpha - 1}) = n^2 \prod_{p^\alpha \| n} \left(1 - \frac{1}{p^{\alpha+1}} \right). \end{aligned}$$

Note that it is clear that $\sigma(n)\varphi(n) \leqslant n^2$ as each of the factor in the product is < 1. For the lower bound observe that $p^{\alpha+1} \geqslant p^2$ and so we obtain

$$\sigma(n)\varphi(n) \geqslant n^2 \prod_{p^\alpha \| n} \left(1 - \frac{1}{p^2} \right) \geqslant n^2 \prod_{p} \left(1 - \frac{1}{p^2} \right) = \frac{n^2}{\zeta(2)}.$$

Because we know that $\sigma(n) \leqslant n(\log n + 1)$, the desired bound for $\varphi(n)$ immediately follows.

Solution 6. Let $n = p_1^{a_1} \cdots p_k^{a_k}$. Then we have

$$\frac{d(n)}{n^\epsilon} = \prod_{p^a \| n} \frac{a+1}{p^{a\epsilon}} \leqslant \prod_{\substack{p^a \| n \\ p < 2^{1/\epsilon}}} \frac{a+1}{p^{a\epsilon}}$$

for if $p \geqslant 2^{1/\epsilon}$, then $p^\epsilon \geqslant 2$ and so $p^{a\epsilon} \geqslant 2^a \geqslant a + 1$ which gives $(a+1)/p^{a\epsilon} \leqslant 1$. Now observe that

$$\frac{d(n)}{n^\epsilon} \leqslant \prod_{\substack{p^a \| n \\ p < 2^{1/\epsilon}}} \frac{a+1}{2^{a\epsilon}} \leqslant \prod_{\substack{p^a \| n \\ p < 2^{1/\epsilon}}} \frac{a+1}{a\epsilon \log 2}$$

as $2^{a\epsilon} = e^{a\epsilon \log 2} \geqslant a\epsilon \log 2$. Finally we have

$$\frac{d(n)}{n^\epsilon} \leqslant \prod_{p<2^{1/\epsilon}} \frac{2}{\epsilon \log 2} \leqslant \left(\frac{2}{\epsilon \log 2}\right)^{\pi(2^{1/\epsilon})}.$$

This shows that $d(n) \ll_\epsilon n^\epsilon$.

SOLUTION 7. Note that

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \geqslant \frac{n}{2^{\omega(n)}} \geqslant \frac{n}{d(n)} \gg n^{1-\epsilon}$$

as $1 - 1/p \geqslant 1/2$ for every prime p and $d(n) \geqslant 2^{\omega(n)}$ for every $n \in \mathbb{N}$.

We present another solution which involves bounding the product $\prod_{p|n}\left(1 - \frac{1}{p}\right)$ from below. Let n be a positive integer. Then we have

$$\log \prod_{p|n} \left(1 - \frac{1}{p}\right) = \sum_{p|n} \log\left(1 - \frac{1}{p}\right) = -\sum_{p|n} \sum_{m=1}^{\infty} \frac{1}{mp^m} = -\sum_{m=1}^{\infty} \frac{1}{m} \sum_{p|n} \frac{1}{p^m}.$$

Let $p_1 < p_2 < \cdots$ be the sequence of primes. Then for $K > 1$ we have

$$\sum_{p|n} \frac{1}{p^m} \leqslant \sum_{k<K} \frac{1}{p_k^m} + \frac{\omega(n)}{p_K^m}.$$

This then leads to

$$\begin{aligned} \sum_{m=1}^{\infty} \frac{1}{m} \sum_{p|n} \frac{1}{p^m} &\leqslant \sum_{m=1}^{\infty} \frac{1}{m} \sum_{k<K} \frac{1}{p_k^m} + \omega(n) \sum_{m=1}^{\infty} \frac{1}{mp_K^m} \\ &= -\sum_{k<K} \log\left(1 - \frac{1}{p_k}\right) - \omega(n) \log\left(1 - \frac{1}{p_K}\right). \end{aligned}$$

Using the inequality $\omega(n) \leqslant \log_2 n$ we obtain

$$\log \prod_{p|n} \left(1 - \frac{1}{p}\right) \geqslant \sum_{k<K} \log\left(1 - \frac{1}{p_k}\right) + \frac{\log n}{\log 2} \log\left(1 - \frac{1}{p_K}\right).$$

If we denote

$$c_K = \sum_{k<K} \log\left(1 - \frac{1}{p_k}\right) \quad \text{and} \quad \epsilon_K = -\frac{1}{\log 2} \log\left(1 - \frac{1}{p_K}\right),$$

then we have

$$\log \varphi(n) = \log n + \log \prod_{p|n} \left(1 - \frac{1}{p}\right) \geqslant c_K + (1 - \epsilon_K) \log n.$$

Hence we conclude that

$$\varphi(n) \geqslant e^{c_K} n^{1-\epsilon_K}.$$

Since $\epsilon_K \to 0$ as $K \to \infty$ we get that $\varphi(n) \gg n^{1-\epsilon}$ for every $\epsilon > 0$.

SOLUTION 8. Note that if $q|n$, then $e(an/q) = 1$ for every $1 \leqslant a \leqslant q$ and so we have

$$\frac{1}{q} \sum_{a=1}^{q} e(an/q) = \frac{1}{q} \sum_{a=1}^{q} 1 = 1.$$

Now suppose that $q\nmid n$. Then we have $e(n/q) \neq 1$ and so

$$\frac{1}{q}\sum_{a=1}^{q} e(an/q) = \frac{1}{q}\sum_{a=1}^{q} e(n/q)^a = \frac{1}{q}\left(\frac{e(n/q)^{q+1}-1}{e(n/q)-1} - 1\right) = 0$$

as $e(n/q)^{q+1} = e(n/q)$.

Observe that

$$c_q(n) = \sum_{\substack{a=1\\(a,q)=1}}^{q} e(an/q) = \sum_{a=1}^{q} e(an/q) \sum_{d\,|\,(a,q)} \mu(d) = \sum_{a=1}^{q} e(an/q) \sum_{\substack{d\,|\,a\\d\,|\,q}} \mu(d).$$

Changing the order of summation we get

$$c_q(n) = \sum_{d\,|\,q} \mu(d) \sum_{\substack{a=1\\d\,|\,a}}^{q} e(an/q) = \sum_{d\,|\,q} \mu(d) \sum_{r=1}^{q/d} e(rdn/q) = \sum_{d\,|\,q} \mu(d) \sum_{r=1}^{q/d} e(rn/(q/d)).$$

We can rewrite $c_q(n)$ as

$$c_q(n) = \sum_{d\,|\,q} \mu(q/d) \sum_{r=1}^{d} e(rn/d).$$

Finally, applying the identity in part (a) we obtain

$$c_q(n) = \sum_{\substack{d\,|\,q\\d\,|\,n}} d\mu(q/d) = \sum_{d\,|\,(q,n)} d\mu(q/d).$$

Using the triangle inequality, we get

$$|c_q(n)| \leqslant \sum_{d\,|\,(q,n)} d \leqslant \sum_{d\,|\,n} d = \sigma(n).$$

Hence, $c_q(n) = O(1)$ as a function of q with a fixed n.

We rewrite $\sigma(n)$ as

$$\sigma(n) = n\sum_{d\,|\,n} \frac{1}{d} = n\sum_{d=1}^{n} \frac{1}{d}\left(\frac{1}{d}\sum_{a=1}^{d} e(an/d)\right)$$

since $\frac{1}{d}\sum_{a=1}^{d} e(an/d)$ is the characteristic function of the divisors of n by part (a). This results in

$$\sigma(n) = n\sum_{d=1}^{n} \frac{1}{d^2}\sum_{a=1}^{d} e(an/d).$$

Since the factor $\sum_{a=1}^{d} e(an/d) = 0$ for $d > n$ by part (a), we can extend the above finite sum to an infinite sum as

$$\sigma(n) = n\sum_{d=1}^{\infty} \frac{1}{d^2}\sum_{a=1}^{d} e(an/d). \tag{3.1}$$

Observe that

$$\begin{aligned}\sum_{a=1}^{d} e(an/d) &= \sum_{q\,|\,d}\ \sum_{\substack{a=1\\(a,d)=q}}^{d} e(an/d) = \sum_{q\,|\,d}\ \sum_{\substack{r=1\\(r,d/q)=1}}^{d/q} e(rqn/d)\\ &= \sum_{q\,|\,d}\ \sum_{\substack{r=1\\(r,d/q)=1}}^{d/q} e(rn/(d/q)) = \sum_{q\,|\,d} c_{d/q}(n) = \sum_{q\,|\,d} c_q(n).\end{aligned}$$

Substituting this into (3.1) we obtain

$$\sigma(n) = n\sum_{d=1}^{\infty}\frac{1}{d^2}\sum_{q\,|\,d} c_q(n) = n\sum_{d=1}^{\infty}\sum_{q\,|\,d}\frac{c_q(n)}{d^2}.$$

Changing the order of summation, we get

$$\begin{aligned}\sigma(n) &= n\sum_{q=1}^{\infty}\sum_{\substack{d=1\\q\,|\,d}}^{\infty}\frac{1}{d^2}c_q(n) = n\sum_{q=1}^{\infty}\sum_{\ell=1}^{\infty}\frac{c_q(n)}{(q\ell)^2}\\ &= n\sum_{q=1}^{\infty}\sum_{\ell=1}^{\infty}\frac{1}{\ell^2}\frac{c_q(n)}{q^2} = n\left(\sum_{\ell=1}^{\infty}\frac{1}{\ell^2}\right)\sum_{q=1}^{\infty}\frac{c_q(n)}{q^2}\\ &= \frac{n\pi^2}{6}\sum_{q=1}^{\infty}\frac{c_q(n)}{q^2},\end{aligned}$$

where we use $\sum_{k=1}^{\infty}\frac{1}{k^2} = \frac{\pi^2}{6}$ in the final equality.

Solution 9. (a): Observe that if $n \in \mathcal{A}_p$, then $p^2 \leqslant n+1$ and so $p \leqslant n$. Consequently $[N]\cap\mathcal{A}_p = \emptyset$ for $p > N$ and so we have

$$\left|[N]\cap\bigcup_{p}\mathcal{A}_p\right| = \left|\bigcup_{p\leqslant N}[N]\cap\mathcal{A}_p\right| \leqslant \sum_{p\leqslant N}|[N]\cap\mathcal{A}_p|.$$

Since there are exactly two elements of $\mathcal{A}_p$ in any set of p^2 consecutive integers we obtain that $|[N]\cap\mathcal{A}_p| \leqslant 2\lceil N/p^2\rceil$ and so

$$\left|[N]\cap\bigcup_{p}\mathcal{A}_p\right| \leqslant 2\sum_{p\leqslant N}\left\lceil\frac{N}{p^2}\right\rceil \leqslant 2N\sum_{p\leqslant N}\frac{1}{p^2} + 2\pi(N).$$

(b): Note that

$$\sum_{p}\frac{1}{p^2} \leqslant \frac{1}{2^2} + \sum_{k=1}^{\infty}\frac{1}{(2k+1)^2} \leqslant \frac{1}{4} + \frac{1}{4}\sum_{k=1}^{\infty}\frac{1}{k(k+1)} = \frac{1}{2}.$$

Let $C = \sum_p \frac{1}{p^2}$. We have shown above that $C < 1/2$. Thus

$$\frac{1}{N}\left|[N]\cap\bigcup_{p}\mathcal{A}_p\right| \leqslant 2C + 2\frac{\pi(N)}{N}.$$

Hence we have

$$\limsup_{N\to\infty} \frac{1}{N}\left|[N]\cap\bigcup_p \mathcal{A}_p\right| \leqslant 2C < 1.$$

as $\pi(N)/N \to \infty$, i.e., the set of primes has density 0. Since $[N]\cap\bigcup_p \mathcal{A}_p$ is the set of all positive integers n up to N such that either $n-1$ or $n+1$ is not squarefree, $\bigcap_p [N]\backslash\mathcal{A}_p = [N]\backslash\left([N]\cap\bigcup_p \mathcal{A}_p\right)$ is the set of all twin squarefree integers. Finally,

$$\liminf_{N\to\infty} \frac{1}{N}\left|\bigcap_p [N]\backslash\mathcal{A}_p\right| = 1 - \limsup_{N\to\infty} \frac{1}{N}\left|[N]\cap\bigcup_p \mathcal{A}_p\right| = 1-2C > 0.$$

This shows that the set of twin squarefree integers has positive (lower) density.

Solution 10. (a): Observe that for an integer N we have

$$\{1 \leqslant m \leqslant N : m \text{ not squarefree}\} \subset \bigcup_p \{1 \leqslant m \leqslant N : p^2|m\},$$

where p runs over all primes. It thus follows that

$$N - Q(N) \leqslant \sum_p \left\lfloor \frac{N}{p^2} \right\rfloor,$$

which is the desired inequality.

(b): Obvious as every prime besides 2 is odd and $(2k+1)^2 = 4k^2+4k+1 > 4k(k+1)$, $\sum_{k=1}^{\infty} \frac{1}{k(k+1)} = 1$.

(c): It now follows by part (b) that

$$Q(N) \geqslant N - \sum_p \left\lfloor \frac{N}{p^2} \right\rfloor \geqslant N - N\sum_p \frac{1}{p^2} > \frac{N}{2}.$$

for every $n \in \mathbb{N}$.

(d): Suppose for the sake of contradiction that $N > 1$ and N cannot be expressed as a sum of two squarefree integers. Then for every $a, b \in \mathbb{N}$ satisfying $a+b=N$ either a or b is not squarefree. It follows that there are at least $(N-1)/2$ (this is the number of ways N can be written as a sum of two positive integers without regard for order) integers up to $N-1$ that are not square free. Hence, we must have

$$Q(N-1) \leqslant (N-1) - \frac{(N-1)}{2} = \frac{N-1}{2}.$$

But this contradicts the inequality in part (c).