On arithmetic functions

Antonio Parrilla Sánchez

November 23, 2025

Abstract

The purpose of this paper is to present a systematic overview of several computational techniques that have emerged in connection with Project Euler problems involving arithmetic functions. While these methods were initially developed and discussed within the private Project Euler forums, accessible only to users who have solved the corresponding problems, many of them were subsequently examined in publicly available discussions. The latter [b; Nisb; Nisa], will constitute the primary sources for this exposition.

1 Introduction

We fix a domain $(R, +, \cdot)$. Our interest lies in the space of functions

$$R^{\mathbb{Z}^+} := \{f \mid f : \mathbb{Z}^+ \to R\}.$$

Definition 1.1. We say that $f \in R^{\mathbb{Z}^+}$ is **completely additive** if given any $n, m \in \mathbb{Z}^+$, then f satisfies that $f(nm) = f(n) + f(m)$.

Definition 1.2. We say that $f \in R^{\mathbb{Z}^+}$ is **completely multiplicative** if given any $n, m \in \mathbb{Z}^+$, then f satisfies that $f(nm) = f(n)f(m)$. This means that f is a multiplicative homomorphism of monoids.

Definition 1.3. Given $f \in R^{\mathbb{Z}^+}$, we say that f is **additive** if given any $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$, then f satisfies that $f(nm) = f(n) + f(m)$.

It is clear that every completely additive function is additive.

We define

$$\mathrm{Add}(R) := \{f \in R^{\mathbb{Z}^+} \mid f \text{ is additive}\}.$$

Definition 1.4. Given $f \in R^{\mathbb{Z}^+}$, we say that f is **multiplicative** if f is not identically zero and given any $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$, f satisfies that $f(nm) = f(n)f(m)$.

It is clear that every completely multiplicative function not identically zero is multiplicative.

We define

$$\mathrm{Mult}(R) := \{f \in R^{\mathbb{Z}^+} \mid f \text{ is multiplicative}\}.$$

Definition 1.5. A function $f \in R^{\mathbb{Z}^+}$ is called **arithmetic** if f is additive or multiplicative.

Remark 1.6. (i) Every additive function $f \in \mathrm{Add}(R)$ satisfies that $f(1) = 0_R$.

Proof. We have that $f(1) = f(1 \cdot 1) = f(1) + f(1)$, from which it follows that $f(1) = 0_R$. □

(ii) Every multiplicative function f satisfies that $f(1) = 1_R$.

Proof. Since f is not identically zero, there exists $n \in \mathbb{Z}^+$ such that $f(n) \neq 0_R$.

Therefore, $f(n) \cdot 1_R = f(n) = f(n \cdot 1) = f(n) \cdot f(1)$, from which it follows that $f(1) = 1_R$ by the cancellation property of a domain. □

(iii) On the one hand, since the set of prime numbers forms a multiplicative basis of the monoid $\mathbb{Z}^+$, a completely additive/multiplicative function is defined by its values at each prime. Moreover, any assignment of values to the primes extends uniquely to a completely additive/multiplicative function.

On the other hand, arithmetic functions are completely determined by its values on prime powers and as in the previous case, every possible evaluation on prime powers gives rise to a arithmetic function.

We list numerous important examples of arithmetic functions.

Example 1.7. (i) The natural logarithm, $\log : \mathbb{Z}^+ \to \mathbb{R}$ is an (completely) additive function.

(ii) The function $\Omega : \mathbb{Z}^+ \to \mathbb{N}$ defined as the number of prime factors with multiplicities is completely additive. If $p_1, \ldots, p_r$ are distinct primes, then $\Omega\left(p_1^{\alpha_1} \cdot \cdots \cdot p_r^{\alpha_r}\right) = \alpha_1 + \cdots + \alpha_r$.

(iii) The function $\omega : \mathbb{Z}^+ \to \mathbb{N}$ defined as the number of distinct prime factors is completely additive. If $p_1, \ldots, p_r$ are distinct primes, then $\omega\left(p_1^{\alpha_1} \cdot \cdots \cdot p_r^{\alpha_r}\right) = r$.

(iv) Let τ denote the function $\tau : \mathbb{Z}^+ \to \mathbb{Z}^+$ that counts the number of positive divisors of a number. If we write $n = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$ where $p_1, \dots, p_r$ are distinct primes, the positive divisors of n correspond bijectively to elements of the set $A := \{0, \dots, k_1\} \times \cdots \times \{0, \dots, k_r\}$, where the i-th component represents the exponent of the i-th prime in the divisor.

Therefore, $\tau(p_1^{k_1} \cdot \dots \cdot p_r^{k_r}) = (k_1+1) \cdot \dots \cdot (k_r+1)$. It is obvious that this function is multiplicative.

(v) Let σ denote the function $\sigma : \mathbb{Z}^+ \to \mathbb{Z}^+$ that counts the sum of the positive divisors of a number. For a prime power p^k, it is easy to see that $\sigma(p^k) = 1 + p + \cdots + p^k = \frac{p^{k+1}-1}{p-1}$. If we write $n = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$ where $p_1, \dots, p_r$ are distinct primes, then

$$\sigma(p_1^{k_1}) \dots \sigma(p_r^{k_r}) = (1+p_1+\dots p_1^{k_1}) \dots (1+p_r+\dots p_r^{k_r}) = \sum_{(a_1,\dots,a_r)\in A} p_1^{a_1} \cdot \dots \cdot p_r^{a_r} = \sigma(p_1^{k_1} \cdot \dots \cdot p_r^{k_r}).$$

It follows that σ is multiplicative.

(vi) Let $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ denote the **Mbius** function. It is defined by

$$\mu(1) = 1, \quad \mu(p) = -1 \text{ for each prime } p, \quad \mu(p^k) = 0 \text{ for } k \geq 2,$$

and extended multiplicatively to all positive integers, i.e.,

$$\mu\Big(p_1^{k_1} \cdots p_r^{k_r}\Big) = \mu(p_1^{k_1}) \cdots \mu(p_r^{k_r}).$$

Equivalently, for any positive integer n:

$$\mu(n) = \begin{cases} 0, & \text{if } n \text{ is not square-free,} \\ (-1)^r, & \text{if } n \text{ is the product of } r \text{ distinct primes.} \end{cases}$$

Thus, μ is a multiplicative function that vanishes on non-square-free numbers and alternates in sign depending on the parity of the number of prime factors for square-free numbers.

(vii) Let $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ denote the Euler totient function, defined by

$$\varphi(n) := \operatorname{Card}(\{d \in \{1, \dots, n\} \mid \gcd(d, n) = 1\}).$$

We prove that φ is multiplicative. Let $n, m \in \mathbb{Z}^+$ with $\gcd(n, m) = 1$. For $x \in \{n, m, nm\}$ set

$$B_x := \{d \in \{1, \dots, x\} \mid \gcd(d, x) = 1\}.$$

Define a map $f : B_n \times B_m \to B_{nm}$ by

$$f(a, b) \equiv bn + am \pmod{nm},$$

where we take the representative in $\{1, \dots, nm\}$ of the residue class of $bn + am$.

Since $\gcd(n, m) = 1$ we have

$$\gcd(f(a, b), n) = \gcd(bn + am, n) = \gcd(am, n) = \gcd(a, n) = 1,$$

and similarly $\gcd(f(a, b), m) = \gcd(b, m) = 1$. Hence $f(a, b) \in B_{nm}$, which implies that f is well-defined.

Next we prove the injectivity of f. If $f(a_1, b_1) = f(a_2, b_2)$ then

$$(b_1 - b_2)n \equiv (a_2 - a_1)m \pmod{nm}.$$

As $\gcd(n, m) = 1$, it follows that $n \mid (a_2 - a_1)$ and $m \mid (b_1 - b_2)$. But $a_1, a_2 \in \{1, \dots, n\}$ and $b_1, b_2 \in \{1, \dots, m\}$, so $n \mid (a_2 - a_1)$ (resp. $m \mid (b_1 - b_2)$) implies $a_1 = a_2$ (resp. $b_1 = b_2$). Thus f is injective.

We finnish by proving the surjectivity of f. Let $s \in B_{nm}$, so $\gcd(s, nm) = 1 = \gcd(s, n) = \gcd(s, m)$. By Bzout's identity there exist integers u, v with $un + vm = 1$. Then

$$s = s(un + vm) = (su)n + (sv)m.$$

Put $a \equiv sv \pmod{n}$ and $b \equiv su \pmod{m}$ (take the representatives in $\{1, \ldots, n\}$ and $\{1, \ldots, m\}$ respectively). Since $\gcd(s, n) = \gcd(v, n) = 1$ and $\gcd(s, m) = \gcd(u, m) = 1$, we have $(a, b) \in B_n \times B_m$ and $f(a, b) \equiv bn + am \equiv (su)n + (sv)m \equiv s \pmod{nm}$. Hence $f(a, b) = s$ and f is surjective.

Therefore f is a bijection and

$$\varphi(nm) = \operatorname{Card}(B_{nm}) = \operatorname{Card}(B_n \times B_m) = \operatorname{Card}(B_n) \cdot \operatorname{Card}(B_m) = \varphi(n)\varphi(m),$$

so φ is multiplicative.

(viii) Let $\varepsilon : \mathbb{Z}^+ \to \{0, 1\}$ be defined by

$$\varepsilon(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases}$$

ε is a multiplicative function.

(ix) For $r \in \mathbb{R}$, we define $\mathrm{id}_r : \mathbb{Z}^+ \to \mathbb{R}^+$ as $\mathrm{id}_r(x) = x^r$. This function is (completely) multiplicative for every choice of r. When $r \in \mathbb{N}$, we consider $\mathrm{id}_r : \mathbb{Z}^+ \to \mathbb{Z}^+$ as a monoid endomorphism. We denote $\mathrm{id}_0 \coloneqq I$ and $\mathrm{id}_1 \coloneqq \mathrm{id}$. id is also additive.

Next we study several function operations over arithmetic functions.

Proposition 1.8. *Let $f, g \in \operatorname{Add}(R)$. Then*

(i) $f + g \in \operatorname{Add}(R)$.

(ii) For every $\alpha \in R$, $\alpha f \in \operatorname{Add}(R)$.

Proof. (i) $f + g$ is additive since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$\begin{aligned}(f + g)(nm) = f(nm) + g(nm) = (f(n) + f(m)) + (g(n) + g(m)) = \\ (f(n) + g(n)) + (f(m) + g(m)) = (f + g)(n) + (f + g)(m).\end{aligned}$$

(ii) αf is additive since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$(\alpha f)(nm) = \alpha \cdot f(nm) = \alpha \cdot (f(n) + f(m)) = \alpha \cdot f(n) + \alpha \cdot f(m) = (\alpha f)(n) + (\alpha f)(m).$$

□

Proposition 1.9. *If f is completely additive and g is multiplicative, then $f \circ g \in \operatorname{Add}(R)$.*

Proof. $f \circ g$ is additive since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$(f \circ g)(nm) = f(g(nm)) = f(g(n)g(m)) = f(g(n)) + f(g(m)) = (f \circ g)(n) + (f \circ g)(m).$$

□

Proposition 1.10. *Let $f, g \in \operatorname{Mult}(R)$. Then*

(i) $f \cdot g \in \operatorname{Mult}(R)$.

(ii) If $g(n) \in R^\times$ for all $n \in \mathbb{Z}^+$, then $\frac{f}{g} \in \operatorname{Mult}(R)$.

(iii) $f + g \notin \operatorname{Mult}(R)$.

(iv) For every $\alpha \in R \setminus \{1_R\}$, $\alpha f \notin \operatorname{Mult}(R)$.

Proof. (i) $f \cdot g$ is multiplicative since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$(f \cdot g)(nm) = f(nm) \cdot g(nm) = f(n)f(m)g(n)g(m) = f(n)g(n)f(m)g(m) = (f \cdot g)(n)(f \cdot g)(m).$$

(ii) $\frac{f}{g}$ is multiplicative since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$\left(\frac{f}{g}\right)(nm) = \frac{f(nm)}{g(nm)} = \frac{f(n)f(m)}{g(n)g(m)} = \frac{f(n)}{g(n)}\frac{f(m)}{g(m)} = \left(\frac{f}{g}\right)(n)\left(\frac{f}{g}\right)(m).$$

(iii) By Remark 2.6, every multiplicative function satisfies $f(1) = 1_R$. But

$$(f + g)(1) = f(1) + g(1) = 1_R + 1_R = 2_R \neq 1_R,$$

so $f + g$ cannot be multiplicative. Hence $f + g \notin \mathrm{Mult}(R)$.

(iv) Again, every multiplicative function must take value 1_R at 1. But

$$(\alpha f)(1) = \alpha f(1) = \alpha \neq 1_R,$$

since $\alpha \in R \setminus \{1_R\}$. Hence $\alpha f \notin \mathrm{Mult}(R)$.

□

Proposition 1.11. *If f is completely multiplicative and g is multiplicative, then $f \circ g \in \mathrm{Mult}(R)$.*

Proof. $f \circ g$ is multiplicative since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$(f \circ g)(nm) = f(g(nm)) = f(g(n)g(m)) = f(g(n)) \cdot f(g(m)) = (f \circ g)(n) \cdot (f \circ g)(m).$$

□

Problems

Ex 1. For $\alpha \in \mathbb{R}$, let $\sigma_\alpha : \mathbb{Z}^+ \to \mathbb{R}^+$ be defined as

$$\sigma_\alpha(n) := \sum_{d|n} d^\alpha.$$

If $\alpha \in \mathbb{N}$, we can consider σ_α as an endomorphism.

Prove that for every choice of $\alpha \in \mathbb{R}$, σ_α is multiplicative. Find the multiplicative functions that were presented in the examples that belong to the familiy $\{\sigma_\alpha\}_{\alpha \in \mathbb{R}}$.

Ex 2. Prove that for every prime power p^k with $k \in \mathbb{Z}^+$, it is satisfied that $\varphi(p^k) = p^{k-1}(p-1)$. Using the fact that φ is multiplicative, conclude the general formula for φ, with the input given as a product of distinct primes.

Ex 3. Classify all the arithmetic functions with $R = \mathbb{Z}_2$.

2 Introduction

We fix a domain $(R, +, \cdot)$. Our interest lies in the space of functions

$$R^{\mathbb{Z}^+} := \{f \mid f : \mathbb{Z}^+ \to R\}.$$

Definition 2.1. We say that $f \in R^{\mathbb{Z}^+}$ is **completely additive** if given any $n, m \in \mathbb{Z}^+$, then f satisfies that $f(nm) = f(n) + f(m)$.

Definition 2.2. We say that $f \in R^{\mathbb{Z}^+}$ is **completely multiplicative** if given any $n, m \in \mathbb{Z}^+$, then f satisfies that $f(nm) = f(n)f(m)$. This means that f is a multiplicative homomorphism of monoids.

Definition 2.3. Given $f \in R^{\mathbb{Z}^+}$, we say that f is **additive** if given any $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$, then f satisfies that $f(nm) = f(n) + f(m)$.

It is clear that every completely additive function is additive.

We define

$$\mathrm{Add}(R) := \{f \in R^{\mathbb{Z}^+} \mid f \text{ is additive}\}.$$

Definition 2.4. Given $f \in R^{\mathbb{Z}^+}$, we say that f is **multiplicative** if f is not identically zero and given any $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$, f satisfies that $f(nm) = f(n)f(m)$.

It is clear that every completely multiplicative function not identically zero is multiplicative.

We define

$$\mathrm{Mult}(R) := \{f \in R^{\mathbb{Z}^+} \mid f \text{ is multiplicative}\}.$$

Definition 2.5. A function $f \in R^{\mathbb{Z}^+}$ is called **arithmetic** if f is additive or multiplicative.

Remark 2.6. (i) Every additive function $f \in \mathrm{Add}(R)$ satisfies that $f(1) = 0_R$.

Proof. We have that $f(1) = f(1 \cdot 1) = f(1) + f(1)$, from which it follows that $f(1) = 0_R$. □

(ii) Every multiplicative function f satisfies that $f(1) = 1_R$.

Proof. Since f is not identically zero, there exists $n \in \mathbb{Z}^+$ such that $f(n) \neq 0_R$.

Therefore, $f(n) \cdot 1_R = f(n) = f(n \cdot 1) = f(n) \cdot f(1)$, from which it follows that $f(1) = 1_R$ by the cancellation property of a domain. □

(iii) On the one hand, since the set of prime numbers forms a multiplicative basis of the monoid $\mathbb{Z}^+$, a completely additive/multiplicative function is defined by its values at each prime. Moreover, any assignment of values to the primes extends uniquely to a completely additive/multiplicative function.

On the other hand, arithmetic functions are completely determined by its values on prime powers and as in the previous case, every possible evaluation on prime powers gives rise to a arithmetic function.

We list numerous important examples of arithmetic functions.

Example 2.7. (i) The natural logarithm, $\log : \mathbb{Z}^+ \to \mathbb{R}$ is an (completely) additive function.

(ii) The function $\Omega : \mathbb{Z}^+ \to \mathbb{N}$ defined as the number of prime factors with multiplicities is completely additive. If $p_1, \dots, p_r$ are distinct primes, then $\Omega\left(p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}\right) = \alpha_1 + \dots + \alpha_r$.

(iii) The function $\omega : \mathbb{Z}^+ \to \mathbb{N}$ defined as the number of distinct prime factors is completely additive. If $p_1, \dots, p_r$ are distinct primes, then $\omega\left(p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}\right) = r$.

(iv) Let τ denote the function $\tau : \mathbb{Z}^+ \to \mathbb{Z}^+$ that counts the number of positive divisors of a number. If we write $n = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$ where $p_1, \dots, p_r$ are distinct primes, the positive divisors of n correspond bijectively to elements of the set $A \coloneqq \{0, \dots, k_1\} \times \dots \times \{0, \dots, k_r\}$, where the i-th component represents the exponent of the i-th prime in the divisor.

Therefore, $\tau(p_1^{k_1} \cdot \dots \cdot p_r^{k_r}) = (k_1+1) \cdot \dots \cdot (k_r+1)$. It is obvious that this function is multiplicative.

(v) Let σ denote the function $\sigma : \mathbb{Z}^+ \to \mathbb{Z}^+$ that counts the sum of the positive divisors of a number. For a prime power p^k, it is easy to see that $\sigma(p^k) = 1 + p + \dots + p^k = \frac{p^{k+1}-1}{p-1}$. If we write $n = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$ where $p_1, \dots, p_r$ are distinct primes, then

$$\sigma(p_1^{k_1}) \dots \sigma(p_r^{k_r}) = (1+p_1+\dots p_1^{k_1}) \dots (1+p_r+\dots p_r^{k_r}) = \sum_{(a_1,\dots,a_r)\in A} p_1^{a_1} \cdot \dots \cdot p_r^{a_r} = \sigma(p_1^{k_1} \cdot \dots \cdot p_r^{k_r}).$$

It follows that σ is multiplicative.

(vi) Let $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ denote the **Mbius** function. It is defined by

$$\mu(1) = 1, \quad \mu(p) = -1 \text{ for each prime } p, \quad \mu(p^k) = 0 \text{ for } k \geq 2,$$

and extended multiplicatively to all positive integers, i.e.,

$$\mu\Big(p_1^{k_1} \cdots p_r^{k_r}\Big) = \mu(p_1^{k_1}) \cdots \mu(p_r^{k_r}).$$

Equivalently, for any positive integer n:

$$\mu(n) = \begin{cases} 0, & \text{if } n \text{ is not square-free,} \\ (-1)^r, & \text{if } n \text{ is the product of } r \text{ distinct primes.} \end{cases}$$

Thus, μ is a multiplicative function that vanishes on non-square-free numbers and alternates in sign depending on the parity of the number of prime factors for square-free numbers.

(vii) Let $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ denote the Euler totient function, defined by

$$\varphi(n) \coloneqq \mathrm{Card}(\{d \in \{1, \dots, n\} \mid \gcd(d, n) = 1\}).$$

We prove that φ is multiplicative. Let $n, m \in \mathbb{Z}^+$ with $\gcd(n, m) = 1$. For $x \in \{n, m, nm\}$ set

$$B_x \coloneqq \{d \in \{1, \dots, x\} \mid \gcd(d, x) = 1\}.$$

Define a map $f : B_n \times B_m \to B_{nm}$ by

$$f(a, b) \equiv bn + am \pmod{nm},$$

where we take the representative in $\{1, \dots, nm\}$ of the residue class of $bn + am$.

Since $\gcd(n, m) = 1$ we have

$$\gcd(f(a, b), n) = \gcd(bn + am, n) = \gcd(am, n) = \gcd(a, n) = 1,$$

and similarly $\gcd(f(a, b), m) = \gcd(b, m) = 1$. Hence $f(a, b) \in B_{nm}$, which implies that f is well-defined.

Next we prove the injectivity of f. If $f(a_1, b_1) = f(a_2, b_2)$ then

$$(b_1 - b_2)n \equiv (a_2 - a_1)m \pmod{nm}.$$

As $\gcd(n, m) = 1$, it follows that $n \mid (a_2 - a_1)$ and $m \mid (b_1 - b_2)$. But $a_1, a_2 \in \{1, \dots, n\}$ and $b_1, b_2 \in \{1, \dots, m\}$, so $n \mid (a_2 - a_1)$ (resp. $m \mid (b_1 - b_2)$) implies $a_1 = a_2$ (resp. $b_1 = b_2$). Thus f is injective.

We finnish by proving the surjectivity of f. Let $s \in B_{nm}$, so $\gcd(s, nm) = 1 = \gcd(s, n) = \gcd(s, m)$. By Bzout's identity there exist integers u, v with $un + vm = 1$. Then

$$s = s(un + vm) = (su)n + (sv)m.$$

Put $a \equiv sv \pmod{n}$ and $b \equiv su \pmod{m}$ (take the representatives in $\{1, \dots, n\}$ and $\{1, \dots, m\}$ respectively). Since $\gcd(s, n) = \gcd(v, n) = 1$ and $\gcd(s, m) = \gcd(u, m) = 1$, we have $(a, b) \in B_n \times B_m$ and $f(a, b) \equiv bn + am \equiv (su)n + (sv)m \equiv s \pmod{nm}$. Hence $f(a, b) = s$ and f is surjective.

Therefore f is a bijection and

$$\varphi(nm) = \mathrm{Card}(B_{nm}) = \mathrm{Card}(B_n \times B_m) = \mathrm{Card}(B_n) \cdot \mathrm{Card}(B_m) = \varphi(n)\varphi(m),$$

so φ is multiplicative.

(viii) Let $\varepsilon : \mathbb{Z}^+ \to \{0, 1\}$ be defined by

$$\varepsilon(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases}$$

ε is a multiplicative function.

(ix) For $r \in \mathbb{R}$, we define $\mathrm{id}_r : \mathbb{Z}^+ \to \mathbb{R}^+$ as $\mathrm{id}_r(x) = x^r$. This function is (completely) multiplicative for every choice of r. When $r \in \mathbb{N}$, we consider $\mathrm{id}_r : \mathbb{Z}^+ \to \mathbb{Z}^+$ as a monoid endomorphism. We denote $\mathrm{id}_0 \coloneqq I$ and $\mathrm{id}_1 \coloneqq \mathrm{id}$. id is also additive.

Next we study several function operations over arithmetic functions.

Proposition 2.8. *Let $f, g \in \mathrm{Add}(R)$. Then*

(i) $f + g \in \mathrm{Add}(R)$.

(ii) For every $\alpha \in R$, $\alpha f \in \mathrm{Add}(R)$.

Proof. (i) $f + g$ is additive since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$\begin{aligned}(f + g)(nm) = f(nm) + g(nm) = (f(n) + f(m)) + (g(n) + g(m)) = \\ (f(n) + g(n)) + (f(m) + g(m)) = (f + g)(n) + (f + g)(m).\end{aligned}$$

(ii) αf is additive since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$(\alpha f)(nm) = \alpha \cdot f(nm) = \alpha \cdot (f(n) + f(m)) = \alpha \cdot f(n) + \alpha \cdot f(m) = (\alpha f)(n) + (\alpha f)(m).$$

□

Proposition 2.9. *If f is completely additive and g is multiplicative, then $f \circ g \in \mathrm{Add}(R)$.*

Proof. $f \circ g$ is additive since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$(f \circ g)(nm) = f(g(nm)) = f(g(n)g(m)) = f(g(n)) + f(g(m)) = (f \circ g)(n) + (f \circ g)(m).$$

□

Proposition 2.10. *Let $f, g \in \mathrm{Mult}(R)$. Then*

(i) $f \cdot g \in \mathrm{Mult}(R)$.

(ii) If $g(n) \in R^\times$ for all $n \in \mathbb{Z}^+$, then $\frac{f}{g} \in \mathrm{Mult}(R)$.

(iii) $f + g \notin \mathrm{Mult}(R)$.

(iv) For every $\alpha \in R \setminus \{1_R\}$, $\alpha f \notin \mathrm{Mult}(R)$.

Proof. (i) $f \cdot g$ is multiplicative since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$(f \cdot g)(nm) = f(nm) \cdot g(nm) = f(n)f(m)g(n)g(m) = f(n)g(n)f(m)g(m) = (f \cdot g)(n)(f \cdot g)(m).$$

(ii) $\frac{f}{g}$ is multiplicative since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$\left(\frac{f}{g}\right)(nm) = \frac{f(nm)}{g(nm)} = \frac{f(n)f(m)}{g(n)g(m)} = \frac{f(n)}{g(n)}\frac{f(m)}{g(m)} = \left(\frac{f}{g}\right)(n)\left(\frac{f}{g}\right)(m).$$

(iii) By Remark 2.6, every multiplicative function satisfies $f(1) = 1_R$. But

$$(f + g)(1) = f(1) + g(1) = 1_R + 1_R = 2_R \neq 1_R,$$

so $f + g$ cannot be multiplicative. Hence $f + g \notin \text{Mult}(R)$.

(iv) Again, every multiplicative function must take value 1_R at 1. But

$$(\alpha f)(1) = \alpha f(1) = \alpha \neq 1_R,$$

since $\alpha \in R \setminus \{1_R\}$. Hence $\alpha f \notin \text{Mult}(R)$.

□

Proposition 2.11. *If f is completely multiplicative and g is multiplicative, then* $f \circ g \in \text{Mult}(R)$.

Proof. $f \circ g$ is multiplicative since for $n, m \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$,

$$(f \circ g)(nm) = f(g(nm)) = f(g(n)g(m)) = f(g(n)) \cdot f(g(m)) = (f \circ g)(n) \cdot (f \circ g)(m).$$

□

Problems

Ex 4. For $\alpha \in \mathbb{R}$, let $\sigma_\alpha : \mathbb{Z}^+ \to \mathbb{R}^+$ be defined as

$$\sigma_\alpha(n) \coloneqq \sum_{d|n} d^\alpha.$$

If $\alpha \in \mathbb{N}$, we can consider σ_α as an endomorphism.

Prove that for every choice of $\alpha \in \mathbb{R}$, σ_α is multiplicative. Find the multiplicative functions that were presented in the examples that belong to the familiy $\{\sigma_\alpha\}_{\alpha \in \mathbb{R}}$.

Ex 5. Prove that for every prime power p^k with $k \in \mathbb{Z}^+$, it is satisfied that $\varphi(p^k) = p^{k-1}(p-1)$. Using the fact that φ is multiplicative, conclude the general formula for φ, with the input given as a product of distinct primes.

Ex 6. Classify all the arithmetic functions with $R = \mathbb{Z}_2$.

2.1 Dirichlet convolution

From now on we suppose that we are working in a domain $(R, +, \cdot)$. Now we present a new operation over $R^{\mathbb{Z}^+}$.

Definition 2.12. Given $f, g \in R^{\mathbb{Z}^+}$, we define the **Dirichlet convolution** of f and g as the function $f * g : \mathbb{Z}^+ \to R$ given by

$$(f * g)(n) \coloneqq \sum_{\substack{k|n \\ (k \in \mathbb{Z}^+)}} f(k) \cdot g\left(\frac{n}{k}\right).$$

That last formulation is equivalent to

$$(f * g)(n) = \sum_{\substack{k_1 \cdot k_2 = n \\ (k_1, k_2 \in \mathbb{Z}^+)}} f(k_1) \cdot g(k_2).$$

Notice the similarities between the Dirichlet convolution and the usual product of polynomials. While the Dirichlet convolution is a multiplicative convolution, the usual polynomial product is an additive one. For the image at $n \in \mathbb{Z}^+$ of the Dirichlet convolution of $f, g \in R^{\mathbb{Z}^+}$ we range over $k_1, k_2 \in \mathbb{Z}^+$ satisfying $k_1 \cdot k_2 = n$, while for the image at $n \in \mathbb{N}$ of the polynomial multiplication of $f, g \in R^{\mathbb{N}}$ we range over $k_1, k_2 \in \mathbb{N}$ satisfying $k_1 + k_2 = n$.

We continue studying some fundamental properties of the Dirichlet convolution.

Proposition 2.13.

(i) For every $f, g \in R^{\mathbb{Z}^+}$, $f * g = g * f$.

(ii) For every $f, g, h \in R^{\mathbb{Z}^+}$, $(f * g) * h = f * (g * h)$.

(iii) For every $f \in R^{\mathbb{Z}^+}$, $f * \varepsilon = \varepsilon * f = f$ and it is the only element in $R^{\mathbb{Z}^+}$ with this property.

(iv) $(R^{\mathbb{Z}^+}, *)$ is an abelian monoid. Let $G(R) \coloneqq \{f \in R^{\mathbb{Z}^+} \mid f(1) \in R^\times\}$. Then, $(G(R), *)$ is the abelian group consisting of the invertible elements of $(R^{\mathbb{Z}^+}, *)$.

Proof. (i) With the equivalent formulation of the Dirichlet convolution is easily provable. For every $n \in \mathbb{Z}^+$,

$$(f * g)(n) = \sum_{k_1 k_2 = n} f(k_1) g(k_2) = \sum_{k_2 k_1 = n} f(k_2) g(k_1) = \sum_{k_1 k_2 = n} g(k_1) f(k_2) = (g * f)(n).$$

(ii) For every $n \in \mathbb{Z}^+$,

$$((f * g) * h)(n) = \sum_{k' k_3 = n} (f * g)(k') \cdot h(k_3) = \sum_{k' k_3 = n} (\sum_{k_1 k_2 = k'} f(k_1) \cdot g(k_2)) h(k_3) =$$

$$\sum_{k_1 k_2 k_3 = n} f(k_1) \cdot g(k_2) \cdot h(k_3) = \sum_{k_1 k' = n} f(k_1) (\sum_{k_2 k_3 = k'} g(k_2) \cdot h(k_3)) =$$

$$\sum_{k_1 k' = n} f(k_1) \cdot (g * h)(k') = (f * (g * h))(n)$$

(iii) Remember that ε is defined as

$$\varepsilon(n) = \begin{cases} 1_R, & \text{if } n = 1, \\ 0_R, & \text{otherwise.} \end{cases}$$

By commutativity of $*$, it suffices to verify that for every $f \in R^{\mathbb{Z}^+}$, $\varepsilon * f = f$.

For every $n \in \mathbb{Z}^+$,

$$(\varepsilon * f)(n) = \sum_{k|n} \varepsilon(k) \cdot f(\frac{n}{k}) = f(n) + \sum_{\substack{k|n \\ k \neq 1}} \varepsilon(k) \cdot f(\frac{n}{k}) = f(n) + 0_R = f(n).$$

We conclude that ε is the identity element, which is unique because if any other element $g \in R^{\mathbb{Z}^+}$ is also an identity element, then $g = g * \varepsilon = \varepsilon$.

(iv) The previous parts prove that $(R^{\mathbb{Z}^+}, *)$ is an abelian monoid.

If $f \in R^{\mathbb{Z}^+}$ has a Dirichlet inverse f^{-1}, then

$$\varepsilon(1) = (f^{-1} * f)(1) = f^{-1}(1) \cdot f(1).$$

Therefore, $f \in G(R)$.

Now let $f \in G(R)$, we will prove that there exists the Dirichlet inverse $f^{-1} \in R^{\mathbb{Z}^+}$. We will define it recursively in order to ascertain that $f^{-1} * f = \varepsilon$.

$$f^{-1}(n) = \begin{cases} f(1)^{-1}, & \text{if } n = 1, \\ -f(1)^{-1} \sum\limits_{\substack{k|n \\ k \neq n}} f^{-1}(k) f(\frac{n}{k}), & \text{if } n > 1. \end{cases}$$

It is clear that f^{-1} is well-defined, so $(G(R), *)$ is the abelian group given by restricting ourself to the invertible elements of $(R^{\mathbb{Z}^+}, *)$.

□

Proposition 2.14. $(\mathrm{Mult}(R), *)$ *is an abelian monoid. Furthermore,* $\mathrm{Mult}(R) = G(R) \cap \mathrm{Mult}(R)$ *is the abelian group consisting of the invertible elements of* $(\mathrm{Mult}(R), *)$

Proof. Since $\varepsilon \in \mathrm{Mult}(R)$ and $\mathrm{Mult}(R) \subseteq R^{\mathbb{Z}^+}$, we only need to verify that $*$ is an internal operation on $\mathrm{Mult}(R)$, that is, the Dirichlet convolution of multiplicative functions is again a multiplicative function.

Let $f, g \in \mathrm{Mult}(R)$ be fixed. If we are given $p \in \mathbb{Z}^+$ prime and $k \in \mathbb{N}$, then

$$(f * g)(p^k) = \sum_{i=0}^{k} f(p^i) g(p^{k-i}).$$

Now, if we are given $n = p_1^{k_1} \dots p_r^{k_r}$ with $p_1, \dots, p_r \in \mathbb{Z}^+$ distinct primes,

$$(f * g)(p_1^{k_1}) \dots (f * g)(p_r^{k_r}) \cdot = \left(\sum_{i=0}^{k} f(p_1^i) g(p_1^{k_1 - i}) \right) \dots \left(\sum_{i=0}^{k} f(p_r^i) g(p_r^{k_r - i}) \right) =$$
$$\sum_{0 \leq a_1 \leq k_1, \dots, 0 \leq a_r \leq k_r} f(p_1^{a_1}) g(p_1^{k_1 - a_1}) \dots f(p_r^{a_r}) g(p_r^{k_r - a_r}) =$$
$$\sum_{0 \leq a_1 \leq k_1, \dots, 0 \leq a_r \leq k_r} f(p_1^{a_1} \dots p_r^{a_r}) g(p_1^{k_1 - a_1} \dots p_r^{k_r - a_r}) = \sum_{l_1 l_2 = n} f(l_1) g(l_2) = (f * g)(n).$$

Therefore, the Dirichlet convolution $f * g$ extends multiplicatively to every positive integer and we conclude that it is a multiplicative function.

It only remains to prove that the Dirichlet inverse of a multiplicative invertible function is multiplicative. Let $f \in \mathrm{Mult}(R)$ be fixed.

Let $p \in \mathbb{Z}^+$ be a prime and let $k \in \mathbb{N}$. We define $g \in \mathrm{Mult}(R)$ as the multiplicative function whose evaluation on prime powers coincides with f^{-1}, that is,

$$g(p_1^{k_1} \dots p_r^{k_r}) \coloneqq f^{-1}(p_1^{k_1}) \dots f^{-1}(p_r^{k_r}).$$

$f * g \in \mathrm{Mult}(R)$ as we have proved and for every prime power p^k,

$$(f * g)(p^k) = \sum_{i=0}^{k} f(p^i) g(p^{k-i}) = \sum_{i=0}^{k} f(p^i) f^{-1}(p^{k-i}) = (f * f^{-1})(p^k) = \varepsilon(p^k).$$

Since $f * g$ coincides with ε in every prime power and both are multiplicative, $f * g = \varepsilon$. Since we have uniqueness of inverses in the abelian group $(R^{\mathbb{Z}^+}, *)$, we deduce that $f^{-1} = g \in \mathrm{Mult}(R)$. □

Example 2.15. In this example we compute the Dirichlet inverse of the Mbius function μ, $\mu^{-1} \in \operatorname{Mult}(R)$ (when $\operatorname{char}(R) = 2$ the Mbius function degenerates, but it is not relevant to the computation of its inverse). Since $\mu^{-1} \in \operatorname{Mult}(R)$, $\mu^{-1}(1) = 1$.

We try to see how the inverse behaves on power of primes, since it is multiplicative; we fix a prime $p \in \mathbb{Z}^+$. We will prove by induction on $k \in \mathbb{N}$ that $\mu^{-1}(p^k) = 1$. The base case has been proved already because $\mu^{-1}(1) = 1$.

The induction hypothesis is that $\mu^{-1}(p^0) = \mu^{-1}(p) = \cdots = \mu^{-1}(p^k) = 1$.

$$\mu^{-1}(p^{k+1}) = -(\mu^{-1}(p^0)\mu(p^{k+1}) + \mu^{-1}(p^1)\mu(p^k) + \cdots + \mu^{-1}(p^{k-1})\mu(p^2) + \mu^{-1}(p^k)\mu(p^1)) = -\mu(p) = 1.$$

Therefore, we only need to extend multiplicatively μ^{-1} to every positive integer, which gives that $\mu^{-1}(n) = 1$ for every $n \in \mathbb{Z}^+$. In conclusion, $\mu^{-1} = I$.

Definition 2.16. For every $r \in \mathbb{R}$, we define $\sigma_\alpha \coloneqq I * \operatorname{id}_\alpha$.

It is important to notice that $\sigma_0 = \tau$ and $\sigma_1 = \sigma$.

Example 2.17. Suppose we are asked to compute

$$\sum_{i=1}^{n} \frac{n}{\gcd(i,n)}.$$

A naive algorithm that iterates over the sum and computes the gcd would belong to $\mathcal{O}(n\log(n))$. However, it can be computed more efficiently.

If we sum over all possible options of the cofactor of the gcd, it follows that

$$\sum_{i=1}^{n} \frac{n}{\gcd(i,n)} = \sum_{d|n} \sum_{\substack{i\in\{1,\ldots,n\} \\ \gcd(n,i)=\frac{n}{d}}} d = \sum_{d|n} \left(d \cdot \left(\sum_{\substack{i\in\{1,\ldots,n\} \\ \gcd(n,i)=\frac{n}{d}}} 1 \right) \right).$$

Next we make the change of variables $j \cdot \frac{n}{d} = i$. Then,

$$\sum_{\substack{i\in\{1,\ldots,n\} \\ \gcd(n,i)=\frac{n}{d}}} 1 = \sum_{\substack{j\in\{1,\ldots,d\} \\ \gcd(d,j)=1}} 1 = \varphi(d).$$

Therefore,

$$\sum_{i=1}^{n} \frac{n}{\gcd(i,n)} = \sum_{d|n} d \cdot \varphi(d) = (I * (\operatorname{id} \cdot \varphi))(n).$$

In conclusion, we can compute $\sum_{i=1}^{n} \frac{n}{\gcd(i,n)}$ as fast as the multiplicative function $I * (\operatorname{id} \cdot \varphi)$, which is much better than the naive approach.

Problems

Ex 7. Prove that the Dirichlet convolution is a bilinear operator in $R^{\mathbb{Z}^+}$ with the usual structure of R-module. That is, prove that for every $f, g, h \in R^{\mathbb{Z}^+}$ the Dirichlet convolution satisifes that $(f+g)*h = (f*h)+(g*h)$ and for every $f, g \in R^{\mathbb{Z}^+}$ and $c \in R$, we have that $(cf)*g = c(f*g)$.

Is it also true that for every $f, g, h \in R^{\mathbb{Z}^+}$ $(f \cdot g)*h = (f*h)\cdot(g*h)$?

Ex 8. Compute the Dirichlet inverse of id, id_2, τ and σ.

Ex 9. Compute the Dirichlet inverse of the not necessarily multiplicative functions $\alpha\cdot\mathrm{id}$ for $\alpha \in \mathbb{Z}\backslash\{0\}$.

Ex 10. Prove that the Dirichlet inverse of id_α is $\mu\cdot\mathrm{id}_\alpha$. Deduce the expression of the Dirichlet inverse of σ_α.

Ex 11. Using the fact that $\varphi = \mathrm{id}*\mu$ compute the Dirichlet inverse of φ.

Ex 12. Let $f \in R^{\mathbb{Z}^+}$ be completely multiplicative. Prove that for every $g \in R^{\mathbb{Z}^+}$ we have that g is multiplicative if and only if $f*g$ is multiplicative.

Ex 13. For every $f \in R^{\mathbb{Z}^+}$ and $k \in \mathbb{Z}^+$ we define $f^{*k} \in R^{\mathbb{Z}^+}$ as

$$f^{*k} = \underbrace{f*f*\cdots*f}_{k \text{ times}}.$$

We also define $f^{*0} = \varepsilon$. Describe the function I^{*k} for $k \in \mathbb{N}$.

Ex 14. Von Mangoldt function $\Lambda : \mathbb{Z}^+ \to \mathbb{R}$ is defined as

$$\Lambda(n) = \begin{cases} \log(p), & \text{if } n = p^k \text{ with } p \text{ prime and } 0 < k, \\ 0 & \text{otherwise.} \end{cases}$$

Prove that $\log = I*\Lambda$.

2.2 Mbius inversion

Next, we explain an important application of the Dirichlet convolution.

Definition 2.18. We define an operator $\mathcal{S} : R^{\mathbb{Z}^+} \to R^{\mathbb{Z}^+}$ defined by $\mathcal{S}(f) = f * I$, that is,

$$\mathcal{S}(f)(n) \coloneqq \sum_{d|n} f(d).$$

We have that $\mathcal{S}^{-1}(f) = f * \mu$, which implies that $\mathcal{S}$ is a bijective correspondence. Moreover, $\mathcal{S} : \mathrm{Mult}(R) \to \mathrm{Mult}(R)$ is also a biyective correspondence. Given $F \in R^{\mathbb{Z}^+}$, we call $\mathcal{S}^{-1}(F)$ the **Mbius inverse** of F.

Example 2.19. (i) Since $I = \mu^{-1}$, $\mathcal{S}(\mu) = \varepsilon$.

$\mathcal{S}^{-1}(\mu) = \mu * \mu$ is a bit more complicated. We fix a prime p and $k \in \mathbb{N}$.

$$S^{-1}(\mu)(p^k) = (\mu * \mu)(p^k) = \begin{cases} \mu(1)\mu(1) = 1_R, & \text{if } k = 0, \\ \mu(1)\mu(p) + \mu(p)\mu(1) = -2_R, & \text{if } k = 1, \\ \mu(1)\mu(p^2) + \mu(p)\mu(p) + \mu(p^2)\mu(1) = 1_R, & \text{if } k = 2, \\ \mu(1)\mu(p^k) + \mu(p)\mu(p^{k-1}) + \cdots + \mu(p^k)\mu(1) = 0_R, & \text{if } k \geq 3. \end{cases}$$

$S^{-1}(\mu)$ is the function that extends multiplicatively that evaluation.

(ii) $\mathcal{S}(\varepsilon) = I$ because ε is the identity and as we have seen, $\mathcal{S}^{-1}(\varepsilon) = \mu$.

(iii) $\mathcal{S}^{-1}(s) = s * \mu = \varepsilon$ and $\mathcal{S}(s) = \tau$ because

$$\mathcal{S}(I)(n) = \sum_{d|n} I(d) = \sum_{d|n} 1 = \tau(n).$$

(iv) $\mathcal{S}(\mathrm{id}) = \sigma$ because

$$\mathcal{S}(s)(n) = \sum_{d|n} \mathrm{id}(d) = \sum_{d|n} d = \sigma(n).$$

$\mathcal{S}^{-1}(\mathrm{id}) = \mathrm{id} * \mu$ is a bit more complicated. We fix a prime p and $k \in \mathbb{N}$.

$$(\mathrm{id} * \mu)(p^k) = \begin{cases} \mathrm{id}(1)\mu(1) = 1_R, & \text{if } k = 0, \\ \mathrm{id}(1)\mu(p) + \mathrm{id}(p)\mu(1) = p_R - 1_R, & \text{if } k = 1, \\ \mathrm{id}(1)\mu(p^k) + \cdots + \mathrm{id}(p^{k-1})\mu(1) + \mathrm{id}(p^k)\mu(1) = p_R^{k-1}(p_R - 1_R), & \text{if } k \geq 2. \end{cases}$$

$S^{-1}(\mathrm{id})$ is the function that extends multiplicatively that evaluation, which is Euler totient function φ.

Example 2.20. The usefulness of Mbius inversion lies beyond what we have seen. They constitute an effective method to simplify computation. For example, suppose we are asked to compute

$$\sum_{i=1}^{n} \sum_{j=1}^{i} \gcd(i, j).$$

We have already seen that $S(\varphi) = \mathrm{id}$, that is, $\mathrm{id} = I * \varphi$, so it follows that

$$\sum_{i=1}^{n} \sum_{j=1}^{i} \gcd(i, j) = \sum_{i=1}^{n} \sum_{j=1}^{i} (I * \varphi)(\gcd(i, j)) = \sum_{i=1}^{n} \sum_{j=1}^{i} \sum_{d|\gcd(i,j)} \varphi(d).$$

For fixed $i \in \{1, \ldots, n\}$, lets simplify $\sum_{j=1}^{i} (I * \varphi)(\gcd(i, j))$.

If we fix $d \mid i$, then $d \mid \gcd(i,j)$ if and only if $d \mid j$. There are $\left\lfloor \frac{i}{d} \right\rfloor = \frac{i}{d}$ possible values of j that satisfy the last condition, namely $d, 2d, \dots, \frac{i}{d}d$. Therefore, we can deduce that

$$\sum_{i=1}^{n}\sum_{j=1}^{i}\gcd(i,j) = \sum_{i=1}^{n}\sum_{j=1}^{i}\sum_{d \mid \gcd(i,j)} \varphi(d) = \sum_{i=1}^{n}\sum_{d \mid i}\frac{i}{d}\cdot\varphi(d) = \sum_{i=1}^{n}(\mathrm{id} * \varphi)(i).$$

The only remaining problem is how to compute the prefix sum of $(\mathrm{id} * \varphi)$. This function is multiplicative, and its value at a prime power p^k with $k > 0$ is given by

$$(\mathrm{id} * \varphi)(p^k) = \sum_{i=0}^{k}\varphi(p^i)\cdot\mathrm{id}(p^{k-i}) = (1 \cdot p^k + (p-1)\cdot p^{k-1} + \cdots + (p-1)p^{k-2}\cdot p\, + (p-1)p^{k-1}\cdot 1) = \\ p^{k-1}\cdot(p + k(p-1)) = p^{k-1}\cdot((k+1)p - k)\,.$$

$\mathrm{id} * \varphi$ can be precomputed in linear time with a linear sieve. This let us compute $\sum_{i=1}^{n}\sum_{j=1}^{i}\gcd(i,j)$ in $\mathcal{O}(n)$, which is better than the naive approach in $\mathcal{O}(n^2\log(n))$. We will see later more advanced methods for computing prefix sums.

Example 2.21. Now we do a more difficult example. Suppose we have an array $A[1:n]$ where $1 \le A[i] \le L$ for every $i \in \{1,\dots,n\}$. We are asked to compute

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\mathrm{lcm}(A[i],A[j]).$$

Let $d = \gcd(A[i],A[j])$, if we rewrite the formula iterating over the possible gcd we get

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\mathrm{lcm}(A[i],A[j]) = \sum_{d=1}^{L}\sum_{\substack{i\in\{1,\dots,n\}\\ d\mid A[i]}}\sum_{\substack{j\in\{1,\dots,n\},d\mid A[j]\\ d=\gcd(A[i],A[j])}}\frac{A[i]A[j]}{d} =$$

$$\sum_{d=1}^{L}\sum_{\substack{i\in\{1,\dots,n\}\\ d\mid A[i]}}\sum_{\substack{j\in\{1,\dots,n\}\\ d\mid A[j]}}\frac{A[i]A[j]}{d}\cdot\varepsilon\left(\gcd\left(\frac{A[i]}{d},\frac{A[j]}{d}\right)\right) =$$

$$\sum_{d=1}^{L}\sum_{\substack{i\in\{1,\dots,n\}\\ d\mid A[i]}}\sum_{\substack{j\in\{1,\dots,n\}\\ d\mid A[j]}}\frac{A[i]A[j]}{d}\cdot(I * \mu)\left(\gcd\left(\frac{A[i]}{d},\frac{A[j]}{d}\right)\right) =$$

$$\sum_{d=1}^{L}\sum_{\substack{i\in\{1,\dots,n\}\\ d\mid A[i]}}\sum_{\substack{j\in\{1,\dots,n\}\\ d\mid A[j]}}\frac{A[i]A[j]}{d}\cdot\sum_{k\mid\gcd\left(\frac{A[i]}{d},\frac{A[j]}{d}\right)}\mu(k) =$$

$$\sum_{d=1}^{L}\sum_{k=1}^{\left\lfloor\frac{L}{d}\right\rfloor}\mu(k)\sum_{\substack{i\in\{1,\dots,n\}\\ dk\mid A[i]}}\sum_{\substack{j\in\{1,\dots,n\}\\ dk\mid A[j]}}\frac{A[i]A[j]}{d} =$$

$$\sum_{d=1}^{L}\sum_{k=1}^{\left\lfloor\frac{L}{d}\right\rfloor}\frac{\mu(k)}{d}\sum_{\substack{i\in\{1,\dots,n\}\\ dk\mid A[i]}}\sum_{\substack{j\in\{1,\dots,n\}\\ dk\mid A[j]}}A[i]A[j].$$

Now, we change variables. Let $r = k \cdot d$, it follows that

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \operatorname{lcm}(A[i], A[j]) =$$

$$\sum_{d=1}^{L}\sum_{k=1}^{\left\lfloor \frac{L}{d} \right\rfloor} \frac{\mu(k)}{d} \sum_{\substack{i\in\{1,\dots,n\}\\ dk \mid A[i]}} \sum_{\substack{j\in\{1,\dots,n\}\\ dk \mid A[j]}} A[i]A[j] =$$

$$\sum_{r=1}^{L}\sum_{d \mid r} \frac{\mu\left(\frac{r}{d}\right)}{d} \sum_{\substack{i\in\{1,\dots,n\}\\ r \mid A[i]}} \sum_{\substack{j\in\{1,\dots,n\}\\ r \mid A[j]}} A[i]A[j] =$$

$$\sum_{r=1}^{L}\sum_{d \mid r} \frac{\mu\left(\frac{r}{d}\right)}{d} \cdot \left(\sum_{\substack{i\in\{1,\dots,n\}\\ r \mid A[i]}} A[i] \right)^2 .$$

Let $a : \{1, \dots, L\} \to \mathbb{Z}^+$ be defined as

$$a(r) \coloneqq \sum_{\substack{i\in\{1,\dots,n\}\\ r \mid A[i]}} A[i].$$

a_r can be precomputed doing a sieve in $\mathcal{O}(L \log(L))$. It is important to count the number of occurrences in the array of each integer in the range $\{1, \dots, L\}$, which gives a cost in $\Omega(n)$.

Therefore, the formula simplifies as follows.

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \operatorname{lcm}(A[i], A[j]) =$$

$$\sum_{r=1}^{L}\sum_{d \mid r} \frac{\mu\left(\frac{r}{d}\right)}{d} \cdot \left(\sum_{\substack{i\in\{1,\dots,n\}\\ r \mid A[i]}} A[i] \right)^2 =$$

$$\sum_{r=1}^{L}\sum_{d \mid r} \frac{\mu\left(\frac{r}{d}\right)}{d} \cdot a(r)^2 =$$

$$\sum_{r=1}^{L} a(r)^2 \cdot \left(\frac{I}{\mathrm{id}} * \mu \right)(r).$$

$\left(\frac{I}{\mathrm{id}} * \mu\right)$ is a multiplicative function. For each prime power p^k with $k > 0$, the value at $\left(\frac{I}{\mathrm{id}} * \mu\right)$ is

$$\left(\frac{I}{\mathrm{id}} * \mu \right)(p^k) = \left(\frac{1}{p^k} \cdot 1 + \frac{1}{p^{k-1}} \cdot (-1) + 0 \right) = -\frac{p-1}{p^k}.$$

Therefore $\frac{I}{\mathrm{id}} * \mu = \frac{\mathrm{id} * \mu}{\mathrm{id}}$ and since $r \mid a(r)$, the final formula can be simplified to

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \operatorname{lcm}(A[i], A[j]) = \sum_{r=1}^{L} \frac{a(r)^2}{r} \cdot (\mathrm{id} * \mu)(r).$$

Since we already have a cost $\mathcal{O}(L \log(L))$ computing $a(r)$, the cost of computing $\mathrm{id} * \mu$ is absorbed in $\mathcal{O}(L \log(L))$. In conclusion this algorithm runs in $\mathcal{O}(L \log(L) + n)$, while the naive approach runs in $\mathcal{O}(n^2 \log(L))$. The cost in extra space is in $\mathcal{O}(L + n)$.

Example 2.22. Finally, we provide a second example illustrating the same method. Suppose that we have an array $A[1 : n]$ of pairwise different elements such that $1 \leq A[i] \leq L$ for every $i \in \{1, \dots, n\}$.

We are asked to compute the number of subsets of size l such that the elements of the subset have no common divisor other than 1.

$$\sum_{1\le i_1<\cdots<i_l\le n} \varepsilon\left(\gcd\left(A[i_1],\ldots,A[i_l]\right)\right) =$$

$$\sum_{1\le i_1<\cdots<i_l\le n} \left(I*\mu\right)\left(\gcd\left(A[i_1],\ldots,A[i_l]\right)\right) =$$

$$\sum_{1\le i_1<\cdots<i_l\le n} \left(\sum_{d\mid\gcd(A[i_1],\ldots,A[i_l])} \mu(d)\right) =$$

$$\sum_{d=1}^{L} \left(\sum_{\substack{1\le i_1<\cdots<i_l\le n\\ d\mid A[i_1],\ldots,d\mid A[i_l]}} \mu(d)\right) =$$

$$\sum_{d=1}^{L} \mu(d)\cdot\left(\sum_{\substack{1\le i_1<\cdots<i_l\le n\\ d\mid A[i_1],\ldots,d\mid A[i_l]}} 1\right).$$

In the last equation,

$$\sum_{\substack{1\le i_1<\cdots<i_l\le n\\ d\mid A[i_1],\ldots,d\mid A[i_l]}} 1$$

gives the number of subsets of size l of A where each element is divisible by d.

If we define $f(d)$ as the number of elements of A divisible by d, the number of subsets of size l where each element is divisible by d is $\binom{f(d)}{l}$, where $\binom{f(d)}{l}=0$ when $f(d)<l$. It follows the following equation.

$$\sum_{1\le i_1<\cdots<i_l\le n} \varepsilon\left(\gcd\left(A[i_1],\ldots,A[i_l]\right)\right) =$$

$$\sum_{d=1}^{L} \mu(d)\cdot\left(\sum_{\substack{1\le i_1<\cdots<i_l\le n\\ d\mid A[i_1],\ldots,d\mid A[i_l]}} 1\right) =$$

$$.\sum_{d=1}^{L} \mu(d)\cdot\binom{f(d)}{l}.$$

The values $\mu(d)$ can be precomputed with a sieve in $\mathcal{O}(L)$ time. Moreover, by storing for each square-free integer d its prime factorization during the same sieve, we can compute all values of $f(d)$ in $\mathcal{O}(L\log(L))$ time and $\mathcal{O}(L)$ space. The binomial coefficient can be computed in $\mathcal{O}(L\cdot l)$ time and $\mathcal{O}(L)$ space. The final complexity of the algorithm belongs to $\mathcal{O}(L\cdot(\log(L)+l))$ in time and $\mathcal{O}(L)$ in space.

Problems

Ex 15. In Example 2.21 and Example 2.22 we derived the final formula directly. However, it is usually easier to apply the inclusion-exclusion principle to this kind of problem. Work out each of the examples mentioned with the inclusion-exclusion principle and deduce the same solution.

Ex 16. Give an algorithm for computing the number of coprimes pairs in the range $\{1, \dots, n\}$ in $\mathcal{O}(n)$ time and explain its extra space complexity.

Ex 17. Give an algorithm for computing $\sum_{i=1}^{n} \sum_{j=1}^{n} \operatorname{lcm}(i, j)$ in $\mathcal{O}(n)$ time and explain its extra space complexity.

Ex 18. Let Σ be an alphabet of size k. Consider words of size $n \in \mathbb{Z}^+$, that is Σ^n. We define A_d for $d \mid n$ as the number of words in Σ^n with exact period d and B_d as the number of words in Σ^n with exact period d up to rotation. Use Mbius inversion to give a formula for A_n and deduce B_n.

2.3 Further prefix sum optimization

Again we are interested in computing the prefix sum for some $f \in R^{\mathbb{Z}^+}$,

$$\Sigma_f(n) := \sum_{k=1}^{n} f(k).$$

If we want to compute $\Sigma_f(n)$, then we will search a decomposition $h = g * f$.

We start by giving two important lemmas.

Lemma 2.23. *Let $k_1, k_2, k_3 \in \mathbb{Z}^+$, then*

$$\left\lfloor \frac{\left\lfloor \frac{k_1}{k_2} \right\rfloor}{k_3} \right\rfloor = \left\lfloor \frac{k_1}{k_2 \cdot k_3} \right\rfloor.$$

Proof. By the division algorithm for positive integers, there exists unique $q_1, r_1 \in \mathbb{N}$ with $r_1 < k_2$ such that $k_1 = k_2 q_1 + r_1$. q_1 coincides with $\left\lfloor \frac{k_1}{k_2} \right\rfloor$.

Again by the division algorithm for positive integers, there exists unique $q_2, r_2 \in \mathbb{N}$ with $r_2 < k_3$ such that $q_1 = k_3 q_2 + r_2$. Therefore, $q_2 = \left\lfloor \frac{q_1}{k_3} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{k_1}{k_2} \right\rfloor}{k_3} \right\rfloor$.

Substituting $q_1 = k_3 q_2 + r_2$ in the first division yields that

$$k_1 = (k_2 k_3) q_2 + (k_2 r_2 + r_1).$$

Next we prove that the previous equation is the integer division of k_1 by $k_2 k_3$. Since integer division is unique, we only need to check that $q_2, (k_2 r_2 + r_1) \in \mathbb{N}$ and $k_2 r_2 + r_1 < k_2 k_3$. The first condition is obviously true and for the second one

$$k_2 r_2 + r_1 < k_2 r_2 + k_2 = k_2(r_2 + 1) \leq k_2 k_3.$$

By the uniqueness of integer division,

$$\left\lfloor \frac{\left\lfloor \frac{k_1}{k_2} \right\rfloor}{k_3} \right\rfloor = q_2 = \left\lfloor \frac{k_1}{k_2 k_3} \right\rfloor.$$

□

Lemma 2.24. *Let $n \in \mathbb{Z}^+$. Then*

$$\text{Card}\left(\left\{ \left\lfloor \frac{n}{d} \right\rfloor \,\middle|\, 1 \leq d \leq n \right\}\right) \leq 2\lfloor \sqrt{n} \rfloor.$$

Proof.

$$\text{Card}\left(\left\{ \left\lfloor \frac{n}{d} \right\rfloor \,\middle|\, 1 \leq d \leq \lfloor \sqrt{n} \rfloor \right\}\right) \leq \lfloor \sqrt{n} \rfloor.$$

For every $d \in \{\lfloor \sqrt{n} \rfloor + 1, \dots, n\}$, $1 \leq \left\lfloor \frac{n}{d} \right\rfloor \leq \lfloor \sqrt{n} \rfloor$ since $0 = \left\lfloor \frac{n}{d \cdot (\lfloor \sqrt{n} \rfloor + 1)} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{n}{d} \right\rfloor}{\lfloor \sqrt{n} \rfloor + 1} \right\rfloor$. Therefore,

$$\text{Card}\left(\left\{ \left\lfloor \frac{n}{d} \right\rfloor \,\middle|\, 1 \leq d \leq n \right\}\right) =$$
$$\text{Card}\left(\left\{ \left\lfloor \frac{n}{d} \right\rfloor \,\middle|\, 1 \leq d \leq \lfloor \sqrt{n} \rfloor \right\}\right) + \text{Card}\left(\left\{ \left\lfloor \frac{n}{d} \right\rfloor \,\middle|\, \lfloor \sqrt{n} \rfloor + 1 \leq d \leq n \right\}\right) \leq 2\lfloor \sqrt{n} \rfloor.$$

□

Now we begin with the optimization. We suppose that $f \in R^{\mathbb{Z}^+}$ can be decomposed as $h = f * g$, so more sophisticated techniques can be used to exploit the structure of f. Then it is satisfied that

$$\Sigma_h(n) = \sum_{k=1}^{n} h(k) = \sum_{k=1}^{n} \sum_{d|k} g(d) \cdot f\left(\frac{k}{d}\right) =$$
$$\sum_{d=1}^{n} \sum_{r=1}^{\left\lfloor \frac{n}{d} \right\rfloor} g(d) \cdot f(r) = \sum_{d=1}^{n} g(d) \cdot \left(\sum_{r=1}^{\left\lfloor \frac{n}{d} \right\rfloor} f(r) \right) = \sum_{d=1}^{n} g(d) \cdot \Sigma_f\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

We can isolate the term for $d = 1$, which gives us

$$\Sigma_h(n) = g(1) \cdot \Sigma_f(n) + \sum_{d=2}^{n} g(d) \cdot \Sigma_f\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

If $g(1) \neq 1$ and we can solve for Σ_f, which yields

$$\Sigma_f(n) = \frac{\Sigma_h(n) - \sum_{d=2}^{n} g(d) \cdot \Sigma_f\left(\left\lfloor \frac{n}{d} \right\rfloor\right)}{g(1)}.$$

Let

$$\begin{aligned} A^-(n) &:= \left\{ \left\lfloor \frac{n}{d} \right\rfloor \,\middle|\, 1 \leq d \leq \lfloor \sqrt{n} \rfloor \right\}, \\ A^+(n) &:= \left\{ \left\lfloor \frac{n}{d} \right\rfloor \,\middle|\, \lfloor \sqrt{n} \rfloor + 1 \leq d \leq n \right\}, \\ A(n) &:= A^-(n) \sqcup A^+(n). \end{aligned}$$

As we have seen in Lemma 2.24, the elements of $A^+(n)$ are bounded above by $\lfloor \sqrt{n} \rfloor$ while the elements of $A^-(n)$ are bounded bellow by $\lfloor \sqrt{n} \rfloor$, since the sequence $\left\lfloor \frac{n}{1} \right\rfloor, \left\lfloor \frac{n}{3} \right\rfloor, \ldots, \left\lfloor \frac{n}{n} \right\rfloor$ is non-increasing and $\lfloor \sqrt{n} \rfloor^2 \leq n$. There are a lot more indices in $A^+(n)$ than in $A^-(n)$, but in $A^+(n)$ several indices collapse to the same value.

Since the sequence $\left\lfloor \frac{n}{1} \right\rfloor, \left\lfloor \frac{n}{3} \right\rfloor, \ldots, \left\lfloor \frac{n}{n} \right\rfloor$ is non-increasing, we can compute an interval partition of $\{1, \ldots, n\}$ such that each interval represents a value of the sequence. Suppose we have $d \in \{1, \ldots, n\}$, how can we compute the interval that contains d?

Let $\left\lfloor \frac{n}{d} \right\rfloor = k$, then for every element x of the same interval as d is satisfied that

$$k \leq \frac{n}{x} < k + 1.$$

Solving for x we get that $\left\lfloor \frac{n}{x} \right\rfloor = k$ if and only if

$$\frac{n}{k+1} < x \leq \frac{n}{k}.$$

That last condition can be written as $x \in \left\{ \left\lfloor \frac{n}{k+1} \right\rfloor + 1, \ldots, \left\lfloor \frac{n}{k} \right\rfloor \right\}$, so the interval of d is

$$\left\{ \left\lfloor \frac{n}{\left\lfloor \frac{n}{d} \right\rfloor + 1} \right\rfloor + 1, \ldots, \left\lfloor \frac{n}{\left\lfloor \frac{n}{d} \right\rfloor} \right\rfloor \right\}.$$

This characterization and the Lemma 2.24 gives us an algorithm in $\mathcal{O}(\sqrt{n})$ that computes iteratively the desired interval partition. Let $\overline{A}$ be such partition. The formula for the prefix sum becomes

$$\Sigma_f(n) = \frac{\Sigma_h(n) - \sum_{(a,b) \in \overline{A}} \left(\Sigma_g(b) - \Sigma_g(a-1)\right) \cdot \Sigma_f\left(\left\lfloor \frac{n}{a} \right\rfloor\right)}{g(1)}.$$

At first it may seem that this formula is recursive but Lemma 2.23 assures us we only need to compute the values that belongs to $A(n)$ in all the recursive calls of the function. Therefore, this can be put as a triangular linear system of $\mathcal{O}(\sqrt{n})$ variables and equations that can be solved via substitution. It is important to notice that the equation with value $\left\lfloor \frac{n}{d} \right\rfloor$ associated involves at most $2 \cdot \sqrt{\left\lfloor \frac{n}{d} \right\rfloor}$ terms by Lemma 2.24. We suppose that we can compute $\Sigma_g(k)$ in $\mathcal{O}(1)$ and $\Sigma_h(k)$ in $\mathcal{O}(\sqrt{k})$.

In conclusion, the cost for solving the variables belonging to $A^+(n)$ is in $\mathcal{O}\left(\sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \sqrt{i}\right)$, where it is included the cost for computing Σ_h.

In order to better understand the cost, we prove the following lemma

Lemma 2.25. *For every $k \in \mathbb{Z}^+$,*

$$\sum_{i=1}^{k} \sqrt{i} \leq k^{\frac{3}{2}}.$$

Proof. We will show it by induction on k. It is obviously true for $k = 1$ and if it is satisfied by k, then

$$\sum_{i=1}^{k+1}\sqrt{i} = \sum_{i=1}^{k}\sqrt{i} + \sqrt{k+1} \leq \sum_{i=1}^{k}\sqrt{i} + \sqrt{3k} \leq \sqrt{k^3} + \sqrt{3k} \leq \sqrt{k^3+3k^2+3k+1} = (k+1)^{\frac{3}{2}}.$$

□

Therefore,

$$\sum_{i=1}^{\lfloor\sqrt{n}\rfloor}\sqrt{i} \leq \lfloor\sqrt{n}\rfloor^{\frac{3}{2}} \leq \left(\sqrt{n}\right)^{\frac{3}{2}} = n^{\frac{3}{4}}.$$

We deduce that the cost for solving the variables belonging to $A^+(n)$ is in $\mathcal{O}(n^{\frac{3}{4}})$.

Now, for solving the variables of $A^-(n)$, the cost is given by $\mathcal{O}\left(\sum_{i=1}^{\lfloor\sqrt{n}\rfloor}\sqrt{\left\lfloor\frac{n}{i}\right\rfloor}\right) = \mathcal{O}\left(\sum_{i=1}^{\lfloor\sqrt{n}\rfloor}\frac{\sqrt{n}}{\sqrt{i}}\right) = \mathcal{O}\left(\sum_{i=1}^{\lfloor\sqrt{n}\rfloor}\frac{\lfloor\sqrt{n}\rfloor}{\sqrt{i}}\right)$, where it is included the cost for computing Σ_h.

As before, in order to better understand the cost, we prove a lemma.

Lemma 2.26. *For every $k \in \mathbb{Z}^+$,*

$$\sum_{i=1}^{k}\frac{k}{\sqrt{i}} \leq 8\sqrt{k^3}.$$

Proof. Again, we show it by induction on k. It is obviously true for $k = 1$ and if it is satisfied by k, then

$$\sum_{i=1}^{k+1}\frac{k+1}{\sqrt{i}} = \sum_{i=1}^{k}\frac{k+1}{\sqrt{i}} + \frac{k}{\sqrt{k+1}} \leq \frac{k+1}{k}\cdot\sum_{i=1}^{k}\frac{k}{\sqrt{i}} + \frac{k}{\sqrt{k+1}} \leq$$
$$\frac{8(k+1)}{k}\sqrt{k^3} + \frac{k}{\sqrt{k+1}} = 8(k+1)\sqrt{k} + \frac{k\sqrt{k+1}}{k+1}.$$

The square of this last term satisifies that

$$\left(8(k+1)\sqrt{k} + \frac{k\sqrt{k+1}}{k+1}\right)^2 = 64(k^3+2k^2+k) + \frac{k^2}{k+1} + 16k\sqrt{k(k+1)} \leq$$
$$64(k^3+2k^2+k) + k + 16k(k+1) = 64k^3 + 144k^2 + 18k <$$
$$64k^3 + 192k^2 + 192k + 64 = \left(8\sqrt{k+1}\right)^2.$$

Therefore, we have proved that for $k \in \mathbb{Z}^+$

$$\sum_{i=1}^{k}\frac{k}{\sqrt{i}} \leq 8\sqrt{k^3}.$$

□

Substituting $k = \lfloor\sqrt{n}\rfloor$ in the last equation proves that solving the variables in $A^-(n)$ can be done in $\mathcal{O}\left(\sum_{i=1}^{\lfloor\sqrt{n}\rfloor}\frac{\lfloor\sqrt{n}\rfloor}{\sqrt{i}}\right) \subseteq \mathcal{O}\left(n^{\frac{3}{4}}\right)$

In conclusion, the whole algorithm runs in $\mathcal{O}(n^{\frac{3}{4}})$.

Nevertheless, if f is multiplicative we can precompute the values of Σ_f in the range $\{1,\ldots,m\}$ in $\mathcal{O}(m)$ with a sieve. Since we already have a cost in $\Omega(\sqrt{n})$ by iterating over the interval partition, we can suppose that $\lfloor\sqrt{n}\rfloor < m$. Therefore, our total cost would be in $\mathcal{O}(m)$ for precomputing Σ_f with a sieve and then $\mathcal{O}\left(\sum_{i=1}^{\lfloor\frac{n}{m}\rfloor}\sqrt{\left\lfloor\frac{n}{i}\right\rfloor}\right) = \mathcal{O}\left(\sqrt{m}\cdot\sum_{i=1}^{\lfloor\frac{n}{m}\rfloor}\sqrt{\frac{\lfloor\frac{n}{m}\rfloor}{i}}\right) = \mathcal{O}\left(\frac{\sqrt{m^2}}{\sqrt{n}}\cdot\sum_{i=1}^{\lfloor\frac{n}{m}\rfloor}\frac{\lfloor\frac{n}{m}\rfloor}{\sqrt{i}}\right) \subseteq \mathcal{O}\left(\frac{n}{\sqrt{m}}\right)$ for solving the remaining values of Σ_f in $A^-(n)$. Taking $\alpha \in [0,1]$ and $m = n^\alpha$ yields the total cost of $\mathcal{O}\left(\max\left\{n^\alpha, n^{1-\frac{\alpha}{2}}\right\}\right)$, which is minimized with $\alpha = \frac{2}{3}$.

The conclusion is that computing the prefix sum of such a multiplicative function can be done in $\mathcal{O}\left(n^{\frac{2}{3}}\right)$ precomputing with a sieve Σ_f until $\left\lfloor n^{\frac{2}{3}}\right\rfloor$ and then applying the previous algorithm. This method uses $\mathcal{O}\left(n^{\frac{2}{3}}\right)$ extra space and can be further optimized with a segmented sieve reaching $\mathcal{O}\left(\sqrt{n}\right)$ in extra space.

Problems

2.4 Dirichlet hyperbola method

We are interested in computing the prefix sum for some $f \in R^{\mathbb{Z}^+}$,

$$\Sigma_f(n) := \sum_{k=1}^{n} f(k).$$

As we have seen, computing prefix quickly can solve efficiently several problems. A classical approach for computing prefix sums of $f \in R^{\mathbb{Z}^+}$ is based on the **Dirichlet hyperbola method**.

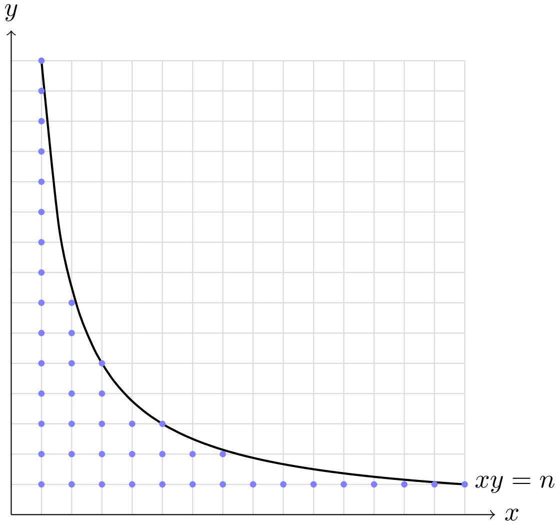
Let $f \in R^{\mathbb{Z}^+}$ and n be fixed. Suppose we are given $f = g * h$ for some $g, h \in R^{\mathbb{Z}^+}$. Then we can write

$$\sum_{k=1}^{n} f(k) = \sum_{k=1}^{n} \sum_{xy=k} g(x) \cdot h(y).$$

At first it may seem that our situation has worsened but we can view the two sumatoriums as the integer points below the hyperbola $\{(x, y) \in \mathbb{R}^2 \mid x \cdot y = n\}$, that is, the region where we have to sum the values of $g(x) \cdot h(y)$ is

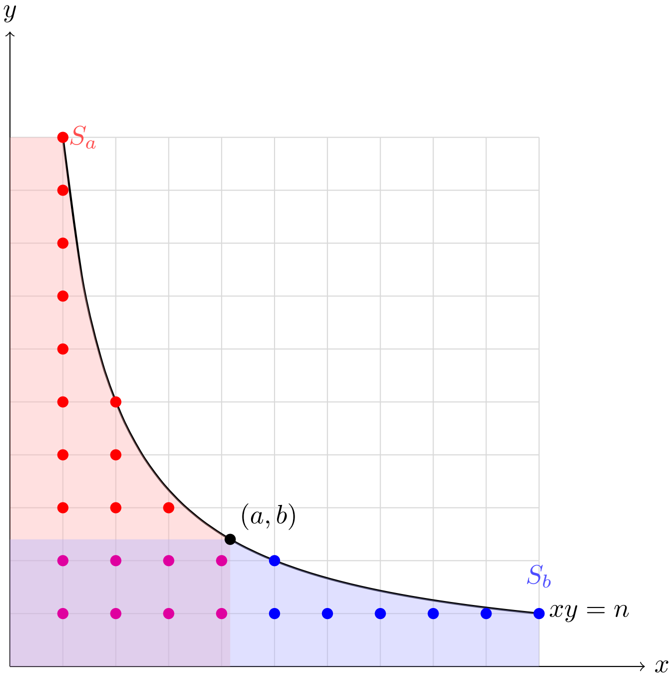
$$Z := \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid x \cdot y \leq n\}$$

For $n = 15$, Z corresponds with the blue dots of the following diagram:



Now suppose we are given $a, b \in \mathbb{R}^2$ such that $a \cdot b = n$. We will use a, b to divide Z. This division will not be disjoint, so we must take care of the intersection in order to use the inclusion-exclusion principle.

$$S_a := \{(x, y) \in \mathbb{R}^2 \mid xy \leq n,\ x \leq a\},$$
$$S_b := \{(x, y) \in \mathbb{R}^2 \mid xy \leq n,\ y \leq b\},$$
$$Z_a := S_a \cap Z = \{(x, y) \in Z \mid x \leq \lfloor a \rfloor\},$$
$$Z_b := S_a \cap Z_b = \{(x, y) \in Z \mid y \leq \lfloor b \rfloor\},$$
$$Z_a \cap Z_b = \{(x, y) \in Z \mid x \leq \lfloor a \rfloor,\ y \leq \lfloor b \rfloor\}.$$



For $n = 10$ and $a = \sqrt{n}+1$, $b = \frac{n}{a}$, we represent the region S_a (red) and S_b (blue) under the hyperbola. The integer points in $Z_a \setminus Z_b$ are red, the points in $Z_b \setminus Z_a$ are blue, and the points in $Z_a \cap Z_b$ are purple.

Therefore, by the inclusion-exclusion principle, we obtain that

$$\begin{aligned}\Sigma_f(n) = \sum_{k=1}^{n} f(k) = &\sum_{k=1}^{n}\sum_{xy=k} g(x)\cdot h(y) = \sum_{(x,y)\in Z} g(x)\cdot h(y) = \\ &\sum_{(x,y)\in Z_a} g(x)\cdot h(y) + \sum_{(x,y)\in Z_b} g(x)\cdot h(y) - \sum_{(x,y)\in Z_a\cap Z_b} g(x)\cdot h(y) = \\ &\sum_{x=1}^{\lfloor a\rfloor}\sum_{y=1}^{\lfloor \frac{n}{x}\rfloor} g(x)\cdot h(y) + \sum_{y=1}^{\lfloor b\rfloor}\sum_{x=1}^{\lfloor \frac{n}{y}\rfloor} g(x)\cdot h(y) - \sum_{x=1}^{\lfloor a\rfloor}\sum_{y=1}^{\lfloor b\rfloor} g(x)\cdot h(y) = \\ &\sum_{x=1}^{\lfloor a\rfloor}\left(g(x)\cdot\sum_{y=1}^{\lfloor \frac{n}{x}\rfloor} h(y)\right) + \sum_{y=1}^{\lfloor b\rfloor}\left(h(y)\cdot\sum_{x=1}^{\lfloor \frac{n}{y}\rfloor} g(x)\right) - \left(\sum_{x=1}^{\lfloor a\rfloor} g(x)\right)\cdot\left(\sum_{y=1}^{\lfloor b\rfloor} h(y)\right).\end{aligned}$$

We will see several examples where this method provides a cost in $\mathcal{O}(\sqrt{n})$ taking $a = b = \sqrt{n}$.

Example 2.27.

(i) Since $\tau = s * s$, if we take $a = b = \sqrt{n}$ and $g = h = s$, then it follows that

$$\begin{aligned}\sum_{k=1}^{n}\tau(k) = &\sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor \frac{n}{x}\rfloor} s(x)\cdot s(y) + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\sum_{x=1}^{\lfloor \frac{n}{y}\rfloor} s(x)\cdot s(y) - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\sqrt{n}\rfloor} s(x)\cdot s(y) = \\ &\sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor \frac{n}{x}\rfloor} 1 + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\sum_{x=1}^{\lfloor \frac{n}{y}\rfloor} 1 - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\sqrt{n}\rfloor} 1 = \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\left\lfloor\frac{n}{x}\right\rfloor + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\left\lfloor\frac{n}{y}\right\rfloor - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\lfloor\sqrt{n}\rfloor = \\ &2\cdot\left(\sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\left\lfloor\frac{n}{x}\right\rfloor\right) - \lfloor\sqrt{n}\rfloor^2.\end{aligned}$$

(ii) Since $\sigma = \mathrm{id} * s$, if we take $a = b = \sqrt{n}$, $g = \mathrm{id}$ and $h = s$, following the previous example we derive

$$\begin{aligned}\sum_{k=1}^{n}\sigma(k) = {} & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\frac{n}{x}\rfloor}\mathrm{id}(x)\cdot s(y) + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\sum_{x=1}^{\lfloor\frac{n}{y}\rfloor}\mathrm{id}(x)\cdot s(y) - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\mathrm{id}(x)\cdot s(y) = \\ & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\frac{n}{x}\rfloor} x + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\sum_{x=1}^{\lfloor\frac{n}{y}\rfloor} x - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\sqrt{n}\rfloor} x = \\ & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor} x\cdot\left\lfloor\frac{n}{x}\right\rfloor + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\frac{\left\lfloor\frac{n}{y}\right\rfloor\cdot\left(\left\lfloor\frac{n}{y}\right\rfloor+1\right)}{2} - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\lfloor\sqrt{n}\rfloor\cdot x = \\ & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor} x\cdot\left\lfloor\frac{n}{x}\right\rfloor + \frac{\lfloor\frac{n}{x}\rfloor\cdot(\lfloor\frac{n}{x}\rfloor+1)}{2} - \lfloor\sqrt{n}\rfloor\cdot x.\end{aligned}$$

(iii) Let $f \in \mathrm{Mult}(\mathbb{Z}^+)$ be such that $f = \mathrm{id} * \mathrm{id}$. It is easily veryfiable that for prime powers it is satisfied that $f(p^k) = (k+1)\cdot p^k$ and for other values we can extend multiplicatively. Again, we will give a formula for $\sum_{k=1}^{n} f(k)$, computable in $\mathcal{O}(\sqrt{n})$. We take $a = b = \sqrt{n}$ and $g = h = \mathrm{id}$.

$$\begin{aligned}\sum_{k=1}^{n} f(k) = {} & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\frac{n}{x}\rfloor}\mathrm{id}(x)\cdot\mathrm{id}(y) + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\sum_{x=1}^{\lfloor\frac{n}{y}\rfloor}\mathrm{id}(x)\cdot\mathrm{id}(y) - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\mathrm{id}(x)\cdot\mathrm{id}(y) = \\ & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\frac{n}{x}\rfloor} x\cdot y + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor}\sum_{x=1}^{\lfloor\frac{n}{y}\rfloor} x\cdot y - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor}\sum_{y=1}^{\lfloor\sqrt{n}\rfloor} x\cdot y = \\ & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor} x\cdot\sum_{y=1}^{\lfloor\frac{n}{x}\rfloor} y + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor} y\cdot\sum_{x=1}^{\lfloor\frac{n}{y}\rfloor} x - \sum_{x=1}^{\lfloor\sqrt{n}\rfloor} x\cdot\sum_{y=1}^{\lfloor\sqrt{n}\rfloor} y = \\ & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor} x\cdot\frac{\lfloor\frac{n}{x}\rfloor\cdot(\lfloor\frac{n}{x}\rfloor+1)}{2} + \sum_{y=1}^{\lfloor\sqrt{n}\rfloor} y\cdot\frac{\left\lfloor\frac{n}{y}\right\rfloor\cdot\left(\left\lfloor\frac{n}{y}\right\rfloor+1\right)}{2} - \left(\frac{\lfloor\sqrt{n}\rfloor\cdot(\lfloor\sqrt{n}\rfloor+1)}{2}\right)^2 = \\ & \sum_{x=1}^{\lfloor\sqrt{n}\rfloor} x\cdot\left(\left\lfloor\frac{n}{x}\right\rfloor\cdot\left(\left\lfloor\frac{n}{x}\right\rfloor+1\right)\right) - \left(\frac{\lfloor\sqrt{n}\rfloor\cdot(\lfloor\sqrt{n}\rfloor+1)}{2}\right)^2.\end{aligned}$$

Now we will continue where we left. The equation previous to the examples can be rewritten as

$$\Sigma_f(n) = \sum_{x=1}^{\lfloor a\rfloor}\left(g(x)\cdot\Sigma_h\left(\left\lfloor\frac{n}{x}\right\rfloor\right)\right) + \sum_{y=1}^{\lfloor b\rfloor}\left(h(y)\cdot\Sigma_g\left(\left\lfloor\frac{n}{y}\right\rfloor\right)\right) - \Sigma_g\left(\lfloor a\rfloor\right)\cdot\Sigma_h\left(\lfloor b\rfloor\right).$$

If we denote as A_x the interval partition of $\{1,\ldots,\lfloor a\rfloor\}$ according to the value of $\lfloor\frac{n}{d}\rfloor$ and A_y the interval partition of $\{1,\ldots,\lfloor b\rfloor\}$, the previous formula can be rewritten as

$$\begin{aligned}\Sigma_f(n) = & \sum_{(a_x,b_x)\in A_x}\left(\left(\Sigma_g(b_x)-\Sigma_g(a_x-1)\right)\cdot\Sigma_h\left(\left\lfloor\frac{n}{a_x}\right\rfloor\right)\right) + \\ & \sum_{(a_y,b_y)\in A_Y}\left(\left(\Sigma_h(b_y)-\Sigma_h(a_y-1)\right)\cdot\Sigma_g\left(\left\lfloor\frac{n}{a_y}\right\rfloor\right)\right) - \Sigma_g\left(\lfloor a\rfloor\right)\cdot\Sigma_h\left(\lfloor b\rfloor\right).\end{aligned}$$

If we can compute $\Sigma_g(k) \in \mathcal{O}(k^\alpha)$ and $\Sigma_h(k) \in \mathcal{O}(k^\beta)$ for $\alpha, \beta \in [0,1]$, the total cost would be in $\mathcal{O}(\sum_{i=1}$

Problems

References

[b] Adamant. *Dirichlet Convolution. Part 1: Fast Prefix Sum Computations*. Codeforces. URL: https://codeforces.com/blog/entry/117635 (visited on 12/08/2025).

[Nisa] Suzune Nisiyama. *[Tutorial] Math Note Dirichlet Convolution*. Codeforces. URL: https://codeforces.com/blog/entry/54150 (visited on 12/08/2025).

[Nisb] Suzune Nisiyama. *[Tutorial] Math Note Mbius Inversion*. Codeforces. URL: https://codeforces.com/blog/entry/53925 (visited on 12/08/2025).