# Number Theory

## 1 The fundamental theorem of arithmetic

An integer $p > 1$ is a prime number if its only positive divisors are $1$ and $p$ (by convention, $p = 1$ is not considered a prime number). The prime numbers form an infinite set. Indeed, if there was finitely many prime numbers $p_1 < p_2 < \cdots < p_k$, then $q := p_1 p_2 \cdots p_k + 1 > p_k$ would not be prime, hence it would be divisible by some prime number $p_i$, but then $p_i | q - p_1 \cdots p_i \cdots p_k = 1$, which is absurd. In fact, the prime number theorem states that the number $\pi(n)$ of primes less than or equal to $n$ behaves like $n/\ln(n)$ as $n \to \infty$.

The fundamental theorem of arithmetic states that every integer $n > 1$ can be written uniquely (up to the order of factors) as product of primes.

## 2 Euclid algorithm and its consequences

Two integers $n > 1$ and $m > 1$ are called coprime (or relatively prime) if they share no common prime factor. Stated differently, $n$ and $m$ are coprime if their greatest common divisor is $1$. The notions of greatest common divisor and least common multiple are self-explanatory. With obvious notations, we have $\gcd(n, m) \cdot \mathrm{lcm}(n, m) = n \cdot m$. The greatest common divisor of $n$ and $m$ can be found via Euclid algorithm: with $n > m$, set $r_0 = n$, $r_1 = m$, and produce $r_k$ inductively for $k \geq 2$ from the division of $r_{k-2}$ by $r_{k-1}$ as

$$r_{k-2} = q_{k-1} r_{k-1} + r_k, \qquad 0 \leq r_k < r_{k-1}.$$

Since the sequence of nonnegative numbers $(r_k)_{k \geq 0}$ is strictly decreasing, it eventually reaches $r_K = 0$, and $\gcd(n, m) = r_{K-1}$. This is the case because $\gcd$ is preserved at each iteration, i.e.,

$$\gcd(r_{k-2}, r_{k-1}) = \gcd(r_{k-1}, r_k), \qquad k \geq 2, \tag{1}$$

hence $\gcd(n, m) = \gcd(r_0, r_1) = \gcd(r_{K-2}, r_{K-1}) = r_{K-1}$ where the latter equality is due to the fact that $r_{K-2}$ divides $r_{K-1}$. The set of integer combinations is also preserved at each iteration, i.e.,

$$\{p r_k + q r_{k-1}, (p, q) \in \mathbb{Z}\} = \{p r_{k+1} + q r_k, (p, q) \in \mathbb{Z}\}, \qquad k \geq 2, \tag{2}$$

so the equality between the first and last sets gives

$$\{pn + qm, (p, q) \in \mathbb{Z}\} = \gcd(n, m)\mathbb{Z}.$$

This implies in particular Bézout lemma, i.e.,

$$\gcd(n, m) = 1 \iff \exists\, p, q \in \mathbb{Z} \text{ such that } pn + qm = 1.$$

In turn, the latter is used to prove Euclid lemma (obvious with prime factor decompositions, but needed in the uniqueness part of the fundamental theorem of arithmetic) which says that

> if $m$ divides $nr$ and if $m$ and $n$ are coprime, then $m$ divides $r$.

To see this, write $nr = dm$ and $pn + qm = 1$, so that $r = (pn + qm)r = pdm + qmr = (pd + qr)m$.

## 3 Euler totient function

Define the Euler function $\phi$ on the positive integers by

$$\phi(n) := \mathrm{card}\{k \in [1:n] \text{ such that } k \text{ and } n \text{ are coprime}\}.$$

Note that, if $p$ is prime and if $s \geq 1$ is an integer, then $\phi(p^s) = p^s - p^{s-1} = p^s(1-1/p)$ (because there are $p^{s-1}$ integers in $[1:p^s]$ that are not coprime with $p^s$, namely $p, 2p, 3p, \ldots, p^{s-1}p = p^s$). Note also that $\phi$ is multiplicative, meaning that $\phi(nm) = \phi(n)\phi(m)$ whenever $n$ and $m$ are coprime (this is a consequence of the Chinese remainder theorem, see *Modular Arithmetic*). Combining these two facts with the prime factor decomposition $n = p_1^{s_1} p_2^{s_2} \cdots p_\ell^{s_\ell}$ of a positive integer gives the formula

$$\phi(n) = n \prod_{p \,\mathrm{prime},\, p|n} \Big(1 - \frac{1}{p}\Big).$$

Multiplying out the right-hand side yields

$$\phi(n) = \sum_{d|n} \frac{n}{d}\, \mu(d) = \sum_{d|n} d\, \mu\Big(\frac{n}{d}\Big), \tag{3}$$

where $\mu$ is the Möbius function defined by $\mu(1) = 1$ and, for $m > 1$,

$$\mu(m) := \begin{cases} (-1)^\ell & \text{if } m = p_1 p_2 \cdots p_\ell \text{ is a product of } \ell \text{ distinct primes,} \\ 0 & \text{if } p^2 | m \text{ for some prime } p. \end{cases}$$

This can be concisely written as $\phi = \mathrm{id} * \mu$, where the Dirichlet convolution is the commutative operation defined, for two functions $a, b$ on positive integers, by

$$(a * b)(n) = \sum_{ij=n} a(i) b(j).$$

This operation has an identity given by $e(1) = 1$ and $e(m) = 0$, $m > 1$, and is associative, since

$$[a * (b * c)](n) = \sum_{im=n} a(i)(b*c)(m) = \sum_{im=n} a(i) \sum_{jk=m} b(j)c(k) = \sum_{ijk=n} a(i)b(j)c(k),$$

$$[(a * b) * c](n) = \sum_{km=n} (a*b)(m)c(k) = \sum_{km=n} \sum_{ij=m} a(i)b(j)c(k) = \sum_{ijk=n} a(i)b(j)c(k).$$

Let us also notice that, for an integer $m > 1$ decomposed in prime factors as $m = p_1^{s_1} p_2^{s_2} \cdots p_\ell^{s_\ell}$,

$$\sum_{d|m} \mu(d) = \sum_{r_1,\ldots,r_\ell \in \{0,1\}} \mu(p_1^{r_1} p_2^{r_2} \cdots p_\ell^{r_\ell}) = \sum_{h=0}^{\ell} \binom{\ell}{h} (-1)^\ell = (1-1)^\ell, \qquad \text{i.e.,} \qquad \sum_{d|m} \mu(d) = 0.$$

Since the sum takes the value $1$ for $m = 1$, we have $\mu * 1 = e$. Now, if $a = b * \mu$, then $a * 1 = b * \mu * 1 = b * e = b$, and conversely, if $a * 1 = b$, then $b * \mu = a * 1 * \mu = a * e = a$. Spelling out the convolutions leads to Möbius inversion formula: for functions $a, b$ on positive integers,

$$a(n) = \sum_{d|n} b(d)\, \mu(n/d) \quad \text{for all } n \geq 1 \iff b(n) = \sum_{d|n} a(d) \quad \text{for all } n \geq 1.$$

Taking $a = \phi$ and $b = \mathrm{id}$ in the latter and using (3) gives Euler formula, that is

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

# 4 Exercises

Ex.1: Verify the statements made in (1) and (2).

Ex.2: Prove that the distance between two consecutive prime numbers is unbounded.

Ex.3: Prove that the product of three consecutive integers is never a perfect power (i.e., not a perfect square, not a perfect cube, etc.).

Ex.4: For an integer $n \geq 1$, prove that $n^4 - 7n^2 + 1$ cannot be a perfect square.

Ex.5: If $n$ is an integer with prime factor decomposition $n = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$, let $f(n) := \sum_{i=1}^{\ell} k_i p_i$ and $g(n) := \lim_{m \to \infty} \underbrace{f \circ \cdots \circ f}_{m \text{ times}}(n)$. Evaluate $g(100)$ and $g(10^{10})$. Find all odd integers $n > 1$ such that $n/2 < g(n) < n$.