1 Divisibility and Factorization

1.1 Divisibility

Definition 1.1 (Divisibility). *Let $a, b \in \mathbf{Z}$. We say that a* ***divides*** *b (equivalently, a* ***is a divisor of*** *b, or b* ***is divisible by*** *a, or a* ***is a factor of*** *b) if there exists $c \in \mathbf{Z}$ such that $b = ac$. We write $a \mid b$ if a divides b, and $a \nmid b$ if a does* not *divide b.*

Proposition 1.2 (Elementary properties of divisibility).

(i) *(Transitivity) Let $a, b, c \in \mathbf{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

(ii) *(Linear combinations) Let $a, b, c \in \mathbf{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid bn + cm$ for any $n, m \in \mathbf{Z}$. In particular, if $a \mid b$ and $a \mid c$, then $a \mid b + c$ and $a \mid b - c$.*

(iii) *(Size of divisors) Let $a, b \in \mathbf{Z}$, with $b \neq 0$. If $a \mid b$, then $|a| \leq |b|$. In particular, any* positive *divisor a of a* positive *integer b must fall in the interval $1 \leq a \leq b$.*

(iv) *(Divisibility and ratios) Let $a, b \in \mathbf{Z}$ with $a \neq 0$. Then $a \mid b$ holds if and only if $\frac{b}{a} \in \mathbf{Z}$.*

Definition 1.3 (Greatest integer function). *For any $x \in \mathbf{R}$, the* ***greatest integer function*** *$[x]$ is defined as the greatest integer m satisfying $m \leq x$. An alternative notation for $[x]$ is $\lfloor x \rfloor$, the* ***floor function****.*

Theorem 1.4 (Division Algorithm). *Given $a, b \in \mathbf{Z}$ with $b > 0$ there exist unique $q, r \in \mathbf{Z}$ such that $a = qb + r$ and $0 \leq r < b$. Moreover, q and r are given by the formulas $q = [a/b]$ and $r = a - [a/b]b$.*

1.2 Primes

Definition 1.5 (Primes and composite numbers). *Let $n \in \mathbf{N}$ with $n > 1$. Then n is called a* ***prime*** *if its only* positive *divisors are 1 and n; it is called* **composite** *otherwise. Equivalently, n is composite if it can be written in the form $n = ab$ with $a, b \in \mathbf{Z}$ and $1 < a < n$ (and hence also $1 < b < n$); and n is prime otherwise.*

Remark. The number 1 is not classified in this manner, i.e., 1 is neither prime nor composite.

Proposition 1.6 (Existence of prime factors). *Let $n \in \mathbf{N}$ with $n > 1$. Then n has at least one prime factor (possibly n itself); i.e., there exists a prime p with $p \mid n$.*

Proposition 1.7 (Primality test). *Let $n \in \mathbf{N}$ with $n > 1$. Then n is prime if and only if n is not divisible by any prime p with $p \leq \sqrt{n}$.*

Theorem 1.8 (Euclid's Theorem). *There are infinitely many primes.*

Theorem 1.9 (Gaps between primes). *There are arbitrarily large gaps between primes; i.e., for every $n \in \mathbf{N}$, there exist at least n consecutive composite numbers.*

Definition 1.10 (Prime counting function). *Let $x \in \mathbf{R}$ with $x > 0$. Then $\pi(x)$ is the number of primes p with $p \leq x$.*

***Theorem 1.11** (Prime Number Theorem). *The prime counting function $\pi(x)$ satisfies*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Definition 1.12 (Mersenne and Fermat primes).

(i) *The numbers of the form $M_p = 2^p - 1$, where p is prime, are called **Mersenne numbers;** a Mersenne number that is prime is called a **Mersenne prime**.*

(ii) *The numbers of the form $F_n = 2^{2^n} + 1$, where $n = 0, 1, \ldots,$ are called **Fermat numbers;** a Fermat number that is prime is called a **Fermat prime**.*

Conjectures (Famous conjectures about primes)**.**

(i) ***Mersenne primes:*** *There are infinitely many Mersenne primes.*

(ii) ***Fermat primes:*** *There are only finitely many Fermat primes.*

(iii) ***Twin Prime Conjecture:*** *There infinitely many primes p such that $p + 2$ is also prime.*

(iv) ***Goldbach Conjecture:*** *Every* even *integer $n \geq 4$ can be expressed as a sum of two primes (not necessarily distinct), i.e., n can be written in the form $n = p_1 + p_2$, where p_1 and p_2 are primes.*

1.3 The greatest common divisor

Definition 1.13 (Greatest common divisor)**.** *Let $a, b \in \mathbf{Z}$, with a and b not both 0. The **greatest common divisor (gcd)** of a and b, denoted by $\gcd(a, b)$, or simply (a, b), is defined as the largest among the commons divisor of a and b; i.e.,*

$$(a, b) = \gcd(a, b) = \max\{d : d \mid a \text{ and } d \mid b\}.$$

*If $(a, b) = 1$, then a and b are called **relatively prime** or **coprime**.*

More generally, the greatest common divisor of n integers $a_1, \ldots, a_n$, not all 0, is defined as

$$(a_1, \ldots, a_n) = \max\{d : d \mid a_i \text{ for } i = 1, 2, \ldots, n \ \}.$$

Proposition 1.14 (Elementary properties of the gcd)**.** *Let $a, b \in \mathbf{Z}$, with a and b not both 0.*

(i) $(a, b) = (-a, b) = (a, -b) = (-a, -b)$.

(ii) $(a, b) = (a + bn, b) = (a, b + am)$ *for any* $n, m \in \mathbf{Z}$.

(iii) $(ma, mb) = m(a, b)$ *for any* $m \in \mathbf{N}$.

(iv) *If* $d = (a, b)$, *then* $(a/d, b/d) = 1$.

(v) *Let* $d \in \mathbf{N}$. *Then* $d \mid (a, b)$ *holds if and only if* $d \mid a$ *and* $d \mid b$.

Theorem 1.15 (Linear combinations and the gcd)**.** *Let $a, b \in \mathbf{Z}$ with a and b not both 0, and let $d = (a, b)$. Then there exist $n, m \in \mathbf{Z}$ such that $d = na + mb$, i.e., d is a linear combination of a and b with integer coefficients. Moreover, the set of all such linear combinations is exactly equal to the set of integer multiples of d, and d is the least positive element of this set; i.e.,*

$$\{an + bm : n, m \in \mathbf{Z}\} = \{dq : q \in \mathbf{Z}\}$$

and

$$d = \min\{an + bm : n, m \in \mathbf{Z},\ an + bm > 0\}.$$

Theorem 1.16 (Euclidean Algorithm). *Let $a, b \in \mathbf{Z}$ with $a \geq b > 0$. Set $r_0 = a$, $r_1 = b$ and define $r_2, r_3, \dots, r_j$ by iteratively applying the division algorithm as follows, until a remainder* 0 *is obtained:*

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, \quad 0 < r_3 < r_2 \\ &\dots \\ r_{j-2} &= r_{j-1} q_{j-1} + r_j, \quad 0 < r_j < r_{j-1} \\ r_{j-1} &= r_j q_j. \end{aligned}$$

Then (a, b) is equal to the last non-zero remainder, i.e., $(a, b) = r_j$. Moreover, by tracing back the above chain of equations, one obtains an explicit *representation of (a, b) as a linear combination of a and b.*

1.4 The least common multiple

Definition 1.17 (Least common multiple). *Let $a, b \in \mathbf{Z}$, with a and b both nonzero. The* ***least common multiple (lcm) of** a **and** b*, denoted by $[a, b]$, is defined as the smallest positive integer that is divisible by both a and b; i.e.,*

$$[a, b] = \min\{m \in \mathbf{N} : a \mid m \text{ and } b \mid m\}.$$

More generally, the least common multiple of n nonzero integers $a_1, \dots, a_n$ is defined as

$$[a_1, \dots, a_n] = \min\{m \in \mathbf{N} : a_i \mid m \text{ for } i = 1, 2, \dots, n \ \}.$$

Proposition 1.18 (Elementary properties of the lcm). *Let a, b be nonzero integers.*

(i) $[a, b] = [-a, b] = [a, -b] = [-a, -b]$.

(ii) $[ma, mb] = m[a, b]$ *for any* $m \in \mathbf{N}$.

(iii) $[a, b] = \dfrac{|ab|}{(a, b)}$.

(iv) *Let $m \in \mathbf{N}$. Then $[a, b] \mid m$ holds if and only if $a \mid m$ and $b \mid m$.*

1.5 The Fundamental Theorem of Arithmetic

Lemma 1.19 (Euclid's Lemma). *If $a, b \in \mathbf{Z}$, and p is a prime such that $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if $a_1, \dots, a_n \in \mathbf{Z}$ and p is a prime such that $p \mid a_1 \cdots a_n$, then there exists an i with $1 \leq i \leq n$ such that $p \mid a_i$.*

Theorem 1.20 (Fundamental Theorem of Arithmetic). *Every integer greater than* 1 *has a unique factorization into primes; that is, every integer $n > 1$ can be represented in the form*

$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

where the p_i are distinct primes, and the exponents α_i are positive integers. Moreover, this representation is unique except for the ordering of the primes p_i.

Notation. *Given an integer $n > 1$, its prime factorization can be represented in any one of the following forms:*

(i) $$n = \prod_{i=1}^{s} p_i, \quad p_1, \dots, p_s \textit{ primes (}\text{not necessarily distinct}\textit{);}$$

(ii) $$n = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad p_1, \dots, p_r \text{ distinct } \textit{primes}, \quad \alpha_1, \dots, \alpha_r \text{ positive } \textit{integers;}$$

(iii) $$n = \prod_{i=1}^{t} p_i^{\alpha_i}, \quad p_1, \dots, p_t \text{ distinct } \textit{primes}, \quad \alpha_1, \dots, \alpha_t \text{ nonnegative } \textit{integers;}$$

(iv) $$n = \prod_{p \textit{ prime}} p^{\alpha_p}, \quad \alpha_p \text{ nonnegative } \textit{integers}, \ \alpha_p = 0 \textit{ for all but finitely many } p.$$

In the last form, p runs through all primes, so the product is formally an infinite product. However, since $\alpha_p = 0$ for all but finitely p, all but finitely many terms of the product are 1, so the product is de facto a finite product.

The forms (iii) and (iv) are particularly useful when considering the prime factorizations of several integers, since they allow one to express all factorizations with respect to a common "basis" of primes p_i (e.g., the set of all primes that divide at least one *of the given integers, or the set of* all *primes). As an illustration, here are some representations of the prime factorization of $n = 20$:*

$$\begin{aligned} 20 &= 2 \cdot 2 \cdot 5, \\ 20 &= 2^2 \cdot 5^1, \\ 20 &= 2^2 \cdot 3^0 \cdot 5^1 \\ 20 &= 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdots \end{aligned}$$

An additional advantage of the forms (iii) and (iv) is that they allow one to represent the integer 1 (to which the Fundamental Theorem of Arithmetic does not apply) formally *in the same form, as a product of prime powers, by taking all exponents to be 0:*

$$1 = \prod_{i=1}^{t} p_i^0 \quad \textit{or} \quad 1 = \prod_{p} p^0.$$

Proposition 1.21 (Divisibility, gcd, and lcm in terms of prime factorizations)**.** *Let $a, b \in \mathbf{N}$ with prime factorizations (of the form (iii) above) given by*

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{r} p_i^{\beta_i},$$

where the p_i are distinct *primes and the exponents α_i and β_i are* nonnegative *integers.*

(i) *Then "a divides b" holds if and only if $\alpha_i \le \beta_i$ for all i.*

(ii) *The gcd and lcm of a and b are given by*

$$(a, b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}, \quad [a, b] = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}.$$

1.6 Primes in arithmetic progressions

Definition 1.22 (Arithmetic progression). *A sequence of the form*

$$a, a+b, a+2b, a+3b, \dots, \tag{1.1}$$

where a and b are integers, is called an ***arithmetic progression****.*

***Theorem 1.23** (Dirichlet's Theorem on Primes in Arithmetic Progressions). *Let $a, b \in \mathbf{N}$ with $(a, b) = 1$. Then the arithmetic progression* (1.1) *contains infinitely many primes.*

2 Congruences

2.1 Definitions and basic properties; applications

Definition 2.1 (Congruences)**.** *Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$. We say that a* ***is congruent to*** *b* ***modulo*** *m, and write $a \equiv b \bmod m$, if $m \mid a-b$ (or, equivalently, if $a = b+mx$ for some $x \in \mathbf{Z}$). The integer m is called the* ***modulus*** *of the congruence.*

Proposition 2.2 (Elementary properties of congruences)**.** *Let $a, b, c, d \in \mathbf{Z}$, $m \in \mathbf{N}$.*

(i) *If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a + c \equiv b + d \bmod m$.*

(ii) *If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $ac \equiv bd \bmod m$.*

(iii) *If $a \equiv b \bmod m$, then $a^n \equiv b^n \bmod m$ for any $n \in \mathbf{N}$.*

(iv) *If $a \equiv b \bmod m$, then $f(a) \equiv f(b) \bmod m$ for any polynomial $f(n)$ with integer coefficients.*

(v) *If $a \equiv b \bmod m$, then $a \equiv b \bmod d$ for any positive divisor d of m.*

Proposition 2.3 (Congruences as equivalence relation)**.** *Let $m \in \mathbf{N}$. The congruence relation modulo m is an equivalence relation, i.e., satisfies the following properties, for any $a, b, c \in \mathbf{Z}$:*

(i) *(Reflexivity) $a \equiv a \bmod m$.*

(ii) *(Symmetry) If $a \equiv b \bmod m$, then $b \equiv a \bmod m$.*

(iii) *(Transitivity) If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.*

Definition 2.4 (Residue classes)**.** *Let $m \in \mathbf{N}$. The equivalence classes defined by the congruence relation modulo m are called the* ***residue classes modulo*** *m. For any $a \in \mathbf{Z}$, $[a]$ denotes the equivalence class to which a belongs, i.e.,*

$$[a] = \{n \in \mathbf{Z} : n \equiv a \bmod m\}.$$

Definition 2.5 (Complete residue system)**.** *A set of integers $r_1, \dots, r_m$ is called a* ***complete residue system modulo*** *m, if it contains exactly one integer from each equivalence class modulo m.*

Definition 2.6 (Least nonnegative residue)**.** *Let $m \in \mathbf{N}$. Given any integer n, the* ***least nonnegative residue of*** *n* ***modulo*** *m is the unique integer r such that $n \equiv r \bmod m$ and $0 \le r < m$; i.e., r is the remainder upon division of n by m by the division algorithm.*

2.2 Linear congruences in one variable

Theorem 2.7 (Solutions of linear congruences in one variable)**.** *Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$, and consider the congruence*

$$ax \equiv b \bmod m. \tag{2.1}$$

Let $d = (a, m)$.

(i) *(Existence of a solution) The congruence* (2.1) *has a solution $x \in \mathbf{Z}$ if and only if $d \mid b$.*

(ii) *(Number of solutions) Suppose $d \mid b$. Then $ax \equiv b \bmod m$ has exactly d pairwise incongruent solutions x modulo m. The solutions are of the form $x = x_0 + km/d$, $k = 0, 1, \dots, d-1$, where x_0 is a particular solution.*

(iii) *(Construction of a solution) Suppose $d \mid b$. Then a particular solution can be constructed as follows: Apply the Euclidean algorithm to compute $d = (a, m)$, and, working backwards, obtain a representation of d as a linear combination of a and m. Multiply the resulting equation through with (b/d). The new equation can be interpreted as a congruence of the desired type,* (2.1)*, and reading off the coefficient of a gives a particular solution.*

Corollary 2.8. *Let $a \in \mathbf{Z}$ and $m \in \mathbf{N}$. If $(a, m) = 1$, the congruence*

$$ax \equiv 1 \bmod m \tag{2.2}$$

has a unique solution x modulo m; if $(a, m) \neq 1$, the congruence has no solution.

Definition 2.9 (Modular inverses)**.** *A solution x to the congruence* (2.2)*, if it exists, is called a **modular inverse of** a (with respect to the modulus m) and denoted by $\overline{a}$.*

Remark. Note that $\overline{a}$ is not uniquely defined. The definition depends implicitly on the modulus m. In addition, for a given modulus m, $\overline{a}$ is only *unique modulo m*; i.e., any $x \in \mathbf{Z}$ with $x \equiv \overline{a} \bmod m$ is also a a modular inverse of m.

2.3 The Chinese Remainder Theorem

Theorem 2.10 (Chinese Remainder Theorem)**.** *Let $a_1, \dots, a_r \in \mathbf{Z}$ and let $m_1, m_2, \dots, m_r \in \mathbf{N}$ be given such that $(m_i, m_j) = 1$ for $i \neq j$. Then the system*

$$x \equiv a_i \bmod m_i \qquad (i = 1, \dots, r) \tag{2.3}$$

has a unique solution x modulo $m_1 \cdots m_r$.

Corollary 2.11 (Structure of residue systems modulo $m_1 \cdots m_r$)**.** *Let $m_1, \dots, m_r \in \mathbf{N}$ with $(m_i, m_j) = 1$ for $i \neq j$ be given and let $m = m_1 \cdots m_r$. There exists a 1-1 correspondence between complete systems of residues modulo m and r-tupels of complete systems of residues modulo $m_1, \dots, m_r$. More precisely, if, for each i, a_i runs through a complete system of residues modulo m_i, then the corresponding solution x to the simultaneous congruence* (2.3) *runs through a complete system of residues modulo m.*

2.4 Wilson's Theorem

Theorem 2.12 (Wilson's Theorem)**.** *Let p be a prime number. Then*

$$(p-1)! \equiv -1 \bmod p. \tag{2.4}$$

Theorem 2.13 (Converse to Wilson's Theorem)**.** *If p is an integer ≥ 2 satisfying* (2.4)*, then p is a prime number.*

Remark. The converse to Wilson's Theorem can be stated in contrapositive form as follows: *If n is composite, then $(n-1)!$ is **not** congruent to -1 modulo n.* In fact, the following much stronger statement holds: *If $n > 4$ and n is composite, then $(n-1)! \equiv 0 \bmod n$.* Thus, for $n > 4$, $(n-1)!$ is congruent to either -1 or 0 modulo n; the first case occurs if and only if n is prime, and the second occurs if and only if n is composite.

2.5 Fermat's Theorem

Theorem 2.14 (Fermat's Little Theorem)**.** *Let p be a prime number. Then, for any integer a satisfying $(a,p) = 1$,*

$$a^{p-1} \equiv 1 \bmod p. \tag{2.5}$$

Corollary 2.15 (Fermat's Little Theorem, Variant)**.** *Let p be a prime number. Then, for any integer a,*

$$a^p \equiv a \bmod p. \tag{2.6}$$

Corollary 2.16 (Inverses via Fermat's Theorem)**.** *Let p be a prime number, and let a be an integer such that $(p,a) = 1$. Then $\overline{a} = a^{p-2}$ is an inverse of a modulo p.*

Remark. In contrast to Wilson's Theorem, Fermat's Theorem does not have a corresponding converse; in fact, there exist numbers p that satisfy the congruence in Fermat's Theorem, but which are compositive. Such "false positives" to the Fermat test are rare, but they do exist, movitating the following definition:

Definition 2.17 (Pseudoprimes and Carmichael numbers)**.** *An integer $p \geq 2$ that is composite, but satisfies the Fermat congruence* (2.5)*, is called a **pseudoprime to the base** a, or a-**pseudoprime**. A 2-pseudoprime is simply called a **pseudoprime**. An integer p that is a pseudoprime to all bases $a \in \mathbf{N}$ with $(a,p) = 1$ is called a **Carmichael number**.*

2.6 Euler's Theorem

Definition 2.18 (Reduced residue system)**.** *Let $m \in \mathbf{N}$. A set of integers is called a* ***reduced residue system modulo*** *m, if (i) its elements are pairwise incongruent modulo m, and (ii) every integer n with $(n, m) = 1$ is congruent to an element of the set. Equivalently, a reduced residue system modulo m is the subset of a complete residue system consisting of those elements that are relatively prime with m.*

Definition 2.19 (Euler phi-function)**.** *Let $m \in \mathbf{N}$. The* ***Euler phi-function****, denoted by $\varphi(m)$, is defined by*

$$\varphi(m) = \#\{1 \le n \le m : (n, m) = 1\},$$

i.e., $\varphi(m)$ is the number of elements in a reduced system of residues modulo m.

Proposition 2.20. *If $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ is a reduced residue system modulo m, then so is the set $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$, for any integer a with $(a, m) = 1$.*

Theorem 2.21 (Euler's generalization of Fermat's theorem)**.** *Let $m \in \mathbf{N}$. Then, for any integer a such that $(a, m) = 1$,*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{2.7}$$

3 Arithmetic functions

3.1 Some notational conventions

Divisor sums and products: Let $n \in \mathbf{N}$.

- $\displaystyle\sum_{d|n} f(d)$ denotes a sum of $f(d)$, taken over all **positive divisors** d of n.
- $\displaystyle\sum_{p|n} f(p)$ denotes a sum of $f(p)$, taken over all **prime** divisors p of n.
- $\displaystyle\sum_{p^\alpha||n} f(p^\alpha)$ denotes a sum of $f(p^\alpha)$, taken over all **prime powers** p^α that occur in the standard prime factorization of n. (Here the double bar in $p^\alpha||n$ indicates that p^α is the exact power of p dividing n, i.e., $p^\alpha \mid n$, but $p^{\alpha+1} \nmid n$.)
- **Products** over $d \mid n$, $p \mid n$, etc., are defined analogously.

Empty sum/product convention: A sum over an empty set is defined to be 0; a product over an empty set is defined to be 1. Thus, for example, we have

$$\sum_{p^\alpha||1} f(p^\alpha) = 0, \quad \prod_{p^\alpha||1} f(p^\alpha) = 1,$$

since there is no prime power p^α satisfying the condition $p^\alpha||1$.

The above notational conventions greatly simplify the statements of formulas involving arithmetic functions. For example, using these conventions the rather clumsy formula

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 1, \\ \prod_{i=1}^r p_i^{\alpha_i - 1}(p_i - 1) & \text{if } n \geq 2 \text{ and } n = \prod_{i=1}^r p_i^{\alpha_i} \\ & \text{with distinct primes } p_i \text{ and } \alpha_i \in \mathbf{N}, \end{cases}$$

can be rewritten as

$$\varphi(n) = \prod_{p^\alpha||n} p^{\alpha-1}(p-1),$$

without having to introduce subscripts or single out the case $n = 1$. (In the latter case, the product is an empty product, so by the empty product convention, it produces the value 1, which is exactly what we need.)

Sums over 1's ("Bateman summation"): A sum in which each summand is equal to 1 simply counts the number of terms in it; for example, $\sum_{d|n} 1$ is the same as $\#\{d \in \mathbf{N} : d \mid n\}$. While this might seem like a contrived way to represent a counting function, in the context of the general theory of arithmetic functions, such representations are often very useful.

3.2 Multiplicative arithmetic functions

Definition 3.1 (Multiplicative arithmetic function)**.** *A function $f : \mathbf{N} \to \mathbf{C}$ is called an* ***arithmetic function****. An arithmetic function f is called* ***multiplicative*** *if it satisfies the relation*

$$f(n_1 n_2) = f(n_1) f(n_2) \tag{3.1}$$

whenever $((n_1, n_2) = 1)$*. If* (3.1) *holds for* ***all*** $n_1, n_2 \in \mathbf{N}$ *(i.e., without the restriction* $(n_1, n_2) = 1$*), then* f *is called* ***completely multiplicative****.*

Proposition 3.2 (Multiplicative functions and prime factorization)**.** *An arithmetic function* f *that is not identically* 0 *(i.e., such that* $f(n) \neq 0$ *for at least one* $n \in \mathbf{N}$*) is multiplicative if and only if it satisfies*

$$f(n) = \prod_{p^\alpha || n} f(p^\alpha) \quad (n \in \mathbf{N}).$$

In particular, any multiplicative function f *that is not identically* 0 *is uniquely determined by its values* $f(p^\alpha)$ *at prime powers and satisfies* $f(1) = 1$*.*

3.3 The Euler phi function and the Carmichael Conjecture

Definition 3.3 (Euler phi function)**.** *The Euler phi function is defined by*

$$\varphi(n) = \#\{1 \leq m \leq n : (m, n) = 1\}.$$

Proposition 3.4 (Properties of $\varphi(n)$)**.**

(i) *(Multiplicativity) The Euler phi function is multiplicative (though not completely multiplicative).*

(ii) *(Explicit formula) For any* $n \in \mathbf{N}$*,*

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

(iii) *(Gauss identity)*

$$\sum_{d|n} \varphi(d) = n \quad (n \in \mathbf{N}).$$

Conjecture (Carmichael conjecture)**.** *Given* $n \in \mathbf{N}$*, the equation* $\varphi(x) = n$ *has either no solution* $x \in \mathbf{N}$ *or more than one solution.*

Remark. The Carmichael conjecture has several local (UIUC) connections: Its originator, R.D. Carmichael, spent most of his career as a professor here at the U of I, and the conjecture first appeared as an "exercise" in a textbook on number theory he wrote (and which he presumably assigned to his students). Also, most of the current records on this conjecture are held by Kevin Ford, who earned his PhD here in the mid 1990s and is now back as a professor. In particular, Ford showed that the Carmichael conjecture is true for all $n \leq 10^{1000000000}$. Moreover, for any $k \in \mathbf{N}$ *except possibly* $k = 1$, there exist infinitely many $n \in \mathbf{N}$ such that the equation $\varphi(x) = n$ has exactly k solutions $x \in \mathbf{N}$. Thus, only the question of whether multiplicity $k = 1$ can occur remains open, and this is precisely the question addressed by the Carmichael conjecture.

3.4 The number-of-divisors functions

Definition 3.5 (Number-of-divisors function)**.** *The* ***number-of-divisors function*** *is defined by*

$$\nu(n) = \#\{d \in \mathbf{N} : d \mid n\} = \sum_{d \mid n} 1 \quad (n \in \mathbf{N}).$$

This function is often simply called the ***divisor function****; alternate, and more common, notations for it are $d(n)$ (for "**d**ivisor") and $\tau(n)$ (for "**T**eiler", the German word for "divisor").*

Proposition 3.6 (Properties of $\nu(n)$)**.**

(i) *(Multiplicativity) The function $\nu(n)$ is multiplicative (though not completely multiplicative).*

(ii) *(Explicit formula) For any $n \in \mathbf{N}$,*

$$\nu(n) = \prod_{p^\alpha || n} (\alpha + 1)$$

3.5 The sum-of-divisors functions and perfect numbers

Definition 3.7. *Sum-of-divisors function The* ***sum-of-divisors function*** *is defined by*

$$\sigma(n) = \sum_{d \mid n} d \quad (n \in \mathbf{N}).$$

Proposition 3.8 (Properties of $\sigma(n)$)**.**

(i) *(Multiplicativity) The function $\sigma(n)$ is multiplicative (though not completely multiplicative).*

(ii) *(Explicit formula) For any $n \in \mathbf{N}$,*

$$\sigma(n) = \prod_{p^\alpha || n} \frac{p^{\alpha+1} - 1}{p - 1}$$

Definition 3.9 (Perfect numbers)**.** *An positive integer n is called* **perfect** *if it is equal to the sum of its positive divisors $d \mid n$, with $1 \leq d < n$ (i.e., not counting $d = n$). Equivalently, n is perfect if and only if $\sigma(n) = 2n$.*

Example. The first 4 perfect numbers are $6(= 1+2+3)$, $28(= 1+2+4+7+14)$, 496, and 8128.

Theorem 3.10 (Characterization of even perfect numbers)**.** *An* even *positive integer n is perfect if and only if it is of the form*

$$n = 2^{p-1}(2^p - 1),$$

where $2^p - 1$ is a Mersenne prime.

Corollary 3.11. *There exist infinitely many even perfect numbers if and only if there exist infinitely many Mersenne primes.*

Example. The above four perfect numbers $6, 28, 496, 8128$ correspond to the first four Mersenne primes, $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, and $2^7 - 1 = 127$.