

# Math 453: Elementary Number Theory

## Definitions and Theorems

(Class Notes, Spring 2011 – A.J. Hildebrand)

Version 5-4-2011

### Contents

<b>About these notes</b>	<b>3</b>
<b>1 Divisibility and Factorization</b>	<b>4</b>
1.1 Divisibility . . . . .	4
1.2 Primes . . . . .	4
1.3 The greatest common divisor . . . . .	5
1.4 The least common multiple . . . . .	6
1.5 The Fundamental Theorem of Arithmetic . . . . .	6
1.6 Primes in arithmetic progressions . . . . .	8
<b>2 Congruences</b>	<b>9</b>
2.1 Definitions and basic properties; applications . . . . .	9
2.2 Linear congruences in one variable . . . . .	10
2.3 The Chinese Remainder Theorem . . . . .	10
2.4 Wilson's Theorem . . . . .	11
2.5 Fermat's Theorem . . . . .	11
2.6 Euler's Theorem . . . . .	12
<b>3 Arithmetic functions</b>	<b>13</b>
3.1 Some notational conventions . . . . .	13
3.2 Multiplicative arithmetic functions . . . . .	13
3.3 The Euler phi function and the Carmichael Conjecture . . . . .	14
3.4 The number-of-divisors functions . . . . .	15
3.5 The sum-of-divisors functions and perfect numbers . . . . .	15
3.6 The Moebius function and the Moebius inversion formula . . . . .	16
3.7 Algebraic theory of arithmetic function . . . . .	17

---

3.8	Arithmetic Functions: Summary Table . . . . .	18
<b>4</b>	<b>Quadratic residues</b>	<b>19</b>
4.1	Quadratic residues and nonresidues . . . . .	19
4.2	The Legendre symbol . . . . .	19
4.3	The law of quadratic reciprocity . . . . .	20
<b>5</b>	<b>Primitive roots</b>	<b>21</b>
5.1	The order of an integer . . . . .	21
5.2	Primitive roots . . . . .	21
5.3	The Primitive Root Theorem . . . . .	22
<b>6</b>	<b>Continued fractions</b>	<b>23</b>
6.1	Definitions and notations . . . . .	23
6.2	Convergence of infinite continued fractions . . . . .	23
6.3	Properties of Convergents . . . . .	24
6.4	Expansions of real numbers into continued fractions . . . . .	25
<b>7</b>	<b>Topics in Computational Number Theory</b>	<b>26</b>
7.1	Some Basic Concepts . . . . .	26
7.2	Primality Tests . . . . .	26
7.3	The RSA Encryption Scheme . . . . .	28

## About these notes

One purpose of these notes is to serve as a handy reference for homework problems, and especially for proof problems. The definitions given here (e.g., of divisibility) are the “authoritative” definitions, and you should use those definitions in proofs. The results stated here are those you are free to use and refer to in proofs; in general, anything else (e.g., a theorem you might have learned in high school) is not allowed.

Another purpose is to serve as a cheat/review sheet when preparing for exams. The definitions and theorems contained in these notes are those you need to know in exams.

Finally, the notes may be useful as a quick reference or refresher on elementary number theory for those taking more advanced number theory classes (e.g., analytic or algebraic number theory).

The notes are loosely based on the Strayer text, though the material covered is pretty standard and can be found, in minor variations, in most undergraduate level number theory texts. The chapters correspond to those in Strayer, but I have made a few small changes in the subdivision of the chapters.

The definitions and results can all be found (in some form) in Strayer, but the numbering is different, and I have made some small rearrangements, for example, combining several lemmas into one proposition, demoting a “theorem” in Strayer to a “proposition”, etc. The goal in doing this was to streamline the presentation by having several layers of results, with a clear delineation between the various types of results:

- **Theorems:** Those are the key results, usually with descriptive names attached (e.g., “Fundamental Theorem of Arithmetic”). These results typically have more difficult proofs, often well above homework level.
- **“Starred” theorems:** Results whose statement you should know, but whose proof is beyond the scope of an undergraduate number theory course, are indicated by an asterisk. A typical example is the Prime Number Theorem.
- **Propositions:** A proposition typically collects some simple, but very useful, properties of a concept. The proofs are generally on the easy side, and many (but not all) are at a level that would be reasonable to ask for in an exam.
- **Corollaries:** A corollary is attached to a particular theorem (or proposition), and presents a simple consequence of the theorem, or restates the theorem in a special case. The derivation of a corollary from the corresponding theorem is usually easy, and often immediate.
- **Lemmas:** A lemma is an auxiliary result that is needed (usually) for the proof of a theorem. Lemmas are rarely of interest in their own right, and therefore in general not worth memorizing (in contrast to the other theorem-like structures). Since I do not include the proofs here, I have generally avoided stating lemmas that arise in those proofs. If a result that is stated as “Lemma” in Strayer is important in its own right and worthy of memorizing, I have elevated it to the status of a “Proposition” or “Theorem”.

# 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

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

**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  $n = 0, 1, \dots$ , 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 common divisors 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  $a_1, \dots, a_n$ , not all 0, is defined as

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

**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:*

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

*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)  $[a, b] = \frac{|ab|}{(a, b)}$ .
- (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  $\alpha_i$  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)  $n = \prod_{i=1}^s p_i$ ,  $p_1, \dots, p_s$  primes (not necessarily distinct);
- (ii)  $n = \prod_{i=1}^r p_i^{\alpha_i}$ ,  $p_1, \dots, p_r$  distinct primes,  $\alpha_1, \dots, \alpha_r$  positive integers;
- (iii)  $n = \prod_{i=1}^t p_i^{\alpha_i}$ ,  $p_1, \dots, p_t$  distinct primes,  $\alpha_1, \dots, \alpha_t$  nonnegative integers;
- (iv)  $n = \prod_{p \text{ prime}} p^{\alpha_p}$ ,  $\alpha_p$  nonnegative integers,  $\alpha_p = 0$  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  $n = 20$ :

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

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:

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

**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  $\alpha_i$  and  $\beta_i$  are nonnegative integers.

- (i) Then “ $a$  divides  $b$ ” holds if and only if  $\alpha_i \leq \beta_i$  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*

$$(1.1) \quad a, a + b, a + 2b, a + 3b, \dots,$$

*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  $a \equiv b \pmod{m}$ , 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  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$ .
- (ii) If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$ .
- (iii) If  $a \equiv b \pmod{m}$ , then  $a^n \equiv b^n \pmod{m}$  for any  $n \in \mathbf{N}$ .
- (iv) If  $a \equiv b \pmod{m}$ , then  $f(a) \equiv f(b) \pmod{m}$  for any polynomial  $f(n)$  with integer coefficients.
- (v) If  $a \equiv b \pmod{m}$ , then  $a \equiv b \pmod{d}$  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)  $a \equiv a \pmod{m}$ .
- (ii) (Symmetry) If  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$ .
- (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.,

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

**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  $n \equiv r \pmod{m}$  and  $0 \leq r < m$ ; 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*

$$(2.1) \quad ax \equiv b \pmod{m}.$$

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  $ax \equiv b \pmod{m}$  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*

$$(2.2) \quad ax \equiv 1 \pmod{m}$$

*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  $\bar{a}$ .*

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

## 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*

$$(2.3) \quad x \equiv a_i \pmod{m_i} \quad (i = 1, \dots, r)$$

*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  $r$ -tuples 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*

$$(2.4) \quad (p-1)! \equiv -1 \pmod{p}.$$

**Theorem 2.13** (Converse to Wilson's Theorem). *If  $p$  is an integer  $\geq 2$  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  $(n-1)! \equiv 0 \pmod{n}$ .* 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  $(a, p) = 1$ ,*

$$(2.5) \quad a^{p-1} \equiv 1 \pmod{p}.$$

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

$$(2.6) \quad a^p \equiv a \pmod{p}.$$

**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  $\bar{a} = a^{p-2}$  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 composite. Such "false positives" to the Fermat test are rare, but they do exist, motivating 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*

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

*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  $(a, m) = 1$ ,*

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

### 3 Arithmetic functions

#### 3.1 Some notational conventions

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

- $\sum_{d|n} f(d)$  denotes a sum of  $f(d)$ , taken over all **positive divisors**  $d$  of  $n$ .
- $\sum_{p|n} f(p)$  denotes a sum of  $f(p)$ , taken over all **prime** divisors  $p$  of  $n$ .
- $\sum_{p^\alpha||n} f(p^\alpha)$  denotes a sum of  $f(p^\alpha)$ , taken over all **prime powers**  $p^\alpha$  that occur in the standard prime factorization of  $n$ . (Here the double bar in  $p^\alpha||n$  indicates that  $p^\alpha$  is the exact power of  $p$  dividing  $n$ , i.e.,  $p^\alpha | n$ , but  $p^{\alpha+1} \nmid n$ .)
- **Products** over  $d | n$ ,  $p | n$ , 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  $p^\alpha$  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  $\#\{d \in \mathbf{N} : d | n\}$ . 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  $f : \mathbf{N} \rightarrow \mathbf{C}$  is called an **arithmetic function**. An arithmetic function  $f$  is called **multiplicative** if it satisfies the relation*

$$(3.1) \quad f(n_1 n_2) = f(n_1) f(n_2)$$

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 “**divisor**”) and  $\tau(n)$  (for “**Teiler**”, 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  $n \in \mathbf{N}$ ,*

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

### 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  $n \in \mathbf{N}$ ,*

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

**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  $2^7 - 1 = 127$ .

### 3.6 The Moebius function and the Moebius inversion formula

**Definition 3.12** (Moebius function). *The **Moebius function** is defined by*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 p_2 \dots p_r \text{ with distinct primes } p_i, \\ 0 & \text{if } n \text{ is not squarefree, i.e., divisible by a prime power } p^\alpha \text{ with } \alpha > 1. \end{cases}$$

*Remark.* A very similar function is the **Liouville function**  $\lambda(n)$ , which is defined as  $(-1)^r$ , where  $r$  is the *total* number of prime factors of  $n$ , with multiple prime factors counted multiple times. If  $n$  is squarefree, then  $\lambda(n) = \mu(n)$ , but if  $n$  is not squarefree, then  $\mu(n) = 0$ , while  $\lambda(n) = \pm 1$  depending on whether  $n$  has an even or an odd number of prime factors.

While the Liouville function has a simpler definition and may seem the more natural of the two functions, the Moebius function is more useful and more important because of results such those below (which would not be valid for the Liouville function).

**Proposition 3.13** (Properties of  $\mu(n)$ ).

- (i) *(Multiplicativity) The Moebius function is multiplicative (though not completely multiplicative).*
- (ii) *(Moebius function identity)*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

**Theorem 3.14** (Moebius inversion formula). *If  $f$  and  $g$  are arithmetic functions satisfying*

$$f(n) = \sum_{d|n} g(d) \quad (n \in \mathbf{N}),$$

*then*

$$g(n) = \sum_{d|n} f(d)\mu(n/d) = \sum_{d|n} \mu(d)f(n/d) \quad (n \in \mathbf{N}).$$

### 3.7 Algebraic theory of arithmetic function

In this section we develop an algebraic theory of arithmetic functions based on the notion of a **Dirichlet product**. This allows us to restate many of the definitions and results encountered earlier in a simple, elegant, and natural form.

We begin by defining some “trivial” arithmetic functions that are needed in this theory and which can be used to build up other arithmetic functions.

**Definition 3.15** (Trivial arithmetic functions). *The **unit function**  $\mathbf{1}$ , **identity function**  $\mathbf{id}$ , and **delta function**  $\delta$  are the arithmetic functions defined as follows:*

$$\begin{aligned}\mathbf{1}(n) &= 1 \quad (n \in \mathbf{N}), \\ \mathbf{id}(n) &= n \quad (n \in \mathbf{N}), \\ \delta(n) &= \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

*All three of these functions are multiplicative (in fact, completely multiplicative).*

**Definition 3.16** (Dirichlet product of arithmetic functions). *Given two arithmetic functions  $f$  and  $g$ , the **Dirichlet product**  $f \star g$  is the arithmetic function defined by*

$$(f \star g)(n) = \sum_{d|n} f(d)g(n/d) \quad (n \in \mathbf{N}).$$

**Proposition 3.17** (Algebraic properties of Dirichlet product). *Let  $f, g, h$  be arithmetic functions.*

- (i) *(Commutativity)  $f \star g = g \star f$ .*
- (ii) *(Associativity)  $(f \star g) \star h = f \star (g \star h)$ .*
- (iii) *(Identity element)  $f \star \delta = \delta \star f = f$ , where  $\delta$  is defined as above, i.e.,  $\delta(1) = 1$  and  $\delta(n) = 0$  if  $n > 1$ .*
- (iv) *(Dirichlet inverse) If  $f(1) \neq 0$ , then  $f$  has a unique Dirichlet inverse  $f^{\star-1}$ , in the sense that  $f \star f^{\star-1} = \delta$ .*
- (v) *(Preservation of multiplicativity) The Dirichlet product of two multiplicative functions is multiplicative.*
- (vi) *(Multiplicativity of inverse) The Dirichlet inverse of a multiplicative function is multiplicative.*

Using the Dirichlet product notation, we can now restate many of the definitions, identities, and theorems on arithmetic functions encountered earlier in a simple, elegant, very natural, and easy-to-remember form.

**Proposition 3.18** (Dirichlet product versions of identities for arithmetic functions).

- (i) **Gauss identity:**  $\varphi \star \mathbf{1} = \mathbf{id}$
- (ii) **Definition of the divisor function:**  $\nu = \mathbf{1} \star \mathbf{1}$
- (iii) **Definition of the sum-of-divisors function:**  $\sigma = \mathbf{1} \star \mathbf{id}$
- (iv) **Moebius function identity:**  $\mu \star \mathbf{1} = \delta$
- (v) **Moebius inversion formula:** If  $f = g \star \mathbf{1}$ , then  $g = f \star \mu = \mu \star f$ .

## 3.8 Arithmetic Functions: Summary Table

Function	value at $n(\in \mathbf{N})$	value at a prime $p$	value at a prime power $p^\alpha$	properties
$\delta(n)$ (delta function)	1 if $n = 1$ , 0 else	0	0	completely multiplicative, $\delta \star f = f \star \delta = f$ , identity element for Dirichlet product
$\mathbf{1}(n)$ (unit function)	1	1	1	completely multiplicative
$\mathbf{id}(n)$ (identity function)	$n$	$p$	$p^\alpha$	completely multiplicative
$\mu(n)$ (Moebius function)	1 if $n = 1$ , $(-1)^r$ if $n = \prod_{i=1}^r p_i$ ( $p_i$ distinct), 0 otherwise	-1	-1 if $\alpha = 1$ , 0 if $\alpha > 1$	multiplicative, $\mu \star \mathbf{1} = \delta$ (Dirichlet inverse of $\mathbf{1}$ )
$\nu(n) (= d(n) = \tau(n))$ (number-of-divisors function)	$\#\{d \in \mathbf{N} : d \mid n\}$	2	$\alpha + 1$	multiplicative, $\nu = \mathbf{1} \star \mathbf{1}$
$\varphi(n)$ (Euler phi function)	$\#\{1 \leq m \leq n : (m, n) = 1\}$	$p - 1$	$p^{\alpha-1}(p - 1)$	multiplicative, $\varphi \star \mathbf{1} = \mathbf{id}$ (Gauss identity)
$\sigma(n)$ (sum-of-divisors function)	$\sum_{d \mid n} d$	$p + 1$	$\frac{p^{\alpha+1} - 1}{p - 1}$	multiplicative, $\sigma = \mathbf{id} \star \mathbf{1}$

Table 1: Summary of important arithmetic functions

## 4 Quadratic residues

### 4.1 Quadratic residues and nonresidues

**Definition 4.1** (Quadratic residues and nonresidues). Let  $m \in \mathbf{N}$  and  $a \in \mathbf{Z}$  be such that  $(a, m) = 1$ . Then  $a$  is called a **quadratic residue modulo  $m$**  if the congruence

$$(4.1) \quad x^2 \equiv a \pmod{m}$$

has a solution (i.e., if  $a$  is a “perfect square modulo  $m$ ”), and  $a$  is called a **quadratic nonresidue modulo  $m$**  if (4.1) has no solution.

*Remarks.* (i) Note that, by definition, integers  $a$  that do not satisfy the condition  $(a, m) = 1$  are not classified as quadratic residues or nonresidues. In particular, 0 is considered neither a quadratic residue nor a quadratic nonresidue (even though, for  $a = 0$ , (4.1) has a solution, namely  $x = 0$ ).

(ii) While the definition of quadratic residues and nonresidues allows the modulus  $m$  to be an arbitrary positive integer, in the following we will focus exclusively on the case when  $m$  is an odd prime  $p$ .

**Proposition 4.2** (Number of solutions to quadratic congruences). Let  $p$  be an odd prime, and let  $a \in \mathbf{Z}$  with  $(a, p) = 1$ .

- (i) If  $a$  is a quadratic nonresidue modulo  $p$ , the congruence (4.1) has no solution.
- (ii) If  $a$  is a quadratic residue modulo  $p$ , the congruence (4.1) has exactly two incongruent solutions  $x$  modulo  $p$ . More precisely, if  $x_0$  is one solution, then a second, incongruent, solution is given by  $p - x_0$ .

**Proposition 4.3** (Number of quadratic residues and nonresidues). Let  $p$  be an odd prime. Then among the integers  $1, 2, \dots, p - 1$ , exactly half (i.e.,  $(p - 1)/2$ ) are quadratic residues modulo  $p$ , and exactly half are quadratic nonresidues modulo  $p$ .

### 4.2 The Legendre symbol

**Definition 4.4** (Legendre symbol). Let  $p$  be an odd prime, and let  $a$  be an integer with  $(a, p) = 1$  (or, equivalently,  $p \nmid a$ ). The **Legendre symbol of  $a$  modulo  $p$** , denoted by  $\left(\frac{a}{p}\right)$ , is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

*Remark.* Note that the modulus in this definition, and in all results below, is restricted to odd primes (i.e., a prime other than 2). One can extend the definition, and most of the results, to composite moduli, but things get a lot more complicated then.

**Proposition 4.5** (Properties of the Legendre Symbol). Let  $p$  be an odd prime, and let  $a, b \in \mathbf{Z}$  with  $(a, p) = 1$  and  $(b, p) = 1$ .

- (i) (Periodicity in numerator) If  $a \equiv b \pmod{p}$ , then  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .
- (ii) (Complete multiplicativity in numerator)  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .

$$(iii) \text{ (Value at squares)} \left(\frac{a^2}{p}\right) = 1.$$

$$(iv) \text{ (Value at } -1) \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

$$(v) \text{ (Value at } 2) \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

**Proposition 4.6** (Euler's Criterion). *Let  $p$  be an odd prime, and let  $a \in \mathbf{Z}$  with  $(a, p) = 1$ . Then  $a$  is a quadratic residue modulo  $p$  if  $a^{(p-1)/2} \equiv 1 \pmod{p}$ , and a quadratic nonresidue if  $a^{(p-1)/2} \equiv -1 \pmod{p}$ ; equivalently,*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

### 4.3 The law of quadratic reciprocity

**Theorem 4.7** (Quadratic reciprocity law (Gauss 1795)). *Let  $p$  and  $q$  be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

*Equivalently,*

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}, \\ \left(\frac{q}{p}\right) & \text{otherwise.} \end{cases}$$

*Remarks.* (i) The first form of the reciprocity law is the cleaner and more elegant form, and the one in which the law is usually stated. However, for applications, the second form is more useful. In this form the law says that numerator and denominator in a Legendre symbol (assuming both are distinct odd primes) can be interchanged in all cases except when both numerator and denominator are congruent to 3 modulo 4, in which case the sign of the Legendre symbol flips after interchanging numerator and denominator. Put differently, this form states that  $p$  is a quadratic residue modulo  $q$  if and only if  $q$  is a quadratic residue modulo  $p$ , except in the case when both  $p$  and  $q$  are congruent to 3 modulo 4; in the latter case  $p$  is a quadratic residue modulo  $q$  if and only if  $q$  is a quadratic nonresidue modulo  $p$ .

(ii) Note that the reciprocity law requires numerator and denominator to be distinct odd primes. In particular, it does not apply directly to cases where the numerator is composite, negative, or an even number. However, these cases can be reduced to the prime case using the multiplicativity of the Legendre symbol along with the special values at  $-1$  and  $2$  (see Proposition 4.5):

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

In fact, these last two relations are called the **First Supplementary Law** and **Second Supplementary Law**, as they “supplement” the quadratic reciprocity law.

## 5 Primitive roots

### 5.1 The order of an integer

**Definition 5.1** (Order of an integer). *Let  $m \in \mathbf{N}$  and  $a \in \mathbf{Z}$  be such that  $(a, m) = 1$ . The **order** of  $a$  **modulo**  $m$ , denoted by  $\text{ord}_m a$ , is the least positive integer  $k$  such that*

$$(5.1) \quad a^k \equiv 1 \pmod{m}.$$

In order for this definition to make sense, there has to be at least one positive integer  $k$  for which (5.1) holds. The existence of such a  $k$  is guaranteed by Euler's Theorem (Theorem 2.21), which states that, under the same assumptions on  $m$  and  $a$  as in the definition, (5.1) holds for  $k = \varphi(m)$ . Thus, the order  $\text{ord}_m a$  is well-defined, and it is at most equal to  $\varphi(m)$ .

**Proposition 5.2** (Properties of an order). *Let  $m \in \mathbf{N}$  and  $a \in \mathbf{Z}$  be such that  $(a, m) = 1$ , and let  $\text{ord}_m a$  be the order of  $a$  modulo  $m$ . Then:*

- (i) (*Periodicity*) *If  $b \equiv a \pmod{m}$ , then  $\text{ord}_m b = \text{ord}_m a$ .*
- (ii) (*Relation to Euler phi*)  *$\text{ord}_m a$  is a divisor of  $\varphi(m)$ .*
- (iii) (*Characterization of "good" exponents*) *The set of positive integers  $k$  for which the congruence (5.1) holds consists exactly of the positive integer multiples of  $\text{ord}_m a$ .*
- (iv) (*Order of powers of  $a$* ) *For any positive integer  $i$ ,*

$$\text{ord}_m a^i = \frac{\text{ord}_m a}{(\text{ord}_m a, i)}.$$

*In particular,  $\text{ord}_m a^i = \text{ord}_m a$  if and only if  $(\text{ord}_m a, i) = 1$ .*

**Proposition 5.3** (Number of elements of given order). *Let  $p$  be an odd prime. Then the possible orders of integers modulo  $p$  are exactly the positive divisors of  $p - 1 (= \varphi(p))$ . Moreover, given any positive divisor  $d \mid p - 1$ , there exist exactly  $\varphi(d)$  incongruent integers  $a$  with  $\text{ord}_p a = d$ .*

### 5.2 Primitive roots

The question when the order of an integer  $a$  modulo  $m$  is equal to its maximal possible value, the "Euler order"  $\varphi(m)$ , motivates the following definition.

**Definition 5.4** (Primitive root). *Let  $m \in \mathbf{N}$  and  $a \in \mathbf{Z}$  be such that  $(a, m) = 1$ . Then  $a$  is called a **primitive root modulo**  $m$  if  $\text{ord}_m a = \varphi(m)$ , i.e., if the order of  $a$  is equal to the maximal possible value.*

**Proposition 5.5** (Primitive roots and reduced systems of residues). *Let  $m \in \mathbf{N}$ , and suppose  $r$  is a primitive root modulo  $m$ . Then the set*

$$\{r, r^2, \dots, r^{\varphi(m)}\}$$

*is a system of reduced residues modulo  $m$ . That is, the elements in this set are pairwise incongruent modulo  $m$ , and every integer  $a$  with  $(a, m) = 1$  is congruent modulo  $m$  to an element in the above set.*

### 5.3 The Primitive Root Theorem

**Theorem 5.6** (Existence of Primitive Roots). *Let  $m$  be a positive integer. Then there exists a primitive root modulo  $m$  if and only if  $m$  has one of the following forms:*

- (i)  $m = p^\alpha$ , where  $p$  is an odd prime and  $\alpha \in \mathbf{N}$ .
- (ii)  $m = 2p^\alpha$ , where  $p$  is an odd prime and  $\alpha \in \mathbf{N}$ .
- (iii)  $m = 1, 2, 4$ .

**Theorem 5.7** (Number of primitive roots). *Let  $m$  be of one of the forms in the Primitive Root Theorem, so that there exists at least one primitive root modulo  $m$ . Then there exist exactly  $\varphi(\varphi(m))$  incongruent primitive roots modulo  $m$ .*

## 6 Continued fractions

### 6.1 Definitions and notations

**Definition 6.1** (Continued fractions). A finite or infinite expression of the form

$$(6.1) \quad a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

where the  $a_i$  are real numbers, with  $a_1, a_2, \dots > 0$ , is called a **continued fraction** (c.f.). The numbers  $a_i$  are called the **partial quotients** of the c.f.

The continued fraction (6.1) is called **simple** if the partial quotients  $a_i$  are all integers. It is called **finite** if it terminates, i.e., if it is of the form

$$(6.2) \quad a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n}}}$$

and **infinite** otherwise.

**Notation** (Bracket notation for continued fractions). The continued fractions (6.1) and (6.2) are denoted by  $[a_0, a_1, a_2, \dots]$  and  $[a_0, a_1, a_2, \dots, a_n]$ , respectively. In particular,

$$[a_0] = a_0, \quad [a_0, a_1] = a_0 + \frac{1}{a_1}, \quad [a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, \quad \dots$$

*Remarks.* (i) Note that the first term,  $a_0$ , is allowed to be negative or 0, but all subsequent terms  $a_i$  must be positive. This requirement ensures that there are no zero denominators and that any finite c.f. (6.2), and all of its convergents, are well-defined.

(ii) In the sequel we will focus on the case of simple c.f.'s, i.e., c.f.'s where all partial quotients are integers.

### 6.2 Convergence of infinite continued fractions

**Definition 6.2** (Convergents). The **convergents** of a (finite or infinite) c.f.  $[a_0, a_1, a_2, \dots]$  are defined as

$$C_0 = [a_0], \quad C_1 = [a_0, a_1], \quad C_2 = [a_0, a_1, a_2], \dots$$

If the c.f. is simple, its convergents  $C_i$  represent rational numbers, denoted by

$$C_i = \frac{p_i}{q_i},$$

where  $p_i/q_i$  is in reduced form.

**Definition 6.3** (Convergence of infinite continued fractions). An infinite c.f.  $[a_0, a_1, a_2, \dots]$  is called **convergent** if its sequence of convergents  $C_i = [a_0, a_1, \dots, a_i]$  converges in the usual sense, i.e., if the limit

$$\alpha = \lim_{i \rightarrow \infty} C_i = \lim_{i \rightarrow \infty} [a_0, a_1, \dots, a_i]$$

exists (and is a real number). In this case, we say that the continued fraction  $[a_0, a_1, a_2, \dots]$  **represents** the number  $\alpha$ , or is a **continued fraction expansion** of  $\alpha$ , and we write

$$\alpha = [a_0, a_1, a_2, \dots].$$

**Theorem 6.4** (Convergence of infinite simple c.f.'s). *Any infinite simple c.f.  $[a_0, a_1, \dots]$  is convergent and thus represents some real number.*

### 6.3 Properties of Convergents

**Proposition 6.5** (Formulas for  $p_i$  and  $q_i$ ). *Let  $\alpha = [a_0, a_1, \dots]$  be a simple c.f. with convergents  $C_i = [a_0, a_1, \dots, a_i] = \frac{p_i}{q_i}$ .*

(i) **Recursion formula:** *The numbers  $p_i$  and  $q_i$  are given by the recurrence*

$$\begin{aligned} p_i &= a_i p_{i-1} + p_{i-2}, \\ q_i &= a_i q_{i-1} + q_{i-2} \end{aligned}$$

*for  $i = 1, 2, \dots$ , along with the initial conditions  $p_0 = a_0, p_{-1} = 1, q_0 = 1, q_{-1} = 0$ .*

(ii) **Matrix representation:** *For  $i = 0, 1, 2, \dots$*

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix}$$

**Theorem 6.6** (Properties of convergents). *The convergents  $C_i = p_i/q_i$  of an infinite simple continued fraction  $\alpha = [a_0, a_1, a_2, \dots]$  satisfy:*

- (i)  $(p_i, q_i) = 1$  for  $i = 0, 1, \dots$ ; i.e., the fractions  $p_i/q_i$  are reduced.
- (ii)  $q_1 < q_2 < \dots$ ; i.e., for  $i \geq 1$ , the denominators  $q_i$  are strictly increasing.
- (iii)  $C_0 < C_2 < C_4 < \dots < \alpha < \dots < C_5 < C_3 < C_1$ . That is, the even-indexed convergents form an increasing sequence, while the odd-indexed convergents form a decreasing sequence, with the value of the c.f. sandwiched between both sequences.
- (iv)  $C_{i+1} - C_i = \frac{(-1)^i}{q_i q_{i+1}}$  for  $i = 0, 1, 2, \dots$
- (v)  $\left| \frac{p_i}{q_i} - \alpha \right| < \frac{1}{q_i q_{i+1}}$  for  $i = 0, 1, 2, \dots$
- (vi) **Best approximation property:** *For any rational number  $a/b$  with  $a \in \mathbf{Z}$ ,  $b \in \mathbf{N}$ , and  $1 \leq b \leq q_i$ ,*

$$\left| \frac{p_i}{q_i} - \alpha \right| \leq \left| \frac{a}{b} - \alpha \right|,$$

*with equality if and only if  $a/b = p_i/q_i$ . That is, the convergent  $p_i/q_i$  is the best-possible approximation to  $\alpha$  among all rational numbers with the same or smaller denominator.*

## 6.4 Expansions of real numbers into continued fractions

**Proposition 6.7** (Continued fraction algorithm). *Given a real number  $\alpha$ , define successively real numbers  $\alpha_0, \alpha_1, \dots$ , and integers  $a_0, a_1, \dots$  by*

$$\begin{aligned} \alpha_0 &= \alpha, & a_0 &= [\alpha_0], \\ \alpha_1 &= \frac{1}{\alpha_0 - [\alpha_0]}, & a_1 &= [\alpha_1], \\ \alpha_2 &= \frac{1}{\alpha_1 - [\alpha_1]}, & a_2 &= [\alpha_2], \\ &\dots & &\dots \end{aligned}$$

where  $[x]$  denotes the integer part of  $x$  (i.e., the “floor function”). Stop the algorithm if  $\alpha_n$  is an integer (and thus  $a_n = \alpha_n$ ); otherwise continue indefinitely. Then  $[a_0, a_1, \dots]$  is a simple c.f. that represents the number  $\alpha$ . Moreover, for any  $i \geq 0$  we have

$$\alpha_i = [a_i, a_{i+1}, \dots], \quad \alpha = [a_0, a_1, \dots, a_{i-1}, \alpha_i].$$

**Theorem 6.8** (Continued fraction expansion of rational numbers). *Any finite simple c.f. represents a rational number. Conversely, any rational number  $\alpha$  can be expressed as a simple finite c.f.  $\alpha = [a_0, a_1, \dots, a_n]$ . Moreover, under the requirement that  $a_n > 1$ , this representation is unique. Thus, there is a one-to-one correspondence between rational numbers and finite simple c.f.’s with last partial quotient greater than 1.*

**Theorem 6.9** (Continued fraction expansion of irrational numbers). *Any infinite simple c.f. represents an irrational number. Conversely, any irrational number  $\alpha$  can be expressed as a simple infinite c.f.  $\alpha = [a_0, a_1, a_2, \dots]$ , and this representation is unique. Thus, there is a one-to-one correspondence between irrational numbers and infinite simple c.f.’s.*

**Theorem 6.10** (Continued fraction expansion of quadratic irrationals). *The c.f. expansion of a quadratic irrational (i.e., a solution of a quadratic equation with integer coefficients) is eventually periodic, i.e., of the form*

$$[a_0, \dots, a_N, \overline{a_{N+1}, \dots, a_{N+p}}],$$

where the bar indicates the periodic part. Conversely, any infinite simple c.f. that is eventually periodic represents a quadratic irrational. Thus, there is a one-to-one correspondence between quadratic irrationals and infinite, eventually periodic simple c.f.’s.

## 7 Topics in Computational Number Theory

### 7.1 Some Basic Concepts

**Running Time:** A fundamental notion that allows one to quantify and compare the efficiency of algorithms. The running time of an algorithm is the number of “basic” operations it takes to complete given an input of “size”  $n$ .

Depending on the context, “basic” operation can refer to simple arithmetic operations like addition or multiplication, or single bit operations (AND, OR, etc.), or individual CPU instructions. For the applications we consider here, it does not matter much which interpretation one uses.

The “size” of an input is measured in terms of the number of bits, or digits. Thus, for example, an integer with 1000 digits (decimal or binary) would have size around 1000. In general, if  $N$  is a large integer, then its size  $n$  is proportional to  $\log N$ . *It is important to keep in mind that the appropriate yardstick when measuring running times is not the size of the integer itself, but its logarithm.*

**Polynomial Time:** A key benchmark for running times is “polynomial time”, i.e., a running time that, for an input of size  $n$ , is of order of a fixed power of  $n$ . In a sense, this is best-possible, as reading in an input of size  $n$  in bit-by-bit fashion already requires  $n$  bit operations. Finding algorithms that are polynomial time, or proving that no such algorithms exist for a particular problem, is one of the fundamental problems in the theory of algorithms.

**Factoring versus Multiplying:** By the Fundamental Theorem of Arithmetic, there is a one-to-one correspondence between finite tuples of prime factors  $(p_1, \dots, p_r)$  with  $p_1 \leq \dots \leq p_r$  and integers  $n \geq 2$ , given by the bijection  $(p_1, \dots, p_r) \leftrightarrow n = p_1 \dots p_r$ . However, from a computational point of view the two directions of this bijection are vastly different: Going from left to right simply requires multiplying together the prime factors  $p_i$ , a trivial operation that can be carried out in polynomial time. By contrast, the reverse direction requires factoring an integer into its prime factors and is a computationally much harder task. The fact that one direction in this equivalence is easy from a computational point of view, while the other is hard, is the basis of most modern cryptographic schemes.

**Primality Testing versus Factoring:** Another crucial difference from a computational point of view lies between primality testing algorithms and factoring algorithms. A factoring algorithm takes as input a number  $n$  and produces as output its complete prime factorization. By contrast, a primality testing algorithm produces as output PRIME or COMPOSITE (and possibly also INCONCLUSIVE), without exhibiting any factors.

Computationally, primality testing is much easier, and faster, than factoring. There are algorithms known that test primality in polynomial time. By contrast, there are no known polynomial time factoring algorithms, and it is conjectured that none exist.

### 7.2 Primality Tests

**Trial Division:** Let  $n \geq 2$ . For  $d = 2, 3, \dots, \lfloor \sqrt{n} \rfloor$ , check if  $d \mid n$  (e.g., using division with remainder).

- If  $d \mid n$  for some  $2 \leq d \leq \sqrt{n}$ , then  $n$  is composite, and  $d$  is a proper divisor of  $n$ .
- If  $d \nmid n$  for all  $2 \leq d \leq \sqrt{n}$ , then  $n$  is prime.

*Comments:* As a general primality test, Trial Division is not practical since it requires about  $\sqrt{n}$  operations to determine the primality of an integer. However, it is useful as an initial test to detect integers that have a small prime factor and eliminate these from further consideration

before applying more sophisticated tests. Also, in contrast to all of the tests below, Trial Division produces explicit factors, and it can be used recursively to completely factor a composite number.

**Wilson’s Test:** Let  $n \geq 2$ . Compute  $(n - 1)! \pmod n$ .

- If  $(n - 1)! \not\equiv -1 \pmod n$ , then  $n$  is composite.
- If  $(n - 1)! \equiv -1 \pmod n$ , then  $n$  is prime.

*Comments:* Unlike the Fermat Test below, Wilson’s Test is an “if and only if” statement, and thus provides an ironclad guarantee of compositeness or primality. As a practical primality test, however, it is not very useful since there is no efficient (fast) way to compute  $(n - 1)!$  modulo  $n$ .

**Fermat Test:** Let  $n \geq 2$ . Pick an integer  $a$  with  $(a, n) = 1$ , and compute  $a^{n-1} \pmod n$ .

- If  $a^{n-1} \not\equiv 1 \pmod n$ , then  $n$  is composite.
- If  $a^{n-1} \equiv 1 \pmod n$ , then  $n$  is likely (but not guaranteed) prime.

*Comments:* The Fermat test is very fast: Using repeated squaring to compute the powers  $a^{n-1}$  modulo  $n$ , it can be performed in polynomial time.

The test has no “false negatives”: If a number  $n$  fails the test, i.e., if  $a^{n-1} \not\equiv 1 \pmod n$ , then  $n$  is *guaranteed* composite.

The test does have “false positives”: There are numbers  $n$  that pass the Fermat test, i.e., satisfy  $a^{n-1} \equiv 1 \pmod n$ , but are composite. Such numbers are called *pseudoprimes* (to base  $a$ ). Luckily, false positives are extremely rare. For example, out of the first billion integers  $n$  that pass the base-2 Fermat test (i.e., satisfy  $2^{n-1} \equiv 1 \pmod n$ ), only about 20,000 are false positives (i.e., pseudoprimes). Thus, in this range, the test is 99.998% accurate. This makes the Fermat test very useful as a test that identifies “probable primes”, i.e., numbers that are, with very high probability, prime, and which can then be subjected to further tests (such as Lucas’ Test below).

**Lucas Test:** Let  $n \geq 2$ . Let  $a$  be an integer with  $(a, n) = 1$ , and suppose the following two conditions hold:

- $a^{n-1} \equiv 1 \pmod n$ .
- $a^{(n-1)/q} \not\equiv 1 \pmod n$  for every prime divisor  $q \mid n - 1$ .

Then  $n$  is prime.

*Comments:* This test fixes the “hole” in Fermat’s test: The first condition is simply the Fermat test, while the second, additional, condition guarantees that  $n$  is indeed a prime.

The downside of Lucas’ test is that, in order to verify that this additional condition is satisfied, one first needs to find all prime factors of  $n - 1$ . For general integers  $n$ , this is a much harder problem than the problem of testing  $n$  for primality. However, the test can be useful for integers for which the prime factorization of  $n - 1$  is known in advance, such as Fermat numbers. In the fact, in this special case conditions in Lucas’ test can be further simplified to yield the following test for the primality of Fermat numbers:

**Pépin’s Test:** Let  $F_m = 2^{2^m} + 1$  be the  $m$ -th Fermat number. Then  $F_m$  is prime if and only if

$$3^{(F_m - 1)/2} \equiv -1 \pmod{F_m}.$$

*Comments:* This test, and variations of it (for example, with 3 replaced by 5), is useful in testing Fermat numbers for primality. A key feature of this test is the “if and only if” character: If the stated congruence holds,  $F_m$  is guaranteed to be prime; if it does not hold,  $F_m$  is guaranteed to be composite.

### 7.3 The RSA Encryption Scheme

**Encryption basics:** An encryption scheme takes a message  $M$  and creates an encrypted version  $E$  of this message by applying an appropriate one-to-one function,  $f$ , the *encryption function*, to  $M$ :  $E = f(M)$ . The associated decryption scheme works the same way, with the encrypted message  $E$  as input, and the inverse function,  $f^{-1}$ , as a *decryption function* that recovers the original message:  $M = f^{-1}(E)$ .

A classic example of an encryption scheme is the “Caesar cipher”, which shifts each letter in the alphabet forward by 3, so that A gets mapped to D, B maps to E, C maps to F, etc.

**Private key encryption versus public key encryption:** In the example of the Caesar cipher, anyone who knows the encryption function (“shift the letter forward by 3”) is able to deduce the corresponding decryption function (“shift the letter backward by 3”) and thus can decrypt any messages encrypted with the same function. Thus, in order for the encryption to remain secure, *both the encryption function and the decryption function have to be kept secret*.

Encryption schemes with this property are called **private key encryption**, or **symmetrical encryption**, as encryption and decryption play a symmetrical role, and both need to be kept “private” (i.e., secret).

By contrast, **public key encryption**, or **asymmetrical encryption**, is an encryption scheme where the encryption function  $f$  is such that knowing  $f$  does not give away the decryption function  $f^{-1}$ . Hence the encryption function  $f$  can safely be made public (in the form of the “public key”), and only the decryption function has to be kept secret (the “private key”).

An encryption function  $f$  suitable for a public key encryption must have the following properties: (i) the function  $f$  must be easy to compute; (ii) its inverse,  $f^{-1}$ , must be hard to compute; (iii) there must exist a “backdoor” approach that allows easy computation of  $f^{-1}$  given an appropriate “private key”.

**The RSA encryption scheme:** This encryption scheme, named after its inventors in the mid 1970s (Rivest, Shamir, and Adleman), has become the gold standard for public key encryption. It works as follows.

- Two primes,  $p$  and  $q$ , are generated, and *kept secret*. Typically,  $p$  and  $q$  will have around 100 decimal digits. Computationally, this is relatively easy to do, for example, by randomly testing numbers of the desired size for primality until a prime is found.
- The **encryption modulus**,  $m = pq$ , is computed, by multiplying the two primes. Computationally, this is a trivial task. The modulus  $m$  is *made public*.
- A **public encryption exponent**,  $e$ , is chosen, subject to the condition  $(e, \varphi(m)) = 1$ . A common choice is  $2^{16} + 1 = 65,537$ , the largest known Fermat prime.
- A corresponding **secret decryption exponent**,  $d$ , is computed by solving the congruence  $ed \equiv 1 \pmod{\varphi(m)}$ . This requires knowing  $\varphi(m)$ , or equivalently, the (secret) prime factorization of the modulus  $m$ . Given this prime factorization, a solution to the above congruence can be found quickly via the Euclidean algorithm.
- **Encryption and decryption:** For simplicity, assume the message  $M$  to be encrypted is a positive integer smaller than each of the primes  $p$  and  $q$ .<sup>1</sup> This assumption ensures that  $M$  is in the range  $1 \leq M < m$  (so that  $M$  is completely determined by its remainder modulo  $m$ ) and also satisfies  $(M, m) = (M, pq) = 1$ . The encryption and decryption functions in the RSA scheme are then defined as follows.

<sup>1</sup>A general message can be converted to a sequence of such numbers by first encoding the characters as numerical values (e.g., ASCII codes) and then breaking the resulting numerical sequence into blocks of suitable size.

- **Encryption:** To encrypt  $M$ , compute  $M^e \bmod m$ . The result, expressed as the least positive residue modulo  $m$ , is the encrypted message  $E$ . The pair  $(e, m)$  consisting of the (public) encryption exponent and the (public) modulus is the public “encryption key”. Anyone who has this key (i.e., knows the values of  $e$  and  $m$ ) can encrypt a message.
- **Decryption:** To decrypt an encrypted message  $E$ , compute  $E^d \bmod m$ . The result, expressed as the least positive residue modulo  $m$ , is the original message  $M$ ; see below for a proof. The pair  $(d, m)$  consisting of the private (i.e., secret) decryption exponent and the (public) modulus is the private “decryption key”.

Computationally, both encryption and decryption are “modular exponentiations” that can be performed quickly using the repeated squaring trick. For example, with  $e = 2^{16} + 1 = 65,537$  as exponent, computing  $M^e \bmod m$  requires only 17 operations.<sup>2</sup>

#### Why it works:

- **Existence of decryption exponent  $d$ .** The decryption exponent  $d$  is defined as a solution to the congruence  $(*) \quad ed \equiv 1 \pmod{\varphi(m)}$ . For the system to work, we need to be guaranteed that such a solution exists. Now,  $(*)$  is a linear congruence of the form  $ax \equiv 1 \pmod{n}$ . By the general theory for such congruences, a solution  $x$  exists if and only if  $(a, n) = 1$ , and in this case there is a unique solution in the range  $1 \leq x \leq n$ . In the case of  $(*)$ , the condition for the existence of a solution  $d$  becomes  $(e, \varphi(m)) = 1$ , and since  $e$  was chosen to satisfy the latter condition, this shows that  $(*)$  has a solution  $d$ . Moreover, the general theory guarantees that there is a solution  $d$  in the range  $1 \leq d \leq \varphi(m)$ .
- **Decryption returns the original message.** Here we show that the above decryption algorithm indeed returns the original message, i.e., that  $E^d \equiv M \pmod{m}$ .

First, note that by the congruence  $(*)$ , there exists a nonnegative integer  $k$  such that  $de = 1 + k\varphi(m)$ . Then, since  $M^{\varphi(m)} \equiv 1 \pmod{m}$  by Euler’s Theorem,

$$E^d = (M^e)^d = M^{ed} = M^{1+k\varphi(m)} = M \cdot (M^{\varphi(m)})^k \equiv M \cdot 1^k = M,$$

**What makes RSA (relatively) secure:** The above argument shows that the RSA scheme works correctly, in the sense that the decryption function is well-defined ( $d$  always exists) and that it returns the original message.

The security of the RSA scheme, and its usefulness in practice, relies on the fact that encrypting a message using the public key  $(e, m)$  is computationally easy, while decrypting a message knowing only the public key is computationally hard, to the point of being infeasible if the modulus is in the 200+ digit range. Here is a rundown of the computational complexity of the key tasks involved:

- **Primality testing is easy:** Current algorithms can test integers of thousands of digits in fractions of a second. Thus, finding the large primes needed in the RSA scheme is easy.
- **Factoring is hard (as far as we know):** All known factoring algorithms are only effective up to a hundred digits or so. Factoring a 200+ digit integer composed of two large prime factors, such as those arising in the RSA scheme, cannot be done in a reasonable amount of time.
- **Modular exponentiation is easy:** Given an exponent  $e$  and a modulus  $m$ , computing  $M^e \bmod m$  can be done quickly using the repeated squaring trick.

---

<sup>2</sup>Compute successively  $M^2, M^{2^2} = (M^2)^2, M^{2^3} = (M^{2^2})^2, \dots, M^{2^{16}}$ , and multiply the last result,  $M^{2^{16}}$ , by  $M$ , reducing modulo  $m$  at each stage.

- **Computing modular inverses is easy:** Solving an equation  $ax \equiv 1 \pmod{n}$  for  $x$  can be done quickly by applying the Euclidean algorithm to  $(a, n)$ . Hence, determining the decryption exponent  $d$  via the congruence (\*) is easy, *provided the modulus in (\*),  $\varphi(m)$  is known.*
- **Computing  $\varphi(m)$ , given  $m$ , is hard if the prime factorization of  $m$  is not known.** In fact, in the case when  $m = pq$  is a product of two prime factors, computing  $\varphi(m)$  is just as hard as factoring  $m$ . This makes it near impossible to compute the decryption exponent  $d$  via the congruence (\*) without knowing the prime factorization of  $m$ .
- **Computing  $\varphi(m)$  is easy if the prime factorization of  $m$  is known.** If the prime factorization of  $m$  is known, we can use the explicit formula  $\varphi(p_1^{\alpha_1} \dots p_r^{\alpha_r}) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \dots (p_r^{\alpha_r} - p_r^{\alpha_r-1})$ . In particular, if  $m = pq$ , then  $\varphi(m) = (p-1)(q-1)$ .