

# Number Theory

2018A7PS0193P



## CHAPTER 1

### Fundamentals

#### 1. Notation

For the rest of this course, the following notation will be followed:

- (1)  $\mathbb{N}$  is the set of natural numbers
- (2)  $\mathbb{Z}$  is the set of integers
- (3)  $\mathbb{W}$  is the set of whole numbers, i.e.  $\mathbb{W} = \mathbb{N} \cup \{0\}$

#### 2. Induction

Often in number theory, we use inductive proofs to prove our arguments. Induction consists of the following steps:

- (1) Define an induction hypothesis  $P(k)$
- (2) Verify it works for some base case  $k = b$ . It is possible multiple base cases need to be verified.
- (3) Assuming  $P(k)$  is true, show that it implies that  $P(k + 1)$  is true

Remember that  $P(k)$  is a statement, not a function. You cannot multiply it by some constant or perform any operations on it.

In weak induction (like in the steps given above), we only assume that  $P(k)$  is true. However in strong induction, we assume that  $P(i)$  is true  $\forall i \in [b, k]$ , and use this to prove that  $P(k+1)$  is true.

EXERCISE. Prove that the principle of strong induction is true given that the principle of weak induction is true.

SOLUTION. Let us assume that  $P(1), \dots, P(b)$  is true. If  $P(1), \dots, P(k)$  are true for some  $k \geq b$ , then  $P(k + 1)$  is true. Then, we must show that  $P(n)$  is true for all  $n \geq 1$ .

Let  $Q(n)$  be the statement that  $P(1), \dots, P(n)$  are true. Of course, in the base case,  $Q(1)$  is true. Let  $Q(k)$  be true, where  $K \geq 1$ . This means that  $P(1), \dots, P(k)$  is true, so  $P(k + 1)$  must be true. Hence,  $Q(k + 1)$  is true.

So, by Weak induction,  $Q(n)$  is true  $\forall n \geq 1$ , which implies that  $P(n)$  is true  $\forall n \geq 1$ . ■

### 3. Well Ordering Principle

**THEOREM 1.1** (Well Ordering Principle). Every non empty set of non-negative integers has a least element.

This is not true about negative integers - consider the case of infinite sets, like the set of all integers. There is no well defined least element.

**LEMMA 1.2.** The well ordering principle is equivalent to the principle of mathematical induction.

**PROOF.** First, let us prove that WOP  $\Rightarrow$  PMI. Let  $P(n)$  be a statement that depends on  $n \in \mathbb{N}$ . Suppose that:

- $P(1)$  is true
- $P(k)$  is true implies  $P(k+1)$  is true for all  $k \in \mathbb{N}$ .

We have to show that  $P(n)$  is true for all  $n \in \mathbb{N}$ . Let :

$$S = \{n \in \mathbb{N} : P(n) \text{ is true}\}$$

This means we must show that  $S = \mathbb{N}$ . Let  $T := \mathbb{N} \setminus S$ , i.e.  $T$  is the complement. Let us assume that  $S \neq \mathbb{N}$ .

By WOP,  $T$  has a least element, say  $m$ . Note that  $m \geq 2$  since  $1 \in S$ . Then,  $m-1 \notin T$  and  $m-1 \in S$ . As such,  $P(m-1)$  must be true! However, by our initial assumptions, that would mean  $P(m)$  is true as well, so  $m \in S$ . This creates a contradiction, since  $m \in T$ . Hence,  $S = \mathbb{N}$ .

Now, let us prove that PMI  $\Rightarrow$  WOP.

Consider the statement  $P(n)$  that every non empty set of non-negative integers of size  $n$  has a least element. It is clear that the base case  $P(1)$  is true. Now, let us assume that  $P(k)$  is true - what can we say about  $P(k+1)$ . When we insert an element, we have two cases:

- (1) The inserted element is less than the least element. In this case, there is a new least element, and  $P(k+1)$  is true.

- (2) The inserted element is not less than the least element. In this case, the least element is the same, and  $P(k+1)$  is true.

Hence, by PMI, we can say that  $P(n)$  is true  $\forall n \in \mathbb{N}$ , i.e., WOP is true.

Since  $\text{PMI} \Rightarrow \text{WOP}$  and  $\text{WOP} \Rightarrow \text{PMI}$ ,  $\text{PMI} \Leftrightarrow \text{WOP}$ . □

#### 4. Binomial Theorem

**THEOREM 1.3** (Binomial Theorem). Let  $x, y \in \mathbb{C}$  and let  $n \in \mathbb{N}$ , then

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

**COROLLARY 1.3.1.**

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

**LEMMA 1.4** (Pascal's Identity).

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

**LEMMA 1.5.**

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} = F_n$$

#### 5. Pigeonhole Principle

**THEOREM 1.6.** If  $n$  items are put into  $m$  containers, with  $n > m$ , then at least one container must contain more than one item.



## CHAPTER 2

### Division

#### 1. Division Algorithm

**THEOREM 2.1.** Let  $a, b \in \mathbb{Z}$  with  $b > 0$ . Then, there exist unique integers  $q$  and  $r$  such that  $a = bq + r$ ,  $r \in [0, b)$ .

**PROOF.** Let  $S = \{a - bn : n \in \mathbb{Z}, a - bn \geq 0\}$ . This set is always non-empty:

- If  $a \geq 0$ , then  $a \in S$
- If  $a < 0$ , then if  $n = a$ , we have  $a - ab \in S$  since  $b \geq 1$ .

By WOP,  $S$  has a least element, say  $r$ . So, there exists  $q \in \mathbb{Z}$  such that  $r = a - bq$ . Since  $r \in S$ , we have  $r \geq 0$ .

Suppose  $r \geq b$ . Then:

$$\begin{aligned} a - b(q + 1) &= a - bq - b = r - b \geq 0 \\ &\Rightarrow a - b(q + 1) \in S \\ &\Rightarrow r - b \in S \end{aligned}$$

However,  $r - b < r$ , and  $r$  is the least element! This gives us a contradiction. So,  $r < b$ .

As such, we have proved the existence of this solution. Now we must prove it's uniqueness.

Suppose there exists  $p, r, q', r'$ , such that:

$$\begin{aligned} a &= bq + r, 0 \leq r < b \\ a &= bq' + r', 0 \leq r' < b \end{aligned}$$

Assume WLOG  $q \geq q'$ . Now,

$$r' - r = b(q - q')$$

If  $q > q'$ , then  $r' - r \geq b$ . However,  $r' - r < b$ . So, this is a contradiction, and  $q' = q$ . The solution must be unique.

□

DEFINITION 1. If  $a, b \in \mathbb{Z}$ , we say that  $a$  divides  $b$  if  $b = ak$  for some  $k \in \mathbb{Z}$ . This is denoted by  $a|b$

Some properties of division are:

- If  $a|b$ , then  $\pm a|\pm b$
- If  $a|b$  and  $b|c$  then  $a|c$  (Transitivity)
- If  $a|b$  and  $a|c$  then  $a|bx + cy$  (Linear Combination)
- If  $a|b$  and  $b \neq 0$ , then  $|a| \leq |b|$  (Bounds by divisibility)
- $a|b$  and  $b|a$ , then  $b = \pm a$ .

## 2. Base $b$ representations

THEOREM 2.2. Let  $b \in \mathbb{N}$  with  $b \geq 2$ . Then every positive integer can be expressed uniquely as

$$N = a_k b^k + \dots + a_1 b + a_0$$

where  $k \geq 0, a_k \neq 0$  and  $0 \leq a_i < b$  for  $i = 0, \dots, k$ . This is denoted by  $N = (a_k, \dots, a_1 a_0)_b$

PROOF. By the division algorithm, there exist unique integers  $q_0$  and  $a_0$  such that:

$$N = q_0 b + a_0, a_0 \in [0, b)$$

Note that  $q_0 < N$ . If  $q_0 \neq 0$  we apply the division algorithm again to find unique integers  $q_1$  and  $a_1$  such that:

$$q_0 = q_1 b + a_1, a_1 \in [0, b)$$

Then,

$$N = (q_1 b + a_1)b + a_0 = q_1 b^2 + a_1 b + a_0$$

We continue till we get a quotient  $q_k = 0$ . This will terminate since  $q_k < \dots < q_2 < q_1 < q_0 < N$ , forming a decreasing sequence of non-negative integers and eventually reaching zero. From this, we get:

$$N = a_k b^k + \dots + a_1 b + a_0$$

Hence, the solution always exists.



Suppose  $N$  has two distinct expansions. We can write it as:

$$\begin{aligned} N &= a_k b^k + \dots + a_1 b + a_0 \\ &= c_k b^k + \dots + c_1 b + c_0 \end{aligned}$$

where  $0 \leq a_i, c_j < b$  for all  $i, j$ . Let  $d_i = a_i - c_i$ . Then,  $\sum_{i=0}^k d_i b^i = 0$ . The  $d_i$  cannot all be zero as the two expansions are assumed distinct. Let  $j$  be the least integer,  $0 \leq j \leq k$ , such that  $d_j \neq 0$ . Then,  $\sum_{i=j}^k d_i b^i = 0$ . Dividing by  $b^j$ , we find that  $\sum_{i=j}^k d_i b^{i-j} = 0$ . Thus,

$$d_j + b \left( \sum_{i=j+1}^k d_i b^{i-j-1} \right) = 0$$

This implies that  $b | d_j$  and since  $d_j \neq 0$ , we get that  $b = |b| \leq |d_j|$ . However,  $|d_j| < b$ . Hence, we have a contradiction, and the two expansions cannot be distinct. Hence, the solution is also always unique.  $\square$

LEMMA 2.3. If  $N = (a_k \dots a_1 a_0)_b$ , then:

$$\begin{aligned} bN &= (a_k \dots a_1 a_0 0)_b \\ \left\lfloor \frac{N}{b} \right\rfloor &= (a_k \dots a_1)_b \end{aligned}$$

This is a trivial result, which can be thought of as a left or right bitwise shift.

LEMMA 2.4 (Particular case of Legendre's formula). Let  $n \in \mathbb{N}$  and let  $e$  denote the highest power of 2 dividing  $n!$ . Then

$$e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor$$

This is always a finite sum. This can alternatively expressed as, if  $n = (a_k \dots a_1 a_0)_2$ , then:

$$e = n - (a_k + \dots + a_1 + a_0)$$

PROOF. It is clear that  $e$  is the sum of the no. of positive multiples of  $2^i$  which are  $\leq n$ , for all  $i$ . So, this can be calculated by:

$$e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor$$

$\square$

Thus, if  $r$  denotes the number of ones in the binary expansion of  $n$ , then  $2^{n-r}$  is the highest power of 2 dividing  $n!$ . Further,

- $2^n \nmid n!$  for  $n \in \mathbb{N}$
- $2^{n-1} \mid n!$  if and only if  $n$  is a power of 2.

## CHAPTER 3

### Properties of Numbers

#### 1. Prime and Composite Numbers

DEFINITION 2. A positive integer  $p > 1$  is called prime if its only positive divisors are 1 and  $p$ . A positive integer which is not prime is called composite.

The number 1 is neither prime nor composite.

LEMMA 3.1. Every integer  $n \geq 2$  has a prime factor.

PROOF. Let  $P(n)$  be the statement that  $n$  has a prime factor. Then  $P(2)$  is true, since 2 is a prime factor of 2. Let  $k \geq 2$ . Assume  $P(2) \dots P(k)$  are true.

If  $k + 1$  is prime, then  $k + 1$  is a prime factor of itself. So  $P(k + 1)$  is true.

If  $k + 1$  is composite, then there exists  $d \in [2, k]$  such that  $d | k + 1$ . By the induction hypothesis,  $d$  has a prime factor  $p$ . Since  $p | d$  and  $d | k + 1$ ,  $p | k + 1$ . So  $p$  is a prime factor of  $k + 1$ , and  $P(k + 1)$  is true. By PSI,  $P(n)$  is true for all  $n \geq 2$ .  $\square$

THEOREM 3.2 (Euclid). There are infinitely many primes.

PROOF. Suppose there are finitely many primes  $p_1, \dots, p_k$ . Let

$$N = p_1 \dots p_k + 1$$

Since  $N \geq 2$ , it must have a prime factor. Hence, there exists  $i \in [1, k]$  such that  $p_i | N$ . Since  $p_i | N$  and  $p_i | p_1 p_2 \dots p_k$ , we get that  $p_i | N - p_1 p_2 \dots p_k$ , i.e.,  $p_i | 1$ . However,  $p_i \geq 2$ , which gives us a contradiction. So, there must be infinitely many primes.  $\square$

EXERCISE. For  $n \geq 1$ , let  $p_n$  be the  $n$ th prime. Prove that

$$p_n \leq 2^{2^{n-1}}$$

SOLUTION. Let  $P(n)$  be the statement that  $p_n \leq 2^{2^{n-1}}$ . It is clear that this is true for the base case  $P(1)$ . Let us assume that  $P(1), \dots, P(k)$  is true for  $k \geq 1$ . We observed in

Euclid's proof that  $p_1 \dots p_k + 1$  is not divisible by any of  $p_1 \dots p_k$ . Hence if  $p_i$  denotes a prime factor of  $p_1 \dots p_k + 1$ , then  $i \geq k + 1$ .

$$p_{k+1} \leq p_i \leq p_1 \dots p_k + 1$$

Using the inductive hypothesis, we find that

$$\begin{aligned} p_{k+1} &\leq p_1 \dots p_k + 1 \leq 2 \cdot 2^2 \cdot 2^{2^2} \dots 2^{2^{k-1}} + 1 \\ &= 2^{\sum_{j=0}^{k-1} 2^j} + 1 = 2^{2^k - 1} + 1 \leq 2^{2^k} \end{aligned}$$

So,  $P(k + 1)$  is true. So, by PSI, the result has been proven. ■

DEFINITION 3. The product of the first  $n$  prime numbers is called the  $n^{\text{th}}$  primorial and is denoted by  $p_n\#$ .

DEFINITION 4. Euclid numbers are integers of the form  $E_n = p_n\# + 1$ .

All Euclid numbers are not primes -  $E_6$  is not a prime!

THEOREM 3.3. Every composite number  $n$  has a prime factor  $\leq \lfloor \sqrt{n} \rfloor$

PROOF. Since  $n$  is composite, there exists integers  $k, l \in (1, n)$  such that

$$n = kl$$

If  $k > \sqrt{n}$  and  $l > \sqrt{n}$  then  $kl > n$ , which is false. So, one of them must be less than or equal to  $\sqrt{n}$ . □

So, if  $n > 1$  has no prime factors  $\leq \lfloor \sqrt{n} \rfloor$ , then  $n$  is prime. We can use this as a test of primality.

It is faster to do this using the Sieve of Eratosthenes. Using this, we can test primality of the first  $n$  integers in  $O(n \log \log n)$  instead of  $O(n\sqrt{n})$ . This is a pretty well known algorithm so it's left to the reader to see it on cp-algorithms.

THEOREM 3.4. There is no non-constant polynomial  $f(x)$  with integer coefficients such that  $f(n)$  is prime for all integer  $n$ .

PROOF. Suppose such a polynomial  $f(x)$  exists:

$$f(x) = a_k x^k + \dots + a_1 x + a_0, k \geq 1, a_k \neq 0$$

Let  $b \in \mathbb{Z}$ . Then  $f(b)$  is a prime number, say  $p$ . Let  $t \in \mathbb{Z}$ . We have:

$$\begin{aligned} f(b+tp) &= a_k(b+tp)^k + \dots + a_1(b+tp) + a_0 \\ &= (a_k b^k + \dots a_1 b + a_0) + p \cdot g(t) \\ &= f(b) + p \cdot g(t) = p(1 + g(t)) \end{aligned}$$

where  $g(t)$  is a polynomial in  $t$ . Since  $p|f(b+tp)$  and it must be prime, so  $f(b+tp) = p$ . This implies that  $f$  assumes the value  $p$  infinitely many times. This is a contradiction, since a polynomial of degree  $k$  cannot assume the same value  $k$  times.  $\square$

## 2. Prime Counting function

Let  $x$  be a positive real number. We define :

$$\pi(x) = \sum_{p \leq x} 1$$

where  $p$  denotes a prime. So  $\pi(x)$  counts the number of primes  $\leq x$ . This is called the prime counting function.

**THEOREM 3.5 (Prime Number Theorem).**

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

This essentially states that  $\pi(x) \sim \frac{x}{\log x}$ . The proof is too complicated to be covered in this course.

## 3. Gaps between Primes

The following lemma states that we can find a gap between primes of any arbitrary length.

**LEMMA 3.6.** For every  $n \in \mathbb{N}$ , there are  $n$  consecutive integers that are all composite.

**PROOF.** Consider the numbers:

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$$

It is clear that for  $n \geq 1$ ,  $2|(n+1)! + 2$ . However,  $(n+1)! + 2 \neq 2$ . So,  $(n+1)! + 2$  cannot be prime, and must be composite. We can extend this to each of the given numbers, and prove that they are all composite.  $\square$

**DEFINITION 5.** A pair  $(p, q)$  of primes with  $p < q$  is called a twin prime pair if  $q - p = 2$ .

It is unknown how many twin primes exist. It is conjectured that there are infinitely many twin primes, but this has not yet been proved.

**THEOREM 3.7** (Bertrand's Postulate). For every integer  $n \geq 2$ , there is always at least one prime between  $n$  and  $2n$ .

This was verified by Bertrand but proved by Chebyshev. It is sometimes called Chebyshev's theorem. The proof of this result goes beyond the scope of this course.

**REMARK.** Do not use this result unless mentioned that we can, in the exam .

**EXERCISE.** Using Bertrand's postulate, prove that for  $n \geq 2$ :

$$p_n < 2^n$$

**SOLUTION.** Left as an exercise for me, TODO. ■

**EXERCISE.** Prove that if  $2^m + 1$  is prime, then  $m = 2^n$  for some  $n$ .

**SOLUTION.** Here, we use the following lemma - if  $k$  is odd, then  $x^k + 1$  is divisible by  $x + 1$ . Suppose that  $m$  has an odd factor  $k$ . Then, we can express  $m$  as  $kp$ . So,

$$2^{kp} + 1 = (2^p)^k + 1$$

From our lemma, this is divisible by  $2^p + 1$  which is a number other than 1 and itself. This means  $2^m + 1$  cannot be prime if it has an odd factor, and hence  $m$  must be a power of 2. ■

#### 4. Fermat Numbers

**DEFINITION 6.** Fermat numbers are  $f_n$  such that:

$$f_n = 2^{2^n} + 1$$

**LEMMA 3.8** (Recursive definition).

$$f_n = f_{n-1}^2 - 2f_{n-1} + 2$$

This result is obvious from expanding the RHS, so the proof is not given here.

**EXERCISE.** Prove that  $f_n$ ,  $n \geq 2$ , all end in 7.

SOLUTION. Let  $P(n)$  be the statement that  $f_n$  ends in 7. This is true for our base case  $P(2)$ . Let us assume that  $P(k-1)$  is true, i.e.  $f_k \bmod 10 = 7$ . So, by the recursive definition:

$$\begin{aligned} f_k &= f_{k-1}^2 - 2f_{k-1} + 2 \bmod 10 \\ &= 7^2 - 2 * 7 + 2 \bmod 10 \\ &= 7 \bmod 10 \end{aligned}$$

So, by PMI,  $P(n)$  is true for all  $n \geq 2$ . ■

LEMMA 3.9 (Duncan's Identity).

$$f_0 f_1 \dots f_{n-1} = f_n - 2$$

PROOF. Let  $P(n)$  be the statement that this is true for  $f_n$ . This is clearly true for the base case  $P(1)$ . Let us assume  $P(k)$  is true, i.e.

$$f_0 f_1 \dots f_{k-1} = f_k - 2$$

$$f_0 f_1 \dots f_k = f_k (f_k - 2) = f_k^2 - 2f_k = f_{k+1} - 2$$

The above result comes from the recursive definition. Since  $P(k+1)$  follows from  $P(k)$ , by PMI, Duncan's identity is true. □

THEOREM 3.10. Every prime factor of  $f_n$ ,  $n \geq 2$ , is of the form  $k \cdot 2^{n+2} + 1$ .

PROOF. To be discussed later in the course. □

This theorem can be helpful to quickly find the primality of  $f_n$ . For instance,  $f_4$  is prime - we can see this by checking all the numbers of the form  $2^6 k + 1$  which are less than  $\sqrt{f_4}$ . This cuts down the search space and makes primality checking faster.

## 5. Fibonacci Numbers

DEFINITION 7. Fibonacci numbers are numbers of the form:

$$F_n = F_{n-1} + F_{n-2}$$

where  $F_1 = 1, F_2 = 1$

LEMMA 3.11.

$$\sum_{i=1}^k F_i = F_{k+2} - 1$$

LEMMA 3.12 (Cassini's Formula).

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n, n \geq 2$$

The proofs of lemmas 5.1 and 5.2 come directly from induction, so I am not discussing the proof here.

## 6. Lucas Numbers

DEFINITION 8. Lucas numbers are numbers  $L_n$  such that:

$$L_n = L_{n-1} + L_{n-2}$$

where  $L_1 = 1, L_2 = 3$ .

THEOREM 3.13 (Binet's formulas). Let  $\alpha = \frac{1+\sqrt{5}}{2}$  and  $\beta = \frac{1-\sqrt{5}}{2}$ .

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

$$L_n = \alpha^n + \beta^n$$

PROOF. TODO

□



## CHAPTER 4

# Greatest Common Divisor and Least Common Multiple

### 1. Greatest Common Divisor

DEFINITION 9. Let  $a, b \in \mathbb{Z}$ , not both zero. The greatest common divisor of  $a$  and  $b$  is the positive integer  $d$  such that:

- $d|a$  and  $d|b$
- If  $c$  is a positive integer such that  $c|a$  and  $c|b$ , then  $c \leq d$ .

This is generally denoted by  $(a, b)$ .

The GCD of two non-zero numbers always exists and is unique. Observe that  $(a, b) = (a, -b) = (-a, b) = (-a, -b)$ . If  $a \neq 0$ , then  $(a, 0) = |a|$ .

DEFINITION 10.  $a, b \in \mathbb{Z}$  are relatively prime (coprime) if  $(a, b) = 1$ .

EXERCISE. Prove that  $(F_n, F_{n+1}) = 1$  for  $n \geq 1$ .

SOLUTION. From Cassini's formula, we know that:

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n$$

Let  $d = (F_n, F_{n+1})$ . Since  $d|F_n$  and  $d|F_{n+1}$ , we have  $d|F_{n-1}F_{n+1} - F_n^2$ . So  $d|(-1)^n$ . This means that  $|d| \leq |(-1)^n|$ . Since  $d$  is a positive number,  $d = 1$ . ■

EXERCISE. Prove that  $(f_m, f_n) = 1$  for distinct non-negative  $m, n$ .

SOLUTION. Suppose  $m < n$ . Let  $d = (f_m, f_n)$ . Since  $d|f_m$  and  $d|f_n$ ,  $d|f_n - (f_0 \dots f_m \dots f_{n-1})$ . From Duncan's identity, this implies that  $d|2$ . Since  $d > 0$ ,  $d = 1$  or  $d = 2$ . However, Fermat numbers are always odd - so  $d \neq 2$ . This implies that  $d = 1$ . ■

THEOREM 4.1. Let  $a, b \in \mathbb{Z}$ , not both zero. Then there exist integers  $x_0, y_0$  such that:

$$(a, b) = ax_0 + by_0$$

PROOF. Consider the set  $S = \{ax + by > 0 : a, b \in \mathbb{Z}\}$ . Let  $d = \min S$ . Suppose that  $d$  does not divide  $a$ . Then by division algorithm:

$$\begin{aligned} a &= qd + r \\ qd &= a - r \\ q(ax + by) &= a - r \\ r &= a(1 - qx) - bqy \end{aligned}$$

So,  $r$  is a linear combination of  $a$  and  $b$ , and since  $r > 0$ ,  $r \in S$ . From division algorithm,  $r < d$ , which contradicts the fact that  $d = \min S$ . So, by contradiction,  $d$  divides  $a$  (and by similar argument,  $d$  divides  $b$ ). We also know that any common divisor of  $a$  and  $b$  must divide  $d$ . This is obvious since if  $a = uc$  and  $b = vc$ , then  $d = ax + by = c(ux + vy)$ , so  $c|d$ . From these two facts, it is clear that  $d$  is the GCD, and is of the form  $ax + by$ .  $\square$

EXERCISE. Let  $a, b \in \mathbb{N}$ . If  $b = aq + r$ , then  $(a, b) = (a, r)$ .

SOLUTION. Let  $d = (a, b)$  and  $e = (b, r)$ . We need to show that  $d = e$ . Since  $d|a$  and  $d|b$ ,  $d|a - bq = r$ . So  $d$  is a common divisor of  $b$  and  $r$ . Hence  $d \leq e$ . Similarly, as  $e|b$  and  $e|r$ ,  $e$  divides  $bq + r = a$ . Thus  $e$  is a common divisor of  $a$  and  $b$ , so  $e \leq d$ . Thus,  $e = d$ .  $\blacksquare$

EXERCISE. Let  $a, b, c \in \mathbb{N}$ . Prove that  $(ac, bc) = c(a, b)$ .

SOLUTION. Let  $d = (a, b)$ . Then  $d|a$  and  $d|b$ , so  $d|ca$  and  $d|cb$ . There exist integers  $x, y$  such that:

$$\begin{aligned} d &= ax + by \\ cd &= (ac)x + (bc)y \end{aligned}$$

If  $e$  is a positive integer such that  $e|ac$  and  $e|bc$ , then  $e|(ac)x + (bc)y$ , i.e.  $e|cd$ . So,  $cd$  is the GCD of  $ac$  and  $bc$ .  $\blacksquare$

THEOREM 4.2. Let  $a, b \in \mathbb{Z}$ , not both zero. Then  $(a, b) = 1$  if and only if there exist integers  $x_0, y_0$  such that  $ax_0 + by_0 = 1$ .

PROOF. If  $(a, b) = 1$ , there must exist  $x_0, y_0$  such that  $ax_0 + by_0 = 1$ , from Theorem 4.1. Conversely, suppose there exists  $x_0, y_0 \in \mathbb{Z}$ , such that

$$ax_0 + by_0 = 1$$

Let  $d = (a, b)$ . Then  $d|ax_0 + by_0$ , which means that  $d|1$ . Since  $d \in \mathbb{N}$ ,  $d = 1$ .  $\square$

COROLLARY 4.2.1. Let  $d = (a, b)$ . Then,  $(\frac{a}{d}, \frac{b}{d}) = 1$

COROLLARY 4.2.2. If  $(a, b) = 1$ , and  $a$  and  $b$  both divide  $c$ , then  $ab|c$ .

THEOREM 4.3 (Euclid's Lemma). If  $a|bc$  and  $(a, b) = 1$ , then  $a|c$ .

PROOF.

$$ax + by = 1$$

$$acx + bcy = c$$

Since  $a|acx$  and  $a|bcy$ , so  $a|c$ . □

EXERCISE. Let  $m, n \in \mathbb{N}, m > 2$ . If  $F_m|F_n$ , prove that  $m|n$ .

PROOF. We know that:

$$F_n = F_{n-m}F_{m-1} + F_{n-m+1}F_m$$

Since  $F_m|F_n$  and  $F_m|F_{n-m+1}F_m$ , we get  $F_m|F_n - F_{n-m+1}F_m$  and hence  $F_m|F_{n-m}F_{m-1}$ . But, we also know that  $(F_m, F_{m-1}) = 1$ . By Euclid's Lemma,  $F_m|F_{n-m}$ .

From the division algorithm, let  $n = mq + r$ . Suppose  $r > 0$ . From our previous result,  $F_m|F_{n-m}$ , so  $F_m|F_{n-2m} \dots F_m|F_r$ . This means that  $F_m \leq F_r$ . But  $r < m$ , so  $F_r < F_m$ . This is a contradiction. So  $r = 0$ . Hence proved. □

DEFINITION 11. Let  $n \geq 2$  and let  $a_1, \dots, a_n \in \mathbb{Z}$ , not all zero. The GCD of  $a_1, \dots, a_n$  is the largest positive integer that divides each  $a_i$ . This is denoted by  $a_1, \dots, a_n$ .

This has the following properties:

- $(a_1, a_2, \dots, a_n)$  is the least positive integer that is a linear combination of  $a_1, \dots, a_n$ .
- $(a_1, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n)$
- If  $d|a_1, \dots, a_n$  and  $(d, a_i) = 1$  for all  $i \in [1, n-1]$ , then  $d|a_n$ .
- If  $a_1, \dots, a_n$  are pairwise relatively prime, then  $(a_1, \dots, a_n) = 1$ .

## 2. Euclidean Algorithm

We are given  $a, b \in \mathbb{Z}$ , not both zero, and want to compute  $(a, b)$ . The algorithm to do this works as follows:

- (1) If  $a$  or  $b$  are negative, replace with their absolute value.
- (2) If  $a > b$ , then swap  $a$  and  $b$ .
- (3) If  $a = 0$ , then  $(a, b) = b$ .
- (4) If  $a > 0$ , write  $b = aq + r$ . Then,

$$(a, b) = (r, a)$$

Go to step 3 with  $a = r$  and  $b = a$  respectively.

This is called the Euclidean Algorithm.

To express  $(a, b)$  as a linear combination of  $a$  and  $b$  where  $0 \leq a \leq b$ , we create a table with four columns with headings  $x, y, r, q$ . We denote the rows as  $R_{-1}, R_0, R_1, \dots, R_{i-1}$  and the entries in  $R_i$  as  $x_i, y_i, r_i, q_i$ . Suppose we have filled  $R_{i-1}$  for some  $i \geq 1$ . To fill  $R_i$ , we first compute  $q_i$ , which is the quotient obtained on dividing  $r_{i-2}$  by  $r_{i-1}$ . Next,  $R_i = R_{i-2} - q_i R_{i-1}$ . This is known as the Extended Euclidean Algorithm.

**THEOREM 4.4** (Lame's theorem). Let  $b \geq a \geq 2$ . The number of divisions required to compute  $(a, b)$  by the Euclidean algorithm is at most 5 times the number of decimal digits in  $a$ .

**PROOF.** Suppose that  $a$  contains  $k$  decimal digits and takes  $n$  divisions to compute  $(a, b)$ . We need to show that  $n \leq 5k$ . Let  $r_0 = b, r_1 = a$ . Applying Division algorithm repeatedly, we have:

$$r_0 = r_1 q_1 + r_2, 0 < r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3, 0 < r_3 < r_2$$

...

$$r_{n-1} = r_n \cdot q_n + 0$$

We can prove that  $q_i \geq 1$  for  $1 \leq i \leq n-1$  and  $q_n \geq 2$ . This is because if  $q_n$  is 1, then  $r_{n-1} = r_n$ , which is a contradiction. If  $q_i = 0$ , then  $r_{i-1} = r_{i+1}$ , which is also a contradiction.

We claim that  $r_{n-i} \geq F_{i+2}$  for  $1 \leq i \leq n-1$ . This is true for the base case, where  $r_{n-1} \geq F_3 = 2$ .

$$\begin{aligned} r_{n-j} &= r_{n-(j-1)}q_{n-(j-1)} + r_{n-(j-2)} \\ &\geq r_{n-(j-1)} + r_{n-(j-2)} \\ &\geq F_{j+1} + F_j = F_j + 2 \end{aligned}$$

In particular,  $a = r_1 \geq F_{n+1}$ . Now  $10^k > a \geq F_{n+1}\alpha^{n-1}$ , where  $\alpha = \frac{1+\sqrt{5}}{2}$  and  $n \geq 3$ . Taking logarithms and using the fact that  $\log \alpha > 1/5$ , we get that  $n \leq 5k$ .  $\square$

### 3. Least Common Multiple

DEFINITION 12. Let  $a, b \in \mathbb{N}$ . We say that a positive integer  $l$  is the least common multiple of  $a$  and  $b$  if

- $a$  and  $b$  both divide  $l$
- $c$  is a positive integer divisible by both  $a$  and  $b$ , then  $l \leq c$ .

It is generally denoted by  $[a, b]$ .

EXERCISE. Prove that  $(a, b)[a, b] = ab$ .

SOLUTION. Let  $d = (a, b)$  and let  $k = ab/d$ . Obviously,  $k \in \mathbb{N}$ . We have to show that  $k = [a, b]$ . We first prove that  $a$  and  $b$  both divide  $k$ . Write

$$a = da_1, b = db_1, a_1, b_1 \in \mathbb{Z}$$

Then,  $k = \frac{ab}{d} = ab_1 = ba_1$ . Hence  $a$  and  $b$  both divide  $k$ . Suppose  $c$  is a positive integer divisible by both  $a$  and  $b$ . Write

$$c = aa', c = bb', a', b' \in \mathbb{Z}$$

Since  $d = (a, b)$ , there exists integers  $x$  and  $y$  such that:

$$d = ax + by$$

Then

$$\frac{c}{k} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \frac{c}{b}x + \frac{c}{a}y = b'x + a'y \in \mathbb{Z}$$

Hence  $k$  divides  $c$ . Since  $c \neq 0$ , this implies  $k \leq c$ . Therefore, by definition,  $k = [a, b]$  and  $(a, b)[a, b] = ab$ .  $\blacksquare$

#### 4. Fundamental Theorem of Arithmetic

**THEOREM 4.5** (Fundamental Theorem of Arithmetic). Every integer  $n \geq 2$  can be written as a product of primes and the factorization into primes is unique up to the order of the factors.

**PROOF.** Let  $P(n)$  be the statement that  $n$  can be written as a product of primes.  $P(2)$  is true, since it is a prime. Let  $k \geq 2$  and  $P(2), \dots, P(k)$  is true. If  $k+1$  is prime, then  $P(k+1)$  is immediately true. If it is composite, then  $k+1$  is of the form  $a \cdot b$  where  $2 \leq a, b \leq k$ . By induction hypothesis, since  $P(a)$  and  $P(b)$  is true,  $P(k+1)$  is also true.

Suppose that

$$n = p_1 p_2 \dots p_r = q_1 \dots q_s$$

Assume  $r \leq s$ . Since if  $p_1 | q_1 \dots q_s$ ,  $p_1 = q_i$  for some  $i$ ,  $1 \leq i \leq s$ . We can cancel this out and keep doing this till we get

$$1 = q_{i_1} q_{i_2} \dots q_{i_{s-r}}$$

However,  $q_i$  is a prime. This is a contradiction unless  $s = r$ . Hence uniqueness is proved.  $\square$