Fall 2023

Connecting Number Theory with High School Mathematics

Andre Richmond

Connecting Number Theory with High School Mathematics

By

Andre Richmond

B.A, Northern Illinois University, 2017

Thesis

Submitted in partial fulfillment of the requirements for the Degree

of Master of Science with a Major in Mathematics

Governors State University

University Park, IL 60484

2023

Table of Contents

Abstract

Number theory is the study of natural numbers and one of the oldest branches of mathematics. Elementary number theory concepts are integrated into K-12 learning experience. This paper will identify ideas and methods in elementary number theory that could be connected to K-12 education and taught in high school classrooms. In fact, Common Core Standards in Mathematics include some basic concepts and skills in elementary number theory. In this study, we will focus on the greatest common divisor, Euclid's algorithm, least common multiple, factorization and divisibility criteria (divisible by 2, 3, 4, 5, 6, 8, 9, and 11). We hope that learning these contents could foster students' interests in mathematics and help them develop computational and reasoning skills.

Chapter 1: Prime Numbers

1.1 What are Prime Numbers?

Early on in elementary school, prime numbers are covered in our educational system. Between fourth and fifth grades, students are expected by the Common Core Standards to learn about prime numbers. To help students develop their understanding of division and multiplication, the common core state standards present this concept at an early age. If a teacher writes some integers greater than 1 such as $2, 3, 4, 5, 6, 7$ and 8 on the board and asks students to find the factors for each number, they can understand that $2, 3, 5,$ and 7 have no other positive factors except 1, and itself but $4 = 2(2),\ 6 = 2(3)$ and $8 = 2(2)(2)$. We say that $4, 6$ and 8 are divisible by 2 and 2 is their common divisor. In general, if a, b and c are integers and $a = bc$, then we say that a is divisible by b and c or b divides a and c divides a, written $b|a$ and $c|a$.

Definition 1.1.1. *A **prime number** is a natural number that is greater than 1 and not a product of two smaller natural numbers other than 1 and itself.*

Example 1.1.1. The integers 2, 3, 5, 13, 101, and 163 are primes.

Definition 1.1.2. *An integer greater than 1 that is not prime is called a **composite number**.*

Example 1.1.2. The integers $4 = 2(2),\ 8 = 4 \cdot 2,\ 33 = 3 \cdot 11,\ 111 = 3\ \cdot 37\ ,$ and $1001 = 7 \cdot 11 \cdot 13$ are composite.

1.2 Infinitely Many Primes Numbers

Even just imagining it might seem impossible, there exist an unlimited number of primes, and we do not know all of them. There are several techniques to demonstrate the existence of an endless number of primes. We will discuss Euclid's proof of the infinity of primes in the following paragraph.

Suppose that $p_1 = 2 < p_2 = 3 < \ldots < p_r$ are all the primes. Let $P = p_1 p_2 \ldots p_r + 1$. Then by the assumption, P is not a prime. If p is a prime dividing P, then p cannot be any of $p_1, p_2, \ldots, p_r$, otherwise p would divide the difference $P - p_1 p_2 \ldots p_r = 1$, which is impossible. So, this prime p is a new prime which is not included in the list of primes: $p_1, p_2, \ldots, p_r$. We get a contradiction and reach the conclusion that there are infinitely many primes.

1.3 Basic Properties of Divisibility

Theorem 1.3.1. *If a, b, and c are integers with $a|b$ and $b|c$, then $a|c$.*

Proof. Because $a|b$ and $b|c$, there are integers e and f such that $ae = b$ and $bf = c$. Hence, $c = bf = (ae)f = a(ef)$, and we conclude that $a|c$. □

Example 1.3.1. If n is composite, then we can write $n = ab$, where a and b are integers with $1 < a \leq b < n$. We must have $a \leq \sqrt{n}$, since otherwise $b \geq a > \sqrt{n}$ and $ab > \sqrt{n} \cdot \sqrt{n} = n$. Now, according to Lemma 1.3.1 below, a must have a prime divisor, which is proven to be smaller than or equal to a by Theorem 1.3.1 and is also a divisor of n (Rosen, 1984).

Well-Ordering Principle. *Any nonempty set of natural numbers has a least element.*

Lemma 1.3.1. *Every integer greater than 1 has a prime divisor.*

Proof. We prove the lemma by contradiction. We assume that there is a positive integer greater than 1 having no prime divisors. Then, since the set of positive integers greater than 1 with no prime divisors is nonempty, the well-ordering property tells us that there is a least positive integer n greater than 1 with no prime divisors. Because n has no prime divisors and n divides n, we see that n is not prime. Hence, we can write $n = ab$ with $1 < a < n$ and $1 < b < n$. Because $a < n, a$ must have a prime divisor. By Theorem1.3.1, any divisor of a is also a divisor of n, so

n must have a prime divisor, contradicting the fact that n has no prime divisors. We can conclude that every positive integer greater than 1 has at least one prime divisor. □

For relatively small integer n, there is a method, called the Sieve of Eratosthenes, to find all primes less than n. We will explain the Sieve of Eratosthenes by the following example.

Example 1.3.2. Find all primes less than 100.

Step 1. List all integers from 1 to 100.

Step 2. Keep 2 and mark out 1 and all multiples of 2 which are greater than 2.

Step 3. Keep 3 and mark out all multiples of 3 that are greater than 3.

Step 4. Keep 5 and mark out all multiples of 5 that are greater than 5.

Step 5. Continue in this way until on the list all composite numbers are marked.

Note: 7 is the next prime number after 5.

~~1~~	**2**	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~

Figure 1.3.1: Using the sieve of Eratosthenes to find the primes less than 100.

Chapter 2: Greatest Common Divisor

2.1 Connecting GCD with K-12

The greatest common divisor (GCD), also called the greatest common factor (GCF), of two or more integers is the largest positive integer that is a divisor of all the given integers. An especially useful property of the GCD is that it can be represented as a sum of the given numbers with integer coefficients. From here it immediately follows that the greatest common divisor of several numbers is divisible by any other common divisor of these numbers.

The greatest common divisor plays a similar role in our schools but may be better known as the greatest common factor in the Common Core Standards (**The Number System 6.NS.B.4)**. GCF is introduced in school around 6^{th} grade. Students at this level are expected to be able to list all the factors for every number up to 100. Between the grades of 9 and 12, more specifically in Algebra 1 and Algebra 2, the greatest common factor is revisited. In this chapter, we will go over some concepts on divisors and GCD.

2.2 Divisibility

Divisibility is a main concept in number theory.

Definition 2.2.1. (1) *Let a and b be two integers. If there is an integer c such that $b = ac$, then we say that a divides b, written $a|b$.*

(2) *If $a|b$, we say that a is a divisor or factor of b and b is a multiple of a.*

(3) *If a is not a factor of b, then we say that a does not divide b, written $a \nmid b$.*

To avoid notation confusion, two different symbols $a|b$ (divisibility relation) and a/b (a quotient obtained when a is divided by b) should be stressed in class to students.

Example 2.2.1. The following examples demonstrate the idea of integer divisibility:

$13|182, -5|30, 17|289, 6 \nmid 44, 7 \nmid 50, -3|33,$ and $17|0$.

Example 2.2.2. The divisors of 6 are $\pm 1, \pm 2, \pm 3,$ and ± 6. The divisors of 17 are $\pm 1,$ and ± 17. The divisors of 100 are $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50,$ and ± 100.

Example 2.2.3. Because $11|66$ and $66|198$, by Theorem 2.2.1, $11|198$.

Theorem 2.2.1. *Let $a, b, c, m,$ and n be integers. If $c|a$ and $c|b$, then $c|(ma + nb)$.*

Proof. Because $c|a$ and $c|b$, there are integers e and f such that $a = ce$ and $b = cf$. Hence, $ma + nb = mce + ncf = c(me + nf)$. Consequently, we see that $c|(ma + nb)$. □

Example 2.2.4. As $3|21$ and $3|33$, Theorem 2.2.2 tells us that 3 divides $21 \cdot 5 + 3 \cdot 33 = 105 + 99 = 204$.

Theorem 2.2.2. (**The Division Algorithm**). *If a and b are integers such that $b > 0$, then there are unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.*

In Theorem 2.2.2, q is called the quotient and r is called the remainder. We also call a the dividend and b the divisor. By the division algorithm, a is divisible by b if and only if the remainder r in the division algorithm is 0. Let us look at some examples of the division algorithm.

Example 2.2.5. If $a = 133$ and $b = 21$, then $q = 6$ and $r = 7$, because $133 = 21 \cdot 6 + 7$ and $0 \leq 7 < 21$. Likewise, if $a = -50$ and $b = 8$, then $q = -7$ and $r = 6$, because $-50 = 8 \cdot (-7) + 6$ and $0 \leq 6 < 8$.

We will use the Well-Ordering Principle to prove Theorem 2.2.2.

Proof. Consider the set S of all integers of the form $a - bk$, where k is an integer, that is, $S = \{a - bk | k \in Z\}$. Let T be the set of all nonnegative integers in S. T is nonempty, because $a - bk$ is positive whenever k is an integer with $k < a/b$. By the well-ordering, T has a least element

$r = a - bq$ (for an integer q). We know that $r \geq 0$ by construction. If $r \geq b$, then $r > r - b = a - bq - b = a - b(q + 1) \geq 0$, which contradicts the choice of $r = a - bq$ as the least nonnegative integer of the form $a - bk$. Hence, $0 \leq r < b$. We complete the proof of existence of q and r.

To show that these values for q and r are unique, assume that we have two equations $a = bq_1 + r_1$ and $a = bq_1 + r_2$, with $0 \leq r_1 < b$ and $0 \leq r_2 < b$. By subtracting the second equation from the first equation, we find that $0 = b(q_1 - q_2) + (r_1 - r_2)$. Hence, we see that $r_2 - r_1 = b(q_1 - q_2)$ which gives that b divides $r_2 - r_1$. Because $0 \leq r_1 < b$ and $0 \leq r_2 < b$, we have $-b < r_2 - r_1 < b$. Hence, b can divide $r_2 - r_1$ only if $r_2 - r_1 = 0$ or $r_1 = r_2$. Because $bq_1 + r_1 = bq_2 + r_2$ and $r_1 = r_2$, we have $q_1 = q_2$. This shows that the quotient q and the remainder r are unique. □

Example 2.2.6. Let $a = 1028$ and $b = 34$. Then $a = bq + r$ with $0 \leq r < b$, where $q = 30$ and $r = 8$.

Example 2.2.7. Let $a = -380$ and $b = 75$. Then $a = bq + r$ with $0 \leq r < b$, where $q = -6$ and $r = -380 - (-6)75 = 70$.

Divisibility Rules

The divisibility rules are a set of criteria for determining if a large number can be divided by a smaller number. The following are the rules for divisibility for numbers 1 through 6.

- Each positive integer can be divided by 1.
- If the dividend's final digit is even, then it can be divided by 2.
- A positive integer is divisible by three if the sum of dividend's total digits is multiple of three.

• If the dividend's final two digits can be divided by four, then this integer is divisible by four.

• If the dividend's last digit is 0 or 5, the integer is divisible by 5.

• If the dividend is divisible by 2 and 3, then the integer is divisible by 6.

We will prove them in Chapter 5 as well as explain more divisibility rules.

2.3 Greatest Common Divisor

If a and b are integers, not both 0, then the set of common divisors of a and b is a finite set of integers, always containing the integers $+1$ and -1. We are interested in the largest integer among the common divisors of the two integers.

Definition 2.3.1. *The **greatest common divisor** of two integers a and b, which are not both 0, denoted by (a, b) is the largest integer that divides both a and b.*

The greatest common divisor is also denoted by $gcd(a, b)$.

Example 2.3.1. The common divisors of 24 and 84 are $\pm1, \pm2, \pm3, \pm4, \pm6$, and ±12. Hence, $(24, 84) = 12$. Similarly, looking at sets of common divisors, we find that $(15, 81) = 3$, $(100, 5) = 5$, $(17, 25) = 1$, $(0, 44) = 44$, $(-6, -15) = 3$, and $(-17, 289) = 17$.

We are particularly interested in pairs of integers sharing no common divisors greater than 1. Such pairs of integers are called relatively prime.

Definition 2.3.2. *The integers a and b, with $a \neq 0$ and $b \neq 0$, are **relatively prime** if a and b have greatest common divisor $(a, b) = 1$.*

Example 2.3.2. Because $(25, 42) = 1$, 25 and 42 are relatively prime.

Theorem 2.3.1. *Let a and b be integers with $(a, b) = d$, then $(a/d, b/d) = 1$. In other words, a/d and b/d are relatively prime.*

Proof. Let a and b be integers with $(a, b) = d$. We will show that a/d and b/d have no common positive divisors other than 1. Assume that e is a positive integer such that $e|(a/d)$ and $e|(b/d)$. Then there are integers k and l with a$/d = ke$ and $b/d = le$, so that $a = dek$ and $b = del$. Hence, the product de is a common divisor of a and b. Because d is the greatest common divisor of a and b, $de \leq d$, so that e must be 1. Consequently, $(a/d, b/d) = 1$. □

The following corollary shows that every fraction equals a fraction in the simplest form.

Corollary 2.3.1. *If a and $b \neq 0$ are integers, then $a/b = p/q$ for some integers p and $q \neq 0$ with $(p, q) = 1$.*

Proof. Suppose that a and $b \neq 0$ are integers. Set $p = a/d$ and $q = \frac{b}{d}$, where $d = (a, b)$. Then $p/q = (a/d)/(b/d) = a/b$. By Theorem 2.3.1, $(p, q) = 1$, proving the corollary. □

Theorem 2.3.2. *Let a, b, and c be integers. Then $(a + cb, b) = (a, b)$.*

Proof. Let $d = (a, b)$ and $d' = (a + cb, b)$. Since $d|a$ and $d|b$, by Theorem 2.2.1, $d|(a + cb)$. So d is a common divisor of $a + cb$ and b which gives $d \leq d'$. Similarly, since $d'|(a + cb)$ and $d'|b$, we have $d'|a$ and $d'|b$. Therefore d' is a common divisor of a and b which shows $d' \leq d$. So $d = d'$. □

We will show that the greatest common divisor of the integers a and b, not both 0, can be written as a sum of multiples of a and b. To phrase this better, we use the following definition.

Definition 2.3.3. *If a and b are integers, then a **linear combination** of a and b is a sum of the form $ma + nb$, where both m and n are integers.*

Example 2.3.3 What are the linear combinations $9m + 15n$, where m and n are both integers? Among these combinations are $-6 = 1(9) + (-1)15;\ -3 = (-2)9 + 1(15);\ 0 = 0(9) +$

$0(15);\ 3 = 2(9) + (-1)15;\ 6 = (-1)9 + 1(15)$; and so on. It can be shown that the set of all linear combinations of 9 and 15 is the set $\{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$.

Theorem 2.3.3. *The greatest common divisor of the integers a and b, not both 0, is the least positive integer that is a linear combination of a and b.*

Proof. Let d be the least positive integer that is a linear combination of a and b. There is a least such positive integer, using the well-ordering property, since at least one of two linear combinations $1 \cdot a + 0 \cdot b$ and $-1 \cdot a + 0 \cdot b$, where $a \neq 0$, is positive. We write

$$d = ma + nb, \qquad (2.3.1)$$

where m and n are integers. We will show that $d|a$ and $d|b$. By the division algorithm, we have $a = dq + r,\ 0 \leq r < d$. From this equation and (2.3.1), we see that $r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb$. This shows that the integer r is a linear combination of a and b. Because $0 \leq r < d$, and d is the least positive linear combination of a and b, we conclude that $r = 0$, and hence $d|a$. In a similar manner, we can show that $d|b$.

We have shown that d, the least positive integer that is a linear combination of a and b, is a common divisor of a and b. What remains to be shown is that it is the greatest common divisor of a and b. To show this, all we need to show is that any common divisor c of a and b must divide d, since any proper positive divisor of d is less than d. Because $d = ma + nb,$ if $c|a$ and $c|b$, then by Theorem 2.2.1, $c|d$, so $d \geq c$. This concludes the proof. □

Theorem 2.3.4. *If a and b are positive integers, then the set of linear combinations of a and b is the set of integer multiples of (a, b).*

Proof. Suppose that $d = (a, b)$. We first show that every linear combination of a and b is a multiple of d. By the definition of greatest common divisor, we know that $d|a$ and $d|b$. Now

every linear combination of a and b is of the form $ma + nb$, where m and n are integers. By Theorem 2.2.1, it follows that d divides $ma + nb$. That is, $ma + nb$ is a multiple of d.

We now show that every multiple of d is also a linear combination of a and b. By Theorem 2.3.3, we know that there are integers r and s such that $d = (a, b) = ra + sb$. Multiplying both sides of the equation $d = ra + sb$ by j, we see that $dj = (jr)a + (js)b$. Consequently, every multiple of d is a linear combination of a and b. This completes the proof.

□

Theorem 2.3.5. *If a and b are integers, not both* 0*, then a positive integer d is the greatest common divisor of a and b if and only if*

i. $d|a \text{ and } d|b$, *and*

ii. *if* c *is an integer with* $c|a \text{ and } c|b$, *then* $c|d$.

Proof. We will first show that the greatest common divisor of a and b has these two properties. Suppose $d = (a, b)$. By the definition of common divisor, we know that $d|a$ and $d|b$. By Theorem 2.3.3, we know that $d = ma + nb$, where m and n are integers. Consequently, if $c|a$ and $c|b$, then by Theorem 2.2.1, $c|d = ma + nb$. We have now shown that if $d = (a, b)$, then properties (i) and (ii) hold.

Now assume that properties (i) and (ii) hold. Then we know that d is a common divisor of a and b. Furthermore, by property (ii), we know that if c is a common divisor of a and b, then $c|d$, so that $d = ck$ for some integer k. Hence, $c = d/k \leq d$. (We have used the fact that a positive integer divided by any nonzero integer is less than that integer.) This shows that a positive integer satisfying (i) and (ii) must be the greatest common divisor of a and b. □

Definition 2.3.4. *Let* $a_1, a_2, \ldots,$ and a_n *be integers, not all* 0. *The* ***greatest common divisor*** *of these integers is the largest integer that is a divisor of all the integers in the set, denoted by* $(a_1, a_2, \ldots, a_n)$.

Note that the order in which the a_i's appear does not affect the result.

Example 2.3.4. We easily see that $(12, 18, 30) = 6$ and $(10, 15, 25) = 5$.

We can use the following lemma to find the greatest common divisor of a set of more than two integers.

Lemma 2.3.1. *If* $a_1, a_2, \ldots, a_n$ *are integers, not all* 0, *then* $(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_2, \ldots, a_{n-2,} (a_{n-1}, a_n))$.

Proof. Let $d = (a_1, a_2, \ldots, a_{n-1}, a_n)$ and $d' = (a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n))$. Then d is a common divisor of a_{n-1} and a_n, and therefore a divisor of (a_{n-1}, a_n). So d is a common divisor of the $n - 1$ integers $a_1, a_2, \ldots, a_{n-2},$ and (a_{n-1}, a_n). This shows that d is not greater than d'. Since $d' | (a_{n-1}, a_n), d' | a_{n-1}$ and $d' | a_n$. As the greatest common divisor of $n - 1$ integers $a_1, \ldots, a_{n-2}$ and $(a_{n-1}, a_n), d'$ is also a common divisor of the n integer $a_1, a_3, \ldots, a_{n-1}, a_n$. So d' is not greater than d. We have shown $d = d'$. □

Example 2.3.5. To find the greatest common divisor of the three integers $105, 140,$ and 350, we use Lemma 2.3.1 to see that $(105, 140, 350) = (105, (140, 350)) = (105, 70) = 35$.

Example 2.3.6. Consider the integers $15, 21,$ and 35. We find that the greatest common divisor of these three integers is 1 using the following steps: $(15, 21, 35) = (15, (21, 35)) = (15, 7) = 1$. Each pair among these integers has a common factor greater than 1, because $(15, 21) = 3$, $(15, 35) = 5,$ and $(21, 35) = 7$.

Example 2.3.6 motivates the following definition.

Definition 2.3.5. *We say that the integers* $a_1, a_2, \ldots, a_n$ *are* ***mutually relatively prime*** *if* $(a_1, a_2, \ldots, a_n) = 1$. *These integers are called* ***pairwise relatively prime*** *if, for all* $i, j = 1, \ldots, n$ *with* $i \neq j$, $(a_i, a_j) = 1$; *that is, if each pair of integers from the set is relatively prime.*

Chapter 3. The Euclidean Algorithm

3.1 Euclidean Algorithm and The Common Core Standards

The ancient Greek mathematician Euclid first described a method to find the greatest common divisor of two integers in his book *Elements* written approximately 300 BC (Shallit, 1994). This method is called the Euclidean Algorithm, which has many applications including a proof of the Fundamental Theorem of Arithmetic and cryptography: a procedure for sending secret messages such as credit card transactions. In Common Core State Standards, 6th graders should be able to find the greatest common divisor of two integers less than or equal to 100. (CCSS.Math.Content.6.NS.B.4). They continue to learn the greatest common divisor through both Algebra 1 and Algebra 2. In Algebra 2, the idea of the Euclidean algorithm for integers can be applied to find the greatest common divisor of two polynomials. In the following section, we discuss the method for integers.

3.2 The Euclidean Algorithm

Theorem 3.2.1 (The Euclidean Algorithm). *Let* $r_0 = a$ *and* $r_1 = b$ *be integers such that* $a \geq b > 0$. *If the division algorithm is successively applied to obtain* $r_j = r_{j+1}q_{j+1} + r_{j+2}$, *with* $0 < r_{j+2} < r_{j+1}$ *for* $j = 0, 1, 2, \ldots, n-2$ *and* $r_{n+1} = 0$, *then* $(a, b) = r_n$, *the last nonzero remainder.*

To prove that the Euclidean algorithm produces the greatest common divisors, the following lemma will be helpful.

Lemma 3.2.1. *If e and d are integers and $e = dq + r$, where q and r are integers, then* $(e, d) = (d, r)$.

Proof. This lemma follows directly from Theorem 2.3.2: $(e, d) = (dq + r, d) = (r, d) = (d, r)$.

□

We now prove that the Euclidean algorithm produces the greatest common divisor of two integers.

Proof. Let $r_0 = a$ and $r_1 = b$ be positive integers with $a \geq b$. By successively applying division algorithm in Theorem 2.2.2, we find that

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_{j-1} + r_j, \quad 0 < r_j < r_{j-1}, \\
&\dots \\
r_{n-4} &= r_{n-3} q_{n-3} + r_{n-2}, \quad 0 < r_{n-2} < r_{n-3}, \\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2}, \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n.
\end{aligned}
$$

We can assume that we eventually obtain a remainder of zero because the sequence of remainders $a = r_0 \geq r_1 > r_2 > \dots \geq 0$ cannot contain more than a terms (because each remainder is an integer). By Lemma 3.2.1, we see that $(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) =$

$\ldots = (r_{n-3}, r_{n-2}) = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n$. Hence, $(a, b) = r_n$, the last nonzero remainder. □

Example 3.2.1. The steps used by the Euclidean algorithm to find $(252, 198)$ are

$$252 = 1 \cdot 198 + 54$$
$$198 = 3 \cdot 54 + 36$$
$$54 = 1 \cdot 36 + 18$$
$$36 = 2 \cdot 18.$$

We summarize these steps in the following table:

Table 3.2.1

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	252	198	1	54
1	198	54	3	36
2	54	36	1	18
3	36	18	2	0

The last nonzero remainder (found in the next-to-last row in the last column) is the greatest common divisor of 252 and 198. Hence, $(252, 198) = 18$.

Example 3.2.2. We apply the Euclidean algorithm to find $(34, 55)$. Note that $b = 34$ and $a = 55$. We have:

$$55 = 34 \cdot 1 + 21$$
$$34 = 21 \cdot 1 + 13$$
$$21 = 13 \cdot 1 + 8$$
$$13 = 8 \cdot 1 + 5$$
$$8 = 5 \cdot 1 + 3$$

$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2.$$

Observe that when the Euclidean algorithm is used to find the greatest common divisor of $b = 34$ and $a = 55$, a total of eight divisions are required. Furthermore, $(34, 55) = 1$, because 1 is the last nonzero remainder.

Definition 3.2.1. *The **Fibonacci sequence** is a series of numbers in which each number (Fibonacci number) is the sum of the two preceding numbers.*

The first few terms are $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$.

Theorem 3.2.2. *Let f_{n+1} and f_{n+2} be successive terms of the Fibonacci sequence, with $n > 1$. Then the Euclidean algorithm takes exactly n divisions to show that $(f_{n+1}, f_{n+2}) = 1$.*

Proof. Applying the Euclidean algorithm, and using the defining relation for the Fibonacci numbers $f_j = f_{j-1} + f_{j-2}$ in each step, we see that

$$f_{n+2} = f_{n+1} \cdot 1 + f_n,$$
$$f_{n+1} = f_n \cdot 1 + f_{n+1},$$
$$\ldots$$
$$f_4 = f_3 \cdot 1 + f_2,$$
$$f_3 = f_2 \cdot 2$$

Hence, the Euclidean algorithm takes exactly n divisions, to show that $(f_{n+2}, f_{n+1}) = f_2 = 1$.

□

Lemma 3.2.2. *If $f_{n-1} + f_{(n-2)} = f_n$ is the n^{th} term in the Fibonacci sequence, then $f_{n+1} > a^{n-1}$, for $n > 2$, where $a = \frac{1+\sqrt{5}}{2}$ is the root of $a^2 - a - 1 = 0$.*

Proof. We will use mathematical induction. Let $P(n)$ be the statement $f_n > a^{n-2}$. We want to show that $P(n)$ is true when $n \geq 3$.

First note that $a < 2 = f_3. a^2 = \frac{3+\sqrt{5}}{2} < 3 = f_4$, so $P(3)$ and $P(4)$ are true.

Induction step: Assume that P(j) is true, namely. $f_j > a^{j-2}$ for all integers j with $3 \leq j \leq k$ for some $k \geq 4$.

We now show that $P(k+1)$ is true, that is, $f_{k+1} > a^{k+1-2} = a^{k-1}$. In fact

$$f_{k+1} = f_k + f_{k-1} > a^{k-2} + a^{k-3} \text{ (by induction hypothesis)}$$

$$= (a+1)a^{k-3} \quad \text{(since a is a root of } x^2 - x - 1 = 0)$$

$$= a^2 \cdot a^{k-3} = a^{k-1}$$

It follows that $P(k+1)$ is true. □

Theorem 3.2.3 (**Lamè's Theorem**). *The number of divisions needed to find the greatest common divisor of two positive integers using the Euclidean algorithm does not exceed five times the number of decimal digits in the smaller of the two integers.*

Proof. When we apply the Euclidean algorithm to find the greatest common divisor of $a = r_0$ and $b = r_1$ with $a > b$, we obtain the following sequence of equations:

$$r_0 = r_1 q_1 + r_2, \quad 0 < r_2 < r_1,$$
$$r_1 = r_2 q_2 + r_3, \quad 0 < r_3 < r_2,$$
$$\dots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1},$$
$$r_{n-1} = r_n q_n.$$

We have used n divisions. We note that each of the quotients $q_1, q_2, \ldots, q_{n-1} \geq 1$, and $q_n \geq 2$, because $r_n < r_{n-1}$. Therefore,

$$r_n \geq 1 = f_2,$$
$$r_{n-1} \geq 2r_n \geq 2f_2 = f_3,$$
$$r_{n-2} \geq r_{n-1} + r_n \geq f_3 + f_2 = f_4,$$
$$r_{n-3} \geq r_{n-2} + r_{n-1} \geq f_4 + f_3 = f_5,$$
$$\ldots$$
$$r_2 \geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n,$$
$$b = r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}.$$

Thus, $b \geq f_{n+1}$. We know that $f_{n+1} > a^{n-1}$ for $n > 2$, where $a = \frac{1+\sqrt{5}}{2}$. Hence, $b > a^{n-1}$. Now, because $\log_{10} a > \frac{1}{5}$, we see that $\log_{10} b > (n - 1) \log_{10} a > \frac{n-1}{5}$. Consequently,

$n - 1 < 5 \log_{10} b$.

Let b have k decimal digits, so that $b < 10^k$ and $\log_{10} b < k$. Hence, we see that $n - 1 < 5k$, and because k is an integer, we can conclude that $n \leq 5k$. □

The Euclidean algorithm can be used to express the greatest common divisor of two integers as a linear combination of these integers. We illustrate this by expressing $(252, 198) = 18$ as a linear combination of 252 and 198. Referring to the steps of the Euclidean algorithm used to find $(252, 198)$, by the next to the last step we see that $18 = 54 - 1 \cdot 36$. By the preceding step, it follows that $36 = 198 - 3 \cdot 54$ which implies that $18 = 54 - 1(198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$. Likewise, by the first step, we have $54 = 252 - 1 \cdot 198$ so that $118 = 4(252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$. This last equation exhibits $18 = (252, 198)$ as a linear combination of 252 and 198.

In general, to see how $d = (a, b)$ may be expressed as a linear combination of a and b, we can rewrite the equations in the Euclidean algorithm backwards and obtain an equation $as + bt = d$, where s and t are integers. This equation is called the Bezout's identity. By the penultimate equation, we have $r_n = (a, b) = r_{n-2} - r_{n-1}q_{n-1}$. This expresses (a, b) as a linear combination of r_{n-2} and r_{n-1}. The second to last equation can be used to express r_{n-1} as $r_{n-3} - r_{n-2}q_{n-2}$. Using this last equation to eliminate r_{n-1} in the previous expression for (a, b), we find that $r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}$, so that $(a, b) = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1} = (1 + q_{n-1}q_{n-2})r_{n-2} - q_{n-1}r_{n-3}$, which expresses (a, b) as a linear combination of r_{n-2} and r_{n-3}. We continue working backward through the steps of the Euclidean algorithm to express (a, b) as a linear combination of each preceding pair of remainders, until we have found (a, b) as a linear combination of $r_0 = a$ and $r_1 = b$. Specifically, if we have found at a particular stage that $(a, b) = sr_j + tr_{j-1}$, then, because $r_j = r_{j-2} - r_{j-1}q_{j-1}$, we have $(a, b) = s(r_{j-2} - r_{j-1}q_{j-1}) + tr_{j-1} = (t - sq_{j-1})r_{j-1} + sr_{j-2}$. This shows how to move up through the equations that are generated by the Euclidean algorithm so that, at each step, the greatest common divisor of a and b may be expressed as a linear combination of a and b.

Chapter 4 Least Common Multiple

4.1 Common Core and Least Common Multiple

The least common multiple (LCM) is introduced as early as 6th grade (**CCSS-Math 6.NS.B.4)** but is used throughout K-12. The least common multiple of two or more integers is the least positive integer that is a multiple of these given integers. Students will build upon their mastery of LCM to find common denominators when adding fractions. One way to calculate the LCM of several integers is to factor each integer into a product of prime numbers. One can also construct the GCD using prime factorization. These methods are taught in elementary and middle schools and reinforced in high school.

4.2 Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be factored uniquely into a product of primes.

Theorem 4.2.1 (Fundamental Theorem of Arithmetic). *Every integer greater than 1 can be written in the form* $p_1^{n_1} p_2^{n_2} \ldots . p_k^{n_k}$*, where* $n_i \geq 0$ *and the* p_i*'s are distinct primes. The factorization is unique, except possibly for the order of the factors.*

For example, $4312 = 2 \cdot 2156 = 2 \cdot 2 \cdot 1078 = 2 \cdot 2 \cdot 2 \cdot 539 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 77 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 7 \cdot 11.$ So $4312 = 2^3 \cdot 7^2 \cdot 11.$

We need two useful lemmas before we prove the Fundamental Theorem of Arithmetic.

Lemma 4.2.1. *If* $a, b,$ *and* c *are positive integers such that* $(a, b) = 1$ *and* $a|bc,$ *then* $a|c.$

Proof. Because $(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Multiplying both sides of this equation by c, we have $acx + bcy = c$. By Theorem 2.2.1, a divides $acx + bcy$, because this is a linear combination of a and bc, both of which are divisible by a. Hence, $a|c$. □

The following consequence of this lemma will be needed in the proof of The Fundamental Theorem of Arithmetic.

Lemma 4.2.2. *If p divides the product $a_1a_2 \ldots a_n$, where p is a prime, and $a_1, a_2, \ldots,$ and a_n are positive integers, then there is an integer i with $1 \leq i \leq n$ such that p divides a_i.*

Proof. We prove this result by induction. The case where $n = 1$ is trivial. Assume that the result is true for n. Consider a product of $n + 1$ integers: $a_1a_2 \ldots a_{n+1}$, that is divisible by the prime p. We know that either $(p, a_1a_2 \ldots a_n) = 1$ or $(p, a_1a_2 \ldots a_n) = p$. If $(p, a_1a_2 \ldots a_n) = 1$, then by Lemma 4.2.1, $p|a_{n+1}$. On the other hand, if $p|a_1a_2 \ldots a_n$ using the induction hypothesis, there is an integer i with $1 \leq i \leq n$ such that $p|a_i$. Consequently, $p|a_i$ for some i with $1 \leq i \leq n + 1$. This proves the result. □

We now begin the proof of the Fundamental Theorem of Arithmetic. First, we will show that every positive integer greater than 1 can be written as the product of primes in at least one way. Then we will show that this product is unique up to the order of primes that appear.

Proof. We use proof by contradiction. Assume that some positive integer cannot be written as the product of primes. Let n be the smallest such integer (such an integer must exist, from the well-ordering property). If n is prime, it is obviously the product of a set of primes, namely the one prime n. If n is not a prime, let $n = ab$, with $1 < a < n$ and $1 < b < n$. Because a and b are smaller than n, each of them is a product of primes. Then we conclude that n is also a product of primes. This contradiction shows that every positive integer can be written as a product of primes.

We now finish the proof of the Fundamental Theorem of Arithmetic by showing that the factorization is unique.

Suppose that there is an integer *n* that has two different factorizations into primes: $n = p_1\, p_2 \ldots p_s = q_1\, q_2 \ldots q_t$, where $p_1, p_2, \ldots, p_s$, and $q_1, q_2, \ldots, q_t$ are all primes. We will prove the claim by induction on the number of primes in the equation.

If n is prime, then $s = t = 1$ and $p_1 = q_1$. The claim is true. Now we assume that n is not a prime. Since p_1 is a prime and $p_1 | q_1 q_2 \ldots q_n$, by lemma 4.2.2, p_1 divides one of the primes in the product. We may change the order in the product and assume that p_1 divides q_1. Since q_1 is also a prime, we have $p_1 = q_1$. Cancelling the common factor p_1 in the equation, we have a new equation $p_2 \ldots . p_n = q_2 \ldots . q_n$. By the inductive assumption, the set of primes $\{p_2, \ldots, p_s\} = \{q_2, \ldots, q_t\}$ and the factorization is unique except the order. □

Example 4.2.1. The Factorization of $120 = 2^3 \cdot 3 \cdot 5$

Image 4.2.1

1	3	5	$3 \cdot 5 = 15$
2	$2 \cdot 3 = 6$	$2 \cdot 5 = 10$	$2 \cdot 3 \cdot 5 = 30$
$2^2 = 4$	$2^2 \cdot 3 = 12$	$2^2 \cdot 5 = 20$	$2^2 \cdot 3 \cdot 5 = 60$
$2^3 = 8$	$2^3 \cdot 3 = 24$	$2^3 \cdot 5 = 40$	$2^3 \cdot 3 \cdot 5 = 120.$

4.3 Least Common Multiple

Definition 4.3.1. *The least common multiple of two nonzero integers a and b is the smallest positive integer that is divisible by a and b, written* $[a, b]$.

In the next example, we write $[a, b] = c$, where a and b are numbers and c is their LCM.

Example 4.3.1. We have the following least common multiples: $[15, 21] = 105,\ [24, 36] = 72, [2, 20] = 20,$ and $[7, 11] = 77.$

The least common multiple of two positive integers a and b is the product divided by the greatest common divisor:

$$[a, b] = \frac{ab}{gcd(a, b)}$$

Example 4.3.2.

$[15, 21] = \frac{15 \cdot 21}{\gcd(15,21)} = 105,$

$[2, 20] = \frac{2 \cdot 20}{\gcd(2,20)} = 20$

$[7, 11] = \frac{7 * 11}{\gcd(7,11)} = 77$

$[24, 36] = \frac{24 \cdot 36}{\gcd(24,36)} = 72$

Chapter 5 Factorization and Division Criteria

5.1 Factorization and Division Criteria in K-12

Students are taught how to factor an integer in elementary school and exposed to prime factorization in middle school through high school. In this chapter, we will present some division criteria which could be introduced to students in middle school or high school.

5.2 Division Criteria

In Chapter 2, by the Division Theorem, an integer *m* is divisible by a positive integer *n* if the remainder is zero and we have $m = nq$ for an integer q. In this section, we will provide some division criteria which can be understood by high school students.

Lemma 5.2.1. *Let a, b and $h > 0$ be integers. If $a = hg_1 + r_1$ and $b = hg_2 + r_2$ where g_1, g_2, r_1 and r_2 are integers, then the remainder of $a + b$ divided by h is equal to the remainder of $r_1 + r_2$ divided by h.*

Proof. This is a direct consequence of the equation $a + b = h(g_1 + g_2) + (r_1 + r_2)$, and that $h(g_1 + g_2)$ is divisible by h. □

An integer *a* can be expanded as a sum with base 10 as follows:

$$a = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0,$$

where $0 \leq r_i < 10,\ i = 0, 1, 2, \ldots, n$ and $r_n \neq 0$.

Divisibility Rules for 2

Any integer m can be written as $m = 2q + r$, where q and r are integers and $r = 0$ or 1. If $r = 0$, then we say that m is even and r =1, we say that m is odd. Since $m = 10n + a$, where n and a are integers and $a = 0, 1, 2, \ldots, 9$, every integer that has the digits $0, 2, 4, 6$, or 8 as its

unit digit can be divided by two (indicating that the number is even). For illustration: 456 ends in 6 so it can be divided by 2;

357 ends in 7 and cannot be divided by 2;

280 ends in 0 and can be divided by 2;

91 ends in 1 and cannot be divided by 2.

Divisibility Rule for 3

We can get the rule by the following calculation

$$10 = 9 + 1 = 3(3) + 1 = 3a_1 + 1,$$

$$10^2 = (9 + 1)^2 = 3a_2 + 1,$$

$$10^3 = (9 + 1)^3 = 3a_3 + 1,$$

where a_1, a_2 and a_3 are integers. By the binomial formula

$$(a + b)^n = a^n + \binom{n}{1} a^{n-1}b + \cdots + \binom{n}{n-1} ab^{n-1} + b^n,$$

we have

$$10^n = (9 + 1)^n = 3a_n + 1,$$

where a_n is an integer. So divided by 3, $r_n 10^n$ has a remainder r_n. By Lemma 5.2.1, divided by 3, $m = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0$ has a remainder $r_0 + r_1 + r_2 + \cdots + r_n$.

Conclusion: if the sum of its digits can be divided by 3, then the number can also be divided by 3. For instance:

624 can be divided by 3: $6 + 2 + 4 = 12$ and 12 can be divided by 3;

431 cannot be divided by 3: $4 + 3 + 1 = 8$, and 8 cannot be divided by 3;

91 cannot be divided by 3: $9 + 1 = 10$ and 10 cannot be divided by 3;

4671 can be divided by 3: $4 + 6 + 7 + 1 = 18$ and 18 can be divided by 3.

Divisibility Rule for 4

An integer is divisible by 4 if and only if the number represented by its last two digits is divisible by 4.

Proof. Any integer can be written as: $a = 100q + r, 0 \leq r < 100$. Since $4|100$, $4|a$ if and only if $4|r$. □

For example, $4|562396$ since $4|96$. 4 is not a factor of 562398 since 98 does not have a factor 4.

Divisibility Rule for 5

We can write any integer $a = 10q + r$ for some integers q and $0 \leq r < 10$. If a is divisible by 5 then r is 0 or 5. Thus, a particular number can be divided by 5 if its unit digit is 0 or 5. For illustration:

380 (it ends in 0) can be divided by 5;

264 (it ends in 4) cannot be divided by 5;

2175 (it ends in 5) can be divided by 5;

403 (it ends in 3) cannot be divided by 5.

Divisibility Rule by 6

An integer is divisible by 6 if and only if it is even and divisible by 3.

Proof. Since $gcd(2, 3) = 1$, an integer a is divisible by 6 if and only if it is divisible by 2 and 3.

□

24 is divisible by 2 and 3, so it is also divisible by 6.

16 is divisible by 2 but not 3, so 6 does not divide 16.

Divisibility Rule by 8

An integer is divisible by 8 if and only if the number represented by its last three digits is divisible by 8.

Proof. By division theorem, an integer a can be written as

$a = 1000q + r$, where $0 \leq r < 1000$. Since $8|1000$, $8|a$ if and only if $8|r$. □

For example, 562396 is not divisible by 8 since 396 is not divisible by 8. 562392 Is divisible by 8 since 392 has a factor 8.

Divisibility Rules for 9

We have $10 = 9 + 1$

$$10^2 = (9+1)^2 = 9^2 + 2(9) + 1 = 9a + 1$$

$$10^3 = 9b + 1, \qquad a, b \in N$$

Similarly, by the binomial formula,

$$(x+y)^n = x^n + \binom{n}{1} x^{n-1}y + \cdots + \binom{n}{n-1} xy^{n-1} + y^n,$$

where $n \in \mathbb{N}$, we have $10^n = (9+1)^n = 9k + 1, k \in \mathbb{N}$. This formula shows that divided by 9, $r_n 10^n$ has the least nonnegative remainder r_n. We can write a positive integer *m* in base 10:

$m = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0$, where $0 \leq r_i \leq 9$, and $r_n > 0$, $i =$ $0, 1, 2, \ldots, n$. By Lemma 5.2.1, m is divisible by 9 if $r_0 + r_1 + \cdots + r_n$ is divisble by 9.

The number can be divided by 9 if the sum of its digits can be divided by 9. For illustration:

2079: $2 + 0 + 7 + 9 = 18$, and 18 can be divided by 9, so 2079 can be divided by 9;

275: $2 + 7 + 5 = 14$, and 14 cannot be divided by 9 so 275 cannot be divided by 9;

9945: $9 + 9 + 4 + 5 = 27$, and 27 can be divided by 9 so 9945 can be divided by 9;

7824: $7 + 8 + 2 + 4 = 21$ and 21 cannot be divided by 9 so 7824 can be divided by 9.

Divisibility Rule for 11

We need the following formulas in this part with 1 being a negative remainder.

$$10 = 11 + (-1)$$

$$10^2 = 11^2 + 2(-1)(11) + (-1)^2 = 11a_1 + 1$$

$$10^3 = 11a_2 + (-1)^3 = 11a_2 + (-1)$$

In general, for $n \in N$,

$$10^n = 11a_n + (-1)^n$$

So divided by 11, 10^n has a remainder $(-1)^n$ and $r_n 10^n$ has a remainder $r_n(-1)^n$. By Lemma 5.2.1, divided by 11,

$$m = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0$$

has a remainder which is equal to the remainder of $r_0 - r_1 + r_2 - \cdots + (-1)^n r_n$.

Conclusion: if the sum of alternative digits of a number is divisible by 11, then that number is divisible by 11. To check whether 2143 is divisible by 11, we compute the sum of its alternate digits: $3 - 4 + 1 - 2 = -2$, which is not divisible by 11, so we conclude that 2143 is not divisible by 11. To check whether 1,331 is divisible by 11, we follow the same steps. $1 - 3 + 3 - 1 = 0$ which is divisible by 11.

5.3 Fermat Factorization Method

Pierre de Fermat (1607-1665) was a French mathematician who made significant contributions to analytic geometry, calculus, number theory and probability theory. The Fermat factorization method is a way to write an odd positive integer as a difference of two squares as follows.

Lemma 5.3.1. *If n is an odd positive integer, then n is the differences of squares of two integers.*

Proof. Let n be an odd positive integer and let $n = ab$ be a factorization of n into two positive integers. Then n can be written as the difference of two squares $n = ab = s^2 - t^2$, where $s = \frac{a+b}{2}$ and $t = \frac{a-b}{2}$ are both integers because a and b are both odd. □

Example 5.3.1. We factor 6077 using the method of Fermat factorization. Because $77 < \sqrt{6077} < 78$, we look for a perfect square in the sequence $78^2 - 6077 = 7$

$$79^2 - 6077 = 164$$

$$80^2 - 6077 = 323$$

$$81^2 - 6077 = 484 = 22^2.$$

Because $6077 = 81^2 - 22^2$, we see that $6077 = (81 - 22)(81 + 22) = 59 \cdot 103$.

The integers $F_n = 2^{2^n} + 1$ are called the Fermat numbers. Fermat conjectured that these integers are all primes. Indeed, the first few are primes, namely, $F_0 = 3, F_1 = 5, F_2 = 17,\ F_3 = 257$, and $F_4 = 65{,}537$. Unfortunately, $F_5 = 2^{2^5} + 1$ is composite, as we will now demonstrate.

Example 5.3.2. The Fermat number $F_5 = 2^{2^5} + 1$ is divisible by 641. We can show that $641 | F_5$ without performing the division, using several not-so-obvious observations. Note that

$$641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4.$$

Hence,

$$2^{2^5} + 1 = 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = (641 - 5^4)2^{28} + 1$$

$$= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1$$

$$= 641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4).$$

Therefore, we see that $641|F_5$.

The following result is a valuable aid in the factorization of Fermat numbers which was discovered by another French mathematician Edouard Lucas.

Theorem 5.3.1. *Every prime divisor of the Fermat number* $F_n = 2^{2^n} + 1$ *can be expressed in the form* $2^{n+2}k + 1$.

Example 5.3.3. From Theorem 5.3.1., we know that every prime divisor of $F_3 = 2^{2^3} + 1 = 257$ must be of the form $2^5 \cdot k + 1 = 32 \cdot k + 1$. Because there are no primes of this form which is greater than 16 and less than 17. we can conclude that $F_3 = 257$ is prime.

Example 5.3.4. When factoring $F_6 = 2^{2^6} + 1$, we use Theorem 5.3.1 to see that all of its prime factors are of the form $2^8 \cdot k + 1 = 256 \cdot k + 1$. Hence, we need only perform trial divisions of F_6 by primes of the form $256 \cdot k + 1$ that do not exceed $\sqrt{F_6}$. After considerable computation, we find that a prime divisor is obtained with $k = 1071$, that is, $274{,}177 = (256 \cdot 1071 + 1)|F_6$.

Conclusion

Illinois state adopted Common and Core Standards in Math on June 24, 2010 which emphasize reasoning skills. Learning elementary number theory could develop students' ability to reason abstractly and rigorously. Number theory has many applications such as coding theory, computing, cryptography, digital information, and physics. In 1974, Dr.Donald Knuth (a mathematician and famous computer scientist) said "...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations." Teaching elementary number theory and discussing its applications in daily life could motivate students' interests in math and science.

References

1. BYJU'S. (n.d.). *Divisibility Rules*. Retrieved from: https://byjus.com/maths/divisibility-rules/#divisibility-of-11

2. Caldwell, C. K. (2021). *Euclid's Proof of the infinitude of Primes*. Retrieved from: https://primes.utm.edu/notes/proofs/infinite/euclids.html

3. Childs, Lindsay N (2009). *A Concrete Introduction to Higher Algebra* (3rd edition). Springer.

4. Dockter, J. (n.d.). *Overview and Uses of the Division Algorithm*. Retrieved from Study.com: https://study.com/learn/lesson/division-algorithm-overview-examples.html#:~:text=The%20division%20algorithm%20is%20basically,0%20and%20less%20than%20b.

5. Encyclopædia Britannica. (n.d.). *Euclidean algorithm*. Retrieved from https://www.britannica.com/science/Euclidean-algorithm

6. *Finding the least common multiple.* Math Planet. Retrieved from: https://www.mathplanet.com/education/pre-algebra/discover-fractions-and-factors/finding-the-least-common-multiple#:~:text=LCM%2C%20the%20least%20common%20multiple,can%20be%20added%20or%20subtracted.

7. *Prime Numbers-Definition, Chart, Examples, Practice Problems*. SplashLearn. Retrieved from: https://www.splashlearn.com/math-vocabulary/algebra/prime-number#0-what-are-prime-numbers-

8. Rosen, K. (2011). *Elementary Number Theory and its Applications*. Addison-Wesley.