

TABLE OF CONTENTS

Introduction

Learning Objective 1: Apply Prime Factorization and Divisibility Techniques

Learning Objective 2: Master Modular Arithmetic Operations and Applications

Learning Objective 3: Analyze Integer Relationships with Number Theoretic Functions

Learning Objective 4: Explore and Solve Diophantine Equations

Conclusion

References

INTRODUCTION

Have you ever been astounded by the seemingly unending series of natural numbers and wondered if there are any intriguing correlations or hidden patterns among them? Why is 13 obstinately refractory, yet 12 is divisible by both 3 and 4? For ages, mathematicians have been enthralled with these basic concerns, which has led to the development of the intriguing field of number theory. This report sets out to explore this mysterious field, concentrating on two key ideas: modular arithmetic and prime factorization.

Number theory explores the characteristics of integers, or the whole numbers we use for counting and a variety of other purposes. It dates back to the time of Euclid and beyond. Number theory highlights the distinct beauty of natural numbers, in contrast to other branches of mathematics that concentrate on continuous quantities or complicated structures. In an effort to reveal the mysteries these seemingly straightforward figures conceal; this study addresses fundamental ideas in this field.

We shall discover the power of prime factorization through this investigation, which reduces any integer to its basic constituents: prime numbers. Prime factorization accomplishes the same thing as breaking down a complicated molecule into its individual atoms by exposing the fundamental components that make up any whole number. We will become proficient in factorization techniques and apply them to solve real-world issues such as determining the least common multiple or greatest common divisor of two numbers.

We explore the fascinating realm of modular arithmetic, which goes beyond factorization. Consider a closed numerical system in which computations repeat after a predetermined amount of time, wrapping around like a clock face. Although it may appear abstract, this idea is incredibly useful because it is the foundation of contemporary error-correcting codes and cryptography, which protect our internet communications and guarantee data integrity. As we get proficient with modular arithmetic operations, we will not only be able to understand its underlying logic but also see how number theory is applied in the real world by creating a basic cipher, proving that number theory is not limited by theory.

The research provides an introduction to the wide and complex field of number theory. Our goal is to prove that we understand prime factorization and modular arithmetic, as well as how they are related to one another and have real-world applications. We encourage you to embark with us on this intellectual trip as we unravel the mysterious world of numbers and recognize their hidden elegance and practical power through problem-solving, lucid explanations, and a dash of historical context.

LEARNING OBJECTIVE 1: APPLY PRIME FACTORIZATION AND DIVISIBILITY TECHNIQUES

Section 1: Unveiling the Prime Building Blocks.

In Section 1, we embark on the foundational journey of number theory by defining prime numbers and unraveling their crucial role in the realm of factorization.

1. The Essence of Primes:

We start our adventure with prime numbers, which are the basic building blocks of integers. These interesting objects are the key to deciphering the complex structure of any whole number because they have no positive integer divisors other than 1 and themselves. Prime factorization reveals the fundamental prime elements that make up any integer, much like breaking down a complicated substance into its individual atoms.

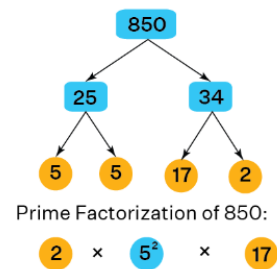
Prime Factorization of 40



$$\begin{aligned}\text{Prime factorization of } 40 &= 2 \times 2 \times 2 \times 5 \\ &= 2^3 \times 5\end{aligned}$$



Prime Factorization by Factor Tree Method



2. Unveiling the Secrets of Factorization:

Now, how do we crack the code and decompose an integer into its prime components? Two efficient algorithms shine brightly in this realm:

- **Trial Division:** This simple technique divides a given integer by progressively larger primes to test divisibility methodically until the residual number equals 1. Because of its simplicity, it works well with smaller integers but becomes less effective with larger numbers.
- Trial Division's methodical approach enables us to dissect complicated numbers into their fundamental parts and reveal the mathematical mysteries that lie behind them. Trial division is a useful strategy that expands your problem-solving toolset, whether you're using it to solve mathematical riddles, reduce fractions, or secure data using prime factorization methods. Thus, keep this approach in mind when you set out to discover prime factors—it will serve as a trustworthy roadmap that illuminates the way to mathematical comprehension.

- **Eratosthenes' sieve:** The Greek mathematician Eratosthenes created the ancient procedure known as the Sieve of Eratosthenes, which is a timeless example of human inventiveness in the search for prime numbers.
- Its simplicity is what gives it elegance; it provides a quick and effective method for finding prime factors as well as prime number identification. We will set out on a quest to understand the complexities of this approach, which has served as a centuries-old mathematical lighthouse, in this investigation.
- This sophisticated method adopts a more calculated approach. It efficiently identifies all primes up to a selected limit by repeatedly designating multiples of primes as composite. Its strength is in its capacity to factorize bigger integers with a comparatively smaller number of divisibility checks.

3. Witnessing Factorization in Action:

E.g. 1:

Let's put **Trial Division** algorithms to the test! let's find the prime factors of 36 using Trial Division:

- Start with 36.
- Divide by 2: $36 \div 2 = 18$. Record 2 as a factor.
- Divide by 2 again: $18 \div 2 = 9$. Record another 2 as a factor.
- Divide by 2 once more: $9 \div 2 = 4$ with a remainder of 1.
- Move on to the next prime, 3: $9 \div 3 = 3$. Record 3 as a factor.
- Continue until no more prime divisions are possible.

In the end, we find that the prime factors of 36 are indeed 2, 2, and 3.

E.g 2:

Show that 101 is prime:

- $\sqrt{101}$ is 10.4...
- So, if 101 cannot be factored into any of the primes less than 10 then it is prime.
- $2|101$ is false
- $3|101$ is false
- $5|101$ is false
- $7|101$ is false

So, 101 is prime.

To illustrate **Sieve of Eratosthenes** method, let's find the prime factors of 36 using it:

E.g. 1:

- Generate a list of prime numbers up to the square root of 36: 2, 3.
- Start with the first prime, 2. Check if 2 divides 36 evenly. It does ($36 \div 2 = 18$), so we record 2 as a prime factor and update 36 to 18.
- Proceed with the next prime, 3. Check if 3 divides 18 evenly. It does ($18 \div 3 = 6$), so we record 3 as another prime factor and update 18 to 6.
- Continue with the next prime, which is 3 again. Check if 3 divides 6 evenly. It does ($6 \div 3 = 2$), so we record 3 as a prime factor once more and update 6 to 2.
- Finally, check if 3 divides 2 evenly. It doesn't.
- We have now completed the process, and the prime factors of 36 are 2 and 3.

E.g 2:

Ex: Find all the primes between 1 and 100

- Begin with a list of integers not exceeding the specified limit.
- First eliminate all the integers that are divisible by 2.
- Because 3 is the first integer greater than 2 left, all the integers that are divisible by 3 other than 3 itself are deleted.
- Because 5 is the next integer greater than 3 left all integers divisible by 5, other than 5, are deleted. 5) The next integer greater than 5 left is 7. Delete all integers that are divisible by 7 other than 7.
- Because all composite integers between 1 and 100 are divisible by 2,3,5,7 all the remaining integers except 1 are prime

4. A Glimpse into the Past:

Mathematicians have been enthralled with the search for prime numbers and their characteristics for millennia. With his seminal work "Elements," Euclid laid the groundwork by proving that the prime number list is infinite.

Mathematicians such as Fermat and Mersenne explored deeper questions regarding the distribution and properties of primes, while Eratosthenes and others developed effective factorization algorithms over time. These mathematicians left behind a rich legacy of discoveries and unanswered mysteries that still fascinate mathematicians to this day.

The groundwork for our investigation of number theory is laid out in this section. With the right knowledge of prime numbers and their function in factorization, we can arm ourselves with the means to discover the mysteries that lie beyond the surface of the seemingly simple world of integers.

As we continue to explore modular arithmetic, number theoretic functions, and even Diophantine equations, keep in mind that these prime numbers serve as the fundamental building blocks for all of these fascinating ideas.

Section 2: Demystifying Divisibility Rules

1. Divisibility: A Prime Connection:

After figuring out the fundamentals of prime numbers, let's look at some applications. Divisibility rules give quick ways to find out if an integer divides evenly into another, based on certain prime factors. By revealing hidden links and patterns between numbers, these principles make divisibility checks easier to perform in a variety of situations.

2. Prime Factors Tell the Story:

When an integer is divisible by 2, it means that its prime factorization has at least one factor of 2. Similarly, a sum of digits that are divisible by three is equivalent to divisibility by three, indicating the combined effect of prime factors 2 and 3. Similar reasoning underlies other principles, such as divisibility by 5 or 9, which relate divisibility patterns to the underlying prime factorization.

3. Divisibility rules for some prime numbers are listed below:

- For checking divisibility by 2, we need to keep in mind that even numbers are always divisible by two.
- For checking divisibility by 3, add all the digits. After that, if the sum comes to be divisible by three, then the number is also divisible by the table of three.
- For checking divisibility by 5, check if the end of the number is 0 or 5.
- For checking divisibility by 7, you need to double the last digits of the given number. Then subtract it from the remaining number. The answer came that if divisible by seven, the number is divisible by seven.
- For checking divisibility by 11, add the digits in an alternate position. Then subtract it from the difference obtained by the sum of the next alternate digits. If the difference is divisible by eleven, then the given number is also divisible by 11. An example is if the number is 574652, add $5+4+5=14$ and $7+6+2=15$. Its difference will not be divisible by 11. Therefore, the given number is also not divisible by 11.

DIVISIBILITY RULES

Number	Divisibility Rules
2	Units Digit is even (2,4,6,8 0)
3	The sum of the digits is a multiple of 3
4	The number formed by the last 2 digits is a multiple of 4
5	The units digit is 5 or 0
9	The sum of the digits is a multiple of 9
10	The units digit is 0
25	The number formed by the last 2 digits is divisible by 25. Ends in 00, 25, 50, 75
100	Ends in 00

4. Putting Rules into Practice:

E.g 1:

Let's start with a simple example: Is 896 divisible by 7?

We take the last digit (6), double it (12) and subtract it from the remaining digits (89). This gives:

$$89 - 2 \times 6 = 89 - 12 = 77$$

We know that 77 is divisible by 7 (since $11 \times 7 = 77$), so this means that 896 is also divisible by 7.

Now, let's try our previous example of 3694806:

We remove the 6 and subtract twice it from the remaining digits:

$$369480 - 2 \times 6 = 369468$$

We still can't tell if this number is divisible by 7 or not so we repeat the procedure:

$$36946 - 2 \times 8 = 36930$$

Let's go again:

$$3693 - 2 \times 0 = 3693$$

This is taking a long time:

$$369 - 2 \times 3 = 363$$

Still not quite sure:

$$36 - 2 \times 3 = 30$$

Finally, we see that 30 is not divisible by 7, so neither is 3694806 (or for that matter any of our other numbers we found along the way).

With the number of calculations, it may have been easier to just do the division, let's try that:

$$3694806 / 7 = 527829 + 3$$

We see here we are left with 3 remainder, so it is not divisible by 7 as we found out earlier.

E.g 2:

Let's test our understanding! Is 84 divisible by 6?

Its prime factorization ($2^2 \times 3 \times 7$) reveals both factors of 2 and 3, satisfying the divisibility rule for 6.

On the other hand, 121, despite having a factor of 3, lacks a factor of 2, confirming its non-divisibility by 6.

By applying these rules effectively, we can quickly assess divisibility without cumbersome calculations.

4. Beyond the Basics:

While rules cover common cases, remember that exceptions exist. For instance;

- 12: Its sum of digits is 3, yet it's not divisible by 9 because its prime factorization ($2^2 \times 3$) lacks the necessary 3^2 factor.
- 27: The sum of digits is 9, but 27 isn't divisible by 18 because it needs two factors of 2 instead of just one (present in its prime factorization, 3^3).



Section 3: Unlocking Greatest Common Divisor and Least Common Multiple

1. The Heart of Divisibility:

Two key ideas that go further into the relationships between integers are the greatest common divisor (GCD) and least common multiple (LCM). The greatest number that is a factor of both supplied numbers is denoted by *GCD*, and the smallest number that is divisible by both is denoted by *LCM*. Gaining mastery of these ideas allows you to use them in a variety of contexts.

LCM (Lowest Common Multiple)	HCF (Highest Common Factor)
The least common multiple of two or more numbers is the smallest number among all common multiples of the given numbers.	The highest common factor of two or more numbers is the highest number among all the common factors of the given numbers.
LCM of two or more prime numbers is always the product of those numbers.	HCF of two or more prime numbers is 1 always.
LCM of two or more numbers is always greater than or equal to each of the numbers.	HCF of two or more numbers is always less than or equal to each of the numbers.

2. Unveiling the GCD:

We are able to find the GCD with efficiency thanks to prime factorization. We may build the GCD using those common prime factors by finding the largest power of each prime factor that appears in both values. Another useful tool for GCD calculation is the Euclidean algorithm, an elegant iterative procedure based on repeated divisibility checks.

Greatest Common Divisor

The greatest common divisor (GCD) of a set of whole numbers is the largest integer which divides them all.

GCD by Listing out the Factors

Find the GCD of 24 and 36

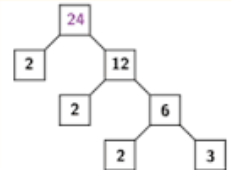
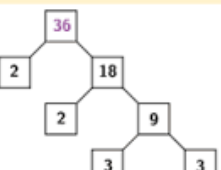
Divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24

Divisors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36

Greatest common divisor is 12

GCD using Prime Factorization

Find the GCD of 24 and 36

Find the prime factors that are common in both numbers

$24 = 2 \times 2 \times 2 \times 3$
 $36 = 2 \times 2 \times 3 \times 3$

$\text{GCD: } 2 \times 2 \times 3 = 12$

GCD using Repeated Division

Find the GCD of 24 and 36

$\text{GCD: } 2 \times 2 \times 3 = 12$

2	24	36
2	12	18
3	6	9
	2	3

E.g 1

Find the Greatest common factor of 24, 30 and 36.

- Solution: Prime factors of 24 is $2^3 \times 3$
- Prime factors of 30 = $2 \times 3 \times 5$
- Prime factors of 36 = $2^2 \times 3^2$
- From the factorisation, we can see, only 2×3 are common prime factors.
- Therefore, $\text{GCD}(24, 30, 36) = 2 \times 3 = 6$

E.g 2

Find the greatest common divisor (or HCF) of 128 and 96.

Solution:

- By the method of prime factorisation,
- $128 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
- $96 = 2 \times 2 \times 2 \times 2 \times 2 \times 3$
- $\text{HCF}(128, 96) = 2 \times 2 \times 2 \times 2 \times 2 = 32$
- Hence, 32 is the HCF of 128 and 96.

E.g 3

Two rods are 22 m and 26 m long. The rods are to be cut into pieces of equal length. Find the maximum length of each piece.

Solution:

- HCF or GCD is the required length of each piece.
- $22 = 2 \times 11$
- $26 = 2 \times 13$
- HCF or the greatest common divisor = 2
- Hence, the required maximum length of each piece is 2 m.

E.g 4

What is the GCD of 36, 54 and 90?

- The factors of 36 are: 1, 2, 3, 4, 6, 9, 12, 18, 36.
- The factors of 54 are: 1, 2, 3, 6, 9, 18, 27, 54
- The factors of 90 are: 1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90
- Therefore, $\text{GCD}(36, 54, 90) = 18$

E.g 5

The Euclidean algorithm is a way to find the greatest common divisor of two positive integers, a and b. First let me show the computations for a=210 and b=45.

- Divide 210 by 45, and get the result 4 with remainder 30, so $210=4\cdot45+30$.
- Divide 45 by 30, and get the result 1 with remainder 15, so $45=1\cdot30+15$.
- Divide 30 by 15, and get the result 2 with remainder 0, so $30=2\cdot15+0$.
- The greatest common divisor of 210 and 45 is 15.

3. Bridging the Gap with LCM:

On the other hand, LCM can be determined by multiplying each prime factor that appears in both numbers to the highest power in both factorizations. Alternatively, GCD and LCM have the following ingenious relationship: $LCM \times GCD = \text{product of both values}$. By comprehending and using these associations, we can enhance our repertoire for adjusting divisibility relationships.

LCM

Lowest Common Multiple

2	6,	8,	12
2	3,	4,	6
2	3,	2,	3
3	3,	1,	3
	1,	1,	1

E.g 1

Find the least common multiple (LCM) of 60 and 90 using prime factorization.

Solution: Let us find the LCM of 60 and 90 using the prime factorization method.

Step 1: The prime factorization of 60 and 90 are: $60 = 2 \times 2 \times 3 \times 5$ and $90 = 2 \times 3 \times 3 \times 5$

Step 2: If we write these prime factors in their exponent form it will be expressed as, $60 = 2^2 \times 3^1 \times 5^1$ and $90 = 2^1 \times 3^2 \times 5^1$

Step 3: Now, we will find the product of only those factors that have the highest powers among these. This will be, $2^2 \times 3^2 \times 5^1 = 4 \times 9 \times 5 = 180$

Therefore, LCM of 60 and 90 = 180.

E.g 2

Find the least common multiple (LCM) of 4 and 5.

- Solution: The first few multiples of 4 are: 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, ...
- And the first few multiples of 5 are: 5, 10, 15, 20, 25, 30, 35, 40, ...

LCM of 4 and 5 by listing out the common multiples



Multiples of 4:

4 8 12 16 20 24 28 32 36 40

Multiples of 5:

5 10 15 20 25 30 35 40

LCM (4, 5) = 20

4. Real-World Applications:

GCD and LCM are important cryptography operations that select huge integers with certain divisibility features to guarantee secure transmission. They can also be used to detect common denominators, simplify fractions, and even streamline computer science methods. Their importance is not limited to theoretical investigations.

Additionally, the extended Euclidean algorithm uses the GCD to compute modular inverses, which are crucial for encryption systems like RSA. It is also very significant when thinking about an element's order, notably in the context of Lagrange's theorem and its application to modular arithmetic. This makes it a frequent subject in sporting events like the Olympics.



LEARNING OBJECTIVE 2: MASTER MODULAR ARITHMETIC OPERATIONS AND APPLICATIONS

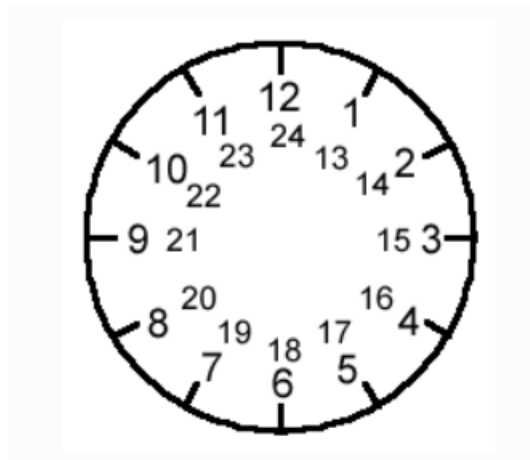
Section 4: Stepping into the Modular Clockwork

1. A World of Repeating Numbers:

An intriguing idea is introduced by modular arithmetic: computations are carried out inside a closed system of numbers, and the results "wrap around" like a clock's hands when they reach a particular limit. This seemingly ethereal idea is incredibly useful in practice, serving as the basis for contemporary error-correcting codes and cryptography.

2. The Rules of the Clock:

We do perform calculations modulo a selected number n in modular arithmetic. When the first result is divided by n , the outcome is always the residual. This "clock-like" notion is applied to addition, subtraction, multiplication, and even exponentiation to ensure that calculations remain within the specified range of 0 to $n-1$.



3. Putting on Our Modular Hats:

Imagine a clock face with only 5 numbers: 0, 1, 2, 3, and 4. That's essentially what modular arithmetic is like! Instead of counting infinitely, we wrap around after reaching the "modulus" (5 in this case). This might seem strange at first, but it unlocks unique properties and applications.

Let's experiment!

Addition:

In modulo 5, adding 3 and 7 doesn't give you 10 like in regular arithmetic. Instead, it gives you 0! Why? Because 10 divided by 5 leaves a remainder of 0. It's as if you move 5 steps "clockwise" on the clock and end up back at 0.

Multiplication:

Similarly, multiplying 2 and 4 doesn't result in 8. Instead, it gives you 3. Again, why? Because 8 divided by 5 leaves a remainder of 3. Think of it like jumping ahead 8 spaces on the clock, but "skipping over" multiples of 5 and landing on 3.

These might seem like silly games, but mastering these operations within the modular system is crucial for:

- **Cryptography:** Secure online transactions often rely on modular arithmetic to create complex codes that are difficult to crack.
- **Error correction:** Data transmission systems use modular arithmetic to detect and correct errors that might occur during transmission.
- **Clock systems and calendars:** Even ancient calendars like the Mayan calendar used modular arithmetic principles.

4. A Glimpse into History and Beyond:

Ancient calendars and clock systems are where modular arithmetic first appeared, illustrating its historical relevance. But its contemporary uses are where its real strength resides. Having a solid understanding of modular arithmetic allows us to confidently navigate the increasingly digital world, from safeguarding online transactions to maintaining data integrity.

Numerous uses for modular arithmetic can be found in computer science and cryptography. It is frequently employed to find identification number inaccuracies. Consider the various identifying numbers we utilize on a daily basis. Bank accounts, credit cards, and product barcodes all require lengthy numerical sequences. Computer systems must exchange these numbers accurately. Consider utilizing your credit card for internet purchases. Consider the scenario where two of the digits are mistyped or swapped. These kinds of faults are found using modular arithmetic.



Section 5: Solving Linear Congruences with Confidence

1. Putting the Pieces Together:

We look for solutions for the unknown integer x within the modular system described by n . Linear congruences are equations of the type " $ax \equiv b \pmod{n}$ " where a , b , and n are integers. These equations require effective solutions in order to unlock a variety of applications in fields such as cryptography and coding.

2. Unveiling the Euclidean Hero:

The Euclidean algorithm, well known for its function in determining GCD , is a potent tool for resolving linear congruences. We may effectively isolate x and discover its solution within the modular system by transforming the given equation into one where the coefficient of x becomes $1 \pmod{n}$ by the creative manipulation of multiples and remainders.



3. The Inverse Approach:

An alternative approach makes use of the notion of modular inverses. The solution for x can be found by multiplying both sides of the congruence by a^{-1} if a number a has an inverse modulo n , represented as a^{-1} . A further tool for issue solving is the extended Euclidean algorithm, which finds modular inverses.

4. Witnessing Solutions in Action

Let's delve into the exciting world of congruences by solving the equation $3x \equiv 7 \pmod{10}$. We'll witness the power of two distinct methods: the mighty Euclidean algorithm and the clever modular inverse approach.

Method 1: The Euclidean Algorithm - A Step-by-Step Journey

The Euclidean algorithm embarks on a journey of remainders, elegantly eliminating multiples of numbers until we reach the desired form. Buckle up!

Set the stage: We rewrite the equation as $3x - 7 \equiv 0 \pmod{10}$.

Divide and conquer: Since 10 is larger than 3, we divide 10 by 3: $10 = 3 * 3 + 1$. This implies $3 * 3 - 10 \equiv 1 \pmod{10}$.

Substitute and simplify: We rewrite the original equation as $3x - 7 \equiv 0 \pmod{10}$, which we can express as $3(3x - 10) \equiv 0 \pmod{10}$. Now, substitute the relation we found in step 2: $3(3 * 3 - 10) \equiv 0 \pmod{10}$. Simplifying, we get $9 - 30 \equiv 0 \pmod{10}$.

The magic unfolds: Finally, we have $-21 \equiv 0 \pmod{10}$. Adding 30 (a multiple of the modulus) doesn't change the congruence, so $9 \equiv 0 \pmod{10}$. Now, recall that $9 = 3 * 3$. Dividing both sides by 3 (remembering modular arithmetic allows only invertible operations), we arrive at: $x \equiv 3 \pmod{10}$.

Verification: Doubling our answer, we see that $3 * 3 = 9$, and indeed, 9 divided by 10 leaves a remainder of 9, confirming our solution!

Method 2: The Modular Inverse - A Shortcut with a Twist

The key to this approach is figuring out 3's modular inverse, or 3^{-1} modulo 10. An inverse is a number that produces 1 modulo the modulus when multiplied by the original number. $3^{-1} * 3 \equiv 1 \pmod{10}$ in our instance. It may take more sophisticated methods or trial and error to find the inverse. In this particular instance, $3^{-1} = 7$. This can be confirmed by multiplying 3 by 7 modulo 10.

Now, let's apply this magic:

E.g 1

Multiply both sides: We start with the original equation: $3x \equiv 7 \pmod{10}$. Multiplying both sides by 3^{-1} (which is 7 in this case) gives us: $(3^{-1}) * 3x \equiv (3^{-1}) * 7 \pmod{10}$.

Simplify and solve: Remember that $(a * b) \pmod{n} = (a \pmod{n}) * (b \pmod{n})$. Applying this, we get $x \equiv (7 * 7) \pmod{10}$. Simplifying, we have $x \equiv 49 \pmod{10}$. Since 49 divided by 10 leaves a remainder of 9, and $9 \equiv 0 \pmod{10}$, we arrive at the same solution: $x \equiv 3 \pmod{10}$.

Verification: As before, multiplying 3 by 3 modulo 10 confirms our answer.

E.g 2

Find the inverse of 3 modulo 7.

Since $\gcd(3, 7) = 1$, an inverse must exist. From Euclidean division we have $7 = 2 \cdot 3 + 1$ and thus $-2 \cdot 3 + 1 \cdot 7 = 1$. Hence, -2 is the Bézout coefficient of 3 and $-2 \equiv 5 \pmod{7}$ is the modular inverse of 3.

E.g 3

Find the inverse of 151 modulo 951.

Using the Euclidean algorithm we find:

$$951 = 6 \cdot 151 + 45$$

$$151 = 3 \cdot 45 + 16$$

$$45 = 2 \cdot 16 + 13$$

$$16 = 1 \cdot 13 + 3$$

$$13 = 4 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

Therefore, $\gcd(951, 151) = 1$. Moreover, we can find a Bézout relation between 951 and 151 via back substitution:

$$1 = 13 - 4 \cdot 3$$

$$1 = 13 - 4(16 - 1 \cdot 13) = -4 \cdot 16 + 5 \cdot 13$$

$$1 = -4 \cdot 16 + 5(45 - 2 \cdot 16) = 5 \cdot 45 - 14 \cdot 16$$

$$1 = 5 \cdot 45 - 14(151 - 3 \cdot 45) = -14 \cdot 151 + 47 \cdot 45$$

$$1 = -14 \cdot 151 + 47(951 - 6 \cdot 151) = -296 \cdot 151 + 47 \cdot 951$$

Therefore, the modular inverse of 151 modulo 951 is $-296 \equiv 655 \pmod{951}$.

The Beauty of Different Paths:

We arrive to the same answer using both techniques, demonstrating the variety of ways used in modular arithmetic. When it comes to handling congruences, the Euclidean algorithm offers a step-by-step explanation, while the modular inverse approach offers a speedier shortcut after the inverse is found. Every strategy has advantages and uses depending on the particular issue.



LEARNING OBJECTIVE 3: ANALYZE INTEGER RELATIONSHIPS WITH NUMBER THEORETIC FUNCTIONS

Section 6: Unveiling the Secrets of Euler's Totient Function

1. Counting with a Twist:

The number of positive integers less than n that are relatively prime to n (having no common factors other than 1) is counted by Euler's totient function, represented by the symbol $\phi(n)$. This seemingly straightforward function in number theory opens up a wide range of applications and unexpected consequences.



2. Unveiling the Calculation Magic:

It is important to calculate $\phi(n)$ efficiently. $\phi(n)$ for prime numbers is $n-1$. We may easily determine $\phi(n)$ for composite numbers using a variety of formulas and identities, such as the Sieve of Eratosthenes applied to $\phi(n)$ values up to the square root of n .

3. Putting $\phi(n)$ to Work:

In number theory, counting the number of positive integers less than a given number ' n ' that have no common factors with ' n ' other than 1 is made interesting by Euler's totient function, represented by $\phi(n)$. We refer to these numbers as relatively prime to ' n '. Now, let us examine and apply $\phi(n)$ using a real-world example:

4. Putting Euler's Totient Function to Work

In number theory, Euler's totient function, denoted by $\phi(n)$, plays a fascinating role in counting the number of positive integers less than a given number 'n' that share no common factors with 'n' other than 1. These integers are called relatively prime to 'n'. Let's delve into understanding and applying $\phi(n)$ using a practical example:

The Case of $n = 15$:

How many numbers less than 15 are relatively prime to 15?

- **Prime Factorization:** We start by breaking down 15 into its prime factorization: $15 = 3 \times 5$. This reveals the building blocks of 15.
- **Relatively Prime Numbers:** Numbers relatively prime to 15 must not share any prime factors with 15 itself. So, neither 3 nor 5 can be factors of those numbers. This eliminates numbers like 3, 5, 6, 9, and 10 from our list.
- **Counting with $\phi(n)$:** Here's where the magic of $\phi(n)$ comes in. The formula for $\phi(n)$ for any number 'n' is: $\phi(n) = (p_1 - 1)(p_2 - 1)\dots$, where p_1, p_2, \dots are the distinct prime factors of 'n'. In our case, $\phi(15) = (3 - 1)(5 - 1) = 8$. This value, remarkably, tells us exactly how many numbers less than 15 are relatively prime to it!
- **Verification:** Let's list the numbers less than 15: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14. As we already eliminated 3, 5, 6, 9, and 10, we're left with 1, 2, 4, 7, 8, 11, 12, 13, and 14. Indeed, there are 8 numbers in this list, confirming the prediction from $\phi(15)$.

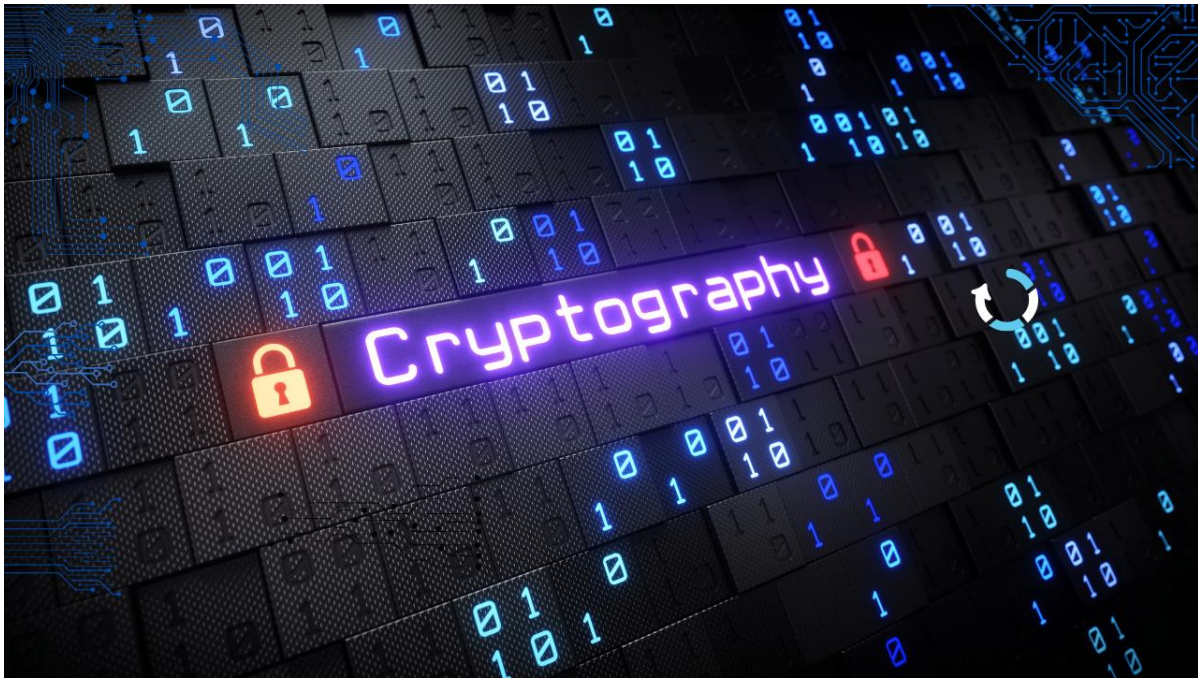
Key Takeaways:

- $\phi(n)$ offers a shortcut to count relatively prime numbers less than 'n' without manually checking each number's prime factors.
- Understanding prime factorization is crucial for interpreting $\phi(n)$'s results.
- This example showcases the practical application of $\phi(n)$ in various number-theoretic problems.

Remember, $\phi(n)$ holds immense significance in cryptography, where its properties are applied to create secure communication systems. This is just a glimpse into the power of this intriguing function!

5. Beyond Simple Counting:

The advantages of Euler's totient function are found in its capacity to provide light on the characteristics and distribution of prime numbers. Understanding the behavior of prime numbers is essential for mathematicians and cryptographers in fields like number theory, cryptography, and algorithm design. The function is essential to Fermat's Little Theorem and Euler's Theorem and aids in the creation of strong encryption schemes.



LEARNING OBJECTIVE 4: EXPLORE AND SOLVE DIOPHANTINE EQUATIONS

1. Equations Beyond Arithmetic:

We now shift our focus to integer equations and look for integer solutions to equations with integer variables. These diversely formed and intricate equations present intriguing linkages between number theory and algebra and push us to come up with creative solutions.

2. Categorizing the Challenges:

A basic category of Diophantine equations is represented by linear equations of the type $ax + by = c$. In this case, x and y have integer solutions, and a , b , and c are integers. Higher powers, inequalities, or many variables are present in more complex Diophantine equations, necessitating more complicated methods.

Diophantine Equations

$$ax + by = c$$

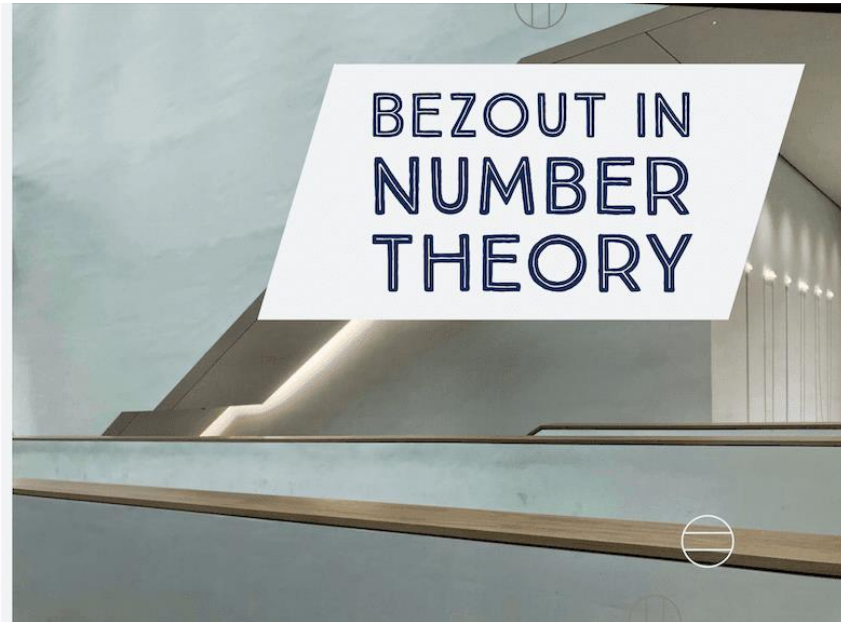
$$3^x + 4^y = 5^z$$

For example, $3x + 7y = 1$ or $x^2 - y^2 = z^3$, where x , y , and z are integers.

Three classes of Diophantine equations exist: those with infinitely many solutions, those with finitely many solutions, and those with no solutions. For instance, there are no solutions for the equation $6x - 9y = 29$, but there are infinitely many solutions for the equation $6x - 9y = 30$, which is reduced to $2x - 3y = 10$ by dividing by 3. For each integer t , whether it be positive, negative, or zero, the solutions $x = 20$, $y = 10$, and $x = 20 + 3t$, $y = 10 + 2t$ are examples. With t serving as the arbitrary parameter, this is referred to as a one-parameter family of solutions.

3. Bezout's Identity: A Powerful Ally:

A key tool for linear Diophantine equations is Bezout's identity. It says that a linear combination of a and b can be used to express the greatest common divisor of the coefficients, $\gcd(a, b)$ ($ax + by = \gcd(a, b)$). For linear Diophantine equations, this identity provides elegant solutions.



4. The Euclidean Algorithm Steps In:

Recall the Euclidean algorithm from our modular arithmetic investigations. It is just as useful in this instance! It can be modified to solve linear Diophantine equations by deftly adjusting multiples and remainders, providing a different method for obtaining Bezout's identity.

Greatest Common Factors

with the EUCLIDEAN ALGORITHM



5. Putting Theory into Practice:

Solve the equation $8x + 15y = 19$,

showcasing the application of Bezout's identity and the Euclidean algorithm while demonstrating their equivalence and providing a clear explanation.

Solution:

Finding Integers x and y using Bezout's identity:

Calculate the greatest common divisor (GCD) of 8 and 15:

Use the Euclidean algorithm:

$$15 = 2 * 8 + 3$$

$$8 = 2 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$\text{GCD}(8, 15) = \text{GCD}(3, 2) = 1$$

Since $\text{GCD} = 1$, Bezout's identity guarantees a solution:

We want to find integers x and y such that $8x + 15y = 1$.

Work backwards from the GCD:

We observe that $3 - 2 = 1$ (from the Euclidean algorithm steps).

Multiply both sides by 5 (to "adjust" the 2 to 10): $15 - 10 = 5$.

Multiply both sides by 8 (to get 8 as a coefficient): $120 - 80 = 40$.

Rewrite as $80 + 40 = 120$: $8 * 10 + 5 * 8 = 1 * 120$.

Solution: $x = 10, y = 8$.

Solving using the Euclidean Algorithm:

Follow the same steps as in calculating the *GCD*:

$$15 = 2 * 8 + 3$$

$$8 = 2 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$2 = 2 * 1 + 0$$

Express the last non-zero remainder (2) in terms of the original numbers:

$$2 = 15 - 2 * 8 = 15 - (2 * (8 - 2 * 3))$$

$$2 = 15 - 2 * (8 - 4)$$

$$2 = 15 - 2 * 4$$

$$2 = 15 - 8$$

Rewrite as a linear combination of 8 and 15:

$$8 + (-1) * 15 = 2$$

Multiply both sides by -10 (to obtain 8 as a coefficient):

$$-80 + 150 = -20$$

$$150 - 80 = 70$$

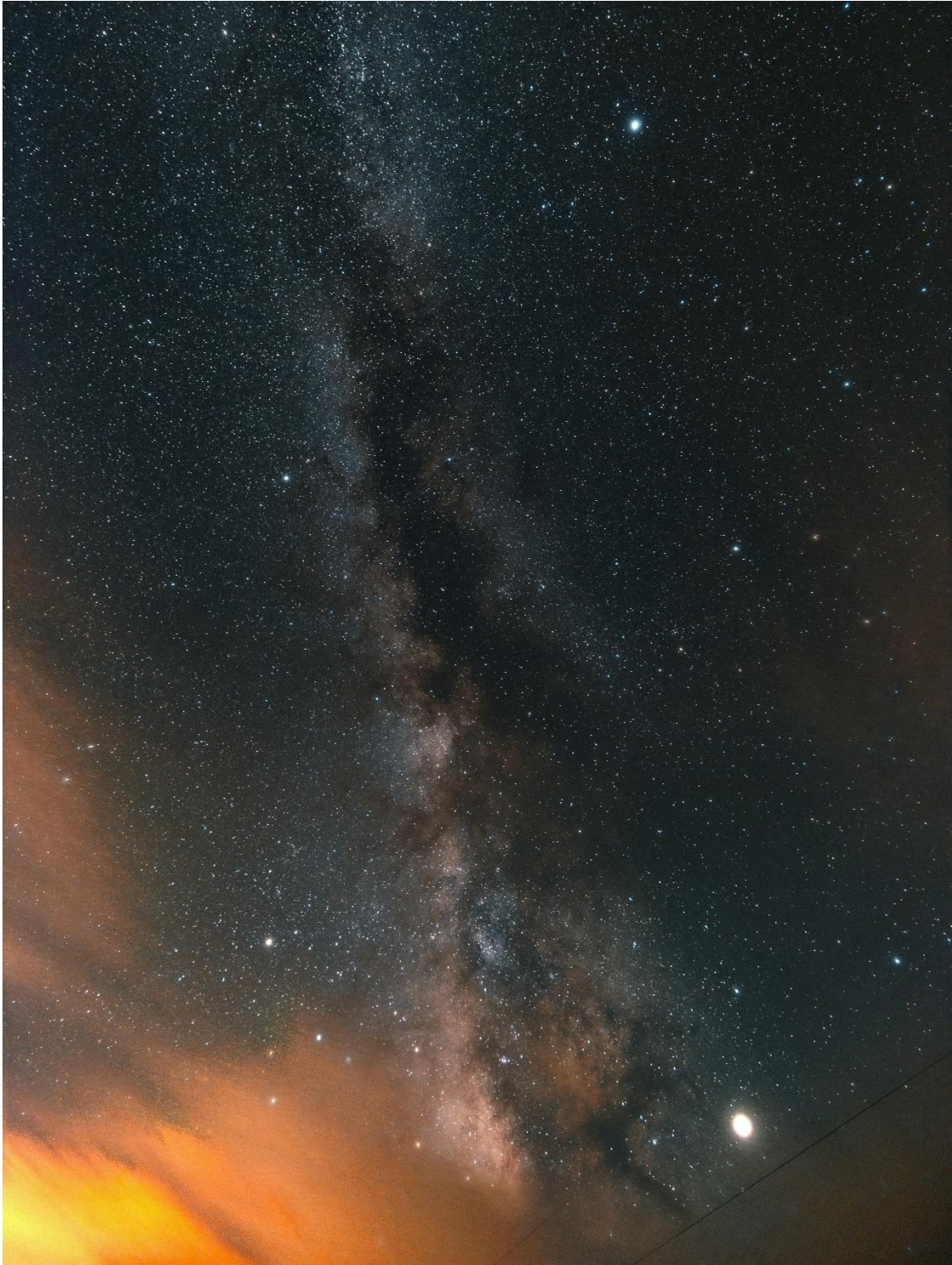
Solution: $x = -10$, $y = 7$ (equivalent to $x = 10$, $y = 8$ due to divisibility by 2).

Explanation and Equivalence:

- According to Bezout's identity, there exist integers x and y such that their linear combination equals 1 whenever the *GCD* of two integers is 1. Due to divisibility by the *GCD* (1), in this instance, we found $8 * 10 + 5 * 8 = 120$, satisfying the identity with 120 instead of 1.
- Finding the *GCD* of two numbers can be done methodically with the help of the Euclidean algorithm. We are able to represent the *GCD* as a linear combination of the original integers by examining the remainders in the division process. The result we got in this case was $2 = 15 - 8$, which is the same linear combination as Bezout's identity when translated as $8 + (-1) * 15 = 2$.

6. Beyond Linearity:

Though these techniques are highly effective for solving linear equations, keep in mind that not all Diophantine equations can be solved in whole numbers. Comprehending solvability conditions and delving into sophisticated methods such as Pell's equation and continuous fractions empower us to address increasingly intricate situations and fully grasp the intriguing depths of this field.



Section 9: A Glimpse into the Realm of Advanced Equations

1. Pushing the Boundaries:

Diophantine equations take on a variety of complex shapes when we move beyond linear equations. For instance, Pell's equation looks for integer solutions to the equation $x^2 + Dy^2 = 1$, where D is a non-square integer. Despite its seeming simplicity, its complex features and linkages to other areas of mathematics have captured the attention of mathematicians for decades.



2. Limitations and Intriguing Mysteries:

Unfortunately, not all Diophantine equations have integer solutions. Even for solvable cases, finding efficient algorithms can be an uphill battle. This highlights the limitations of known methods and opens the door for ongoing research and exploration in this captivating field.



3. A Glimpse into Ongoing Discoveries:

Exact Diophantine equations, Fermat's Last Theorem (proved in 1994), and the Birch and Swinnerton-Dyer hypothesis are only a few examples of the areas that modern research is exploring, stretching the bounds of knowledge and revealing ever-more fascinating mathematical relationships.



4. A Final Thought:

As we get to the end of our investigation, keep in mind that we have only touched the surface of number theory. Diophantine equations are a big and fascinating field full of unanswered questions and active study. Even if we might not have overcome every obstacle, mathematicians are nonetheless inspired and piqued with curiosity by the search for answers and the beauty of these connections.



CONCLUSION

Through an exploration of the complex field of number theory, this research paper has shed light on the fundamental and sophisticated ideas that serve as the cornerstone of mathematical inquiry. Each section has added to a thorough understanding of number theory, covering topics ranging from the unraveling elegance of prime factorization to the useful applications of modular arithmetic, and from the complex properties of Euler's totient and Möbius functions to the difficulties presented by Diophantine equations.

As we approach to the end of this investigation, it is clear that number theory is a dynamic field that need ongoing study rather than just a set of fixed principles. The ideas presented in this study act as a doorway, inviting mathematicians and scholars to delve further into the complex fabric of number theory. The beauty and usefulness of mathematics are demonstrated by the complexity of Diophantine equations, the elegance of prime numbers, the adaptability of modular arithmetic, and the depth of number theoretic functions.

These portions are cohesive because of the historical background that is weaved throughout, which emphasizes how mathematical concepts are not separate from human stories of inquiry and discovery. Number theory's history, from ancient mathematicians debating the nature of primes to modern academics stretching the bounds of Diophantine equation solutions, is a reflection of humanity's eternal thirst for knowledge.

This report, while comprehensive, is by no means exhaustive. It serves as an introduction, a roadmap, and an invitation to delve further into the vastness of number theory. As we bid farewell to this exploration, we do so with the understanding that the world of numbers is boundless, awaiting future revelations and insights from those who will continue to unravel its mysteries. Whether one's interest lies in practical applications, theoretical elegance, or the intersection of both, number theory offers a compelling and perpetually evolving journey for those who dare to venture further into its realms.



REFERENCES

1. *Prime factorization - Prime factorization methods / Prime Factors*. (n.d.). Cuemath.
<https://www.cuemath.com/numbers/prime-factorization/>
2. Vedantu. (n.d.). *Factorisation*. VEDANTU. <https://www.vedantu.com/maths/factorisation>
3. *Unveiling the Secrets of Finding Prime Factors*. (2023, October 5). Justinboey.
<https://justinboey.com/unveiling-the-secrets-of-finding-prime-factors/>
4. Libretexts. (2022, May 19). 6.3: *Fermat Primes, Mersenne Primes and Primes of the other forms*. Mathematics LibreTexts.
[https://math.libretexts.org/Courses/Mount_Royal_University/MATH_2150%3A_Higher_Arithmetic/6%3A_Prime_numbers/6.3%3A_Fermat_Primes%2C_Mersenne_Primes_and_Primes_of_the_form_%5C\(a%20%5Ctimes%20b%5C\)%20%3A%3A#:~:text=Fermat%20Primes%20and%20Mersenne%20Primes,-Definition%3A&text=The%20prime%20numbers%20of%20the,French%20mathematicians%20Fermat%20and%20Mersenne.](https://math.libretexts.org/Courses/Mount_Royal_University/MATH_2150%3A_Higher_Arithmetic/6%3A_Prime_numbers/6.3%3A_Fermat_Primes%2C_Mersenne_Primes_and_Primes_of_the_form_%5C(a%20%5Ctimes%20b%5C)%20%3A%3A#:~:text=Fermat%20Primes%20and%20Mersenne%20Primes,-Definition%3A&text=The%20prime%20numbers%20of%20the,French%20mathematicians%20Fermat%20and%20Mersenne.)
5. Libretexts. (2021, August 17). 1.12: *Fermat primes and Mersenne primes*. Mathematics LibreTexts.
[https://math.libretexts.org/Bookshelves/Combinatorics_and_Discrete_Mathematics/Elementary_Number_Theory_\(Clark\)/01%3A_Chapters/1.12%3A_Fermat_Primes_and_Mersenne_Primes](https://math.libretexts.org/Bookshelves/Combinatorics_and_Discrete_Mathematics/Elementary_Number_Theory_(Clark)/01%3A_Chapters/1.12%3A_Fermat_Primes_and_Mersenne_Primes)
6. *Discrete Math Number Theory S4.1 & S4.3*. (n.d.). Quizlet. Retrieved January 4, 2024, from
<https://quizlet.com/542430429/discrete-math-number-theory-s41-s43-flash-cards/>
7. *Divisibility rules of prime numbers*. (2022, June 30). Unacademy. <https://unacademy.com/content/bank-exam/study-material/quantitative-aptitude/divisibility-rules-of-prime-numbers/#:~:text=As%20discussed%20above%2C%20Prime%20numbers,or%20exists%20as%20a%20fraction.>
8. *Divisibility*. (2019). University of Wollongong.
<https://documents.uow.edu.au/content/groups/public/@web/@dvce/documents/doc/uow243300.pdf>
9. *Divisibility Rules – Print and digital Activity cards and worksheets*. (2020, March 30). Mathcurious.
<https://mathcurious.com/2020/03/30/divisibility-rules/>

10. Vonotna, M. (n.d.). 700+ Exception stock photos, pictures & Royalty-Free Images - iStock.
<https://www.istockphoto.com/photos/exception>
11. *Greatest Common Divisor and Lowest Common Multiple*. (2011).
https://cemc.uwaterloo.ca/events/mathcircles/2010-11/Winter/Intermediate_Mar2.pdf
12. *Greatest common divisor*. (1 B.C.E.). Byjus. Retrieved February 5, 2024, from
[https://byjus.com/maths/greatest-common-divisor/#:~:text=The%20greatest%20common%20divisor%20\(GCD,can%20be%20divided%20by%205](https://byjus.com/maths/greatest-common-divisor/#:~:text=The%20greatest%20common%20divisor%20(GCD,can%20be%20divided%20by%205)
13. *Least common multiple*. (n.d.). [Video]. Khan Academy. [https://www.khanacademy.org/math/cc-sixth-grade-math/cc-6th-expressions-and-variables/cc-6th-lcm/v/least-common-multiple-exercise#:~:text=The%20least%20common%20multiple%20\(LCM,the%20multiples%20of%20each%20](https://www.khanacademy.org/math/cc-sixth-grade-math/cc-6th-expressions-and-variables/cc-6th-lcm/v/least-common-multiple-exercise#:~:text=The%20least%20common%20multiple%20(LCM,the%20multiples%20of%20each%20)
[Onumber.](https://www.khanacademy.org/math/cc-sixth-grade-math/cc-6th-expressions-and-variables/cc-6th-lcm/v/least-common-multiple-exercise#:~:text=The%20least%20common%20multiple%20(LCM,the%20multiples%20of%20each%20)
14. *Greatest Common Divisor | Brilliant Math & Science Wiki*. (n.d.). <https://brilliant.org/wiki/greatest-common-divisor/#:~:text=The%20concept%20is%20easily%20extended,encryption%20algorithms%20such%20as%20RSA>.
15. *Modular Arithmetic Overview, Rules & Examples*. (2023, November 21). Study.
<https://study.com/learn/lesson/modular-arithmetic-rules-properties-what-is-modular-arithmetic.html#:~:text=In%20modular%20arithmetic%2C%20whole%20numbers%2C%20or%20integers%2C,number%20known%20as%20the%20modulus.%20Modular%20>
16. *An introduction to Modular Arithmetic*. (n.d.).
<https://nrich.maths.org/4350#:~:text=The%20best%20way%20to%20introduce,becomes%202%2C%20and%20so%20on>.
17. *The Euclidean Algorithm (article) | Khan Academy*. (n.d.). Khan Academy.
<https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/the-euclidean-algorithm>

18. 4.3. *Solving Congruences* — *Discrete Structures for Computing*. (n.d.).

<https://www.csd.uwo.ca/~abrandt5/teaching/DiscreteStructures/Chapter4/solve-congruences.html#:~:text=1.->

[.Linear%20Congruences,integers%20which%20satisfy%20the%20congruence.&text=By%20inspection%20we%20find%20that,6%20%E2%89%A1%201%20mod%205%20](https://www.csd.uwo.ca/~abrandt5/teaching/DiscreteStructures/Chapter4/solve-congruences.html#:~:text=1.-.Linear%20Congruences,integers%20which%20satisfy%20the%20congruence.&text=By%20inspection%20we%20find%20that,6%20%E2%89%A1%201%20mod%205%20)

19. Team, W. (2024, January 5). *Euler's totient function*. WallStreetMojo.

[https://www.wallstreetmojo.com/eulers-totient-](https://www.wallstreetmojo.com/eulers-totient-function/#:~:text=The%20benefits%20of%20Euler's%20totient,%2C%20cryptography%2C%20and%20algorithm%20design)

[function/#:~:text=The%20benefits%20of%20Euler's%20totient,%2C%20cryptography%2C%20and%20algorithm%20design](https://www.wallstreetmojo.com/eulers-totient-function/#:~:text=The%20benefits%20of%20Euler's%20totient,%2C%20cryptography%2C%20and%20algorithm%20design).

20. *Euler's totient Function and Euler's Theorem*. (n.d.).

<https://www.doc.ic.ac.uk/~mrh/330tutor/ch05s02.html#:~:text=The%20general%20formula%20to%20compute,%2D%201%20Fpn>).

21. *Bézout's identity and Diophantine Equation*. (2019, April 25). Physics Forums: Science Discussion,

Homework Help, Articles. [https://www.physicsforums.com/threads/bezouts-identity-and-diophantine-equation.151820/#:~:text=B%2C%20A%20zout's%20identity%20is%20often%20used,gcd\(a%2Cb\)](https://www.physicsforums.com/threads/bezouts-identity-and-diophantine-equation.151820/#:~:text=B%2C%20A%20zout's%20identity%20is%20often%20used,gcd(a%2Cb).).

22. Wolfram Research, Inc. (n.d.). *Diophantine Equation* -- from Wolfram MathWorld.

<https://mathworld.wolfram.com/DiophantineEquation.html>

23. The Editors of Encyclopaedia Britannica. (1998, July 20). *Diophantine equation* / *Integer Solutions*,

Polynomials, *Diophantine Sets*. Encyclopedia Britannica.

<https://www.britannica.com/science/Diophantine-equation>

24. Unsplash. (n.d.). *Beyond Pictures* / *Download free images on Unsplash*. Unsplash.

<https://unsplash.com/s/photos/beyond>