# Number Theory and Divisibility Issues

Maya Koreth and Dania Rustom

May 21, 2022

**Abstract**

This paper introduces important topics in elementary number theory, with a special focus on divisibility and congruence relations. We further demonstrate these ideas through their applications in various problems, including subsets of integers. Using these concepts, we also define the Euclidean algorithm, modular arithmetic, and primitive roots.

## 1 Introduction

Divisibility, prime numbers, and congruences are some of the most significant topics within number theory. They lay the foundation for critical concepts that allow us to develop new ideas, in order to dive deeper into existing ones. Our paper begins with some important definitions, properties, and theorems regarding divisibility and primes, which we discuss in Section 2. To further understand these concepts, Section 2 also focuses on relevant problems that expand our ways of approaching divisibility ideas.

Section 3 focuses on the definitions of congruence and modular arithmetic, stemming from the ones introduced in Section 2. This section also primarily focuses on congruence applications to Lagrange's Four Square Theorem, a famous problem in number theory.

The last section, Section 4, builds on the definitions in the previous section, and introduces new topics including the Chinese Remainder Theorem, primitive roots, and quadratic residues, concluding with quadratic residue problems.

## 2 Divisibility and Primes

As divisibility and prime numbers are some of the foundations for all of number theory, it is crucial to understand these two key ideas, their properties, and their applications in depth.

**Definition 2.1.** If $ax = b$ for any integer $x$, then we say that $a$ divides $b$, or $a|b$. Conversely, if $ax \neq b$, then $a$ does not divide $b$, or $a \nmid b$.

**Theorem 2.2.** *Properties of Divisibility* [1]

1. *$a|b$ implies $a|bc$ for any integer $c$;*
2. *$a|b$ and $b|c$ implies $a|c$;*
3. *$a|b$ and $a|c$ imply $a|(bx + cy)$ for any integers $x$ and $y$.*

As emphasized in the introduction, prime numbers are, essentially, the building blocks of number theory and hold great importance in understanding other concepts, such as congruencies and modulo arithmetic which are discussed later in Section 3. Their unique characterization and pattern, relative to other numbers, requires more advanced mathematics, and parts of their properties remain a mystery to mathematicians that topics in number theory attempt to unveil.

**Definition 2.3.** If an integer $p$ has no divisor other than 1 and itself, it is called a prime number. Otherwise, it is a composite number. Examples of prime numbers: 2, 3, 5, and 7; examples of composite numbers: 4, 6, 8, and 9.

[1] Although these properties each have their respective proofs, this paper will not highlight them.

The greatest common divisor, or gcd, is a concept that has served as a basis for numerous theorems, perhaps most famously in the Euclidean algorithm, which is an efficient method to compute the gcd of two integers.

**Theorem 2.4.** *The greatest common divisor $g$ of integers $b$ and $c$, denoted as $(b, c) = g$, can be characterized in the following two ways:*

1. *It is the least positive value of $bx + cy$ where $x$ and $y$ range over all integers.*
2. *It is the positive common divisor of $b$ and $c$ which is divisible by every common divisor.*

There are many different properties which stem from the concept of gcd, but only the most relevant ones to problems in Section 2 will be cited in this paper.

**Theorem 2.5.** *For any positive integer $m$, $(ma, mb) = m(a, b)$.*

**Theorem 2.6.** *For any interger $x$, $(a, b) = (b, a) = (a, -b) = (a, b + ax)$.*

There are also special cases of gcd when there are no common divisors between two numbers. The following problems will discuss this special case in depth.

**Definition 2.7.** We say that $a$ and $b$ are relatively prime in case $(a, b) = 1$. This can also be expressed by saying that $a$ and $b$ are coprime, or that $a$ is prime to $b$.

The inverse of both key ideas of divisibility and greatest common divisor is multiples, or the least common multiple.

**Definition 2.8.** If $a|b$, and $a$ is a divisor of $b$, then it is understood that $b$ is a multiple of $a$.
If $a_i|b$ for $i = 1, 2, ..., n$, then integers $a_1, a_2, ..., a_n$ have a common multiple $b$, and the least common multiple of $a$ and $b$, $lcm(a, b)$ denoted as $[a, b]$, is the least of the positive common multiples denoted by $\{a_1, a_2, ..., a_n\}$.

Combinatorial number theory studies the arrangement of objects and can be used to count the maximum number of arrangements possible. It is also commonly used to discern if any particular pattern exists in partitions of sets.

Within combinatorial number theory, one of the most crucial theorems is the pigeonhole principle. It is used frequently in mathematics, and is the basis of other fundamental proofs such as Fermat's Little Theorem, which will be introduced in Section 4.

**Theorem 2.9** (Pigeonhole Principle)**.** *If $n + 1$ elements are placed into $n$ sets, then at least one of the sets contains two or more elements.*

## Divisibility Problems

As emphasized throughout Section 2, theorems regarding prime numbers, divisibility, and the pigeonhole principle have numerous applications. Some applications are explored in depth in simplified problems and examples listed below.

**Theorem 2.10.** *If one chooses more than $n$ numbers from the set $\{1, 2, 3, ..., 2n\}$, then two of them are relatively prime.*

**Example 2.11.** We can start by using a smaller example, with $n = 3$. Then, we have the numbers:

$$\{1, 2, 3, 4, 5, 6\}$$

If we choose $n + 1$ numbers from this set, we can see that 1 and 5 are coprime to all other numbers. This forces us to choose the remaining four numbers, $\{2, 3, 4, 6\}$, but even in this set, 2 and 3 are coprime. Thus, at least two numbers will always be coprime in this set. But how do we prove this?

*Proof of Theorem 2.10.* First let us prove that two consecutive integers are always coprime. To do so, we denote two integers as $n$ and $n + 1$. Then let

$$\gcd(n, n + 1) = g$$

where $g$ is a natural number. By definition, $g|n$ and $g|n+1$, which means that

$$g|(n+1)-n=1$$

This can be derived from the basis principle of the Euclidean algorithm, which states that the greatest common divisor of two numbers does not change if the larger number is replaced by its difference with the smaller number. Thus, the $\gcd(n, n+1) = 1$.
Returning to our original problem, we now see that to pick more than $n$ numbers from the set (i.e more than half), there will always be at least two numbers that are consecutive by the pigeonhole principle. Since consecutive numbers are always coprime, the proof is completed. □

**Theorem 2.12.** *If one chooses more than n numbers from the set* $\{1, 2, 3, ..., 2n\}$*, then one number is a multiple of another.*

**Example 2.13.** Just like in the last problem, we start with a simple example, this time with $n = 3$

$$\{1, 2, 3, 4, 5, 6\}$$

If we break these numbers into their prime factorization, then the set will be:

$$\{1, 2, 3, 2^2, 5, 2 \cdot 3\}$$

1 is a factor of all integers, and 2 is a factor of both 4 or 6. Additionally 3 is also a factor of 6, meaning that 5 is the only number who has no factors other than 1 in the set. Thus we see that it is impossible to pick four numbers so that none are multiples of each other.

*Proof of Theorem 2.12.* Every positive integer can be expressed as the product of an odd integer and a power of 2. This can be proved using the fundamental theorem of arithmetic, which states that every number can be written as a product of primes. Thus if we denote an integer $n$,

$$n = 2^{p_1} \cdot 3^{p_2} \cdot 5^{p_3} \cdot 7^{p_4} ...$$

$$n = 2^{p_1} \cdot (3^{p_2} \cdot 5^{p_3} \cdot 7^{p_4} ...)$$

The terms in brackets are a product of odd numbers, so the whole term will be odd. Thus, if we denote a positive integer as $a$, then

$$a = 2^k(2m-1)$$

where $k \geq 0$ and $m \geq 1$ are natural numbers.

Using this idea, we can now rewrite each of the chosen $n+1$ numbers in this form. However, since there are only $n$ odd numbers in the set, there are only $n$ possibilities for the $2m-1$ factor. Thus, by the pigeonhole principle, there must be two integers who share the same $2m-1$ factor. Therefore, one number will always be a multiple of another. □

**Remark 2.14.** Can this be avoided with exactly $n$ numbers? An $n$ element subset does not have to have two distinct elements in it with one dividing the other. This is easier to model in an example. If we take our $n = 3$ set from earlier, we see that

$$\{2, 3, 5\}$$

is an example of a set with 3 numbers that has no multiples in it. Thus, this proof only holds for sets with more than $n$ numbers.

**Theorem 2.15.** *If 50 numbers are chosen from the set* $\{1, ..., 99\}$*, where no two numbers in the set sum to 99 or 100, then the chosen numbers must be* $\{50, 51, 52, ..., 99\}$*.*

**Example 2.16.** In order to understand this theorem, a smaller set can be used with the same parameters. If the set $\{1, ..., 9\}$ is assigned as set A and no two numbers of the five chosen must sum to 9 or 10, then the chosen numbers must be $\{5, ..., 9\}$. To see why this is, suppose that in this example, we chose the numbers $\{1, 2, 3, 4, 5\}$ instead. Since $4 + 5 = 9$, one of these two numbers must be replaced with another number that's not in the set, say 6. However, since $4 + 6 = 10$, the set violates the rule

yet again, and we must replace either 4 or 6. We can repeat this algorithmically with the set and replace numbers that don't work with the next consecutive number:

$$A \neq \{1, 2, 3, 5, 6\} \because [2] 3 + 6 = 9$$

$$A \neq \{1, 2, 5, 6, 7\} \because 2 + 7 = 9$$

$$A \neq \{1, 5, 6, 7, 8\} \because 1 + 8 = 9$$

$$A = \{5, 6, 7, 8, 9\}$$

Using this process, we can see that the only set that works is $\{5, ..., 9\}$. A similar logical process can be applied to the original set in the theorem.

*Proof of Theorem 2.15.* For the set $A = \{1, ..., 99\}$, we must consider all 49 pairs that add up to 99: $\{1, 98\}, \{2, 97\}, \ldots, \{49, 50\}$. And consider the 49 pairs that add up to 100 as well: $\{1, 99\}, \{2, 98\}, \ldots, \{49, 51\}$.

The chosen set of fifty numbers for this theorem must contain only one number of each pair. Hence, if the solution contains 99, it must not contain 1. If the solution contains 98, it must not contain 2. Proceeding in this pattern illustrates why the chosen set must be $\{50, ..., 99\}$.

To further demonstrate this, suppose that the chosen set is $\{1, ..., 50\}$. As seen in the pairs above, if the set contains both 49 and 50, the set is inconsistent with the problem; hence the set must not contain 49. If the set contains 51 or 52, it cannot contain 48. By following through this way, you will arrive to a new list of $\{50, ..., 99\}$, which must be true and the original set must be a contradiction. □

Theorem 2.15 can further be generalized for any set that follows the outline $\{1, 2, \ldots, 2n - 1\}$.

**Corollary 2.17.** *If $n$ numbers are chosen from the set $\{1, 2, \ldots, 2n - 1\}$ where no pair of numbers sum to $2n - 1$ or $2n$, then the set must be $\{n, n + 1, \ldots, 2n - 1\}$.*

This corollary is true because, as seen in the example, the first number in the set must be half of $2n$ and must be followed with consecutive numbers leading to one less than $2n$, $2n - 1$. The set must be in this format to ensure that no two pairs add up to $2n - 1$ or $2n$. This condition is satisfied because any integer added to $n$ in this set will always be greater than $2n$, for example adding the first two terms will result in $2n + 1$. Therefore, this chosen set will be the only one that will satisfy the other conditions in this theorem, and must be true.

# 3 Congruence relations

As well as the evident significance of divisibility in number theory, another fundamental concept that explains divisibility from another approach is congruence. Congruences can help derive divisibility tests used to prove other theorems or concepts. As other sections in this paper will cover, congruences have numerous applications for other powerful techniques as a foundational tool in number theory. Many other ideas build on congruences, which is why it is crucial to understand its basics and properties.

**Definition 3.1.** If a non-zero integer $m$ divides $a - b$, we say that a is congruent to b modulo m and write $a \equiv b \pmod{m}$. If $m \nmid (a - b)$, then we say that $a$ is not congruent to $b$ modulo $m$, which is written as $a \not\equiv b \pmod{m}$.

Definition **??** skims over the idea of "modulo", or modular arithmetic, which coincides with both the concept and notation of congruences. It is a system which considers the remainders of a number. An easy way to think of it would be the face of a clock: The numbers go from 1 to 12, but once you get to "13 o'clock," it becomes 1 o'clock again. This is the same as taking mod 12 of a number, or "13 is congruent to 1 modulo 12."

[2] In number theory and proofs, "because" is most commonly denoted with the symbol $\because$

**Definition 3.2.** Modulus $m$, an assumed positive integer, is the idea of taking an integer $m$ and cutting it off at a specified point. For example:

$$10 \pmod 3$$

$$10 = 3(3) + 1$$

$$10 \equiv 1 \pmod 3$$

Along with the definitions of congruences and modulo, the concepts come with a list of important properties. The most relevant to this paper with referenced notation are listed below in Theorem 3.3:

**Theorem 3.3.** *Let $a$, $b$, $c$, $d$, $x$, $y$ denote integers. Then:*

1. $a \equiv b \pmod m$, $b \equiv a \pmod m$, *and* $a - b \equiv 0 \pmod m$ *are equivalent statements.*
2. *If* $a \equiv b \pmod m$ *and* $b \equiv c \pmod m$, *then* $a \equiv c \pmod m$.
3. *If* $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$, *then* $ax + cy \equiv bx + dy \pmod m$.
4. *If* $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$, *then* $ac \equiv bd \pmod m$.
5. *If* $a \equiv b \pmod m$ *and* $d|m$, $d > 0$, *then* $a \equiv b \pmod d$.
6. *If* $a \equiv b \pmod m$ *then* $ac \equiv bc \pmod{mc}$ *for* $c > 0$.
7. *If* $a \equiv b \pmod m$ *then* $f(a) \equiv f(b) \pmod m$, *where* $f$ *denotes the value of the function.*

## Lagrange's Four Square Theorem

Lagrange's Four Square Theorem states that any positive integer can be expressed as a sum of four squares. For example,

$$23 = 1^2 + 2^2 + 3^2 + 3^2$$

This theorem was proven by Joseph Louis Lagrange in 1770, and is a special case of the Fermat polygonal number theorem. We will prove this theorem in steps, starting with proving three Lemmas that will aid us in our ultimate proof.

**Lemma 3.4.** *Let $m$ and $n$ each be the sum of four squares. Then $mn$ is the sum of four squares.*

*Proof.* Let us denote $m = a^2 + b^2 + c^2 + d^2$ and $n = w^2 + x^2 + y^2 + z^2$. If we multiply and factor these two equations, we get:

$$mn = (a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2)$$

$$mn = a^2w^2+a^2x^2+a^2y^2+a^2z^2+b^2w^2+b^2x^2+b^2y^2+b^2z^2+c^2w^2+c^2x^2+c^2y^2+c^2z^2+d^2w^2+d^2x^2+d^2y^2+d^2z^2$$

$$mn = (aw - bx - cy - dz)^2 + (ax + bw + cz + dy)^2 + (ay + cw + dx - bz)^2 + (az + dw + by - cx)^2$$

Since all values in the parentheses are integers, $mn$ is a multiple of four squares and the proof is complete.

□

**Lemma 3.5.** *If $2n$ is a sum of two squares, then $n$ is also the sum of two squares.*

*Proof.*

$$2n = (x + y)^2 + (x - y)^2$$

$$2n = 2x^2 + 2y^2$$

$$n = x^2 + y^2$$

If we set $x + y$ equal to $a$ and $x - y$ equal to $b$, we can set up a system of equations and find

$$x = \frac{a + b}{2}$$

and

$$y = \frac{a-b}{2}$$

To make $x$ and $y$ integers, either $a$ and $b$ must both be even, or both must be odd to ensure the numerator is even. However, we can already assume this to be true, because our base equation of $2n$ ensures that $x+y$ $(a)$ and $x-y$ $(b)$ must satisfy these constraints. Since $2n$ is already even, the only way that the base equation holds is if $x+y$ and $x-y$ were either both even or odd.

□

**Lemma 3.6.** *If $p$ is an odd prime, then there exist integers $a, b, k$ such that $a^2+b^2+1 = kp$ and $0 < k < p$.*

*Proof.* For this lemma, we can first assume that $0 \leq a, b \leq p-1$ such $a^2+b^2+1 \equiv 0 \pmod{p}$. If $a$ and $b$ are replaced by $p-a$ and $p-b$, respectively, then the inequality can be rearranged to produce $a, b < \frac{p}{2}$. From this, we have

$$0 < kp = a^2+b^2+1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2$$

This implies that $k < p$, and thus the lemma is satisfied. □

**Theorem 3.7** (Lagrange's four square theorem)**.** *Every positive integer $x$ can be written as the sum of four integer squares.*

*Proof.* By Lemma 3.4, it is sufficient to prove that each prime can be expressed as a sum of four squares. Then all composite integers can be expressed as prime factorization because of the fundamental theorem of arithmetic. If we suppose that $p$ is odd, then by Lemma 3.6 we know

$$mp = a^2+b^2+c^2+d^2 \tag{1}$$

For some $m$, $a$, $b$, $c$, $d$, where $0 < m < p$, Lemma 3.6 states that for any prime $p$, some multiple $0 < m < p$ is the sum of four squares. Since $m = 1$ already solves the identity, we will show that if $m > 1$, then $np$ is also the sum of four squares where $0 < n < m$.

If we assume that $m$ is odd and greater than 1, we can write

$$w \equiv a \pmod{m}$$

$$x \equiv b \pmod{m}$$

$$y \equiv c \pmod{m}$$

$$z \equiv d \pmod{m}$$

where $w$, $x$, $y$, and $z$ are all in the interval $(\frac{-m}{2}, \frac{m}{2})$ included because $w^2 < \frac{m^2}{4}$ which means that $|w| < \frac{m}{2}$. Therefore,

$$w^2+x^2+y^2+z^2 < 4 \cdot \frac{m^2}{4} = m^2$$

From taking equation 1 modulo $m$, we get

$$w^2+x^2+y^2+z^2 \equiv 0 \pmod{m}.$$

Thus, we have $w^2+x^2+y^2+z^2 = nm$ for some integer $n$. Since we proved that $w^2+x^2+y^2+z^2 < m^2$, we know that $n < m$. If $n = 0$ then

$$w = x = y = z = 0$$

so that

$$a \equiv b \equiv c \equiv d \equiv 0 \pmod{m}$$

$$mp = a^2+b^2+c^2+d^2 = m^2q$$

However, this implies $p = mq$ which contradicts the fact that $p$ is prime, so $n$ must be $0 < n < m$. Next, we look at Lemma 3.4, and realize the left side of the equation will be $nm^2p$. The right side is a sum of four squares, in which three of them are multiples of $m$.

$$ax - bw - cz + dy = (aw - bw) + (dy - cz)$$

$$ay + bz - cw - dx = (ay - cw) + (bz - dx)$$

$$az - by + cx - dw = (az - dw) + (cx - by)$$

The last sum can also be expressed as

$$aw + bx + cy + dz \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m}$$

Therefore, the equation in Lemma 3.4 can be divided by $m^2$. The result is a form of $np$ as a sum of four squares, as desired.

□

# 4 Important Congruence Theorems and Primitive Roots

Some important generalizations and theorems stem off of the concept of modular arithmetic. In particular, Fermat's Little Theorem and Euler's generalization build off of each other to form the basis of congruences. The Chinese remainder theorem is used to find a common solution of a system of linear congruences. It is the idea of reducing a linear congruence $ax \equiv b \pmod{m}$ to a set of congruences $ax \equiv b \pmod{m_i}$ where the items in the set $/m_1, m_2, m_3, .../$ are the prime power factors of $m$. The CRT gurantees that as long as $m_1$, $m_2$, and $m_3$ are all pairwise coprime (meaning each pair's gcd is 1), then a solution must exist.

**Theorem 4.1** (Chinese Remainder Theorem)**.** *Suppose $m_1, m_2, ..., m_r$ are pairwise relatively prime positive integers, and suppose $a_1, a_2, ..., a_r$ are integers. Then the congruences $x \equiv a_i \pmod{m_i}$, $i = 1, 2, ..., r$, have common solutions. Any two solutions are congruent modulo $m_1, m_2, ..., m_r$.*

**Example 4.2.** In order to find a solution that satisfies $x \equiv 1 \pmod 4$, $x \equiv 0 \pmod 3$, and $x \equiv 5 \pmod 7$ simultaneously, we first recognize that $m_1 = 4$, $m_2 = 3$, $m_3 = 7$, and $m = m_1 * m_2 * m_3 = 84$. Since each modulo value are relatively prime in pairs, the Chinese Remainder Theorem will allow us to find a value for x that satisfies each congruence:

$$\frac{m}{m_1} = 21, \quad 21 \cdot a_1 \equiv 1 \pmod 4, \quad a_1 = 5$$

$$\frac{m}{m_2} = 28, \quad 28 \cdot a_2 \equiv 1 \pmod 3, \quad a_2 = 9$$

$$\frac{m}{m_1} = 12, \quad 12 \cdot a_3 \equiv 1 \pmod 7, \quad a_3 = 3$$

$$x = (21 \cdot 5 \cdot 1) + (28 \cdot 9 \cdot 0) + (12 \cdot 3 \cdot 5)$$

$$x \equiv 285 \pmod{84} \equiv 33 \pmod{84}$$

As well as the Chinese Remainder Theorem, many congruence theorems also use Euler's Totient Function, which is given in Definition 4.3. Euler's Totient Function is especially relevant for primitive roots, discussed in definition 4.6, which help explain many other proofs in number theory, some of which are shown in Section 4. In order to understand those proofs and theorems, it is crucial to be familiar to this function.

**Definition 4.3.** Euler's totient function $\phi$ is a function such that $\phi(m)$ equals the number of positive integers less than or equal to m that are relatively prime to m.

With this in mind, we can now integrate this definition into other theorems, such as Fermat's Little Theorem:

**Theorem 4.4** (Fermat's Little Theorem)**.** *Let $p$ denote a prime. If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$. For every integer $a$, $a^p \equiv a \pmod p$.*

Fermat's Little Theorem is a fundamental theorem which helps compute powers of integers modulo prime numbers. Elaborating on Fermat's Little Theorem, another important theorem is Euler's Generalization:

**Theorem 4.5** (Euler's Generalization)**.** *If* $(a, m) = 1$*, then* $a^{\phi(m)} \equiv 1 \pmod{m}$.

This is Euler's generalization of Fermat's theorem, both of which are frequently used in elementary number theory. Using Euler's Totient Function, many different theorems can be discovered and many manipulations can be done, such as primitive roots.

**Definition 4.6.** If $a$ belongs to the exponent $\phi(m)$ modulo m, then $a$ is called a primitive root modulo m.

**Definition 4.7.** Let $m$ be a natural number, and let $a$ be any integer with $(a, m) = 1$. Let $h$ be the least positive integer with $ah \equiv 1 \pmod{m}$. Then we say that the order of $a$ modulo $m$ is $h$ (or that $a$ belongs to $h$ modulo $m$).

Primitive roots also allow us to learn more about prime numbers and distinct patterns about them, as we will see in the next few examples.

**Theorem 4.8.** *If $p$ is a prime, then there exist $\phi(p-1)$ primitive roots modulo $p$. The only integers having primitive roots are $p^e$, $2p^e$, 1, 2, and 4, with $p$ an odd prime.*

The quadratic reciprocity law is a continuation of the idea of congruences and is another application of that concept. Within quadratic reciprocity, which helps solve a congruence such as $x^2 \equiv a \pmod{m}$, are quadratic residues and the Legendre symbol, which work together to solve quadratic reciprocity problems.

**Definition 4.9.** For all $a$ such that $a$ is coprime to $m$, or $(a, m) = 1$, $a$ is called a *quadratic residue* modulo $m$ if the congruence $x^2 \equiv a \pmod{m}$ has a solution. If it has no solution, then $a$ is called a *quadratic nonresidue* modulo $m$.

Generally, $a = 0$ is not considered in the list of quadratic residues. Only distinct residues or nonresidues that are distinct modulo $m$ are considered in the list of quadratic residues. For example, if we let $m = 5$, the quadratic residues would be 1 and 4 (or $-1 \pmod{5}$) while the quadratic nonresidues would be 2 and 3. To further determine if an integer is a quadratic residue modulo $m$, the Legendre symbol can be used.

**Definition 4.10.** If $p$ denotes an odd prime and $(a, p) = 1$, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be 1 if $a$ is a quadratic residue, $-1$ if $a$ is a quadratic nonresidue modulo $p$, and 0 if $p|a$.

**Theorem 4.11.** *Properties of the Legendre symbol: Let $p$ be an odd prime and let $a$ and $b$ denote integers relatively prime to $p$. Then*

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3. $a \equiv b \pmod{p}$ *implies that* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
4. $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$, $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

One commonly known answer of the Legendre symbol is $\left(\frac{2}{p}\right)$, which is stated in Theorem 4.12. Although there is an extensive proof to this theorem, this paper will not explain the proof in the level of detail required. Therefore, for problems in Section 4, the following theorem can be assumed as true.

**Theorem 4.12.** *If $p$ is an odd prime and $(a, 2p) = 1$, then* $\left(\frac{a}{p}\right) = (-1)^t$ *where* $t = \sum_{j=1}^{(p-1)/2} \left(\frac{ja}{p}\right)$; *also* $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Definitions 4.9 and 4.10 highlight the important concepts to understand in order to learn about quadratic reciprocity, since they are both used in its definition as well.

**Theorem 4.13** (Quadratic Reciprocity Law)**.** *If $p$ and $q$ are distinct odd primes, where $p \nmid q$ and $q \nmid p$, then*

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

Essentially, Theorem 4.13 explains that if $p$ and $q$ are two different odd primes, but both of the form $4k + 3$, then either $x^2 \equiv p \pmod{q}$ or $x^2 \equiv q \pmod{p}$ is solvable, but not both. If at least one of the distinct odd primes is of the form $4k + 1$, then both congruences are solvable, or both are not.

**Remark 4.14.** Another form of the quadratic reciprocity law is $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{((p-1)/2)((q-1)/2)}$. This is true because $\left(\frac{q}{p}\right)$ can be multiplied on both sides of the standard quadratic reciprocity law, given in theorem 4.13, essentially canceling out the $\left(\frac{q}{p}\right)$ on the left side. In reality, the $p$ values in the denominator are multiplied by each other, creating $p^2$, which becomes 1 based off of the properties of the quadratic reciprocity law. Therefore, it is sufficient to remark that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{((p-1)/2)((q-1)/2)}$ will provide the same value as $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{((p-1)/2)((q-1)/2)}$.

Euler's criterion is also an important part of the Quadratic Reciprocity law. It states that if $p$ is an odd prime then

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

This can be proved by supposing that $a$ is a quadratic residue, with $a \equiv b^2 \pmod{m}$. Then, Fermat's Little Theorem tells us that

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \pmod{p}$$

Thus, this holds for when $a$ is a quadratic residue. The opposite, -1, is true when $a$ is a non-quadratic residue.

## Quadratic Residue Problems

In this section, we explore Quadratic Residue through two practice problems, which utilize the theorems from Theorem 4.11. This is an important application of the concepts we reviewed in the prior section, and shows how many theorems work together to prove certain problems.

**Theorem 4.15.** *For odd primes $p$, find all values $p$ such that* $\left(\frac{10}{p}\right) = 1$.

*Proof.* From the properties of Legendre's symbol, we know that $\left(\frac{10}{p}\right)$ can be rewritten as $\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$. Theorem 4.12 also provides the quadratic reciprocity of $\left(\frac{2}{p}\right)$, which is:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

The properties of Legendre's symbol also provide:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{5-1}{2}\right)}$$

This means that in order to find the correct result that the theorem suggests, the p values for both equations must either both be odd, or both be even. Considering only the $\left(\frac{5}{p}\right)$ equation, we must determine the results of each possible $p$ value.

$$p \equiv 1 \pmod 5 : \left(\frac{p}{5}\right) \equiv \left(\frac{1}{5}\right) \equiv 1$$

$$p \equiv 2 \pmod 5 : \left(\frac{p}{5}\right) \equiv \left(\frac{2}{5}\right) \equiv -1$$

$$p \equiv 3 \pmod 5 : \left(\frac{p}{5}\right) \equiv \left(\frac{3}{5}\right) \equiv -1$$

$$p \equiv 4 \pmod 5 : \left(\frac{p}{5}\right) \equiv \left(\frac{4}{5}\right) \equiv 1$$

After noticing that 2 and 3 are quadratic nonresidues while 1 and 4 are quadratic residues, we need to find the odd and even $p$ values, respectively, for $\left(\frac{2}{5}\right) = (-1)^{(p^2-1)/8}$ using the Chinese Remainder Theorem. In order to find the result we are looking for and satisfy $\left(\frac{10}{p}\right) = 1$, the quadratic residues of 5 must result in a congruence of 1 while the value of $\frac{p^2-1}{8}$ must be even. This is true for $p \equiv 1$ and $p \equiv 7$, which sets the expression to even values 0 and 6, respectively.

$$p \equiv 1 \pmod 5, \quad p \equiv 1 \pmod 8$$

$$m_1 = 5, \;\; m_2 = 8, \;\; m = m_1 m_2 = 40$$

$$\frac{m}{m_1} = 8, \;\; 8 \cdot 2 \equiv 1 \pmod 5$$

$$\frac{m}{m_2} = 5, \;\; 5 \cdot 5 \equiv 1 \pmod 8$$

$$p = (8 \cdot 2 \cdot 1) + (5 \cdot 5 \cdot 1) \equiv 1 \pmod{40}$$

We can repeat this process for $p \equiv 1 \pmod 5$ and $p \equiv 7 \pmod 8$, $p \equiv 4 \pmod 5$ and $p \equiv 1 \pmod 8$, and $p \equiv 4 \pmod 5$ and $p \equiv 7 \pmod 8$. If we do so, we will find that $p \equiv 1, 9, 31, 39 \pmod{40}$. We can also follow these steps for the quadratic nonresidues of 5 and the values of $\frac{p^2-1}{8}$ that will be odd, which is only true for $p \equiv 3$ and $p \equiv 5$. Using the Chinese Remainder Theorem, we find that $p \equiv 3, 13, 27, 37 \pmod{40}$. Therefore, $\left(\frac{10}{p}\right) = 1$ for $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40}$. □

**Theorem 4.16.** *For an odd prime $p$ of the form $p = 2^{2^n} + 1$, an integer $a$ is a primitive root mod $p$ if and only if $\left(\frac{a}{p}\right) = -1$.*

*Proof.* Since $p = 2^{2^n} + 1$, we have $\phi(p) = 2^{2^n}$. It follows that the order is

$$ord_p(a) | \phi(p) = p - 1 = 2^{2^n}$$

.

Using Euler's criterion, which states that

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

we can show that if $a$ is a quadratic non-residue then

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

However, in this case

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

.

Thus, if we were to have $ord_p(a) < p-1$, then we would have that $a^{\frac{p-1}{2}} \equiv 1 \pmod{m}$, which is a contradiction to the original statement. Thus, it must be that $ord_p(a) = p-1$. Since this is true, and $a$ must be primitive.

□

# References


[1] Ivan Niven, Herbert S. Zuckerman, *An Introduction to the Theory of Numbers (4th Edition).*

[2] Gabriel D. Carroll, *Combinatorial Number Theory*