Quadratic Residues in Olympiad Problems

How can quadratic residues determine families of prime divisors?

Word count: 3886

Subject: Mathematics

Contents

1 Introduction

1.1 What is Number Theory?

Number theory is the study of properties of positive integers. Its primary purpose is to "discover [and prove] interesting and unexpected relationships between different sorts of numbers,"[1] for example the proof that there are infinitely many prime numbers and the proof that if a square number is divisible by two, it must be divisible by four.

1.2 Why did I choose to investigate Quadratic Residues?

When learning introductory Number Theory to strengthen my math contest skills, I was fascinated by how elegant modular arithmetic was. Eventually, I took a Number Theory course at a summer camp that introduced me to a variety of exciting and intricate concepts—order, p-adic valuation, multiplicative functions, Diophantine equations, and quadratic residues. However, I never understood quadratic residues very well, and thus believe that I missed out on a world of exploration.

Hence, I would like to use this essay to explore quadratic residues and deepen my own understanding. I will do this by solving olympiad-style questions and exploring my own extension.

This essay will first introduce modular arithmetic, then Euler's Totient Theorem, and then quadratic residues. The essay will then present my solution to a Taiwanese Olympiad problem in order to demonstrate applications and limitations of quadratic residues. Finally, this essay will focus on exploring a problem by Fermat, along with my own extension, on how quadratic residues can determine whether certain families of prime divisors exist.

[1] [1] Silverman.

The purpose of this essay is to demonstrate the usefulness of quadratic residues by exploring its use in Olympiad problems and by exploring relationships between sequences of numbers and families of prime factors.

2 Modular Arithmetic

Modular arithmetic is foundational for number-theoretic exploration. To explain its properties, divisibility must first be defined.

2.1 Divisibility

Informally, a divides b if $\frac{b}{a}$ is both defined and an integer. However, in number theory, we do not often use rational numbers. Thus, the definition for divisibility is given below.

Let $a, b \in \mathbb{Z}$. Define a divides b if there exists $c \in \mathbb{Z}$ such that $ac = b$. This can be written as $a \mid b$. Notice that this definition allows for the inclusion of zero, despite division by zero being undefined. For example, we have $-2 \mid 10$ since $(-2) \cdot (-5) = 10$, $3 \mid 0$ since $3 \cdot 0 = 0$, and $0 \nmid 4$ because there is no integer c that satisfies $0 \cdot c = 4$.

Notice that if p is prime and $x, y \in \mathbb{Z}$, then if $p \mid xy$, then we must either have $p \mid x$ or $p \mid y$, since either x or y has to include the factor of p.

2.2 Modular Arithmetic

We must first define modular arithmetic because quadratic residues only make sense in such a context.

2.2.1 Congruence

Let $a, b, c \in \mathbb{Z}$. Define $a \equiv b \pmod{c}$ — read as a is congruent to b modulo c — if and only if $c \mid a - b$. Here, c is defined as the modulus.

Note that this is equivalent to stating that if $a = cx + b$ for $x \in \mathbb{Z}$, then $a \equiv b \pmod{c}$ and vice versa. Also, note that if $d \in \mathbb{Z}$ is the remainder when a is divided by c, then $a \equiv d \pmod{c}$. Here, d is also known as a residue. For

example, $29 \equiv -4 \equiv 2 \pmod 3$ since $29, -4$, and 2 each has a remainder and residue of 2 when divided by 3. Alternatively, note that $3 \mid 29 - (-4) = 33$ and $3 \mid 2 - (-4) = 6$.

Modular arithmetic thus results in a cyclical nature, similar to the time of day. If there were a 12-hour analog clock currently showing 12 o'clock, the clock would show the same time if 5 hours passed, if 17 hours passed, or if $(5 + 12n)$ hours passed from the same starting time. Since the time on the clock repeats every twelve hours, the modulus is 12. The statement above is akin to stating that $5 \equiv 5 + 12n \pmod{12}$.

The cyclical nature of modular arithmetic can be seen in the graph below.

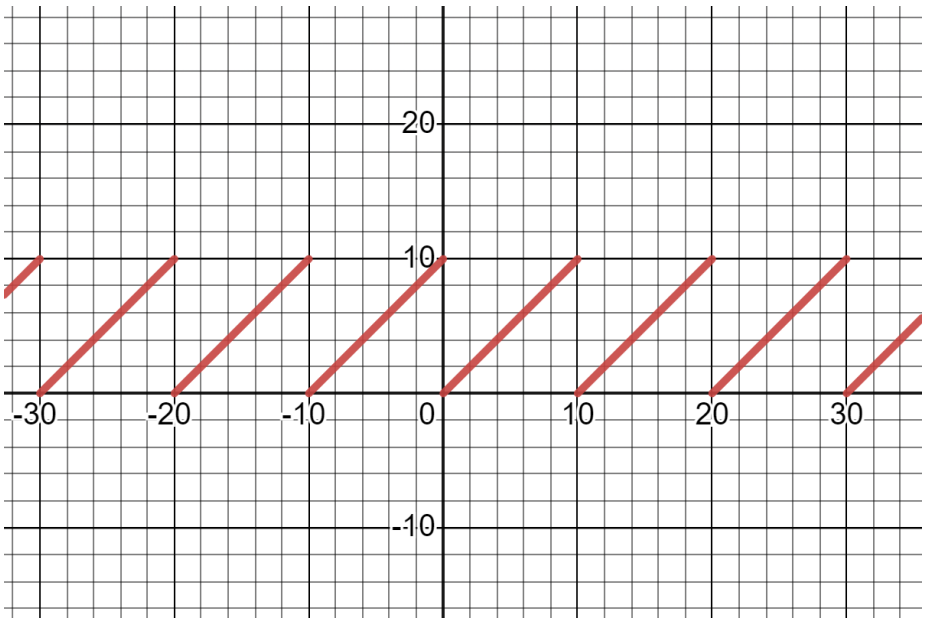

Figure 1: A graph of $y = x - 10 \left\lfloor \frac{x}{10} \right\rfloor$ from Desmos. [3] "Graphing Calculator."

In this graph, all of the points with integral x-coordinates have the y value of the residue of $x \pmod{10}$. While the graph has a y-value for each $x \in \mathbb{R}$, Number

Theory focuses on integers. When restricting the domain to integers, we end up with the graph below.

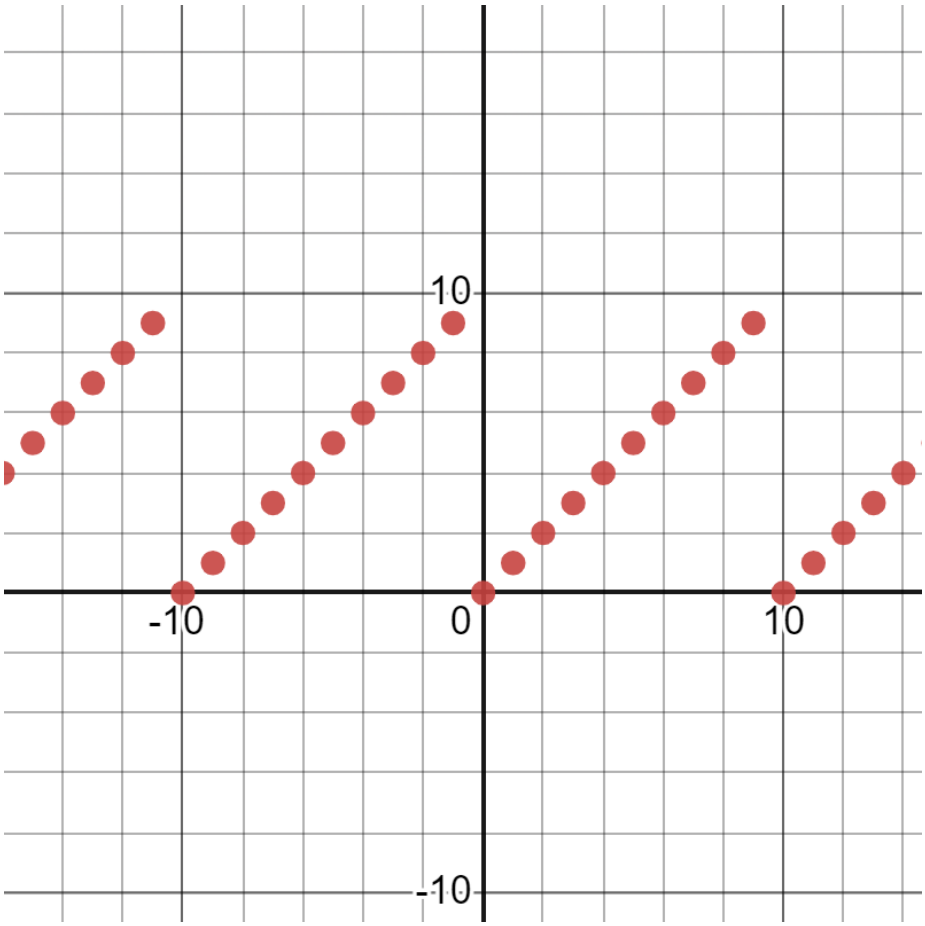

Figure 2: The same graph but restricted to integers. [3] "Graphing Calculator."

From the definition of modular arithmetic provided in this essay, only integral points are defined.

2.2.2 Arithmetic Operations

Let $a, b, m, n, k \in \mathbb{Z}$, where $k \geq 1$. Suppose that $a \equiv m \pmod{k}$ and $b \equiv n \pmod{k}$. Then, the following hold.[2]

$$a + b \equiv m + n \pmod{k}.$$

For example, $12 + 23 \equiv 2 + 3 \equiv 5 \pmod{10}$.

$$a - b \equiv m - n \pmod{k}.$$

For example, $2 - 13 \equiv 2 - 6 \equiv -4 \equiv 3 \pmod{7}$.

$$ab \equiv mn \pmod{k}.$$

For example, $12 \cdot 17 \equiv 2 \cdot 7 \equiv 14 \equiv 4 \pmod{10}$, and $16 \cdot 16 \equiv (-1) \cdot (-1) \equiv 1 \pmod{17}$.

For $x \in \mathbb{Z}$,

$$a^x \equiv m^x \pmod{k}.$$

For example, $23^{2023} \equiv (-1)^{2023} \equiv (-1) \equiv 11 \pmod{12}$.

Notice that the addition, subtraction, and multiplication operators function as expected in modular arithmetic. However, notice that in exponentiation, only the base can be simplified by being taken modulo k.

2.3 Fermat's Little Theorem

Fermat's Little Theorem allows us to simplify the exponent in some certain cases. It is a special case of Euler's Totient Theorem in Appendix A. It states

[2] [2] Rusczyk.

that for a prime p and an integer a such that $p \nmid a$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

For example, $10^{14} \equiv 10^2 \cdot 10^{13-1} \equiv 10^2 \cdot 1 \equiv (-3)^2 \equiv 9 \pmod{13}$.

3 Quadratic Residues

We will first define quadratic residues and then provide interesting properties. Intuitively, quadratic residues represent the perfect squares of a modulus.

3.1 Definition

Let p be a prime. Consider all residues modulo p. Define a residue a to be a quadratic residue modulo p if there exists a solution to the equation $x^2 \equiv a \pmod{p}$. All residues that are not quadratic residues are considered quadratic non-residues. This can be expressed using the Legendre Symbol, which is defined as such.[3]

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } p \nmid a \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 & \text{if } p \mid a \end{cases}$$

For example, consider the prime $p = 13$. Each residue and it squared can be seen in the table below.

$x \bmod 13$	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2	0	1	4	9	16	25	36	49	64	81	100	121	144
$x^2 \bmod 13$	0	1	4	9	3	12	10	10	12	3	9	4	1

Then, the set of quadratic residues is $\{0, 1, 3, 4, 9, 10, 12\}$ — so for example $\left(\frac{12}{13}\right) = 1$ — and the set of quadratic non-residues is $\{2, 5, 6, 7, 8, 11\}$ — so for example $\left(\frac{2}{13}\right) = -1$.

Notice that if $\left(\frac{a}{p}\right) = 1$, then $\left(\frac{a+np}{p}\right) = 1$, and $\left(\frac{a}{p}\right) = -1 \iff \left(\frac{a+np}{p}\right) = -1$ for $n \in \mathbb{Z}$. This is because if $x^2 \equiv a \pmod{p}$, then $x^2 \equiv a + np \equiv a \pmod{p}$.

[3] [9] "Legendre Symbol."

For example, $\left(\frac{15}{13}\right) = \left(\frac{2}{13}\right) = -1$.

Another interesting property is that there are $\frac{p-1}{2}$ non-zero quadratic residues and $\frac{p-1}{2}$ quadratic non-residues.[4] To see why, note that

$$q^2 \equiv r^2 \pmod{p} \iff q^2 - r^2 \equiv 0 \iff (q-r)(q+r) \equiv 0 \iff q \equiv \pm r.$$

Then, each non-zero quadratic residue has exactly two unique non-zero residues that square to it. Since there are $p-1$ non-zero residues, there are $\frac{p-1}{2}$ unique quadratic residues and thus $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic non-residues.

Indeed, in the example with $p = 13$, we find $\frac{13-1}{2} = 6$ non-zero quadratic residues and $\frac{13-1}{2} = 6$ quadratic non-residues.

3.2 Euler's Criterion

Euler's Criterion[5] provides a way to calculate the Legendre symbol with modular exponentiation. It states that for a prime p,

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

We will establish intuition as to why this is true.

When $p = 2$, this is verifiable.

Assume that p is odd. Then, from Fermat's Little Theorem,

$$\begin{aligned} a^{p-1} \equiv 1 \pmod{p} &\implies (a^{p-1} - 1) \equiv 0 \pmod{p} \\ &\implies (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}. \end{aligned}$$

Since the product is congruent to 0, one of the factors must be 0. Suppose

[4] [10] "Number of Quadratic Residues of Prime."
[5] [11] "Euler's Criterion."

$\left(\frac{a}{p}\right) = 1$. Then, there exists x such that $x^2 \equiv a \pmod{p}$. Then, $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$ by Fermat's Little Theorem.

Now suppose $\left(\frac{a}{p}\right) = -1$. In this case, the x above does not exist. Then, intuitively, $a^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod{p}$ but as found above, $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p} \implies a^{\frac{p-1}{2}} + 1 \equiv 0 \implies a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, meaning that if a is not a quadratic residue, we should have $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

This does not formally prove Euler's Criterion because it is not established that for quadratic non-residues, $a^{\frac{p-1}{2}} - 1 \not\equiv 0$. However, sufficient intuition has been established.

3.3 Multiplicativity

A consequence of Euler's Criterion is that for $b, c \in \mathbb{Z}$ and p is a prime, then

$$\left(\frac{b}{p}\right)\left(\frac{c}{p}\right) = \left(\frac{bc}{p}\right).$$

This can be proven as follows.[6]

$$\left(\frac{bc}{p}\right) = (bc)^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \cdot c^{\frac{p-1}{2}} \pmod{p} = \left(\frac{b}{p}\right)\left(\frac{c}{p}\right).$$

For example, when $p = 13$, the set of quadratic residues is $\{0, 1, 3, 4, 9, 10, 12\}$ and the set of quadratic non-residues is $\{2, 5, 6, 7, 8, 11\}$. Notice that $\left(\frac{3}{13}\right)\left(\frac{5}{13}\right) = \left(\frac{15}{13}\right) = \left(\frac{2}{13}\right) = (1)(-1) = -1$, which agrees with our sets.

[6] [13] Andreescu and Dospinescu 402.

3.4 Quadratic Reciprocity Law

The Quadratic Reciprocity Law[7] states that for two distinct odd primes p, q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

However, in my exploration, I found a more useful representation that will be used in our proofs. Since these two primes are distinct, $\left(\frac{q}{p}\right) = \pm 1$. Then, $\left(\frac{q}{p}\right)^2 = 1$. Multiplying both sides by $\left(\frac{q}{p}\right)$ yields

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}. \qquad \text{(Quadratic Reciprocity)}$$

For example, suppose we wish to calculate $\left(\frac{37}{73}\right)$. Quadratic reciprocity yields

$$\left(\frac{37}{73}\right) = \left(\frac{73}{37}\right)(-1)^{\frac{(73-1)(37-1)}{4}} = \left(\frac{73}{37}\right) = \left(\frac{36}{37}\right) = \left(\frac{6}{37}\right)\left(\frac{6}{37}\right) = \left(\frac{6}{37}\right)^2 = 1.$$

Notice that any Legendre symbol can be simplified by using Quadratic Reciprocity, then reducing the top modulo the bottom, factoring, and then repeating until both arguments are small enough to be calculated manually.

[7] [12] "Law of Quadratic Reciprocity."

4 The Taiwanese Olympiad Problem

This problem is from the 1997 Taiwanese Olympiad[8]:

> Let $k = 2^{2^n} + 1$ for some positive integer n. Prove that
> k is a prime if and only if k is a factor of $3^{\frac{k-1}{2}} + 1$.

This problem asks to prove an "if and only if" statement. To do so, I considered the "if" and the "only if" parts separately. I started with the "only if" part since it seemed easier.

4.1 Proving the "only if" direction

The "only if" statement wishes for us to assume that $k = 2^{2^n} + 1$ is a prime, and then prove that $k \mid 3^{\frac{k-1}{2}} + 1$.

I noticed that the statement we wish to prove is equivalent to $3^{2^{2^n-1}} \equiv -1 \pmod{2^{2^n}+1}$. This looks similar to Euler's Criterion. In fact, the equivalent statement in terms of k is $3^{\frac{k-1}{2}} \equiv -1 \pmod{k}$.

Since k is prime, Euler's Criterion can directly be applied, resulting in $\left(\frac{3}{k}\right) \equiv -1$. Quadratic reciprocity states

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}.$$

With $p = 3, q = k$, this yields

$$\left(\frac{3}{k}\right) = \left(\frac{k}{3}\right)(-1)^{\frac{(3-1)(k-1)}{4}} = \left(\frac{k}{3}\right)(-1)^{2^{2^n-1}} = \left(\frac{k}{3}\right) = -1.$$

Note that $(-1)^{2^{2^n-1}} = 1$ for all $n \in \mathbb{Z}^+$. Then, $\left(\frac{k}{3}\right) = -1 \iff k \equiv 2 \pmod{3}$.

Since all of these steps are reversible, it suffices to prove that $k \equiv 2 \pmod{3}$ to

[8] [13] Andreescu and Dospinescu 419.

solve the "only if" direction. We have

$$k = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 = ((-1)^2)^{2^{n-1}} + 1 = 1^{2^{n-1}} + 1 \equiv 1 + 1 \equiv 2 \pmod 3.$$

Note that the first equivalence is true because $2^a \equiv (-1)^a \pmod 3$ for $a \in \mathbb{Z}$.

Thus, the "only if" direction is complete.

This part of the problem demonstrates how concepts in quadratic residues can be used in direct applications to number-theoretic olympiad problems.

4.2 Proving the "if" direction

We will first introduce a useful lemma.

4.2.1 Minimum exponent lemma

Lemma Define $x \in \mathbb{Z}^+$ to be the minimum integer satisfying $a^x \equiv 1 \pmod b$, where $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$. Then, all integers y satisfying $a^y \equiv 1 \pmod b$ must be divisible by x.

The proof is in Appendix C, but here is a diagram to give intuition for the lemma.

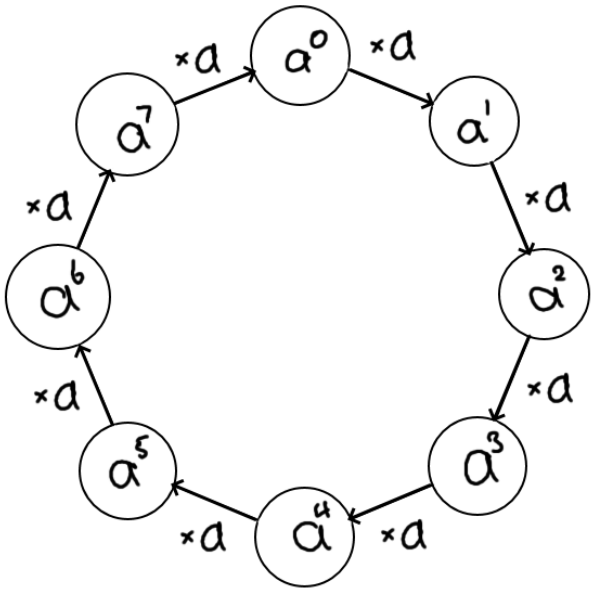

Figure 3: An example where $x = 8$. $a^1, a^2, \cdots, a^7 \neq 1$.

Intuition Imagine beginning at a^0 and going forwards in the cycle y times. The expression a^y is only congruent to 1 if a^y travels a complete number of cycles, implying that $x \mid y$, where x is the minimum cycle length.

4.2.2 The proof

The "if" statement wishes for us to assume that $k = 2^{2^n} + 1 \mid 3^{\frac{k-1}{2}} + 1$, and then prove that k is prime.

I originally tried proof by contradiction. However, this did not lead anywhere useful. I then considered a prime factor p of k, with the goal of proving that p must necessarily be k, which would prove that k is prime.

I noticed that we had $k \mid 3^{\frac{k-1}{2}} + 1 \iff 3^{\frac{k-1}{2}} \equiv -1 \pmod{k}$. Since $p \mid k$, we must also have $p \mid 3^{\frac{k-1}{2}} + 1 \iff 3^{\frac{k-1}{2}} \equiv -1 \pmod{p}$. I noticed that $3^{\frac{k-1}{2}} \equiv -1 \pmod{p}$ looks similar to Euler's Criterion, but it cannot be used here, since we

do not know that the k in the exponent is equal to the modulus p.

Instead, I used $k = 2^{2^n} + 1$ and squared both sides of the congruence below to arrive at

$$3^{\frac{k-1}{2}} \equiv 3^{2^{(2^n-1)}} \equiv -1 \pmod{p} \implies 3^{2^{2^n}} \equiv 1 \pmod{p}.$$

Let x be the minimum exponent with $3^x \equiv 1 \pmod{p}$. Because $3^{2^{2^n}} \equiv 1 \pmod{p}$ from above, $x \mid 2^{2^n}$ by the lemma. However, since $3^{2^{(2^n-1)}} \equiv -1 \pmod{p}$, we must have $x \nmid 2^{(2^n-1)}$. The only value of x satisfying these two conditions is $x = 2^{2^n}$.

Additionally, $3^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem, and $x \mid p-1$ by the lemma. Therefore, $x = 2^{2^n} \leq p - 1 \implies p \geq 2^{2^n} + 1$.

However, from the definition of p, we have $p \mid k \implies p \mid 2^{2^n}+1 \implies p \leq 2^{2^n}+1$. The only value of p satisfying both inequalities is $p = k$, implying that k is prime.

Thus, both directions of the problem have been proven. $\square$

Even though the problem seems to be closely related to quadratic residues, this part demonstrates that quadratic residues were not able to be applied just by changing the direction of proof required. Thus, quadratic residues have their limitations in number theory questions.

5 Fermat's Problem

We will explore some general complex divisibility properties through a problem by Fermat.

Prove that the numbers $3^n + 1$ have no divisor of the form $12k + 11$.[9]

5.1 Proof of Simpler Version

I wish to first solve a simpler version to develop insights. To do so, I assume that the divisor $12k + 11$ is prime. Thus, I will prove that the numbers $3^n + 1$ have no prime divisor of the form $12k + 11$. This will be accomplished by assuming that $3^n + 1$ has a prime divisor of the form $12k + 11$ to arrive at a contradiction.

First, note that if $3^n + 1$ has a prime divisor of the form $p = 12k + 11$, then $p \mid 3^n + 1 \Rightarrow 3^n + 1 \equiv 0 \pmod{p} \Rightarrow 3^n \equiv -1 \pmod{p}$.

We wish to use quadratic residues to arrive at a contradiction.

I noticed that if $n \equiv 0 \pmod 2$, then quadratic residues could be applied, because then $n = 2k$, $k \in \mathbb{Z}$, so $3^n \equiv 3^{2k} \equiv (3^k)^2 \equiv -1 \pmod{p}$, implying that -1 is a quadratic residue. However, using Euler's Criterion,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{(12k+11)-1}{2}} = (-1)^{6k+5} = (-1),$$

implying that -1 is a quadratic non-residue modulo p. Thus, we have arrived at a contradiction if n is even.

Hoping to use a similar argument to arrive at a contradiction, I assumed that $n \equiv 1 \pmod 2$ to complete the casework.

We still have $\left(\frac{-1}{p}\right) = (-1)$ from above. Then, $n = 2k - 1$, $k \in \mathbb{Z}$. This gives $3^n \equiv 3^{2k-1} \equiv -1 \pmod{p}$. Wanting to use quadratic residues, I multiplied both

[9] [13] Andreescu and Dospinescu 422.

sides by 3 to get $3^{2k} \equiv -3 \pmod{p}$, implying that -3 is a quadratic residue modulo p. Using multiplicity of the Legendre symbol and Euler's Criterion gives $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = -\left(\frac{3}{p}\right)$. Using the Quadratic Reciprocity Law with $p = 12k + 11$ gives

$$\left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)(-1)^{\frac{(3-1)(p-1)}{4}} = -\left(\frac{p}{3}\right)(-1)^{6k+5} = \left(\frac{p}{3}\right).$$

We also have $\left(\frac{p}{3}\right) = \left(\frac{12k+11}{3}\right) = \left(\frac{2}{3}\right) = -1$, since 2 is a quadratic non-residue modulo 3. Thus, we have $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = -1$, meaning that -3 is a quadratic non-residue modulo p, which is a contradiction if n is odd.

A contradiction has been established in both cases; thus, the framework for the proof is complete.

5.2 Proof

To solve the full problem, we assume that $x \equiv 11 \pmod{12}$ is a factor of $3^n + 1$ for the sake of contradiction. Writing x in terms of its prime factors gives

$$x = \prod_{i=1}^{y} p_i^{\alpha_i} \equiv 11 \pmod{12}.$$

An important observation is that since 11 and 12 are coprime, no p_i can be 2 or 3. This is because if some $p_k = 2$, then $2 \mid x$. However, $x \equiv 11 \pmod{12} \implies x \equiv 1 \pmod{2}$, which gives us a contradiction. The same argument applies to 3.

Thus, each of the prime factors p_i can only be congruent to $1, 5, 7$, or $11 \pmod{12}$, because all other residues are divisible by either 2 or 3.

Consider p_i, a specific prime divisor of x. Suppose $x = p_i k$, $k \in \mathbb{Z}$. Then,

$$3^n \equiv -1 \pmod{x} \implies x \mid 3^n + 1$$
$$\implies p_i k \mid 3^n + 1 \implies p_i \mid 3^n + 1 \implies 3^n \equiv -1 \pmod{p_i}.$$

Note that this argument applies to all prime factors of x. This means that we can essentially reduce the modulus x to one of its divisors p_i.

Now, we consider two cases. We first find all possible factors x modulo 12 of $3^n + 1$ when $n \equiv 0 \pmod 2$, and then when $n \equiv 1 \pmod 2$, and show that in both cases, $x \equiv 11$ is impossible.

When n is even, we have $n = 2k \implies 3^{2k} \equiv -1 \pmod{p_i}$, meaning that -1 is a quadratic residue modulo p_i. By Euler's Criterion,

$$\left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_i - 1}{2}} = 1 \implies p_i \equiv 1 \pmod 4.$$

Of the possible residues $1, 5, 7, 11 \pmod{12}$, only $1, 5$ are congruent to $1 \pmod 4$. Then, the prime factors that multiply to x must only have residues $1, 5 \pmod{12}$.

Then, $x \equiv 1^{\beta_1} \cdot 5^{\beta_2} \equiv 5^{\beta_2} \pmod{12}$, $\beta_1, \beta_2 \in \mathbb{Z}$.

However, when varying β_2, $x \equiv 5^{\beta_2}$ cycles between 5 and 1. Thus, the set of all possible residues for $x \pmod{12}$ are $\{1, 5\}$ when n is even.

The second case is slightly more involved. Here, we have $n = 2k - 1, k \in \mathbb{Z}$. Then, $3^{2k} \equiv -3 \pmod x$ by multiplying both sides by 3, so $\left(\frac{-3}{p_i}\right) = 1$.

Using multiplicity, we have

$$\left(\frac{-3}{p_i}\right) = \left(\frac{3}{p_i}\right)\left(\frac{-1}{p_i}\right) = 1.$$

Since the product is non-zero, we know that $p_i \nmid 3 \implies p_i \neq 3$. Using the Quadratic Reciprocity Law gives

$$\left(\frac{3}{p_i}\right) = \left(\frac{p_i}{3}\right)(-1)^{\frac{(3-1)(p_i-1)}{4}} = \left(\frac{p_i}{3}\right)(-1)^{\frac{p_i-1}{2}},$$

and Euler's Criterion gives

$$\left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_i-1}{2}}.$$

Then,

$$\left(\frac{-3}{p_i}\right) = \left(\frac{3}{p_i}\right)\left(\frac{-1}{p_i}\right) = \left(\left(\frac{p_i}{3}\right)(-1)^{\frac{p_i-1}{2}}\right)\left((-1)^{\frac{p_i-1}{2}}\right) = \left(\frac{p_i}{3}\right)(-1)^{p_i-1}.$$

Since p_i is an odd prime, we have

$$\left(\frac{-3}{p_i}\right) = \left(\frac{p_i}{3}\right)(-1)^{p_i-1} = \left(\frac{p_i}{3}\right) = 1.$$

This only occurs when $p_i \equiv 1 \pmod 3$, giving only $p \equiv 1, 7 \pmod{12}$ as our options.

We let $x \equiv 1^{\beta_1} \cdot 7^{\beta_2} \equiv 7^{\beta_2} \pmod{12}, \beta_1, \beta_2 \in \mathbb{Z}$. Similar to the first case, when varying β_2, x cycles between 7 and 1. Thus, the set of all possible residues for $x \pmod{12}$ are $\{1, 7\}$ when n is odd.

Thus, the set of all possible residues of $x \pmod{12}$ is $\{1, 5, 7\}$, contradicting our assumption of the existence of $x \equiv 11 \pmod{12}$ and completing our proof.

In this problem, we began by looking at a simpler version for only prime numbers that provided a framework for the more general problem even though interestingly, the original problem does not mention primes. Quadratic residues were used by considering in separate cases the parity of the exponent to eliminate

possible options and ultimately arrive at a contradiction.

6 Extension

I made my own extension of the simpler version of the problem.

> Find all triplets (a, b, c), where $a, b, c \in \mathbb{Z}^+$ such that the numbers $a^n + 1$ have no prime divisor of the form $bk + c$.

In my exploration, I try to find solutions by constructing a proof by contradiction, and noticing the necessary conditions on (a, b, c) for the contradiction to work. I first follow my steps in the original question to derive the most general conditions for this new problem. Then, I try to find specific families of triplets by considering the case when $\gcd(b, c) > 1$, and when $\gcd(b, c) = 1$. In the second case, I experiment with gradually more general cases for a—first an odd prime, then a power of an odd prime, then a product of two powers of odd primes, and then finally any odd number.

6.1 Deriving General Conditions

Our goal is to find general conditions which satisfy the problem to pinpoint specific families of triplets (a, b, c).

Hoping to use a similar line of reasoning as with the original problem, we let $p = bk + c$ and assume for the sake of contradiction that $a^n + 1 \equiv 0 \pmod{p}$. Then, if the triplet (a, b, c) is constructed in a way so that quadratic residues can be used to arrive at a contradiction, then the triplet satisfies the question.

We perform casework on the parity of n. However, for the proof to work, there must be a contradiction in both cases.

Case 1 : If $n = 2k$, $k \in \mathbb{Z}$, then $a^{2k} \equiv -1 \pmod{p}$, implying that $\left(\frac{-1}{p}\right) = 1$. To mimic the contradiction in the original problem, we assume that

$$\left(\frac{-1}{p}\right) = -1 \implies (-1)^{\frac{p-1}{2}} = -1 \implies p = bk + c \equiv 3 \pmod{4}.$$

To guarantee this condition for all k, we must have $4 \mid b$ and $c \equiv 3 \pmod{4}$.

Case 2 : If $n = 2k - 1$, $k \in \mathbb{Z}$, then

$$a^n = a^{2k-1} \equiv -1 \pmod{p} \implies a^{2k} \equiv -a \pmod{p} \implies \left(\frac{-a}{p}\right) = 1.$$

To create a contradiction, we assume that $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = -1$. Since $\left(\frac{-1}{p}\right)$ is assumed to be -1 from case 1, we must have $\left(\frac{-a}{p}\right) = -1 \cdot \left(\frac{a}{p}\right) = -1 \iff \left(\frac{a}{p}\right) = 1$ for all p in order to have a contradiction.

To summarize, we need 3 key conditions to guarantee that the proof by contradiction works:

1. $4 \mid b$
2. $c \equiv 3 \pmod{4}$
3. $\left(\frac{a}{p}\right) = 1$ for all primes $p = bk + c$

Indeed, in the original simplified problem, we have $a = 3, b = 12, c = 11$, which satisfy these three conditions. The third condition is proven in section 5.1.

Thus, the arguments in section 5.1 easily extend to this general extension to provide necessary conditions. However, from here new challenges appear.

6.2 Finding Families of Triplets

The remainder of this extension focuses on finding more specific conditions on a, b, c that guarantees the conditions above. We will consider $\gcd(b, c) > 1$ and $\gcd(b, c) = 1$ separately as mentioned at the beginning of section 6. Because this is very exploratory, many of these sections divide into further subcases.

6.2.1 Case: $\gcd(b, c) > 1$

The problem statement matters only when $bk + c$ is prime. If $\gcd(b, c) > 1$, I noticed that $bk + c$ can only be prime if $k = 0$ and c is prime. Otherwise, the expression $bk + c$ has at least 3 distinct factors: $1, \gcd(b, c)$, and $bk + c$, so it cannot be prime.

Thus, we can satisfy the key conditions with the following:

1. $4 \mid b$
2. $c \equiv 3 \pmod 4$
3. $\left(\frac{a}{c}\right) = 1$, because $\left(\frac{a}{p}\right) = \left(\frac{a}{bk+c}\right) = \left(\frac{a}{b(0)+c}\right) = \left(\frac{a}{c}\right)$
4. c is prime
5. $c \mid b$, because c is prime and $\gcd(b, c) > 1$

These produce a family of solutions (family 1 in section 6.3). This is the only family found by assuming that b, c are not coprime, and so the rest of this extension will assume that $\gcd(b, c) = 1$.

6.2.2 Case: $\gcd(b, c) = 1$, a is an odd prime

Note that since $4 \mid b, c \equiv 3 \pmod 4$ by the key conditions and $p = bk + c$, p can be written as $p = 4x + 3, x \in \mathbb{Z}$. Then, Quadratic Reciprocity yields

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{\frac{(a-1)(p-1)}{4}} = \left(\frac{p}{a}\right)(-1)^{\frac{(a-1)(4x+2)}{4}} = \left(\frac{p}{a}\right)(-1)^{\frac{(a-1)(2x+1)}{2}} = 1.$$

Notice that

$$(-1)^{\frac{(a-1)(2x+1)}{2}} = ((-1)^{2x+1})^{\frac{a-1}{2}} = (-1)^{\frac{a-1}{2}}.$$

Then,

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{\frac{(a-1)}{2}} = 1. \tag{1}$$

To ensure that equation 1 is always true, we will perform further casework on a.

Subcase 1 – $a \equiv 1 \pmod 4$, $\gcd(a, b) = 1$: Here, $a \equiv 1 \pmod 4 \implies (a-1)/2$ is even and $(-1)^{\frac{(a-1)}{2}} = 1$. From equation 1,

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

In other words, in order for the key conditions to be satisfied, $\left(\frac{p}{a}\right)$ must be 1 for all $p = bk + c$.

I noticed that if b and a shared no common factors, then the sequence of integers $bk + c$ would be surjective modulo a. In other words, for every residue x modulo a, there exists a value of k such that $bk + c \equiv x \pmod a$. This turns out to be true even if only prime $bk + c$ are considered.

Surjectivity Lemma: The primes of the form $p = bk + c$, when taken modulo an odd prime a where $a \nmid b$, covers all non-zero residues modulo a infinitely many

times.

The proof of this lemma is lengthy and involves Dirichlet's Theorem[10], but can be found in Appendix D.

The surjectivity lemma shows that if a and b are coprime, $\left(\frac{p}{a}\right)$ cannot always be 1. This is because there are $\frac{p-1}{2}$ non-zero quadratic residues and $\frac{p-1}{2}$ quadratic non-residues, and so primes of the form $bk+c$ must cover both quadratic residues and non-residues, which would result in the existence of a $\left(\frac{p}{a}\right) = \pm 1 \implies \left(\frac{a}{p}\right) = -1$, so the proof by contradiction does not necessarily work.

We have just shown that in this subcase, the proof by contradiction does not work. Thus, for $a \equiv 1 \pmod 4$, we must have $\gcd(a, b) > 1$ to find more families of triplets (a, b, c) that satisfy the key conditions.

Subcase 2 – $a \equiv 3 \pmod 4, \gcd(a, b) = 1$**:** By equation (1), we must have $\left(\frac{p}{a}\right) = -1$ for all values of p. The argument above using the surjectivity lemma still applies, showing that if $\gcd(a, b) = 1$, then the proof by contradiction fails.

Subcase 3 – $\gcd(a, b) > 1$**:** Since a is prime, we must have $a \mid b \implies p = bk + c \equiv c \pmod a$. Then, equation 1 yields

$$\left(\frac{p}{a}\right)(-1)^{\frac{a-1}{2}} = \left(\frac{bk+c}{a}\right)(-1)^{\frac{a-1}{2}} = \left(\frac{c}{a}\right)(-1)^{\frac{a-1}{2}} = 1.$$

We must ensure that the above equation is always true. Two new families of triplets are now found by applying casework on the residue of $a \pmod 4$.

The first is when $a \equiv 1 \pmod 4$ is an odd prime, b is divisible by $4a$, and c is a quadratic residue modulo a. (See family 2 in section 6.3.)

The second family of triplets is when $a \equiv 3 \pmod 4$ is an odd prime, b is

[10] [14] Weisstein.

divisible by $4a$, and c is a quadratic non-residue modulo a. (See family 3 in section 6.3.)

All families of triplets have been found for when a is an odd prime.

6.2.3 $\gcd(b, c) = 1$, a is a power of an odd prime

If we let $a = q^\alpha$, where q is an odd prime, then we have new solutions. If α is even, then equation 1 is always true since $\left(\frac{a}{p}\right) = \left(\frac{(q^{\alpha/2})^2}{p}\right) = 1$. Then, it suffices to have $4 \mid b$ and $c \equiv 3 \pmod 4$, which creates a new family of solutions. (See family 4 in section 6.3.)

If α is odd, then $\alpha = 2x + 1, x \in \mathbb{Z}$. Then, we must have $4 \mid b$, $c \equiv 3 \pmod 4$, and $\left(\frac{q^\alpha}{p}\right) = 1$. However, note that

$$\left(\frac{q^\alpha}{p}\right) = \left(\frac{(q^x)^2}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right). \tag{2}$$

Then, similar families of triplets can be found using the work above when assuming that a is an odd prime. (See family 5 in section 6.3.)

6.2.4 $\gcd(b, c) = 1$, a is the product of powers of 2 odd primes

Now, instead of a being an odd prime, we assume that a is a product of two odd primes, and so we assume

$$a = q^{\alpha_1} \cdot r^{\alpha_2}.$$

In order for the contradiction to be successful, we still must have the key conditions: $4 \mid b$, $c \equiv 3 \pmod 4$, and $\left(\frac{a}{p}\right) = \left(\frac{q^{\alpha_1}}{p}\right)\left(\frac{r^{\alpha_2}}{p}\right) = 1$ for all p. Notice that if α_1 is even, then $\left(\frac{a^{\alpha_1}}{p}\right) = 1$, and the same argument would apply if α_2 is even, which would reduce this to the case above. Thus, we will assume that α_1

and α_2 are odd. Then, by using a similar process to equation 2,

$$\left(\frac{a}{p}\right) = \left(\frac{q^{\alpha_1}}{p}\right)\left(\frac{r^{\alpha_2}}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{r}{p}\right) = 1.$$

Thus, we must find when $\left(\frac{q}{p}\right)\left(\frac{r}{p}\right) = 1$ for all $p = bk + c$.

We apply Quadratic Reciprocity twice to get

$$\left(\frac{q}{p}\right)\left(\frac{r}{p}\right) = (-1)^{\frac{q-1}{2}}(-1)^{\frac{r-1}{2}}\left(\frac{p}{q}\right)\left(\frac{p}{r}\right) = (-1)^{\frac{q+r-2}{2}}\left(\frac{p}{q}\right)\left(\frac{p}{r}\right) = 1. \qquad (3)$$

Our goal is to find constraints on q, r, b, c such that for all $p = bk + c$, equation 3 holds true.

First, I noticed how the exponent of (-1) is constant with respect to k. Thus, $\left(\frac{p}{q}\right)\left(\frac{p}{r}\right)$ must also be constant for equation 3 to always be true. At first, I thought I could easily assume that due to a similar argument made for when a was assumed to be an odd prime, that $\left(\frac{p}{q}\right)$ and $\left(\frac{p}{r}\right)$ must individually be constant. However, the proof is subtle.

Legendre Product Lemma If prime $p = bk + c$ and $\left(\frac{p}{q}\right)\left(\frac{p}{r}\right)$ is constant with respect to k, then $\left(\frac{p}{q}\right)$ and $\left(\frac{p}{r}\right)$ are individually constant.

Proof We assume for the sake of contradiction that $\left(\frac{p}{q}\right)$ and $\left(\frac{p}{r}\right)$ are not individually constant. Then $q \nmid b$, otherwise $\left(\frac{p}{q}\right) = \left(\frac{c}{q}\right)$ which is constant, and similarly for $r \nmid b$. Then, by the surjectivity lemma, $p = bk + c$ covers all nonzero residues modulo both q and r. Now, consider the diagram below, which represents an example where $q = 3$ and $r = 5$.

~~a′~~ b′ c′|~~a′~~ b′ ~~c′~~|~~a′~~ b′ c′|~~a′~~ ~~b′~~ c′|~~a′~~ b′ c′

~~d′~~ e′ f′ ~~g′~~ h′|~~d′~~ ~~e′~~ f′ g′ ~~h′~~|~~d′~~ e′ ~~f′~~ g′ h′

Figure 4: Legendre symbol of residues from 0 to 14 modulo 3 and 5. Multiples of 3 or 5 are crossed out.

Let $(a', b', c') = (\left(\frac{0}{3}\right), \left(\frac{1}{3}\right), \left(\frac{2}{3}\right))$, and $(d', e', f', g', h') = (\left(\frac{0}{5}\right), \cdots, \left(\frac{4}{5}\right))$. In order to have $\left(\frac{p}{q}\right)\left(\frac{p}{r}\right)$ be constant, the product of the elements in each non-crossed-out column has to be equal, because due to the surjectivity lemma, the sequence $bk+c$ only covers all columns that contains neither a' or d'. Then, when varying $p = bk + c$ by increasing k, the expression $\left(\frac{p}{q}\right)\left(\frac{p}{r}\right)$ becomes $b'e', c'f', b'h', a'e'$, $b'f', c'g', b'd', c'e', b'g'$, and $c'h'$. These products must all be equal, yielding $b'e' = b'f' = b'g' = b'h' \implies e' = f' = g' = h'$. Likewise, $b' = c'$.

However, these equalities cannot be true since there are $\frac{q-1}{2}$ non-zero quadratic residues and non-residues (mod q), and similarly for r. The same would apply for any odd primes q, r. Thus, both $\left(\frac{p}{q}\right)$ and $\left(\frac{p}{r}\right)$ have to individually be constant. □

The product lemma and surjectivity lemma together imply that $q \mid b$ and $r \mid b$. Then, our new family of triplets currently has the conditions $a = q^{\alpha_1} r^{\alpha_2}$ for odd α_1, α_2, $4qr|b$, and $c \equiv 3 \pmod 4$, as well as equation 3. To distinguish more families of triplets, we use more casework.

If $qr \equiv 1 \pmod 4 \implies q = r = 1$ or $q = r = 3 \implies (-1)^{\frac{q+r-2}{2}} = 1$, then we must choose c such that $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) \implies \left(\frac{c}{q}\right) = \left(\frac{c}{r}\right)$ to satisfy equation 3. Note that this does produce a family of triplets. (See family 6 in section 6.3.)

Otherwise if $qr \equiv -1 \pmod 4 \implies (q, r) = (1, 3)$ or $(3, 1) \implies (-1)^{\frac{q+r-2}{2}} = -1$, then we must choose c such that $\left(\frac{p}{q}\right) = -\left(\frac{p}{r}\right) \implies \left(\frac{c}{q}\right) = -\left(\frac{c}{r}\right)$. This is

another family of triplets. (See family 7 in section 6.3.)

6.2.5 $\gcd(b, c) = 1$, a is any odd number

Let $a = \prod_{i=1}^{\beta} q_i^{\alpha_i}$. We still must create the key conditions $4 \mid b$, $c \equiv 3 \pmod 4$, and $\left(\frac{a}{p}\right) = 1$ for all primes $p = bk + c$. Notice that if any α_i is even, then it can be ignored by simplifying the exponent similar to in equation 2. Then, without loss of generality, we assume that all α_i are odd and then simplify the exponent as in equation 2, yielding

$$\prod_{i=1}^{\beta} \left(\frac{q_i}{p}\right) = 1.$$

Applying Quadratic Reciprocity for every prime q_i gives

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{\beta} \left(\frac{q_i}{p}\right) = \prod_{i=1}^{\beta} (-1)^{\frac{q_i-1}{2}} \left(\frac{p}{q_i}\right) = 1. \tag{4}$$

From a similar argument using the product and surjectivity lemmas, we must have $q_i \mid b$ for all q_i. We also have $4 \mid b$ from a key condition, so

$$4 \prod_{i=1}^{\beta} q_i \mid b.$$

Then, since

$$\prod_{i=1}^{\beta} (-1)^{\frac{q_i-1}{2}}$$

is constant with respect to k, it suffices to choose values of c such that

$$\prod_{i=1}^{\beta} \left(\frac{c}{q_i}\right) = \prod_{i=1}^{\beta} (-1)^{\frac{q_i-1}{2}},$$

which satisfies equation 4 and thus gives us a new family of triplets. (See family 8 in section 6.3.)

In this section, we found many different family of primes by considering careful casework and then generalizing cases. This took us from finding families where a is an odd prime to families where a is odd.

6.3 Found Families of Triplets

To summarize, the families of triplets found include the following.

1. $\left(\frac{a}{c}\right) = 1$, $c \equiv 3 \pmod 4$, c is prime, and $c \mid b$.
2. $a \equiv 1 \pmod 4$ is an odd prime, $4a \mid b$, $c \equiv 3 \pmod 4$, and $\left(\frac{c}{a}\right) = 1$.
3. $a \equiv 3 \pmod 4$ is an odd prime, $4a \mid b$, $c \equiv 3 \pmod 4$, and $\left(\frac{c}{a}\right) = -1$.
4. a is both odd and a perfect square, $4 \mid b$ and $c \equiv 3 \pmod 4$.
5. $a = q^\alpha \equiv 3 \pmod 4$ where q is an odd prime and α is odd, $4a \mid b$, $c \equiv 3 \pmod 4$, and $\left(\frac{c}{a}\right) = 1$.
6. $a = q^{\alpha_1} r^{\alpha_2}$, where q, r are odd primes and α_1, α_2 are odd, $4qr \mid b$, $c \equiv 3 \pmod 4$, $qr \equiv 1 \pmod 4$, and $\left(\frac{c}{q}\right) = \left(\frac{c}{r}\right)$.
7. $a = q^{\alpha_1} r^{\alpha_2}$, where q, r are odd primes and α_1, α_2 are odd, $4qr \mid b$, $c \equiv 3 \pmod 4$, $qr \equiv 3 \pmod 4$, and $\left(\frac{c}{q}\right) = -\left(\frac{c}{r}\right)$.
8. a is a product of odd powers of primes q_i where $1 \leq i \leq \beta$, $4 \mid b$ and $q_i \mid b$ for each q_i, $c \equiv 3 \pmod 4$, and c is chosen such that

$$\prod_{i=1}^{\beta} \left(\frac{c}{q_i}\right) = \prod_{i=1}^{\beta} (-1)^{\frac{q_i - 1}{2}}.$$

Note that these are not all possible families, since the case where a is even has not been explored.

These families of triplets demonstrate that the results from section 5.1 can be generalized, making it much simpler to generate a wide variety of triplets (a, b, c) that satisfy the problem.

However, this usage of quadratic residues has its limitations. If the proof by contradiction is invalid, there may still be a triplet that can be proven to work via a different method of proof.

7 Conclusion

In this essay, number theoretic concepts were introduced, including modular arithmetic and its arithmetic operations, Euler's Totient Theorem and its corollaries, then quadratic residues and its many theorems, which were then put to use in a Taiwanese Olympiad problem and then in a problem from the mathematician Fermat. Afterwards was a deep exploration of my extension to the problem. Areas for further exploration include exploring in the extension the case where a is even, and extending the Taiwanese Olympiad problem by seeking a generalization of the numbers used.

However, I believe the purpose of this essay—to demonstrate the usefulness of quadratic residues—has been adequately achieved, as the Taiwanese Olympiad problem demonstrated how quadratic residues can be useful but has its limitations, while an extension to Fermat's problem involving families of primes has been explored in depth.

8 References

[1] Silverman, Joseph. "A Friendly Introduction to Number Theory." *A Friendly Introduction to Number Theory*, 2012, https://www.math.brown.edu/johsilve/frint.html. Retrieved August 7, 2022.

[2] Rusczyk, Richard. "Modular Arithmetic/Introduction." *Art of Problem Solving*, 2021, https://artofproblemsolving.com/wiki/index.php/Modular_arithmetic/Introduction. Retrieved August 7, 2022.

[3] "Graphing Calculator." *Desmos*. https://www.desmos.com/calculator. Retrieved August 7, 2022.

[4] Rusczyk, Richard. "Euler's Totient Function." *Art of Problem Solving*, 2021, https://artofproblemsolving.com/wiki/index.php/Euler%27s_totient_function. Retrieved August 7, 2022.

[5] Weisstein, Eric W. "Fundamental Theorem of Arithmetic." *MathWorld*, 2005, https://mathworld.wolfram.com/FundamentalTheoremofArithmetic.html. Retrieved August 7, 2022.

[6] Chorge, Shashank and Vargas, Juan "Proof of Euler's φ (Phi) Function Formula," *Rose-Hulman Undergraduate Mathematics Journal: Vol. 14 : Iss. 2, Article 6*, 2013, https://scholar.rose-hulman.edu/rhumj/vol14/iss2/6/.

[7] Rusczyk, Richard. "Euler's Totient Theorem." *Art of Problem Solving*, 2021, https://artofproblemsolving.com/wiki/index.php/Euler%27s_Totient_Theorem. Retrieved August 7, 2022,

[8] "Primitive Roots." *Brilliant.org*, https://brilliant.org/wiki/primitive-roots/. Retrieved August 7, 2022.

[9] "Legendre Symbol." *Brilliant.org*, https://brilliant.org/wiki/legendre-symbol/. Retrieved August 7, 2022.

[10] "Number of Quadratic Residues of Prime." *ProofWiki*, 2021, https://proofwiki.org/wiki/Number_of_Quadratic_Residues_of_Prime. Retrieved August 7, 2022.

[11] "Euler's Criterion." *ProofWiki*, 2019, https://proofwiki.org/wiki/Euler%27s_Criterion. Retrieved August 7, 2022.

[12] "Law of Quadratic Reciprocity." *Brilliant.org*, https://brilliant.org/wiki/law-of-quadratic-reciprocity/. Retrieved August 7, 2022.

[13] Andreescu, Titu, and Gabriel Dospinescu. *Problems from the Book*. XYZ Press, 2010.

[14] Weisstein, Eric W. "Dirichlet's Theorem." *MathWorld*, 2004, https://mathworld.wolfram.com/DirichletsTheorem.html. Retrieved August 7, 2022.

9 Appendix A: Euler's Totient Theorem

Suppose we have $a^b \pmod{m}$, $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$ and wish to simplify the exponent when m is not a prime, so Fermat's Little Theorem does not apply. This can be done through Euler's Totient Theorem[11], but Euler's Totient Function must first be defined.

Define Euler's Totient Function[12] $\varphi(n)$ as the number of positive integers between 1 and n inclusive that are coprime to n. For example, the 4 positive integers less than or equal to 10 that are coprime to 10 are 1, 3, 7, and 9, so $\varphi(10) = 4$.

Euler's Totient Theorem states that for $a, m \in \mathbb{Z}^+$ such that $\gcd(a, m) = 1$,

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

Notice that as a consequence of Euler's Totient Theorem, when trying to simplify $a^b \pmod{m}$, we have

$$a^b \pmod{m} \equiv a^{b+k\varphi(m)} \pmod{m}$$

for any $k \in \mathbb{Z}$. Then, the minimum exponent that a^b can be simplified to is the remainder when b is divided by $\varphi(m)$. Notice how unlike the 4 operations in the previous section, simplifying the exponent must occur modulo $\varphi(m)$ instead of modulo m. For example,

$$17^{17} \pmod{10} \equiv 7^{17 \bmod \varphi(10)} \equiv 7^{17 \bmod 4} \equiv 7^1 \equiv 7 \pmod{10}.$$

[11] [7] Rusczyk.
[12] [4] Rusczyk.

10 Appendix B: Modular inverses

Traditional division does not exist in modular arithmetic because rational numbers are not defined. However, there are modular inverses. Suppose we have a residue $a \pmod m$. We define the modular inverse a^{-1}, if it exists, to be the residue modulo m such that $a \cdot a^{-1} \equiv 1 \pmod m$. Notice that due to Euler's Totient Theorem, $a^{\varphi(m)} \equiv 1 \pmod m$ if $\gcd(a, m) = 1$. Then, $a^{-1} \equiv a^{\varphi(m)-1} \pmod m$. Thus, when $\gcd(a, m) = 1$, a^{-1} always exists.

It can be proven that there is at most one modular inverse for each element, and that a^{-1} exists modulo m if and only if $\gcd(a, m) = 1$. Here is the proof.

Suppose $\gcd(a, m) = k$, where $a, m, k \in \mathbb{Z}$ for some $k > 1$. Since $k \mid m$, let $m = kx$, $x \in \mathbb{Z}$. Then, we wish to find $a \cdot a^{-1} \equiv 1 \pmod m \iff m \mid (a \cdot a^{-1} - 1) \iff kx \mid (a \cdot a^{-1} - 1)$, which must satisfy $k \mid (a \cdot a^{-1} - 1) \iff a \cdot a^{-1} \equiv 1 \pmod k$ because $k \mid m$. However, $ax \equiv 0 \pmod k$ for all $x \in \mathbb{Z}$, and so a^{-1} does not exist when $\gcd(a, m) > 1$.

Uniqueness of a modular inverse can be proven by considering two modular inverses $a^{-1} \pmod m$, which we will let be $x, y \pmod m$. Then, we have $ax \equiv ay \equiv 1 \pmod m \implies ax - ay \equiv 0 \pmod m \implies a(x - y) \equiv 0 \pmod m$. Since $\gcd(a, m) = 1$, we must have $x - y \equiv 0 \pmod m \implies x \equiv y \pmod m$, meaning that there can only be at most one modular inverse. $\square$

11 Appendix C: Proof that minimum exponent must divide the exponent

Define x to be the minimum exponent satisfying $a^x \equiv 1 \pmod{b}$, $a, x, b \in \mathbb{Z}$. Suppose y satisfies $a^y \equiv 1 \pmod{b}$.

If $y = kx$, then $a^y \equiv a^{kx} \equiv (a^x)^k \equiv 1 \pmod{b}$. Now suppose that there is some integer $y = kx + c$ such that $1 \leq c < x$ that satisfies $a^y \equiv 1 \pmod{b}$. Then, $a^y \equiv a^{kx+c} \equiv a^{kx} \cdot a^c \equiv a^c \equiv 1 \pmod{b}$, implying that c is the minimum since $c < x$. However, we already assumed that x is the minimum, and thus we have a contradiction. Then, we must have $c = 0 \implies y = kx \implies x \mid y$. $\square$

12 Appendix D: Proof that the primes in an arithmetic sequence has infinitely many primes for each non-zero residue

We wish to prove that the primes of the form $p = bk + c$, when taken modulo an odd prime a where $\gcd(a, b) = 1$, covers all non-zero residues modulo a infinitely many times.

I wish to apply Dirichlet's Theorem on Arithmetic Progressions[13], which states that for $a, d \in \mathbb{Z}$ such that $\gcd(a, d) = 1$, there are infinitely many primes of the form $a \pmod{d}$, or in other words, there are infinitely many primes in the arithmetic sequence $a + kd, k \in \mathbb{Z}$. To do so, I must first find the arithmetic sequence for each of the residues x modulo a.

We have $k \equiv (x - c)b^{-1} \pmod{a}$, meaning that $k = (x - c)b^{-1} + ay$ for $y \in \mathbb{Z}$. Plugging this back into $bk + c$ yields

$$bk + c = b((x - c)b^{-1} + ay) + c = bb^{-1}(x - c) + aby + c \equiv x \pmod{a},$$

where y varies and the other variables are constant. Then, for each residue x, we define an arithmetic progression with the common difference ab, and the first term $bb^{-1}(x - c) + c$. This arithmetic sequence has infinitely many primes if $\gcd(ab, bb^{-1}(x - c) + c) = 1$. Since a, b are coprime, the condition above is equivalent to the two conditions $\gcd(a, bb^{-1}(x - c) + c) = 1$ and $\gcd(b, bb^{-1}(x - c) + c) = 1$. Since $bb^{-1}(x - c) + c \equiv (x - c) + c \equiv x \pmod{a}$, this condition holds true if $x \neq 0 \pmod{a}$. Due to the Euclidean Algorithm, $\gcd(b, bb^{-1}(x - c) + c) = \gcd(b, c) = 1$. Thus, primes of the form $bk + c$ will cover all non-zero residues modulo a, proving the lemma. $\square$

[13] [14] Weisstein.