USING A SUPPORT VECTOR MACHINE TO PREDICT PRIMALITY IN COMPARISON WITH THE MILLER-RABIN PROBABILISTIC PRIMALITY TEST

MIGUEL AMEZOLA
B.S. MATHEMATICS
PACIFIC LUTHERAN UNIVERSITY
ADVISORS: DR. TOM EDGAR

Abstract. Using the modular number system and quadratic residues to classify integers as prime or composite. Computationally performing the Fermat primality test and identifying Carmichael numbers. Calculating the Jacobi symbol. Using the Solovay-Strassen test and finding Euler-Jacobi pseudoprimes.

Date: May 9, 2017.

Contents

1. Introduction

1.1. Prime and Composite Numbers.

Definition 1.1.1 (Prime)**.** Let $p \in \mathbb{Z}$, $p > 1$. Then p is prime if and only if for every $a, b \in \mathbb{Z}$, $p = ab$ implies $a = 1$ or $b = 1$. [2]

Definition 1.1.2 (Composite)**.** Let $n \in \mathbb{Z}, n > 1$. Then n is composite if and only if there exists $a, b \in \mathbb{Z}$ such that $n = ab, 1 < a, b < n$. [2]

1.2. Divisibility.

Definition 1.2.1 (Divide [2])**.** Let $a, d \in \mathbb{Z}$. We say that d divides a if there exists $q \in \mathbb{Z}$ such that $a = qd$. We express this in symbols as $d \mid a$ (which is read "d divides a").

Proposition 1.2.1 (Linear combination)**.** *Let $d, m, n, x, y \in \mathbb{Z}$. If $d \mid x$ and $d \mid y$, then $d \mid mx + ny$.*

Proof. Let $d, m, n, x, y \in \mathbb{Z}$ such that $d \mid x$ and $d \mid y$. Since $d \mid x$, then there exists $k \in \mathbb{Z}$ such that $x = kd$. Multiplying by m, we have $mx = mkd$. Since $d \mid y$, then there exists $l \in \mathbb{Z}$ such that $y = ld$. Multiplying by n, we have $ny = nld$. Adding both results yields

$$mx + ny = mkd + nld = (mk + nl)d.$$

Therefore, since $(mk + nl) \in \mathbb{Z}$, we know $d \mid mx + ny$. □

Definition 1.2.2 (Greatest common divisor)**.** Let $a, b \in \mathbb{Z}$ be nonzero. The greatest common divisor of a and b is the largest $d \in \mathbb{N}$ for which $d \mid a$ and $d \mid b$ and is denoted $d = \gcd(a, b)$.

Example 1.2.1. The divisors of 42 are $1, 2, 3, 6, 7, 14, 21, 42$ and the divisors of 49 are $1, 7, 49$. The largest number that appears in both of these lists is 7. Thus, $7 = \gcd(42, 49)$.

However, the greatest common divisor of some integers is 1. For instance, the divisors of 25 are $1, 5, 15$ and the divisors of 28 are $1, 2, 4, 7, 14, 28$. The largest number that appears in both lists is 1. Such numbers are said to be relatively prime.

Proposition 1.2.2. *Let $a, b \in \mathbb{Z}$. Then greatest common divisor of a and b is equal to the smallest positive linear combination of a and b.*

Proof. We will use contradiction. Let $a, b \in \mathbb{Z}$, and suppose $e = ax + by$ is the smallest positive linear combination of a and b. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$ implies that $d \mid ax + ay$ by proposition 1.2.1. Since $d \mid ax + by$, then $d \mid e$, and so $d \leq e$.

Now suppose $e \nmid a$. Thus, $a = qe + r$ for some $q \in \mathbb{Z}$ with $0 < r < e$. Then

$$r = a - qe = a - q(ax - by) = a - qax - qby = a(1 - qx) - b(qy).$$

This means that r is a positive linear combination that is less than e, contradicting the fact that e is the smallest positive linear combination of a and b. Hence, $e \mid a$, and a similar

argument can be used to show that $e \mid b$ as well. Thus, by proposition 1.2.1, $e \mid d$ and $e \mid ax + by$, and so $e \leq d$.

Since we have $d \leq e$ and $e \leq d$, it must be the case that $e = d$. Therefore, the greatest common divisor of a and b is equal to the smallest positive linear combination of a and b. □

Definition 1.2.3 (Relatively prime)**.** Let $a, b \in \mathbb{Z}$. We say a and b are relatively prime if $\gcd(a, b) = 1$.

Proposition 1.2.3. *Let $a, p \in \mathbb{Z}$ such that p is prime and $p \nmid a$, then* $\gcd(a, p) = 1$.

Proof. We will use contradiction. Let $a, p \in \mathbb{Z}$ such that p is prime and $p \nmid a$. Suppose $\gcd(a, p) \neq 1$, then $a = kd$ and $p = ld$ for some $d, k, l \in \mathbb{Z}$ with $d \neq 1$. Since p is prime and $d \neq 1$, then $l = 1$ and $d = p$ by definition 1.1.1. But $a = kd = kp$ if and only if $p \mid a$, contradicting the fact that $p \nmid a$. Therefore, we must conclude that $\gcd(a, p) = 1$. □

2. The Set of All Congruence Classes

Definition 2.0.1 (Congruent [2])**.** Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say that a is congruent to b modulo n if $n \mid (a - b)$, denoted $a \equiv b \pmod{n}$.

Example 2.0.1. Is it true that 34 is congruent to 144 modulo 10? Subtracting 144 from 34, we have $34 - 144 = -110$. Now, does 10 divide this difference? Yes, since $-110 = -11 \cdot 10$. Thus, $34 \equiv 144 \pmod{10}$.

Proposition 2.0.1. *Let $a, b, n \in \mathbb{Z}$. Then the following conditions are all equivalent.*

(1) $a = b + kn$ for some $k \in \mathbb{Z}$;
(2) $n \mid a - b$;
(3) $a \equiv b \pmod{n}$.

Proof. Let $a, b, n \in \mathbb{Z}$. First suppose condition (1). Then $a = b + kn$ implies $a - b = kn$. By the definition of divide, it follows that $n \mid a - b$. Thus, condition (1) implies condition (2).

Now suppose condition (2). Then, by the definition of congruent, $n \mid a - b$ implies $a \equiv b \pmod{n}$. Therefore, condition (2) implies condition (3).

Finally, we would like to show that condition (3) implies condition (1). So, we assume $a \equiv b \pmod{n}$. Then, by the definition of congruent, we know $n \mid a - b$. If follows that there exists $k \in \mathbb{Z}$ such that $a - b = kn$ by the definition of divide. Therefore, condition (3) implies condition (1).

□

Definition 2.0.2 (Congruence Class)**.** Let $a, n \in \mathbb{Z}$ with $n > 0$. We define the congruence class of a modulo n as the set of all integers congruent to a modulo n; that is,

$$\bar{a} := \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}.$$

Definition 2.0.3 ($\mathbb{Z}_n$)**.** Let $n > 0$ be any integer. We define $\mathbb{Z}_n$ to be the set of all congruence classes modulo n, i.e.

$$\mathbb{Z}_n := \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}.$$

Proposition 2.0.2 ($\mathbb{Z}_n \neq \emptyset$)**.** *Let $n > 0$ be any integer. Then $\mathbb{Z}_n \neq \emptyset$.*

Proof. Let $n > 0$ be any integer. Then for $k = 1 \in \mathbb{Z}$, $n = 0 + kn$ implies $n \equiv 0 \pmod{n}$ by proposition 2.0.1. By the definition of congruence classes, it follows that $n \equiv 0 \pmod{n}$ is a member of $\bar{0} \in \mathbb{Z}_n$. Therefore, $\mathbb{Z}_n \neq \emptyset$. □

Proposition 2.0.3. *Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$. Then $\bar{a} = \bar{b}$ if and only if $a \equiv b \pmod{n}$.*

Proof. Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$. First, we would like to show that if $\bar{a} = \bar{b}$, then $a \equiv b \pmod{n}$. Suppose $\bar{a} = \bar{b}$, and let $x \in \bar{a}$. Thus, $x = a + kn$ for some $k \in \mathbb{Z}$ by the definition of congruence classes. Since $\bar{a}$ and $\bar{b}$ are equal sets, then it must be that $x \in \bar{b}$, and so $x = b + ln$ for some $l \in \mathbb{Z}$. Then

$$\begin{aligned} a + kn &= b + ln \\ a - b &= ln - kn \\ a - b &= (l - k)n. \end{aligned}$$

Since $l - k$ is an integer, we conclude that $n \mid a - b$. Thus, by the definition of congruent, $a \equiv b \pmod{n}$.

Conversely, suppose $a \equiv b \pmod{n}$. Then $n \mid a - b$, which means that $a - b = mn$ for some $m \in \mathbb{Z}$. Since m is an integer, it can be written as the sum of two integers, p and q. Hence,

$$\begin{aligned} a - b &= mn \\ a - b &= (p + q)n \\ a - b &= pn + qn \\ a - pn &= b + qn \\ a + (-p)n &= b + qn \end{aligned}$$

Since the left-hand side of this equality is an arbitrary element of $\bar{a}$ and the right-hand side is an arbitrary element of $\bar{b}$, we conclude that these congruence classes must be equal. Therefore, $\bar{a} = \bar{b}$. □

We now define two basic operations $\mathbb{Z}_n$: addition and multiplication.

Definition 2.0.4 (Addition on $\mathbb{Z}_n$)**.** Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$. Then addition on $\mathbb{Z}_n$ is the function $f : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ defined by

$$f[(\bar{a}, \bar{b})] := \overline{a + b},$$

and denoted

$$\bar{a} + \bar{b} := \overline{a + b}.$$

TABLE 1. Group-like Algebraic Structures

	Binary Operation	**Associativity**	**Identity**	**Inverses**	**Commutativity**
Magma	Required	Unneeded	Unneeded	Unneeded	Unneeded
Semigroup	Required	Required	Unneeded	Unneeded	Unneeded
Monoid	Required	Required	Required	Unneeded	Unneeded
Group	Required	Required	Required	Required	Unneeded
Abelian Group	Required	Required	Required	Required	Required

We refer to this addition as addition on $\mathbb{Z}_n$ or addition modulo n.

Definition 2.0.5 (Multiplication on $\mathbb{Z}_n$)**.** Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$. Then multiplication on $\mathbb{Z}_n$ is the function $f : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ defined by

$$f[(\bar{a}, \bar{b})] := \overline{a \cdot b},$$

and denoted

$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}.$$

We refer to this multiplication as multiplication on $\mathbb{Z}_n$ or multiplication modulo n, and use the abbreviation ab for $a \cdot b$.

3. Algebraic Structures with $\mathbb{Z}_n$

Definition 3.0.1 (Binary operation)**.** Let S be a set. We define a binary operation on S to be a function $f : S \times S \to S$ that assigns to each pair $(a, b) \in S \times S$ a unique element $a \circ b \in S$.

A binary operation $\circ$ with the property that $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in S$ is called associative.

3.1. **Magma.**

Definition 3.1.1 (Magma)**.** A magma is a set M together with a binary operation $\circ$ such that for all $a, b \in M$, the unique result of the operation $a \circ b$ is also in M.

Proposition 3.1.1. *Let $n > 0$ be any integer. Then $\mathbb{Z}_n$ is a magma under addition modulo n.*

Proof. Let $n > 0$ be any integer. By proposition 2.0.2, we know that $\mathbb{Z}_n \neq \emptyset$. So, let $\bar{a}, \bar{b} \in \mathbb{Z}_n$. First, we must show that this addition is closed. By the definition of addition on $\mathbb{Z}_n$, we know that $\bar{a} + \bar{b} = \overline{a + b} \in \mathbb{Z}_n$, and so $\mathbb{Z}_n$ is closed under this operation.

Next, we must confirm that this addition assigns a unique element $\bar{a} + \bar{b} \in \mathbb{Z}_n$ to each pair $\bar{a}, \bar{b} \in \mathbb{Z}_n$. Let $\bar{a}', \bar{b}' \in \mathbb{Z}_n$ such that $\bar{a} = \bar{a}'$ and $\bar{b} = \bar{b}'$. Then, by proposition 2.0.1, $a = a' + kn$

and $b = b' + ln$ for some $k, l \in \mathbb{Z}$. Adding both equations, we have $a+b = a'+kn+b'+ln$; which can rewritten as $(a+b) = (a'+b') + mn$ with $m = (k+l) \in \mathbb{Z}$. Again by proposition 2.0.1, we conclude that $a + b \equiv a' + b' \pmod{n}$, and so $\bar{a} + \bar{b} = \overline{a+b} = \overline{a'+b'} = \bar{a}' + \bar{b}'$. Thus, this addition assigns to each pair $(\bar{a}, \bar{b}) \in \mathbb{Z}_n \times \mathbb{Z}_n$ a unique element $\bar{a} + \bar{b} \in \mathbb{Z}_n$. Therefore, $\mathbb{Z}_n$ is a magma under addition modulo n. □

Proposition 3.1.2. *Let $n > 0$ be any integer. Then $\mathbb{Z}_n$ is a magma under multiplication modulo n.*

Proof. Let $n > 0$ be any integer. Then $\mathbb{Z}_n \neq \emptyset$ by proposition 2.0.2. Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$. By the definition of this multiplication, we know $\bar{a} \cdot \bar{b} = \overline{a \cdot b} \in \mathbb{Z}_n$, and so the result of this multiplication is also in $\mathbb{Z}_n$.

Now, we would like to show that this result is unique. So, let $\bar{a}', \bar{b}' \in \mathbb{Z}_n$ with $\bar{a} = \bar{a}'$ and $\bar{b} = \bar{b}'$. Thus, by proposition 2.0.3, we have $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. It follows that n divides both $a - a'$ and $b - b'$, and so $a - a' = kn$ and $b - b' = ln$ for some $k, l \in \mathbb{Z}$. Multiplying the first equality by b and the second by a', we obtain $ba - ba' = bkn$ and $a'b - a'b' = a'ln$. Adding both equations tells us

$$\begin{aligned} ba - ba' + a'b - a'b' &= bkn + a'ln \\ ab - a'b + a'b - a'b' &= (bk + a'l)n \\ ab - a'b' &= mn, \end{aligned}$$

with $m = (bk + a'l) \in \mathbb{Z}$. Hence, $n \mid ab - a'b'$. By proposition 2.0.1, it follows that $\overline{ab} = \overline{a'b'}$, and so $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{a'b'} = \bar{a}' \cdot \bar{b}'$. Thus, each pair $(\bar{a}, \bar{b}) \in \mathbb{Z}_n \times \mathbb{Z}_n$ is mapped to a unique element $\bar{a} \cdot \bar{b} \in \mathbb{Z}_n$. Therefore, $\mathbb{Z}_n$ is a magma under multiplication modulo n. □

3.2. **Semigroup.**

Definition 3.2.1. A semigroup S is an associative magma; that is, $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in S$.

Proposition 3.2.1. *Let $n > 0$ be any integer. Then $\mathbb{Z}_n$ is a semigroup under addition modulo n.*

Proof. Let $n > 0$ be any integer. According to proposition 3.2.1, $\mathbb{Z}_n$ is a magma under addition modulo n. So all we have to show is this addition is associative. So, let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$. Then, by the associativity of addition on the integers, we have

$$(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b} + \bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a} + \overline{b+c} = \bar{a} + (\bar{b} + \bar{c}).$$

Thus, $\mathbb{Z}_n$ is an associative magma, and so we conclude that $\mathbb{Z}_n$ is a semigroup under addition modulo n. □

Proposition 3.2.2. *Let $n > 0$ be any integer. Then $\mathbb{Z}_n$ is a semigroup under multiplication modulo n.*

Proof. Let $n > 0$ be any integer. We know that, under multiplication modulo n, $\mathbb{Z}_n$ is a magma. To show that multiplication on $\mathbb{Z}_n$ is associative, let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$. Then, by the associativity of integer multiplication, we have

$$\begin{aligned}(\bar{a} \cdot \bar{b}) \cdot \bar{c} &= \overline{a \cdot b} \cdot \bar{c} \\ &= \overline{(a \cdot b) \cdot c} \\ &= \overline{a \cdot (b \cdot c)} \\ &= \bar{a} \cdot \overline{b \cdot c} \\ &= \bar{a} \cdot (\bar{b} \cdot \bar{c}).\end{aligned}$$

Therefore, multiplication on $\mathbb{Z}_n$ is associative, and so $\mathbb{Z}_n$ is a semigroup under this operation. □

3.3. **Monoid.**

Definition 3.3.1. A monoid M is a semigroup that has an identity element $e \in M$ such that $e \circ a = a \circ e = a$ for all $a \in M$.

Proposition 3.3.1. *Let $n > 0$ be any integer. Then the set $\mathbb{Z}_n$ forms a monoid under addition modulo n.*

Proof. Let $n > 0$ be any integer. By proposition 3.2.1, $\mathbb{Z}_n$ is a semigroup under addition modulo n. Now we must also show that $\mathbb{Z}_n$ contains an identity element under this operation. We saw in our proof of proposition 2.0.2 that $\bar{0} \in \mathbb{Z}_n$. Let $\bar{a} \in \mathbb{Z}_n$ be arbitrary. Then $\bar{a} + \bar{0} = \overline{a + 0} = \bar{a} = \overline{0 + a} = \bar{0} + \bar{a}$; that is, $\bar{a} + \bar{0} = \bar{a} = \bar{0} + \bar{a}$. Hence, $\bar{0} \in \mathbb{Z}_n$ is an identity element under this addition for all $\bar{a} \in \mathbb{Z}_n$. Therefore, we conclude that the set $\mathbb{Z}_n$ forms a monoid under addition modulo n. □

Proposition 3.3.2. *Let $n > 0$ be any integer. Then the set $\mathbb{Z}_n$ forms a monoid under multiplication modulo n.*

Proof. Let $n > 0$ be any integer. We already know that $\mathbb{Z}_n$ is a semigroup under multiplication modulo n according to proposition 3.2.2. So, all we have left to prove is that $\mathbb{Z}_n$ has an identity element. Since $(n+1) = 1 + kn$ for $k = 1 \in \mathbb{Z}$, we know $(n+1) \equiv 1 \pmod{n}$ by proposition 2.0.1; which is en element in $\bar{1} \in \mathbb{Z}_n$. Thus, $\bar{1} \in \mathbb{Z}_n$. Let $\bar{a} \in \mathbb{Z}_n$. Then, by the commutativity of integer multiplication,

$$\bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a} = \overline{a \cdot 1} = \bar{a} \cdot \bar{1};$$

that is, $\bar{1} \cdot \bar{a} = \bar{a} = \bar{a} \cdot \bar{1}$. Thus, $\mathbb{Z}_n$ has an identity element, namely $\bar{1} \in \mathbb{Z}_n$. Therefore, $\mathbb{Z}_n$ forms a monoid under multiplication modulo n. □

3.4. **Group.**

Definition 3.4.1 (Group)**.** We define a group G to be a monoid that contains an inverse element for each element $a \in G$, denoted by a^{-1}, such that $a \circ a^{-1} = a^{-1} \circ a = e$. A group with the property that $a \circ b = b \circ a$ for $a, b \in G$ is called abelian.

Proposition 3.4.1 (Cancellation laws)**.** *Let G be a group, and let $a, b, c \in G$. Then*

$$b \circ a = c \circ a \text{ implies } b = c \text{ (left cancellation), and}$$

$$a \circ b = a \circ c \text{ implies } b = c \text{ (right cancellation).}$$

Proof. Let G be a group, and let $a, b, c \in G$. Since $a \in G$, then $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$. First, suppose $b \circ a = c \circ a$. Then

$$\begin{aligned} b \circ a &= c \circ a \\ b \circ a \circ a^{-1} &= c \circ a \circ a^{-1} \\ b \circ e &= c \circ e \\ b &= c. \end{aligned}$$

Now suppose $a \circ b = a \circ c$. Then

$$\begin{aligned} a \circ b &= a \circ c \\ a^{-1} \circ a \circ b &= a^{-1} \circ a \circ c \\ e \circ b &= e \circ c \\ b &= c. \end{aligned}$$

Therefore, $b \circ a = c \circ a$ implies $b = c$ and $a \circ b = a \circ c$ implies $b = c$. □

Proposition 3.4.2 (Unique identity)**.** *Let G be a group. Then the identity element $e \in G$ is unique.*

Proof. Let G be a group, let $e \in G$ be the identity element, and let $g \in G$. Suppose $e' \in G$ is also an identity element. Thus, $e \circ g = g$ and $e' \circ g = g$, and so $e \circ g = e' \circ g$. Then, by right cancellation, we have $e = e'$. Therefore, the identity element $e \in G$ is unique □

Proposition 3.4.3 (Unique inverse)**.** *Let G be a group. Then g^{-1} is unique.*

Proof. Let $g, g^{-1}, g'^{-1} \in \mathbb{Z}_n$ with $g \circ g^{-1} = e$ and $g \circ g'^{-1} = e$. Thus, $g \circ g^{-1} = g \circ g'^{-1}$. Then, $g^{-1} = g'^{-1}$ by left cancellation. Therefore, g^{-1} is unique. □

Definition 3.4.2 (Exponential notation)**.** Let G be a group, and let $g \in G$. We first define $g^0 = e$. For $n \in \mathbb{N}, n > 0$, we define

$$g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$$

and

$$g^{-n} = \underbrace{g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}}_{n \text{ times}}.$$

Proposition 3.4.4. *Let G be a group, and let $g, h \in G$. Then, for all $m, n \in \mathbb{Z}$,*

(1) $g^m \circ g^n = g^{m+n}$,
(2) $(g^m)^n = g^{mn}$, *and*
(3) $(g \circ h)^n = (h^{-1} \circ g^{-1})^{-n}$.

Proof. Let G be a group, let $g, h \in G$, and let $m, n \in \mathbb{Z}$. Then, by the definition of exponential notation and the associativity of the group operation, we have

$$\begin{aligned} g^m \circ g^n &= \underbrace{(g \circ g \circ \cdots \circ g)}_{m \text{ times}} \circ \underbrace{(g \circ g \circ \cdots \circ g)}_{n \text{ times}} \\ &= \underbrace{g \circ g \circ \cdots \circ g \circ g \circ g \circ \cdots \circ g}_{m+n \text{ times}} \\ &= g^{m+n} \end{aligned}$$

and

$$\begin{aligned} (g^m)^n &= \underbrace{g^m \circ g^m \circ \cdots \circ g^m}_{n \text{ times}} \\ &= \underbrace{\overbrace{(g \circ g \circ \cdots \circ g)}^{m \text{ times}} \circ \overbrace{(g \circ g \circ \cdots \circ g)}^{m \text{ times}} \circ \cdots \circ \overbrace{(g \circ g \circ \cdots \circ g)}^{m \text{ times}}}_{n \text{ times}} \\ &= \underbrace{g \circ g \circ \cdots \circ g \circ g \circ g \circ \cdots \circ g \circ \cdots \circ g \circ g \circ \cdots \circ g}_{mn \text{ times}} \\ &= g^{mn} \end{aligned}$$

for the first and second equalities. Before continuing, we observe that

$$\begin{aligned} (h^{-1} \circ g^{-1}) \circ (g \circ h) &= h^{-1} \circ g^{-1} \circ g \circ h && \text{(associativity of group operation)} \\ &= h^{-1} \circ e \circ h \\ &= h^{-1} \circ h \circ e && \text{(since } e \circ h = h \circ e\text{)} \\ &= e \circ e \\ &= e. \end{aligned}$$

Thus, $(h^{-1} \circ g^{-1})^{-1} = (g \circ h)$. It follows that

$$\begin{aligned} (h^{-1} \circ g^{-1})^{-n} &= \underbrace{(h^{-1} \circ g^{-1})^{-1} \circ (h^{-1} \circ g^{-1})^{-1} \circ \cdots \circ (h^{-1} \circ g^{-1})^{-1}}_{n \text{ times}} \\ &= \underbrace{(g \circ h) \circ (g \circ h) \circ \cdots \circ (g \circ h)}_{n \text{ times}} \\ &= (g \circ h)^n. \end{aligned}$$

□

Proposition 3.4.5. *Let $n > 0$ be any integer. Then the set $\mathbb{Z}_n$ forms an abelian group under addition modulo n.*

Proof. Let $n > 0$ be any integer. According to proposition 3.3.1, $\mathbb{Z}_n$ is a monoid under addition modulo n. Now we must show that the set $\mathbb{Z}_n$ contains an inverse element for each of its members. Let $\bar{a} \in \mathbb{Z}_n$. Then since $(n-a) = (n-a) + kn$ for $k = 0 \in \mathbb{Z}$ implies that $(n-a) \equiv (n-a) \pmod{n}$, we know that $\overline{a-n} \in Z_n$ by the definition of congruence classes. Adding both of these elements, we have

$$\begin{aligned}
\bar{a} + \overline{n-a} &= \overline{a+n-a} \\
&= \overline{a+(-a)+n} \\
&= \bar{n} \\
&= \overline{n+a-a} \\
&= \overline{n+(-a)+a} \\
&= \overline{n-a} + \bar{a}
\end{aligned}$$

by the commutativity of addition on the integers. Hence, $\bar{a} + \overline{n-a} = \overline{n-a} + \bar{a} = \bar{a}$, and so $\mathbb{Z}_n$ is a group under this operation.

To show that it is abelian, let $\bar{b} \in \mathbb{Z}_n$. Again by the commutativity of integer addition, we have

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}.$$

Since both of these elements were arbitrary, we conclude that this must be true for all elements in $\mathbb{Z}_n$. Therefore, $\mathbb{Z}_n$ forms an abelian group under addition modulo n. □

3.5. **Ring.**

Definition 3.5.1 (Ring)**.** Let R be an abelian group. Then R is a ring if it satisfies the following axioms:

(1) R forms a monoid under a second binary operation $\circ$ that distributes over the group operation, and
(2) the additive identity $0 \in R$ satisfies $0 \circ a = 0$ for all $a \in R$.

Proposition 3.5.1. *Let $n > 0$ be any integer. Then $\mathbb{Z}_n$ forms a ring under addition modulo n and multiplication modulo n.*

Proof. Let $n > 0$ be any integer. Then, by proposition 3.4.5, $\mathbb{Z}_n$ forms an abelian group under addition modulo n. Moreover, $\mathbb{Z}_n$ also forms a monoid under multiplication modulo n — a second binary operation. Next we must show that this multiplication distributes over this addition. Let $\bar{a}, \bar{b}, \bar{c} \in R$. Since multiplication distributes over addition on the integers,

we have

$$\begin{aligned}\bar{a} \cdot (\bar{b} + \bar{c}) &= \bar{a} \cdot \overline{b + c} \\ &= \overline{a(b + c)} \\ &= \overline{a \cdot b + ac} \\ &= \overline{a \cdot b} + \overline{a \cdot c} \\ &= \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}\end{aligned}$$

for left distribution, and

$$\begin{aligned}(\bar{a} + \bar{b}) \cdot \bar{c} &= \overline{a + b} \cdot \bar{c} \\ &= \overline{(a + b)c} \\ &= \overline{a \cdot c + b \cdot c} \\ &= \overline{a \cdot c} + \overline{b \cdot c} \\ &= \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}\end{aligned}$$

for right distribution. Thus, this multiplication distributes over addition modulo n.

Lastly, since $\bar{0} \cdot \bar{a} = \overline{0 \cdot a} = \bar{0}$, we conclude that the product of the additive identity, $\bar{0} \in R$, and any element in R is equal to $\bar{0}$. Therefore, $\mathbb{Z}_n$, together with this addition and this multiplication, forms a ring. □

3.6. **Field.**

Definition 3.6.1 (Field)**.** Let F be a ring under two commutative binary operations. If every nonzero element in R has a multiplicative inverse, then we say F is a field.

Lemma 3.6.1. *Let p be prime. If $\bar{a} \in \mathbb{Z}_p$ such that $\bar{a} \neq \bar{0}$, then* $\gcd(a, p) = 1$.

Proof. Let p be prime, and let $\bar{a} \in \mathbb{Z}_p$ such that $\bar{a} \neq \bar{0}$. Now suppose for the sake of contradiction that $p \mid a$. Then $a = lp$ for some $l \in \mathbb{Z}$. By definition 2.0.2,

$$\bar{a} = \{a + kp : k \in \mathbb{Z}\} = \{lp + kp : k \in \mathbb{Z}\} = \{0 + (l + k)p : k \in \mathbb{Z}\} = \bar{0},$$

and so $\bar{a} = \bar{0}$. But we know $\bar{a} \neq \bar{0}$ and because of this contradiction we must conclude $p \nmid a$. Therefore, by **????**, $\gcd(a, p) = 1$. □

Theorem 3.6.1. *Let p be prime. Then $\mathbb{Z}_p$ forms a field under addition modulo n and multiplication module n.*

Proof. Let p be prime. Since primes are integers greater than 1 and we know, by proposition 3.5.1, $\mathbb{Z}_n$ is a ring for any integer $n > 1$, then $\mathbb{Z}_p$ is a ring. Furthermore, this addition modulo n is commutative since the underlying set of a ring forms an abelian group under this operation. Now we must show that multiplication modulo n is also commutative. Let $\bar{a}, \bar{b} \in \mathbb{Z}_p$. Then, by the commutativity of integer multiplication, $\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \cdot \bar{a}$ as required.

Lastly, we will confirm that every nonzero element in $\mathbb{Z}_p$ has a multiplicative inverse. So, suppose $\bar{a} \neq \bar{0}$. Then by **??**, we have $\gcd(a, p) = 1$. Moreover, this implies that $ax + py = 1$ according to proposition 1.2.2. It follows that $ax = 1 + (-y)p$; that is, $ax \equiv 1 \pmod{p}$ by proposition 2.0.1. Hence, $\overline{a \cdot x} = \bar{a} \cdot \bar{x} = \bar{1}$. Therefore, every nonzero element in $\mathbb{Z}_p$ has a multiplicative inverse, and so we conclude that $\mathbb{Z}_p$ is a field. □

Corollary 3.6.1 (Zero product property)**.** *Let p be prime. If $\bar{a} \cdot \bar{b} = \bar{0}$, then either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$ for all $\bar{a}, \bar{b} \in \mathbb{Z}_p$.*

Proof. Let p be prime, and let $\bar{a}, \bar{b} \in \mathbb{Z}_p$ such that $\bar{a} \cdot \bar{b} = \bar{0}$. If both $\bar{a} = \bar{0}$ and $\bar{b} = \bar{0}$, then

$$\bar{a} \cdot \bar{b} = \bar{0} \cdot \bar{0} = \overline{0 \cdot 0} = \bar{0}.$$

Now let's suppose that $\bar{a}, \bar{b}$ are both not zero. It follows from theorem 3.6.1 that every nonzero element in $\mathbb{Z}_p$ has a multiplicative inverse. So, we proceed with two cases.

Case 1. If $\bar{a} \neq \bar{0}$, then

$$\begin{aligned} \bar{a} \cdot \bar{b} &= \bar{0} \\ \bar{a}^{-1} \cdot \bar{a} \cdot \bar{b} &= \bar{a}^{-1} \cdot \bar{0} \\ \bar{1} \cdot \bar{b} &= \bar{0} \\ \bar{b} &= \bar{0}. \end{aligned}$$

Case 2. If $\bar{b} \neq \bar{0}$, then

$$\begin{aligned} \bar{a} \cdot \bar{b} &= \bar{0} \\ \bar{a} \cdot \bar{b} \cdot \bar{b}^{-1} &= \bar{0} \cdot \bar{b}^{-1} \\ \bar{a} \cdot \bar{1} &= \bar{0} \\ \bar{a} &= \bar{0}. \end{aligned}$$

Therefore, if $\bar{a} \cdot \bar{b} = \bar{0}$, then either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$ for all $\bar{a}, \bar{b} \in \mathbb{Z}_p$.

□

4. A Probabilistic Test for Compositeness

4.1. Fermat's Little Theorem.

Lemma 4.1.1. *Let p be prime. Then for each $\bar{a} \in \mathbb{Z}_p$ with $\bar{a} \neq \bar{0}$, there exists a unique multiplicative inverse.*

Proof. Let p be prime, and let $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. Since $\mathbb{Z}_p$ is a field, we know $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}_p$. Suppose both $\bar{x}, \bar{y} \in \mathbb{Z}_p$ are multiplicative inverses of $\bar{a}$. Then $\bar{a} \cdot \bar{x} = \bar{1}$ and $\bar{a} \cdot \bar{y} = \bar{1}$. Thus, $\bar{a} \cdot \bar{x} = \bar{a} \cdot \bar{y}$, and by left cancellation we have $\bar{x} = \bar{y}$. Therefore, for each $\bar{a} \in \mathbb{Z}_p$ with $\bar{a} \neq \bar{0}$, there exists a unique multiplicative inverse. □

TABLE 2. Multiplication in $\mathbb{Z}_7$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

TABLE 3. Multiplication in $\mathbb{Z}_8$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Lemma 4.1.2. *Let p be prime. If $\bar{a} \in \mathbb{Z}_p$ is its own multiplicative inverse, then $\bar{a} = \bar{1}$ or $\bar{a} = \overline{p-1}$.*

Proof. Let $p \in \mathbb{N}$ be prime, and let $\bar{a} \in \mathbb{Z}_p$ be its own multiplicative inverse. Then $\bar{a} \cdot \bar{a} = \bar{a}^2 = \bar{1}$; that is, $\bar{a}^2 - \bar{1} = (\bar{a}+\bar{1})(\bar{a}-\bar{1}) = \bar{0}$. By corollary 3.6.1, since $\bar{a}+\bar{1} \in \mathbb{Z}_p$ and $\bar{a}-\bar{1} \in \mathbb{Z}_p$ and $(\bar{a}+\bar{1})(\bar{a}-\bar{1}) = \bar{0}$, then either $(\bar{a}+\bar{1}) = \bar{0}$ or $(\bar{a}-\bar{1}) = \bar{0}$. We will consider both cases.

Case 1. If $(\bar{a}+\bar{1}) = \bar{0}$, then $\bar{a} = -\bar{1} = \overline{p-1}$.

Case 2. If $(\bar{a}-\bar{1}) = \bar{0}$, then $\bar{a} = \bar{1}$.

Therefore, $\bar{a} = \bar{1}$ or $\bar{a} = \overline{p-1}$. □

Theorem 4.1.1 (Fermat's Little Theorem [2])**.** *Let p be prime, and let $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. Then*

$$\bar{a}^{p-1} = \bar{1}.$$

Proof. Let p be prime, and let $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. By lemma 4.1.1, we know that $\mathbb{Z}_p$ contains a unique inverse for each of its elements. Furthermore, $\bar{1}^{-1} = \bar{1}$ and $\overline{p-1}^{-1} = \overline{p-1}$ by lemma 4.1.2. Thus, $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{p-1} = \bar{1} \cdot \overline{p-1} = \overline{p-1}$. Then

$$\begin{aligned}(\bar{a} \cdot \bar{1})(\bar{a} \cdot \bar{2}) \cdots (\bar{a} \cdot \overline{p-1}) &= \underbrace{\bar{a} \cdot \bar{a} \cdots \bar{a}}_{p-1 \text{ times}} \cdot \bar{1} \cdot \bar{2} \cdots \bar{a} \cdots \bar{a}^{-1} \cdots \overline{p-1} \\ &= \bar{a}^{p-1} \cdot \overline{p-1}.\end{aligned}$$

Moreover, since this multiplication is a binary operation, we know that each product is equal to a unique element in $\mathbb{Z}_p$. Thus, $(\bar{a} \cdot \bar{1})(\bar{a} \cdot \bar{2}) \cdots (\bar{a} \cdot \overline{p-1}) = \bar{1} \cdot \bar{2} \cdots \overline{p-1}$, where the

right-hand side is some permutation of the elements in $\mathbb{Z}_p$. Hence,

$$\begin{aligned}
\bar{a}^{p-1} \cdot \overline{p-1} &= \bar{1} \cdot \bar{2} \cdots \overline{p-1} \\
\bar{a}^{p-1} \cdot \overline{p-1} &= \overline{p-1} \\
\bar{a}^{p-1} \cdot \overline{p-1} \cdot \overline{p-1} &= \overline{p-1} \cdot \overline{p-1} \\
\bar{a}^{p-1} \cdot \bar{1} &= \bar{1} \\
\bar{a}^{p-1} &= \bar{1}.
\end{aligned}$$

Therefore, if p is prime, then $\bar{a}^{p-1} = \bar{1}$ for all $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. □

4.2. **Miller-Rabin Test.**

Example 4.2.1. Since 29 is prime, we know that $\bar{a}^{28} = \bar{1}$ for all $\bar{a} \in \mathbb{Z}_{29}$ by theorem 4.1.1. In other words, $\bar{a}^{28} - \bar{1} = \bar{0}$. Since $\mathbb{Z}_{29}$ is a field, this polynomial can be factored using the difference of squares. Then

$$\begin{aligned}
\bar{a}^{28} - \bar{1} &= (\bar{a}^{14} + \bar{1})(\bar{a}^{14} - \bar{1}) \\
&= (\bar{a}^{14} + \bar{1})(\bar{a}^{7} + \bar{1})(\bar{a}^{7} - \bar{1}) \\
&= \bar{0}.
\end{aligned}$$

Since 7 is odd, it is not possible to use the difference of squares to factor $(\bar{a}^7 - \bar{1})$ any further. By corollary 3.6.1, we know $(\bar{a}^{14} + \bar{1})(\bar{a}^7 + \bar{1})(\bar{a}^7 - \bar{1}) = \bar{0}$ implies that either $(\bar{a}^{14} + \bar{1}) = \bar{0}$ or $(\bar{a}^7 + \bar{1}) = \bar{0}$ or $(\bar{a}^7 - \bar{1}) = \bar{0}$. Even if we randomly select an $\bar{a} \in \mathbb{Z}_{29}$, we expect this to still be true. So, let $\bar{a} = \bar{7}$. Then we have

$$\begin{aligned}
(\bar{7}^{14} + \bar{1}) &= \bar{2} \\
(\bar{7}^{7} + \bar{1}) &= \bar{2} \\
(\bar{7}^{7} - \bar{1}) &= \bar{0},
\end{aligned}$$

as we expected.

Algorithm 4.2.1 (Miller-Rabin Test for Compositeness)**.** *Let $n \geq 3$ be any odd integer. Then there exists an integer $k > 0$ such that 2^k is the largest power of two that divides $n-1$. If there exists $\bar{a} \in \mathbb{Z}_n$ such that*

$$\bar{a}^{\frac{n-1}{2^k}} \neq \bar{1}$$

and

$$\bar{a}^{\frac{n-1}{2^h}} \neq -\bar{1},$$

for all $h \in \mathbb{Z} : 1 \leq h \leq k$, then n is composite. In this case, the integer a is called a Miller-Rabin witness to the compositeness of n.

Example 4.2.2. We would like to use algorithm 4.2.1 to test the compositeness of 169. Since 2^3 is the largest power of two that divides 168, we must find an $\bar{a} \in \mathbb{Z}_{169}$ such that $\bar{a}^{\frac{168}{2^3}} \neq \bar{1}$ and $\bar{a}^{\frac{168}{2^h}} \neq -\bar{1}$ for all h, $h = 1, 2, 3$. So, we randomly choose $\overline{19} \in \mathbb{Z}_{169}$ and find

that

$$\overline{19}^{\frac{168}{2^3}} = \overline{70}$$
$$\overline{19}^{\frac{168}{2^2}} = -\bar{1}$$
$$\overline{19}^{\frac{168}{2^1}} = \bar{1}.$$

Because $\overline{19}^{\frac{168}{2^2}} = -\bar{1}$, we cannot conclude that 169 is composite. So we randomly select a different $\bar{a} \in \mathbb{Z}_{169}$, namely $\bar{a} = \overline{145}$, and this time discover that

$$\overline{145}^{\frac{168}{2^3}} = \overline{18}$$
$$\overline{145}^{\frac{168}{2^2}} = \overline{155}$$
$$\overline{145}^{\frac{168}{2^1}} = \overline{27}.$$

Hance, 145 is a Miller-Rabin witness to the compositeness of 169 and we conclude that 169 is not prime.

4.3. **Effectiveness of the Miller-Rabin Test.**

5. Support Vector Machine for Binary Classification

Definition 5.0.1 (Support Vector Machine)**.** A Support Vector Machine (SVM) is a learning system that uses a hypothesis space of linear functions in a high dimensional feature space, trained with a learning algorithm from optimisation theory that implements a learning bias derived from statistical learning theory.[1]

- target function — underlying function that maps inputs to outputs (if it exists)
- solution — estimate of the target function by learning algorithm (also called the decision function in classification algorithms)
- hypothesis space — a set or class of candidate solutions (known as hypotheses)
- learning algorithm — uses training data to select a hypothesis
- features — the quantities used to describe the data
- attributes — original quantities from data

"SVM decision function depends on some subset of the training data, called the support vectors."

5.1. **Kernel Induced Feature Spaces.** "Project the data into a higher dimensional feature space to increase the computational power of the linear learning machines." [1]

Definition 5.1.1 (Kernel [1])**.** A kernel is a function K, such that for all $x, z \in X$

$$K(x, z) = (\phi(x) \cdot \phi(z)),$$

where ϕ is a mapping from X to an (inner product) feature space F.

Example 5.1.1. Map input space into new space.

"not scale invariant, so it is highly recommended to scale your data. For example, scale each attribute on the input vector X to [0,1] or [-1,+1], or standardize it to have mean 0 and variance 1."

5.2. **Learning Bias.**

5.3. **Learning Algorithm.**

6. Method

6.1. **Features.**

Training Data. We will use $X \subset \mathbb{R}^n$ and $Y = (-1, 1)$ for binary classification.

Definition 6.1.1 (Training Set)**.** A **training set** is a collection of training examples, which are also called training data. It is usually denoted by $S = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\} \subset X \times Y$, where n is the number of examples. We refer to x_i as examples or instances and y_i as their labels.[1]

Base-b Representations.

Theorem 6.1.1 (Well Ordering Principle)**.** *Every nonempty set of positive integers contains a smallest member.* [4]

Proof. Let $A \subseteq \mathbb{Z}^+ : A \neq \emptyset$. Assume for the sake of contradiction that A does not have a smallest member. Then $1 \notin A$ since $1 \leq n$ for all $n \in \mathbb{Z}^+$. Now we assume positive integers $1, 2, \ldots, k \notin A$. Then $k + 1 \notin A$ since $k + 1$ would be the smallest member of A. Thus, by strong induction $A = \emptyset$, a contradiction. Therefore, A must contain a smallest member. $\square$

Theorem 6.1.2 (The Division Algorithm)**.** *Let $a, b \in \mathbb{Z} : b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.* [2]

Proof. Let $a, b \in \mathbb{Z} : b > 0$, and let $R = \{x \in \mathbb{Z} : a - xb \geq 0\}$. First, we notice that $R \neq \emptyset$ for if $a \leq 0$ and $x = a$ then $a - ab = a(1 - b) \geq 0$, and if $a > 0$ and $x = 0$ then $a - 0 \cdot b \geq 0$.

Thus, by theorem 6.1.1, R contains a smallest member, which we will call r. Hence, $\exists q \in \mathbb{Z} : r = a - qb \geq 0$. Now suppose for the sake of contradiction that $r \geq b$. Then $r = b + n \geq 0$ for some $n \in \mathbb{Z} : n \geq 0$. Hence, $r = b + n = a - qb$ or $n = a - qb - b = a - (q + 1)b \in R$. But $n = a - (q + 1)b < a - ab = r$ is impossible since r is the smallest member of R. So, it must be that $r < b$. Therefore, we have found $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

To complete the proof, we must show that q and r are unique. So, we let $q', r' \in \mathbb{Z}$ and assume $a = q'b + r'$ such that $0 \leq r' < b$. Thus, $a = qb - r = q'b + r'$. In other words, $r - r' = q'b - qb$ or $r - r' = b(q' - q)$. Without loss of generality, we may assume that $r' \leq r$ such that $0 \leq r - r' \leq r < b$. Therefore, $r - r'$ must be a nonnegative multiple of b,

such as $0, b, 2b, 3b, \ldots$, but $r - r' < b$ implies that $r - r' = 0$ or $r = r'$. Also, since $b > 0$, $r - r' = 0 = b(q' - q) = b \cdot 0$. Thus, $q' - q = 0$ or $q' = q$. Therefore, q and r are unique.

□

Corollary 6.1.1. *Let $b \in \mathbb{Z} : b \geq 2$. Then every $N \in \mathbb{Z} : N > 0$ can be expressed uniquely in the form $N = a_k b^k + a_{k-1} b^{b-1} + \cdots + a_1 b + a_0$, where $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, $a_k \neq 0$, and $k \geq 0$.* [3]

6.2. **Training.**

Finding the Best Parameters.

- C: penalty parameter C of the error term
- kernel:
  - linear
  - polynomial
  - rbf
  - sigmoid
- degree: int, degree of polynomial kernel function for 'poly'
- gamma: kernel coefficients for 'rbf', 'poly' and 'sigmoid'
- coef0: independent term in kernel function for 'poly' and 'sigmoid'
- probability: whether to enable probability estimates
- shrinking: whether to use the shrinking heuristic
- tol: tolerance for stopping criterion
- cache_size: specify the size of the kernel cache in MB
- class_weight: if not given, all classes are suppose to have weight one
- verbose: enable verbose output
- max_iter: hard limit on iterations within solver, or -1 for no limit
- decision_function_shape: for more than 2 classes
- random_state: the seed of the pseudo random generator to use when shuffling the data for probability estimation

6.3. **Testing.**

7. Conclusion

```
def fermats_test(n):
        nonwitnesses = []
        witnesses = []
        for a in range(1,n):
                right_hand_side = pow(a,n-1,n)
                if right_hand_side is 1:
                        nonwitnesses.append(a)
                else:
                        witnesses.append(a)
        return [nonwitnesses, witnesses]
```

Between 1 and 560 (inclusive), we have 320 integers a such that for $\bar{a} \in \mathbb{Z}_{561}$, we have $\bar{a}^{650} = \bar{1}$.

1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 19, 20, 23, 25, 26, 28, 29, 31, 32, 35, 37, 38, 40, 41, 43, 46, 47, 49, 50, 52, 53, 56, 58, 59, 61, 62, 64, 65, 67, 70, 71, 73, 74, 76, 79, 80, 82, 83, 86, 89, 91, 92, 94, 95, 97, 98, 100, 101, 103, 104, 106, 107, 109, 112, 113, 115, 116, 118, 122, 124, 125, 127, 128, 130, 131, 133, 134, 137, 139, 140, 142, 145, 146, 148, 149, 151, 152, 155, 157, 158, 160, 161, 163, 164, 166, 167, 169, 172, 173, 175, 178, 179, 181, 182, 184, 185, 188, 190, 191, 193, 194, 196, 197, 199, 200, 202, 203, 205, 206, 208, 211, 212, 214, 215, 217, 218, 223, 224, 226, 227, 229, 230, 232, 233, 235, 236, 239, 241, 244, 245, 247, 248, 250, 251, 254, 256, 257, 259, 260, 262, 263, 265, 266, 268, 269, 271, 274, 277, 278, 280, 281, 283, 284, 287, 290, 292, 293, 295, 296, 298, 299, 301, 302, 304, 305, 307, 310, 311, 313, 314, 316, 317, 320, 322, 325, 326, 328, 329, 331, 332, 334, 335, 337, 338, 343, 344, 346, 347, 349, 350, 353, 355, 356, 358, 359, 361, 362, 364, 365, 367, 368, 370, 371, 373, 376, 377, 379, 380, 382, 383, 386, 388, 389, 392, 394, 395, 397, 398, 400, 401, 403, 404, 406, 409, 410, 412, 413, 415, 416, 419, 421, 422, 424, 427, 428, 430, 431, 433, 434, 436, 437, 439, 443, 445, 446, 448, 449, 452, 454, 455, 457, 458, 460, 461, 463, 464, 466, 467, 469, 470, 472, 475, 478, 479, 481, 482, 485, 487, 488, 490, 491, 494, 496, 497, 499, 500, 502, 503, 505, 508, 509, 511, 512, 514, 515, 518, 520, 521, 523, 524, 526, 529, 530, 532, 533, 535, 536, 538, 541, 542, 545, 547, 548, 551, 553, 554, 556, 557, 559, 560

There are 240 Fermat's witnesses to the compositeness of 561, namely all the multiples of 3, 11, 17 that are less than or equal to 560.

3, 6, 9, 11, 12, 15, 17, 18, 21, 22, 24, 27, 30, 33, 34, 36, 39, 42, 44, 45, 48, 51, 54, 55, 57, 60, 63, 66, 68, 69, 72, 75, 77, 78, 81, 84, 85, 87, 88, 90, 93, 96, 99, 102, 105, 108, 110, 111, 114, 117, 119, 120, 121, 123, 126, 129, 132, 135, 136, 138, 141, 143, 144, 147, 150, 153, 154, 156, 159, 162, 165, 168, 170, 171, 174, 176, 177, 180, 183, 186, 187, 189, 192, 195, 198, 201, 204, 207, 209, 210, 213, 216, 219, 220, 221, 222, 225, 228, 231, 234, 237, 238, 240, 242, 243, 246, 249, 252, 253, 255, 258, 261, 264, 267, 270, 272, 273, 275, 276, 279, 282, 285, 286, 288,

List of Figures

List of Tables

References

[1] Nello Cristianini and John Shawe-Taylor. An introduction to support vector machines: and other kernel-based learning methods. Cambridge University Press, Cambridge, U.K., 2012.

[2] T. Marks J. Pommersheim and E. Flapan. Number Theory: A Lively Introduction with Proofs, Applications, and Stories. John Wiley & Sons, 2010.

[3] T. Koshy. Elementary Number Theory with Applications. Harcoutrt/Academic Press, 2002.

[4] Eric W. Weisstein. "Well Ordering Principle." From MathWorld–A Wolfram Web Resource.

E-mail address: math@miguelamezola.com