Testing for Compositeness

Miller-Rabin vs Support Vector Machine Classification

Miguel Amezola

Department of Mathematics
Pacific Lutheran University

May 11, 2017

Overview

"The problem of distinguishing prime numbers from composite numbers . . . is known to be one of the most important and useful in arithmetic. . . . Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated." — *Disquisitiones Arithmeticae (1801): Article 329*

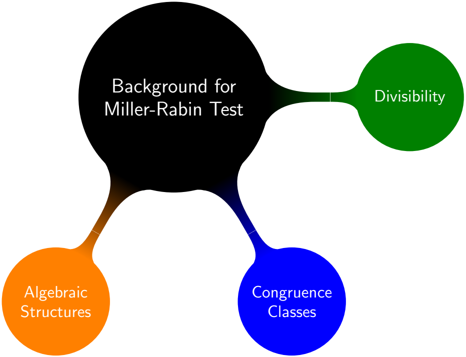
Binary Classification

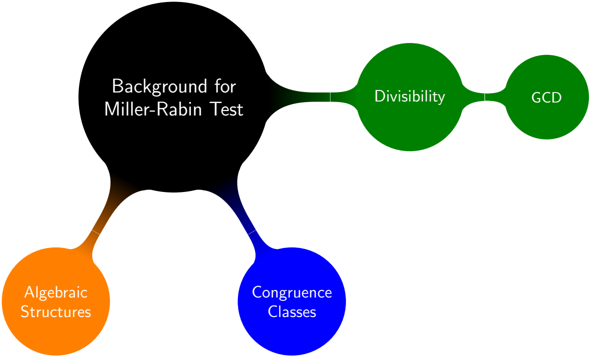
Definition (Prime)

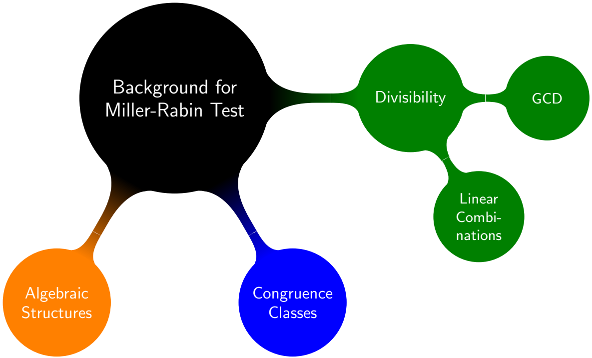
Let $p \in \mathbb{Z}$ with $p > 1$. If $p = ab$ implies $a = 1$ or $b = 1$ for all $a, b \in \mathbb{Z}$, then p is prime. [2]

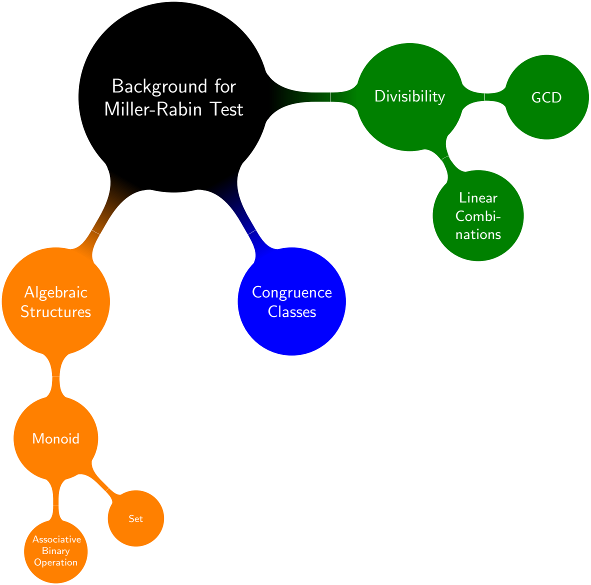
Definition (Composite)

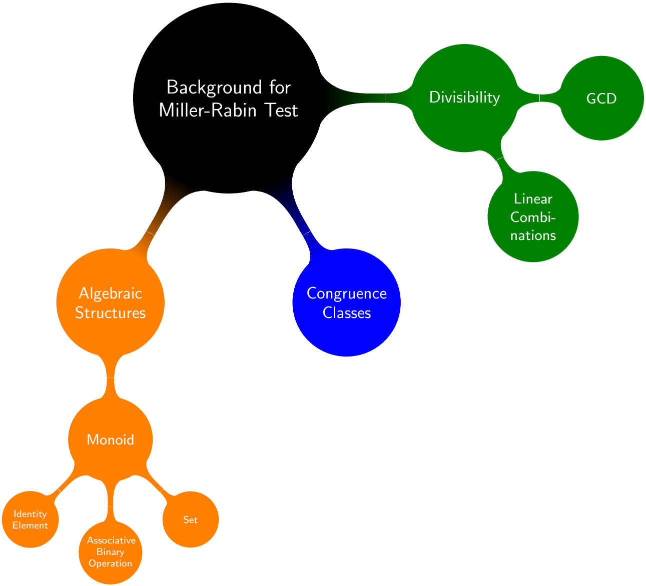
Let $n \in \mathbb{Z}$ with $n > 1$. If there exists $a, b \in \mathbb{Z}$ such that $n = ab$ with $1 < a, b < n$, then n is composite. [2]

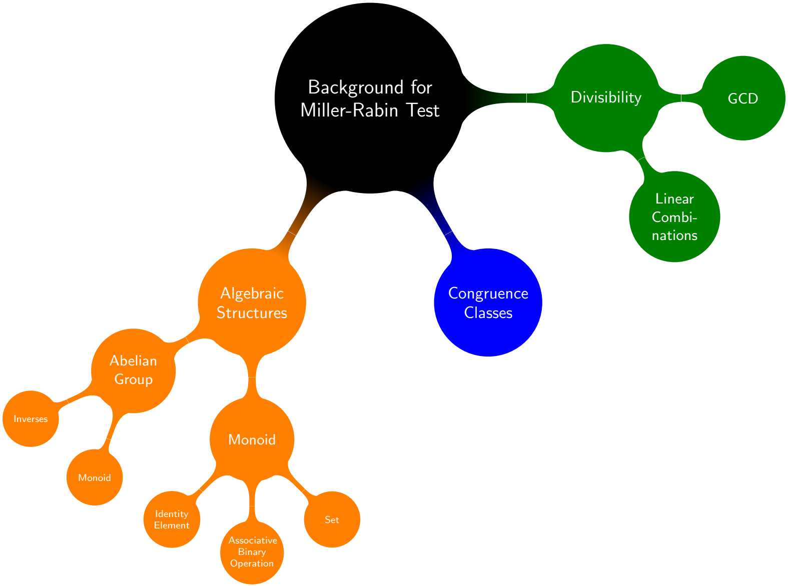

Background for Miller-Rabin Test
Divisibility
Algebraic Structures
Congruence Classes

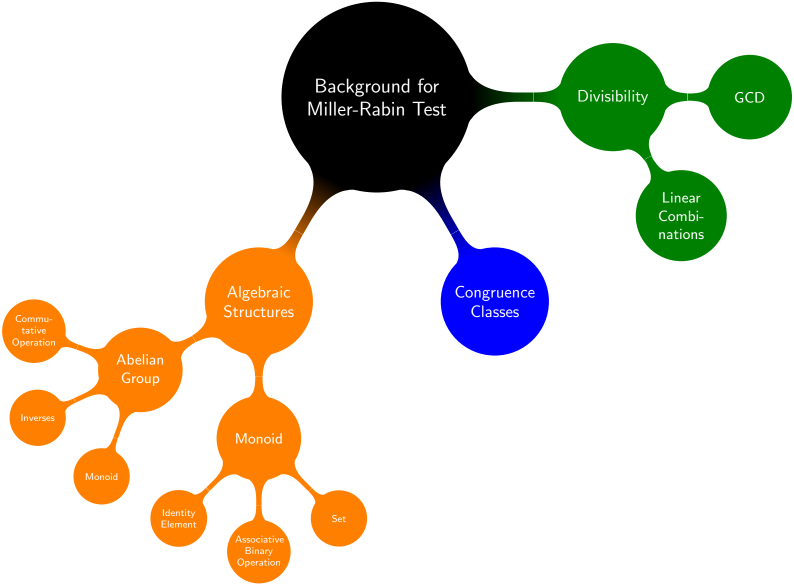

Background for Miller-Rabin Test
Divisibility
GCD
Algebraic Structures
Congruence Classes

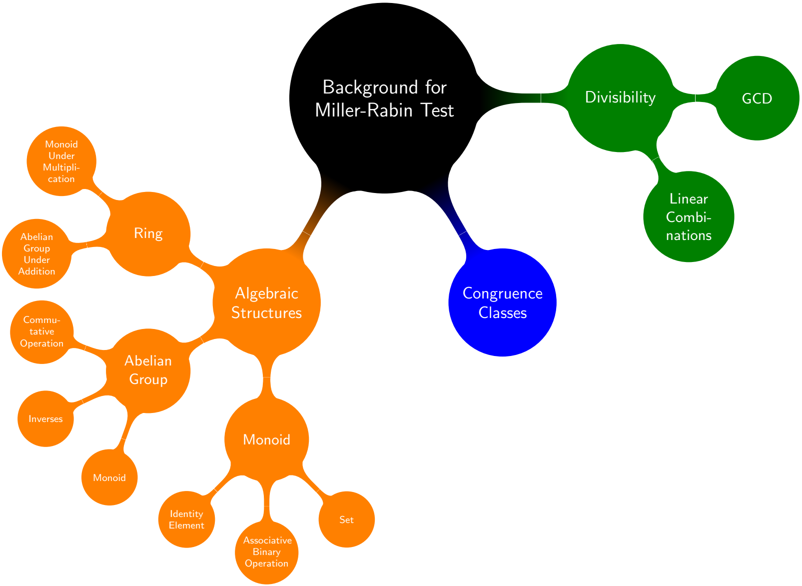

Background for Miller-Rabin Test
Divisibility
GCD
Linear Combi-nations
Algebraic Structures
Congruence Classes

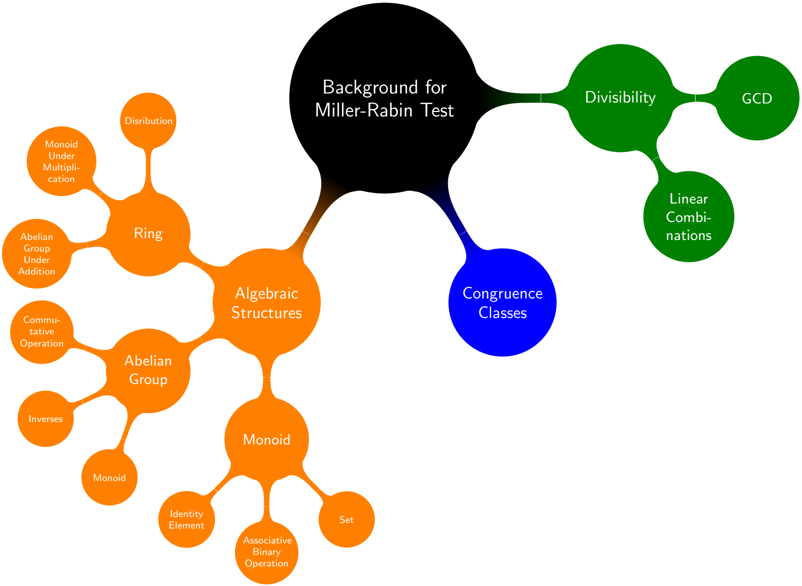

Background for Miller-Rabin Test
Divisibility
GCD
Linear Combi- nations
Congruence Classes
Algebraic Structures
Monoid
Set
Associative Binary Operation


Background for Miller-Rabin Test
Divisibility
GCD
Linear Combi-nations
Congruence Classes
Algebraic Structures
Monoid
Identity Element
Associative Binary Operation
Set


Background for Miller-Rabin Test
Divisibility
GCD
Linear Combi- nations
Congruence Classes
Algebraic Structures
Abelian Group
Inverses
Monoid
Monoid
Identity Element
Associative Binary Operation
Set


Background for Miller-Rabin Test
Divisibility
GCD
Linear Combi-nations
Congruence Classes
Algebraic Structures
Abelian Group
Commu-tative Operation
Inverses
Monoid
Monoid
Identity Element
Associative Binary Operation
Set


Background for Miller-Rabin Test
Divisibility
GCD
Linear Combi-nations
Congruence Classes
Algebraic Structures
Ring
Monoid Under Multipli-cation
Abelian Group Under Addition
Abelian Group
Commu-tative Operation
Inverses
Monoid
Monoid
Identity Element
Associative Binary Operation
Set


Background for Miller-Rabin Test
Divisibility
GCD
Linear Combi- nations
Congruence Classes
Algebraic Structures
Ring
Disribution
Monoid Under Multipli- cation
Abelian Group Under Addition
Abelian Group
Commu- tative Operation
Inverses
Monoid
Monoid
Identity Element
Associative Binary Operation
Set

Overview

Congruence Example

Definition (Congruent)

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 $a \equiv b \pmod{n}$. [2]

Example

Is 34 congruent to 4 modulo 10?

Congruence Example

Definition (Congruent)

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 $a \equiv b \pmod{n}$. [2]

Example

Is 34 congruent to 4 modulo 10?
Subtracting 4 from 34, we have $34 - 4 = 30$.

Congruence Example

Definition (Congruent)

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 $a \equiv b \pmod{n}$. [2]

Example

Is 34 congruent to 4 modulo 10?
Subtracting 4 from 34, we have $34 - 4 = 30$.
Does 10 divide this difference?

Congruence Example

Definition (Congruent)

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 $a \equiv b \pmod{n}$. [2]

Example

Is 34 congruent to 4 modulo 10?
Subtracting 4 from 34, we have $34 - 4 = 30$.
Does 10 divide this difference?
Yes, since $30 = 3 \cdot 10$.

Congruence Example

Definition (Congruent)

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 $a \equiv b \pmod{n}$. [2]

Example

Is 34 congruent to 4 modulo 10?
Subtracting 4 from 34, we have $34 - 4 = 30$.
Does 10 divide this difference?
Yes, since $30 = 3 \cdot 10$.
Thus, $34 \equiv 4 \pmod{10}$.

The Set of All Congruence Classes

Definition (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,

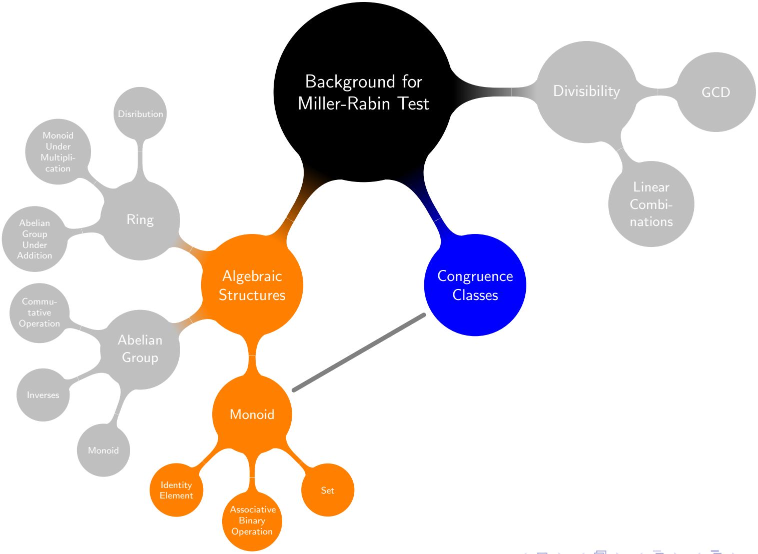
$$\bar{a} := \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}.$$

Definition ($\mathbb{Z}_n$)

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

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

$\mathbb{Z}_n$ Is a Monoid under Multiplication



$\mathbb{Z}_n$ Is a Monoid under Multiplication

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

$\mathbb{Z}_n$ Is a Monoid under Multiplication

- $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$.
- By the associativity of integer multiplication, we have

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

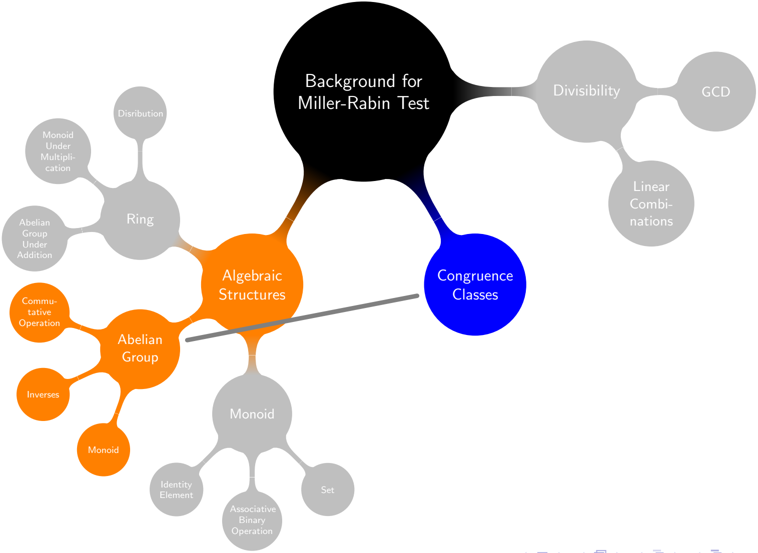
$\mathbb{Z}_n$ Is a Monoid under Multiplication

- $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$.
- By the associativity of integer multiplication, we have

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

- Since $(n+1) = 1 + kn$ for $k = 1 \in \mathbb{Z}$, we know $(n+1) \equiv 1 \pmod{n}$, which is en element in $\bar{1} \in \mathbb{Z}_n$.

$\mathbb{Z}_n$ Is an Abelian Group under Addition



$\mathbb{Z}_n$ Is an Abelian Group under Addition

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

$\mathbb{Z}_n$ Is an Abelian Group under Addition

- $\bar{a} + \bar{b} := \overline{a+b}$
- By the associativity of addition on the integers, we have

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

$\mathbb{Z}_n$ Is an Abelian Group under Addition

- $\bar{a} + \bar{b} := \overline{a+b}$
- By the associativity of addition on the integers, we have

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

- Inverses

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

$\mathbb{Z}_n$ Is an Abelian Group under Addition

- $\bar{a} + \bar{b} := \overline{a+b}$
- By the associativity of addition on the integers, we have

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

- Inverses

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

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

Multiplication Distributes over Addition

- Left Distribution

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

Multiplication Distributes over Addition

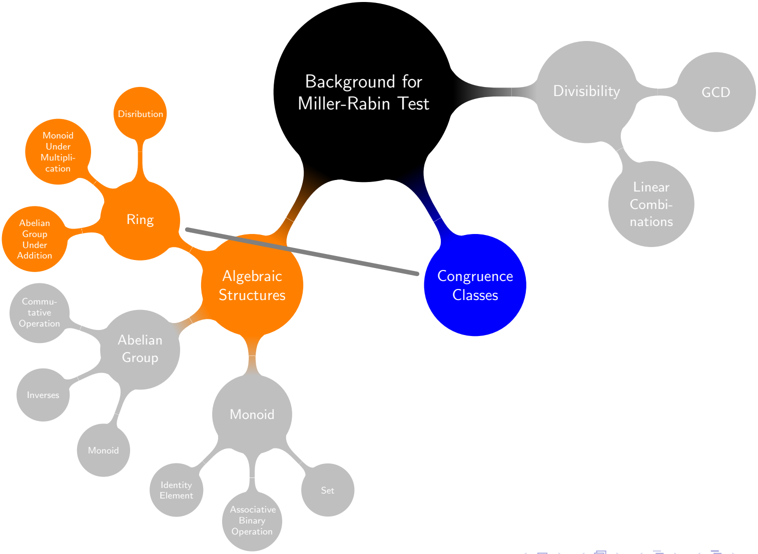
- Left Distribution

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

- Right Distribution

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

$\mathbb{Z}_n$ Is a Ring



$\mathbb{Z}_p$: When n Is Prime

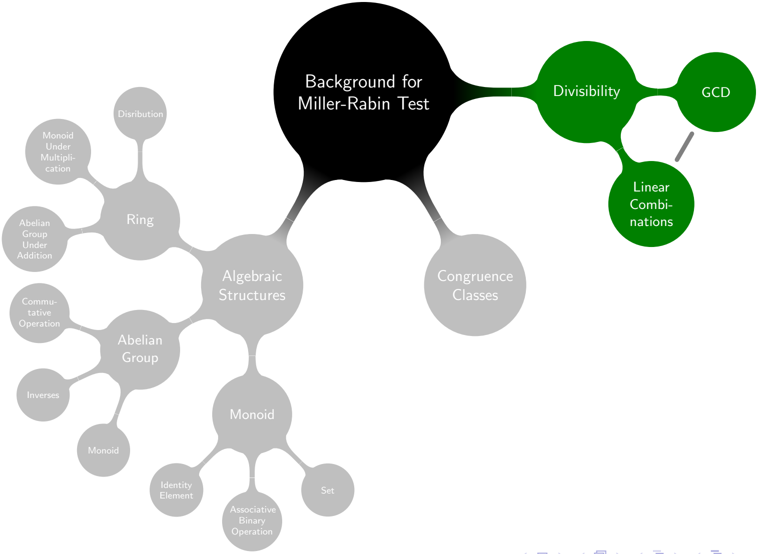
Table: Multiplication in $\mathbb{Z}_7$

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

Table: Multiplication in $\mathbb{Z}_8$

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

Multiplicative Inverses



Multiplicative Inverses

- $\gcd(a, p) = 1$

Multiplicative Inverses

- $\gcd(a, p) = 1$
- $ax + py = 1$

Multiplicative Inverses

- $\gcd(a, p) = 1$
- $ax + py = 1$
- $ax = 1 + (-y)p$ or $ax \equiv 1 \pmod{p}$

Multiplicative Inverses

- $\gcd(a, p) = 1$
- $ax + py = 1$
- $ax = 1 + (-y)p$ or $ax \equiv 1 \pmod{p}$
- Thus, $\overline{a \cdot x} = \bar{a} \cdot \bar{x} = \bar{1}$.

Zero Product Property

- If both $\bar{a} = \bar{0}$ and $\bar{b} = \bar{0}$, then

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

Zero Product Property

- If both $\bar{a} = \bar{0}$ and $\bar{b} = \bar{0}$, then
$$\bar{a} \cdot \bar{b} = \bar{0} \cdot \bar{0} = \overline{0 \cdot 0} = \bar{0}.$$
- If $\bar{a} \neq \bar{0}$, then
$$\begin{aligned} \bar{a} \cdot \bar{b} &= \bar{0} \\ \bar{a}^{-1} \cdot \bar{a} \cdot \bar{b} &= \bar{a}^{-1} \cdot \bar{0} \\ \bar{b} &= \bar{0}. \end{aligned}$$

Zero Product Property

- If both $\bar{a} = \bar{0}$ and $\bar{b} = \bar{0}$, then
$$\bar{a} \cdot \bar{b} = \bar{0} \cdot \bar{0} = \overline{0 \cdot 0} = \bar{0}.$$

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

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

A Pattern Perceptable

Table: Exponents in $\mathbb{Z}_5$

$\bar{a}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{a}^2$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{4}$	$\bar{1}$
$\bar{a}^3$	$\bar{0}$	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{4}$
$\bar{a}^4$	$\bar{0}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$

A Pattern Perceptable

Table: Exponents in $\mathbb{Z}_6$

$\bar{a}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{a}^2$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{3}$	$\bar{4}$	$\bar{1}$
$\bar{a}^3$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{a}^4$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{3}$	$\bar{4}$	$\bar{1}$
$\bar{a}^5$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

Fermat's Little Theorem I

Theorem (Fermat's Little Theorem)

Let p be prime, and let $\bar{a} \in \mathbb{Z}_p$ with $\bar{a} \neq \bar{0}$. Then

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

Fermat's Little Theorem II

Proof.

Let p be prime, and let $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. We know that $\mathbb{Z}_p$ contains a unique inverse for each of its elements. Furthermore, $\bar{1}^{-1} = \bar{1}$ and $\overline{p-1}^{-1} = \overline{p-1}$. 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 $\mathbb{Z}_p$.

Fermat's Little Theorem III

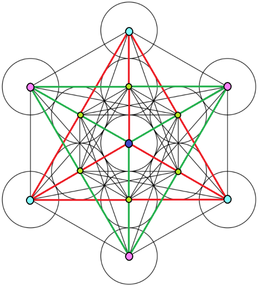
Proof (Cont.)

Hence,

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

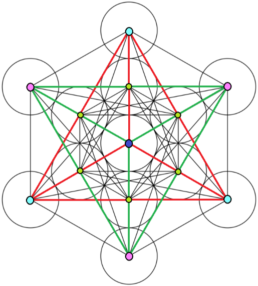
Therefore, if p is prime, then $\bar{a}^{p-1} = \bar{1}$ for all $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$.

Review

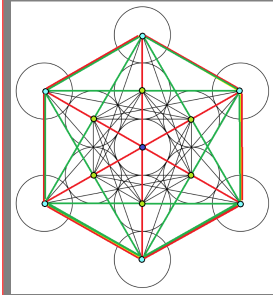


$\mathbb{Z}_n$ is a ring.

Review



$\mathbb{Z}_n$ is a ring.

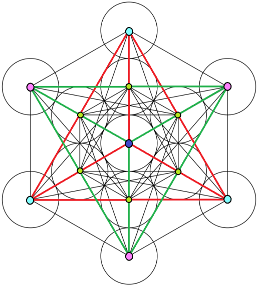


Let p be prime.
Then $\exists \bar{a}^{-1} \in \mathbb{Z}_p$:

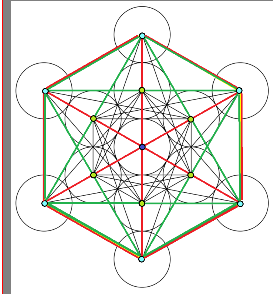
$$\bar{a} \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot \bar{a} = \bar{1}$$

for all $\bar{a} \in \mathbb{Z}_p$

Review



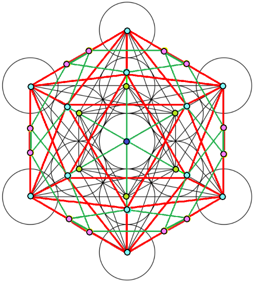
$\mathbb{Z}_n$ is a ring.



Let p be prime.
Then $\exists \bar{a}^{-1} \in \mathbb{Z}_p$:

$$\bar{a} \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot \bar{a} = \bar{1}$$

for all $\bar{a} \in \mathbb{Z}_p$



Let p be prime.
Then $\bar{a}^{p-1} = \bar{1}$.

Overview

Example: Completing the Square in $\mathbb{Z}_{13}$

- Choose $\bar{6} \in \mathbb{Z}_{13}$

Example: Completing the Square in $\mathbb{Z}_{13}$

- Choose $\bar{6} \in \mathbb{Z}_{13}$
- Factor

$$\begin{aligned} \bar{6}^{13-1} &= \bar{1} \\ \bar{6}^{12} - \bar{1} &= \bar{0} \\ (\bar{6}^6 + \bar{1}) \cdot (\bar{6}^6 - \bar{1}) &= \bar{0} \\ (\bar{6}^6 + \bar{1}) \cdot (\bar{6}^3 + \bar{1}) \cdot (\bar{6}^3 - \bar{1}) &= \bar{0} \end{aligned}$$

Example: Completing the Square in $\mathbb{Z}_{13}$

- Choose $\bar{6} \in \mathbb{Z}_{13}$
- Factor

$$\begin{aligned} \bar{6}^{13-1} &= \bar{1} \\ \bar{6}^{12} - \bar{1} &= \bar{0} \\ (\bar{6}^6 + \bar{1}) \cdot (\bar{6}^6 - \bar{1}) &= \bar{0} \\ (\bar{6}^6 + \bar{1}) \cdot (\bar{6}^3 + \bar{1}) \cdot (\bar{6}^3 - \bar{1}) &= \bar{0} \end{aligned}$$

- Zero product product property

$$\begin{aligned} (\bar{6}^6 + \bar{1}) = \bar{0} &\iff \bar{6}^6 = -\bar{1} \\ (\bar{6}^3 + \bar{1}) = \bar{0} &\iff \bar{6}^3 = -\bar{1} \\ (\bar{6}^3 - \bar{1}) = \bar{0} &\iff \bar{6}^3 = \bar{1} \end{aligned}$$

Miller-Rabin Test for Compositeness

Algorithm (Miller-Rabin Test for Compositeness)

Let $n > 0$ be any odd integer. Then there exists an integer $k > 0$ such that 2^k is that 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.

Miller-Rabin Test Example I

Example

We would like 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

$$\overline{19}^{\frac{168}{2^3}} = \overline{70}$$

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

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

Miller-Rabin Test Example II

Example

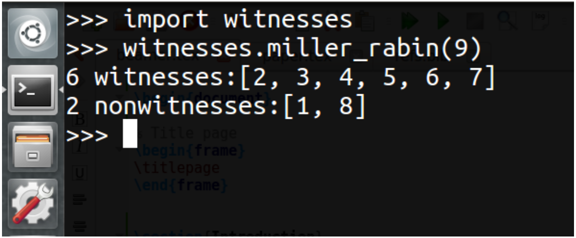
Because $\overline{19}^{\frac{168}{2^2}} = -\overline{1}$, we cannot conclude that 169 is composite. So we randomly select a different $\overline{a} \in \mathbb{Z}_{169}$, namely $\overline{a} = \overline{145}$, and this time discover that

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

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

Effectiveness of the Miller-Rabin Test

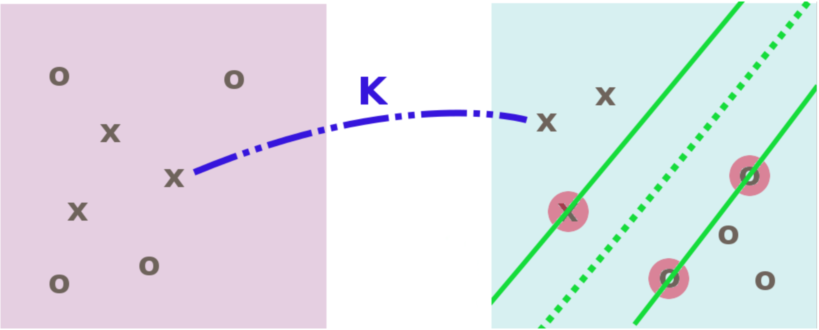
- At least $\frac{3}{4}$ of the integers a in the range $1, 2, \ldots, n-1$ are Miller-Rabin witnesses.
- If we run the test 100 times on a composite number, the probability that we will never find a witness is less than $\left(\frac{1}{4}\right)^{100} = 6.223 \times 10^{-61}$.



Overview

Linear Classification with a Twist

- Use non-linear function K to map input vector to a higher dimensional feature space
- Linear decision function with maximal margin between vectors of different classes



Training Methodology

- Integer range: 2-1000

Training Methodology

- Integer range: 2-1000
- 2,755,256 models using

$$K(\vec{x}, \vec{x}') := \exp\left(-\gamma \|\vec{x} - \vec{x}'\|^2\right)$$

with $\gamma = \frac{1}{n}$, where n is the length of the longest vector in the domain.

Training Methodology

- Integer range: 2-1000
- 2,755,256 models using

$$K(\vec{x}, \vec{x}') := \exp\left(-\gamma \|\vec{x} - \vec{x}'\|^2\right)$$

  with $\gamma = \frac{1}{n}$, where n is the length of the longest vector in the domain.
- Base b representations. For example, let $b = 6$. Then

$$32 \to (5, 2)$$
$$153 \to (4, 1, 3)$$
$$1000 \to (4, 3, 4, 4)$$

Training Methodology

- Integer range: 2-1000
- 2,755,256 models using

$$K(\vec{x}, \vec{x}') := \exp\left(-\gamma \|\vec{x} - \vec{x}'\|^2\right)$$

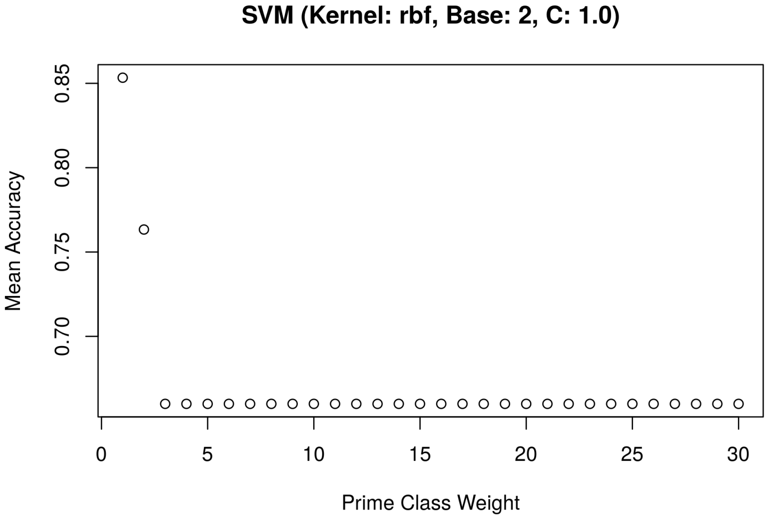
with $\gamma = \frac{1}{n}$, where n is the length of the longest vector in the domain.

- Base b representations. For example, let $b = 6$. Then

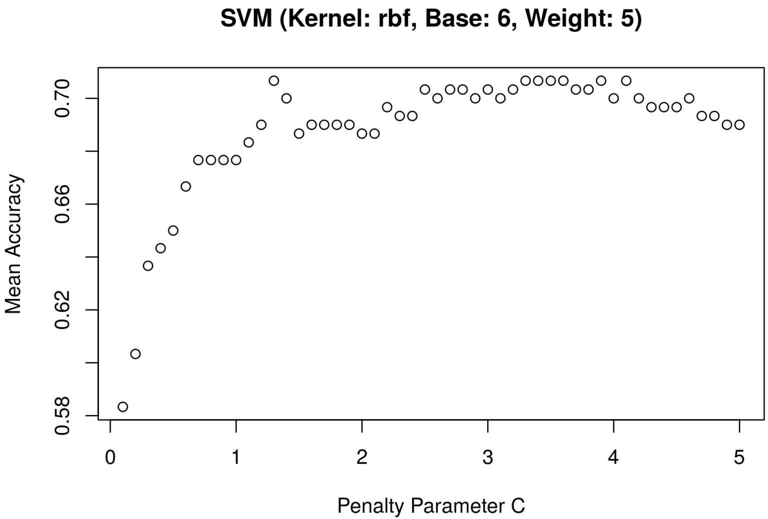
$$32 \to (5, 2)$$
$$153 \to (4, 1, 3)$$
$$1000 \to (4, 3, 4, 4)$$

- Class weight for primes
- Penalty parameter C

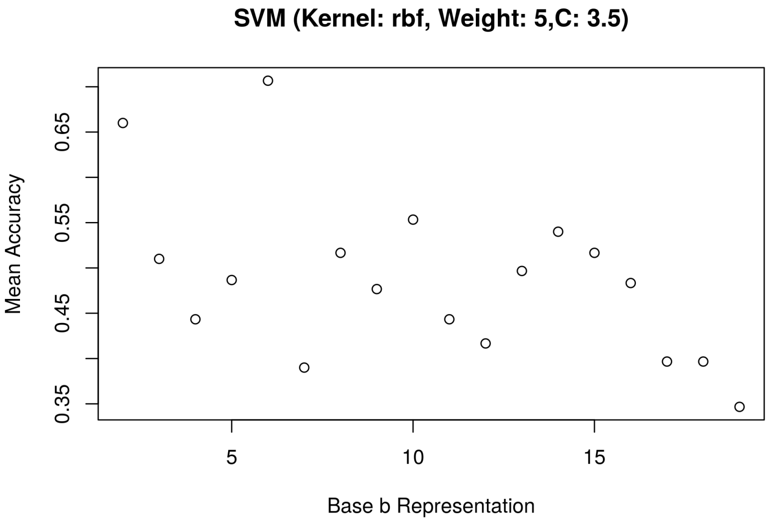
Testing: Class Weight of Primes



Testing: Penalty Parameter C



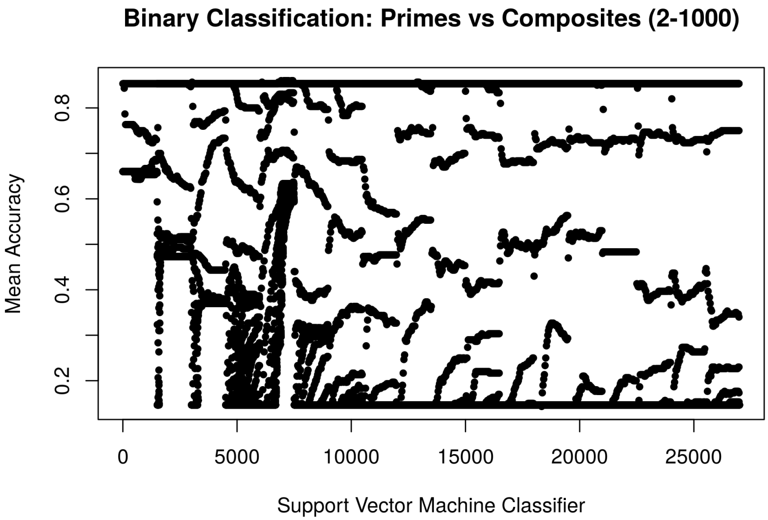
Testing: Base b Representations



Best Models

Base	C	Weight	Accuracy
6	3.2	2	0.86
6	3.7	2	0.86
6	3.8	2	0.86
6	3.9	2	0.86
6	4.0	2	0.86
6	4.1	2	0.86
6	4.7	2	0.86
6	4.8	2	0.86
6	4.9	2	0.86

Conclusion

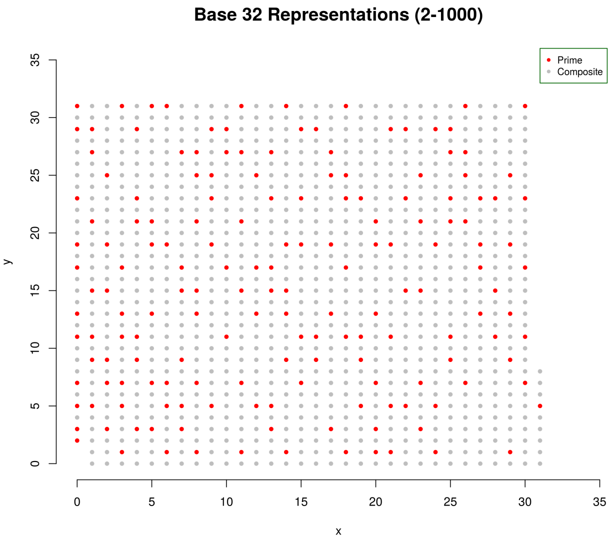

Binary Classification: Primes vs Composites (2-1000)
Mean Accuracy
0.2
0.4
0.6
0.8
0
5000
10000
15000
20000
25000
Support Vector Machine Classifier

Conclusion: Sly Models

- 168 primes between 2 and 1000 (inclusive)

  {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997}
- 16.8% prime and 83.2% composite

Conclusion: Finding the Right K



References

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.

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

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

Acknowledgements

- Professor Tom Edgar
- Professor Yajun An
- My wife, Nora.