Testing for Compositeness

Miller-Rabin vs Support Vector Machine Classification

Miguel Amezola

Department of Mathematics
Pacific Lutheran University

May 9, 2017

Overview

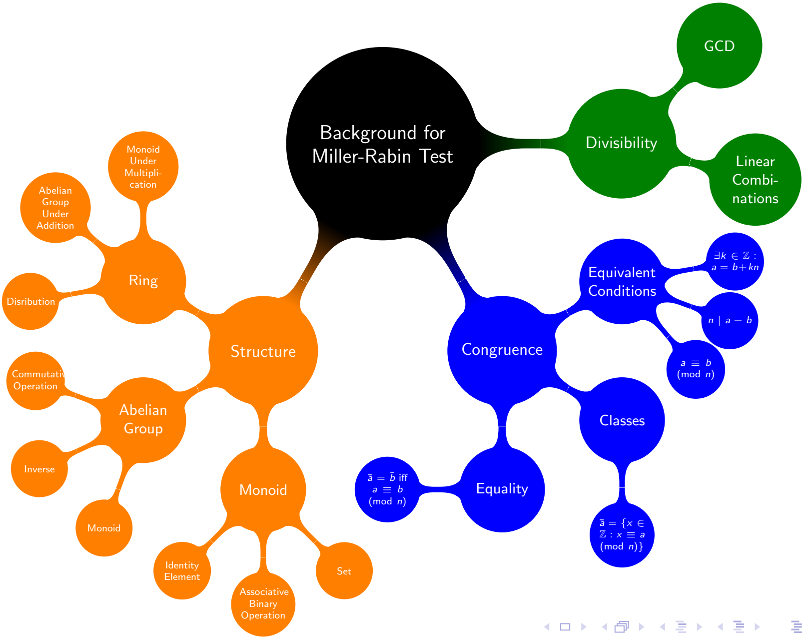
Prime and Composite Numbers

Definition (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 (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]


Background for Miller-Rabin Test
Divisibility
GCD
Linear Combi-nations
Congruence
Equivalent Conditions
$\exists k \in \mathbb{Z}: a = b + kn$
$n \mid a - b$
$a \equiv b \pmod{n}$
Classes
$\bar{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$
Equality
$\bar{a} = \bar{b}$ iff $a \equiv b \pmod{n}$
Structure
Ring
Monoid Under Multipli-cation
Abelian Group Under Addition
Disribution
Abelian Group
Commutati Operation
Inverse
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 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, $34 \equiv 144 \pmod{10}$.

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.

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

The Structure of $\mathbb{Z}_n$

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

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

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

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

Overview

Fermat's Little Theorem I

Theorem (Fermat's Little Theorem [2])

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

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

Fermat's Little Theorem II

Proof.

Let p be prime, and let $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. By **??**, 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 **??**. Thus, $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{p-1} = \bar{1} \cdot \overline{p-1} = \overline{p-1}$. Then

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

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 $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$.

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

$$\overline{145}^{\frac{168}{2^3}} = \overline{18}$$

$$\overline{145}^{\frac{168}{2^2}} = \overline{155}$$

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

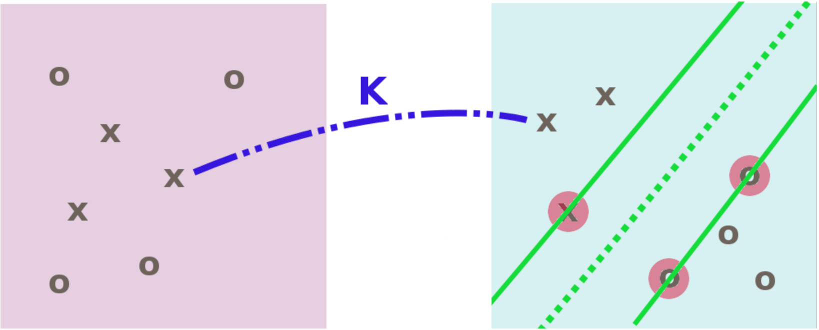
Hence, 145 is a Miller-Rabin witness to the compositeness of 169 and we conclude that 169 is not prime.

Effectiveness of the Miller-Rabin Test

Overview

What is a Support Vector Machine (SVM)?

- 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



Linear Classification

Support Vector Machine

Feature Space

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]

Training Methodology

Definition (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]

Comparison

References I

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