Irreduciblity Tests in $\mathbb{F}_p[x]$

Sathwik Karnik

Mentor: Hyun Jong Kim

December 20, 2016

Cryptosystems

- The RSA Cryptosystem requires 2 distinct large prime factors p and q that will be multiplied together to form $pq = n$.

Primality Tests

- Primality tests are used to determine if a given number is prime.

Primality Tests

- Primality tests are used to determine if a given number is prime.
- Primality tests can help in generating the private keys for a cryptosystem.

Similarities

- Testing if a monic polynomial π is irreducible

Similarities

- Testing if a monic polynomial π is irreducible
- The number of elements in $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ is $p^{\deg f}$

Similarities

- Testing if a monic polynomial π is irreducible
- The number of elements in $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ is $p^{\deg f}$
- Trial Division

Similarities

- Testing if a monic polynomial π is irreducible
- The number of elements in $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ is $p^{\deg f}$
- Trial Division
    - method of testing all the positive integers less than $\sqrt{n}$ in $\mathbb{Z}$

Similarities

- Testing if a monic polynomial π is irreducible
- The number of elements in $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ is $p^{\deg f}$
- Trial Division
  - method of testing all the positive integers less than $\sqrt{n}$ in $\mathbb{Z}$
  - method of testing all the monic irreducible polynomials with degree less than $\frac{1}{2}\deg(f(x))$ in $\mathbb{F}_p[x]$

Irreducibility Tests

Theorem (Fermat)

Let π *be an irreducible in* $\mathbb{F}_p[x]$. *For all nonzero polynomials* $a \in \mathbb{F}_p[x]/\pi\mathbb{F}_p[x]$, $a^{N(\pi)-1} \equiv 1 \pmod{\pi}$.

Irreducibility Tests

Theorem (Fermat)

Let π be an irreducible in $\mathbb{F}_p[x]$. For all nonzero polynomials $a \in \mathbb{F}_p[x]/\pi\mathbb{F}_p[x]$, $a^{N(\pi)-1} \equiv 1 \pmod{\pi}$.

Fermat Witnesses

Consider an arbitrary nonconstant polynomial $f(x) \in \mathbb{F}_p[x]$. Pick an arbitrary a in $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ and check if $a^{N(f)-1} \equiv 1 \pmod{f(x)}$. We call a a Fermat Witness if $a^{N(f)-1} \not\equiv 1 \pmod{f(x)}$. In other words, if there is a Fermat Witness $\pmod{\pi}$ for $\pi \in \mathbb{F}_p[x]$, then π is reducible.

Examples of Fermat Witnesses

Suppose $f(x) = x^5 + x^2 + 2$ in $\mathbb{F}_p[x]$. In this case, $N(f) = 3^5 = 243$. We want to test $a^{242} \equiv 1 \pmod{f}$ when $\deg a < 5$. When $a = x$, a is a Fermat Witness in $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ because $x^{242} \equiv x + 1 \not\equiv 1 \pmod{f(x)}$. This means that $f(x)$ is reducible. Also, note that x relatively prime to $f(x)$.

Fermat Witnesses

Theorem

If $f(x) \in \mathbb{F}_p[x]$ has a nontrivial Fermat Witness, then the proportion of residues in $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ that are Fermat Witnesses for f is greater than 50%.

Fermat Witnesses

Theorem

If $f(x) \in \mathbb{F}_p[x]$ has a nontrivial Fermat Witness, then the proportion of residues in $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ that are Fermat Witnesses for f is greater than 50%.

- Proof is very similar to an analog in $\mathbb{Z}$

Fermat Witnesses

Theorem

If $f(x) \in \mathbb{F}_p[x]$ has a nontrivial Fermat Witness, then the proportion of residues in $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ that are Fermat Witnesses for f is greater than 50%.

- Proof is very similar to an analog in $\mathbb{Z}$
- Uses the notion of grouping the elements of $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ into three pairwise disjoint subsets

Fermat Witnesses

Theorem

If $f(x) \in \mathbb{F}_p[x]$ has a nontrivial Fermat Witness, then the proportion of residues in $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ that are Fermat Witnesses for f is greater than 50%.

- Proof is very similar to an analog in $\mathbb{Z}$
- Uses the notion of grouping the elements of $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ into three pairwise disjoint subsets
  - $A := \{a \in \mathbb{F}_p[x]/f\mathbb{F}_p[x] : \gcd(a, f(x)) > 1\}$

Fermat Witnesses

Theorem

If $f(x) \in \mathbb{F}_p[x]$ has a nontrivial Fermat Witness, then the proportion of residues in $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ that are Fermat Witnesses for f is greater than 50%.

- Proof is very similar to an analog in $\mathbb{Z}$
- Uses the notion of grouping the elements of $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ into three pairwise disjoint subsets
  - $A := \{a \in \mathbb{F}_p[x]/f\mathbb{F}_p[x] : \gcd(a, f(x)) > 1\}$
  - $B := \{a \in \mathbb{F}_p[x]/f\mathbb{F}_p[x] : a^{N(f)-1} \equiv 1 \pmod{f(x)}\}$

Fermat Witnesses

Theorem

If $f(x) \in \mathbb{F}_p[x]$ has a nontrivial Fermat Witness, then the proportion of residues in $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ that are Fermat Witnesses for f is greater than 50%.

- Proof is very similar to an analog in $\mathbb{Z}$
- Uses the notion of grouping the elements of $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ into three pairwise disjoint subsets
  - $A := \{a \in \mathbb{F}_p[x]/f\mathbb{F}_p[x] : \gcd(a, f(x)) > 1\}$
  - $B := \{a \in \mathbb{F}_p[x]/f\mathbb{F}_p[x] : a^{N(f)-1} \equiv 1 \pmod{f(x)}\}$
  - $C := \{a \in \mathbb{F}_p[x]/f\mathbb{F}_p[x] : \gcd(a, f(x)) = 1, a^{N(f)-1} \not\equiv 1 \pmod{f(x)}\}$

Carmichael Polynomials

- Carmichael Polynomials are polynomials $f(x)$ that are false positives to the Fermat Irreducibility Test and have no Fermat Witnesses relatively prime to $f(x)$. Carmichael polynomials also obey the analogous version of Korselt's Criterion that characterizes their irreducible factors.

Carmichael Polynomials

- Carmichael Polynomials are polynomials $f(x)$ that are false positives to the Fermat Irreducibility Test and have no Fermat Witnesses relatively prime to $f(x)$. Carmichael polynomials also obey the analogous version of Korselt's Criterion that characterizes their irreducible factors.
- Korselt's Criterion:

Carmichael Polynomials

- Carmichael Polynomials are polynomials $f(x)$ that are false positives to the Fermat Irreducibility Test and have no Fermat Witnesses relatively prime to $f(x)$. Carmichael polynomials also obey the analogous version of Korselt's Criterion that characterizes their irreducible factors.
- Korselt's Criterion:
  1. $f(x)$ does not have any nonconstant square factors.

Carmichael Polynomials

- Carmichael Polynomials are polynomials $f(x)$ that are false positives to the Fermat Irreducibility Test and have no Fermat Witnesses relatively prime to $f(x)$. Carmichael polynomials also obey the analogous version of Korselt's Criterion that characterizes their irreducible factors.
- Korselt's Criterion:
  1. $f(x)$ does not have any nonconstant square factors.
  2. $\forall$ irreducible $\pi | f(x)$, $N(\pi) - 1 | N(f(x)) - 1$.

Carmichael Polynomials

- Carmichael Polynomials are polynomials $f(x)$ that are false positives to the Fermat Irreducibility Test and have no Fermat Witnesses relatively prime to $f(x)$. Carmichael polynomials also obey the analogous version of Korselt's Criterion that characterizes their irreducible factors.
- Korselt's Criterion:
  1. $f(x)$ does not have any nonconstant square factors.
  2. $\forall$ irreducible $\pi | f(x)$, $N(\pi) - 1 | N(f(x)) - 1$.
- *Example:* The product of two irreducible polynomials π_1 and π_2 such that $\deg \pi_1 = \deg \pi_2$. One such example is $f(x) = x(x+1)$ because $\deg x = \deg(x+1) = 1$, which means that $p - 1 | p^{\deg f} - 1 \Rightarrow p - 1 | p^2 - 1$.

Miller-Rabin

Miller-Rabin Witnesses and Nonwitnesses

We call $a \in \mathbb{F}_p[x]$ with $\deg a < \deg f$ a Miller-Rabin Witness for $f(x) \in \mathbb{F}_p[x]$ if $a^k \not\equiv 1 \pmod{f}$ and $a^{2^i \cdot k} \not\equiv -1 \pmod{f}$ for all $i \in \{0, 1, 2, \ldots, e-1\}$. We say that a is a Miller-Rabin Nonwitness for f if $a^k \equiv 1 \pmod{f}$ or $a^{2^i \cdot k} \equiv -1 \pmod{f}$ for some $i \in \{0, 1, 2, \ldots, e-1\}$.

Miller-Rabin

Miller-Rabin Witnesses and Nonwitnesses

We call $a \in \mathbb{F}_p[x]$ with $\deg a < \deg f$ a Miller-Rabin Witness for $f(x) \in \mathbb{F}_p[x]$ if $a^k \not\equiv 1 \pmod{f}$ and $a^{2^i \cdot k} \not\equiv -1 \pmod{f}$ for all $i \in \{0, 1, 2, \ldots, e-1\}$. We say that a is a Miller-Rabin Nonwitness for f if $a^k \equiv 1 \pmod{f}$ or $a^{2^i \cdot k} \equiv -1 \pmod{f}$ for some $i \in \{0, 1, 2, \ldots, e-1\}$.

Theorem (Miller-Rabin)

Let p be an odd prime. For all nonconstant polynomials $f(x)$ in $\mathbb{F}_p[x]$, $p^{\deg f} > 1$ and is odd. Rewrite $N(f) - 1$ as $2^e \cdot k$ for an odd integer k. The existence of a Miller-Rabin witness implies that f is reducible.

Example of Miller-Rabin

Example

Let $f(x) = x^{10} + x^2 + 3$ be an element of $\mathbb{F}_7[x]$. Then, $N(f) - 1 = 7^{10} - 1 = 2^4 \cdot 17654703$, which means that $e = 4$ and $k = 17654703$. Note that x is a Miller-Rabin Witness for $f(x)$: $x^k \equiv x^9 + 3x^7 + x^5 + 2x^3 + 2x \not\equiv 1 \pmod{f(x)}$ and $x^{2k} \equiv 1 \pmod{f(x)}$.

Miller-Rabin Witnesses

Theorem

If $f(x) \in \mathbb{F}_p[x]$ is a monic reducible and f is not $\pi_1\pi_2$ where π_1 and π_2 are different monic irreducibles of the same degree, then the proportion of Miller-Rabin witnesses for f is at least 75%, with equality if and only if $N(f) = 9$, or equivalently $p = 3$ and $f(x) = (x + c)^2$ where $c \in \mathbb{F}_3$.

Proof Overview

- Split into 3 cases based on the factorization of $f(x)$:

Proof Overview

- Split into 3 cases based on the factorization of $f(x)$:
  - $f(x) = \pi^\alpha$ for $\alpha \in \mathbb{N}$, in which case the proportion of Miller-Rabin Nonwitnesses is given by: $\dfrac{p^{\deg \pi} - 1}{p^{\alpha \deg \pi} - 1} = \dfrac{1}{1 + p^{\deg \pi} + \cdots + p^{\alpha \deg \pi - 1}}$. Since $\alpha \geq 2$, the proportion is at most $\dfrac{1}{1 + p^{\deg \pi}}$, which is maximized when $p = 3$ and $\deg \pi = 1$.

Proof Overview

- Split into 3 cases based on the factorization of $f(x)$:
  - $f(x) = \pi^\alpha$ for $\alpha \in \mathbb{N}$, in which case the proportion of Miller-Rabin Nonwitnesses is given by: $\dfrac{p^{\deg \pi} - 1}{p^{\alpha \deg \pi} - 1} = \dfrac{1}{1 + p^{\deg \pi} + \cdots + p^{\alpha \deg \pi - 1}}$. Since $\alpha \geq 2$, the proportion is at most $\dfrac{1}{1 + p^{\deg \pi}}$, which is maximized when $p = 3$ and $\deg \pi = 1$.
  - $f(x)$ is a Carmichael polynomial

Proof Overview

- Split into 3 cases based on the factorization of $f(x)$:
    - $f(x) = \pi^{\alpha}$ for $\alpha \in \mathbb{N}$, in which case the proportion of Miller-Rabin Nonwitnesses is given by: $\dfrac{p^{\deg \pi} - 1}{p^{\alpha \deg \pi} - 1} = \dfrac{1}{1 + p^{\deg \pi} + \cdots + p^{\alpha \deg \pi - 1}}$. Since $\alpha \geq 2$, the proportion is at most $\dfrac{1}{1 + p^{\deg \pi}}$, which is maximized when $p = 3$ and $\deg \pi = 1$.
    - $f(x)$ is a Carmichael polynomial
    - $f(x)$ is non-Carmichael and has at least 3 distinct irreducible factors

Bounding Proportion of Fermat Witnesses in $\mathbb{F}_p[x]$

Proportion of Fermat Witnesses for Carmichael polynomials:

- Consider the Carmichael polynomial $f(x)$ such that $f(x)$ is the product of two monic irreducibles with the same degree. Since there exist irreducibles with the same degree for any degree in $\mathbb{F}_p[x]$, the upper bound for the proportion of Fermat Witnesses is at most 1:

$f(x) = \pi_1\pi_2$, where $\deg \pi_1 = \deg \pi_2 = k$. Note that the proportion of Fermat Witnesses is $\dfrac{(p^k-1)^2}{p^{2k}-1}$, whose limit as $k \to \infty$ is 1.

Back to Primality Tests in $\mathbb{Z}$

- Is there an upper bound to the proportion of Fermat Witnesses for Carmichael numbers in $\mathbb{Z}$?

Back to Primality Tests in $\mathbb{Z}$

- Is there an upper bound to the proportion of Fermat Witnesses for Carmichael numbers in $\mathbb{Z}$?
- If an upper bound stronger than 1 does exist, then can we find a function of the number that can serve as an upper bound?

Research

- Attempts at bounding the proportion of Fermat Witnesses for Carmichael numbers

Research

- Attempts at bounding the proportion of Fermat Witnesses for Carmichael numbers
  - Generalized for Carmichael numbers with a certain smallest prime factor and a proportion of Fermat Witnesses of less than 50%.

Research

- Attempts at bounding the proportion of Fermat Witnesses for Carmichael numbers
  - Generalized for Carmichael numbers with a certain smallest prime factor and a proportion of Fermat Witnesses of less than 50%.
- Algorithm to distinguish between Carmichael numbers and other composite numbers

Research

- Attempts at bounding the proportion of Fermat Witnesses for Carmichael numbers
  - Generalized for Carmichael numbers with a certain smallest prime factor and a proportion of Fermat Witnesses of less than 50%.
- Algorithm to distinguish between Carmichael numbers and other composite numbers
  - Used the fact that most Carmichael numbers have a proportion of Fermat Witnesses of less than 50%.

Research

- Attempts at bounding the proportion of Fermat Witnesses for Carmichael numbers
  - Generalized for Carmichael numbers with a certain smallest prime factor and a proportion of Fermat Witnesses of less than 50%.
- Algorithm to distinguish between Carmichael numbers and other composite numbers
  - Used the fact that most Carmichael numbers have a proportion of Fermat Witnesses of less than 50%.
  - Can be used in differentiating between Carmichael numbers and prime numbers more efficiently.

Acknowledgements

- My Mentor, Hyun Jong Kim

Acknowledgements

- My Mentor, Hyun Jong Kim
- MIT PRIMES Program

Acknowledgements

- My Mentor, Hyun Jong Kim
- MIT PRIMES Program
- Professor Conrad for providing the necessary readings

Acknowledgements

- My Mentor, Hyun Jong Kim
- MIT PRIMES Program
- Professor Conrad for providing the necessary readings
- My Parents