Fachpraktikum

Primzahltests modifiziert zum Testen von Polynomen auf Irreduzibilität

14.08.2019

Einleitung

- Primzahltests untersuchen: Welche Eigenschaften werden genutzt?

Einleitung

- Primzahltests untersuchen: Welche Eigenschaften werden genutzt?
- Übertragbarkeit auf Polynome über $\mathbb{Z}_q$ bei festem $q \in \mathbb{P}$?

Fermat

Satz von Fermat

Ist p eine Primzahl, so gilt für alle $a \in \mathbb{N}$ mit $p \nmid a$:
$a^{p-1} \equiv 1 \bmod p$

Fermat

Satz von Fermat

Ist p eine Primzahl, so gilt für alle $a \in \mathbb{N}$ mit $p \nmid a$:
$a^{p-1} \equiv 1 \bmod p$

Algebra: $|(\mathbb{Z}_p)^*| = p - 1$

Fermat

Satz von Fermat

Ist p eine Primzahl, so gilt für alle $a \in \mathbb{N}$ mit $p \nmid a$:
$a^{p-1} \equiv 1 \bmod p$

Algebra: $|(\mathbb{Z}_p)^*| = p - 1$

Polynome: $|(\mathbb{Z}_q[x]/f)^*| = q^{deg(f)} - 1$ für irreduzible Polynome f

Fermat

Fermat für Polynome

Ist f irreduzibel über $\mathbb{Z}_q$, so gilt für alle $a \in \mathbb{Z}_q[x]$ mit $f \nmid a$:
$a^{q^{deg(f)}-1} \equiv 1 \bmod f$

Fermat

Fermat für Polynome

Ist f irreduzibel über $\mathbb{Z}_q$, so gilt für alle $a \in \mathbb{Z}_q[x]$ mit $f \nmid a$:
$a^{q^{deg(f)}-1} \equiv 1 \bmod f$

Als Test auf Irreduzibilität: Gilt $a^{q^{deg(f)}-1} \not\equiv 1 \bmod f$, dann ist f nicht irreduzibel.

Carmichael-Polynome

Definition

Ein *Carmichael-Polynom* ist ein zusammengesetztes Polynom f, sodass $a^{q^{deg(f)}-1} \equiv 1 \mod f$ für alle $a \in \mathbb{Z}_q[x]$ mit $deg(ggT(a, f)) = 0$

Carmichael-Polynome

Definition

Ein *Carmichael-Polynom* ist ein zusammengesetztes Polynom f, sodass $a^{q^{deg(f)}-1} \equiv 1 \bmod f$ für alle $a \in \mathbb{Z}_q[x]$ mit $deg(ggT(a, f)) = 0$

Satz

Sei $f \in \mathbb{Z}_q[x]$. Wenn für alle f_i irreduzibel mit $f_i | f$ gilt, dass $f_i^2 \nmid f$ und $deg(f_i) | deg(f)$, dann ist f ein Carmichael-Polynom.

Carmichael-Polynome

Definition

Ein *Carmichael-Polynom* ist ein zusammengesetztes Polynom f, sodass $a^{q^{deg(f)}-1} \equiv 1 \bmod f$ für alle $a \in \mathbb{Z}_q[x]$ mit $deg(ggT(a, f)) = 0$

Satz

Sei $f \in \mathbb{Z}_q[x]$. Wenn für alle f_i irreduzibel mit $f_i | f$ gilt, dass $f_i^2 \nmid f$ und $deg(f_i) | deg(f)$, dann ist f ein Carmichael-Polynom.

$\Rightarrow$ false-positives einfach zu finden

Miller-Rabin

- Finde $s, u \in \mathbb{N}$, u ungerade mit $p - 1 = 2^s u$

Miller-Rabin

- Finde $s, u \in \mathbb{N}$, u ungerade mit $p - 1 = 2^s u$
- Wähle $a \in \mathbb{N}$

Miller-Rabin

- Finde $s, u \in \mathbb{N}$, u ungerade mit $p - 1 = 2^s u$
- Wähle $a \in \mathbb{N}$
- Teste, ob $a^u \equiv 1 \mod p$

Miller-Rabin

- Finde $s, u \in \mathbb{N}, u$ ungerade mit $p - 1 = 2^s u$
- Wähle $a \in \mathbb{N}$
- Teste, ob $a^u \equiv 1 \mod p$
- Für $1 \leq t < s$ teste, ob $a^{2^t u} \equiv -1 \mod p$

Miller-Rabin für Polynome

- Finde $s, u \in \mathbb{N}, u$ ungerade mit $q^{deg(f)} - 1 = 2^s u$

Miller-Rabin für Polynome

- Finde $s, u \in \mathbb{N}$, u ungerade mit $q^{deg(f)} - 1 = 2^s u$
- Wähle $a \in \mathbb{Z}_q[x]$

Miller-Rabin für Polynome

- Finde $s, u \in \mathbb{N}, u$ ungerade mit $q^{deg(f)} - 1 = 2^s u$
- Wähle $a \in \mathbb{Z}_q[x]$
- Teste, ob $a^u \equiv 1 \mod f$

Miller-Rabin für Polynome

- Finde $s, u \in \mathbb{N}, u$ ungerade mit $q^{deg(f)} - 1 = 2^s u$
- Wähle $a \in \mathbb{Z}_q[x]$
- Teste, ob $a^u \equiv 1 \mod f$
- Für $1 \leq t < s$ teste, ob $a^{2^t u} \equiv -1 \mod f$

Schwierigkeiten

Laufzeit:

- Sehr viele Allokationen; gelöst durch In-place-rechnen

Schwierigkeiten

Laufzeit:

- Sehr viele Allokationen; gelöst durch In-place-rechnen
- Potenzierung langsam, da u oft groß

Power-Residue Symbol

Legendre Symbol für Polynome

Definition

Für $d|q-1$ fest, $a, f \in \mathbb{Z}_q[x], f$ irreduzibel, $f \nmid a$:
$(\frac{a}{f})_d \equiv a^{\frac{|f|-1}{d}} \mod f$

Power-Residue Symbol

Legendre Symbol für Polynome

Definition

Für $d | q-1$ fest, $a, f \in \mathbb{Z}_q[x], f$ irreduzibel, $f \nmid a$:
$(\frac{a}{f})_d \equiv a^{\frac{|f|-1}{d}} \mod f$

Reziprozitätsgesetz

Seien f, g irreduzible Polynome. Dann gilt:
$(\frac{g}{f})_d = (-1)^{deg(f) deg(g) \frac{q-1}{d}} \cdot (\frac{f}{g})_d$

Jacobi Symbol

Verallgemeinerung des Power-Residue Symbols: f muss nicht irreduzibel sein.

Reziprozitätsgesetz

Seien f, g teilerfremde Polynome, q die Charakteristik von $\mathbb{Z}_q[x]$ und d ein Teiler von $q-1$. $sgn(f) := lc(f)^{\frac{q-1}{d}}$ Dann gilt:
$\left(\frac{f}{g}\right) \cdot \left(\frac{g}{f}\right)^{-1} = (-1)^{\frac{q-1}{d} \cdot deg(f) \cdot deg(g)} \cdot sgn(f)^{deg(g)} \cdot sgn(g)^{-deg(f)}$

Power-Residue Test

- Nutze Reziprozitätsgesetz, um $(\frac{a}{f})_d$ zu berechnen

Power-Residue Test

- Nutze Reziprozitätsgesetz, um $(\frac{a}{f})_d$ zu berechnen
- Vergleiche Ergebnis mit der Definition

Laufzeit

- Ein Durchlauf sehr schnell; vergleichbar mit *isirreducible*

Laufzeit

- Ein Durchlauf sehr schnell; vergleichbar mit *isirreducible*
- Problem: gibt oft fälschlicherweise `true` aus

Laufzeit

- Ein Durchlauf sehr schnell; vergleichbar mit *isirreducible*
- Problem: gibt oft fälschlicherweise `true` aus
- Abhängig von a

Pocklington

Pocklington Kriterium

Sei $N \in \mathbb{N}_{>1}$. Sei $a \in \mathbb{N}$, s.d. $a^{N-1} \equiv 1 \bmod N$.
Sei p prim, $p|N-1$ und $p > \sqrt{N} - 1$.
Wenn $ggT(a^{\frac{N-1}{p}} - 1, N) = 1$, dann ist N eine Primzahl.

Pocklington

Pocklington für Polynome

Sei f das zu testende Polynom und a ein Polynom, s.d. q Charakteristik des Rings, d der Grad von f. Falls $a^{q^d-1} \equiv 1 \bmod f$ und $\exists p \in [q^{\frac{d}{2}}, \frac{q^{d-1}}{2}]$, p prim, $p|q^{d-1} : ggT(a^{\frac{q^{d-1}}{p}} - 1, f) = 1$, dann ist f irreduzibel.

Laufzeit

Lucas-Folgen

Lineare Rekursionsgleichung $(a_n)_n$ von Grad 2

Satz

χ_c irreduzibel $\Rightarrow per(c) \big| |K|^2 - 1 = (q^{deg(f)})^2 - 1$

Lucas-Folgen

Lineare Rekursionsgleichung $(a_n)_n$ von Grad 2

Satz

χ_c irreduzibel $\Rightarrow per(c) \big| |K|^2 - 1 = (q^{deg(f)})^2 - 1$

Als Test auf Irreduzibilität: $a_{per} \neq a_0$ oder $a_{per+1} \neq a_1 \Rightarrow f$ nicht irreduzibel.

Lucas-Folgen

Lineare Rekursionsgleichung $(a_n)_n$ von Grad 2

Satz

χ_c irreduzibel $\Rightarrow per(c) \big| |K|^2 - 1 = (q^{deg(f)})^2 - 1$

Als Test auf Irreduzibilität: $a_{per} \neq a_0$ oder $a_{per+1} \neq a_1 \Rightarrow f$ nicht irreduzibel.

Verschiedene Möglichkeiten a_{per} zu berechnen:

Lucas-Folgen

Lineare Rekursionsgleichung $(a_n)_n$ von Grad 2

Satz

χ_c irreduzibel $\Rightarrow per(c) \,\big|\, |K|^2 - 1 = (q^{deg(f)})^2 - 1$

Als Test auf Irreduzibilität: $a_{per} \neq a_0$ oder $a_{per+1} \neq a_1 \Rightarrow f$ nicht irreduzibel.

Verschiedene Möglichkeiten a_{per} zu berechnen:

- rekursiv $\Rightarrow$ Laufzeit!

Lucas-Folgen

Lineare Rekursionsgleichung $(a_n)_n$ von Grad 2

Satz

χ_c irreduzibel $\Rightarrow per(c) \big| |K|^2 - 1 = (q^{deg(f)})^2 - 1$

Als Test auf Irreduzibilität: $a_{per} \neq a_0$ oder $a_{per+1} \neq a_1 \Rightarrow f$ nicht irreduzibel.

Verschiedene Möglichkeiten a_{per} zu berechnen:

- rekursiv $\Rightarrow$ Laufzeit!
- explizit mit Matrix

Lucas-Folgen

Lineare Rekursionsgleichung $(a_n)_n$ von Grad 2

Satz

χ_c irreduzibel $\Rightarrow per(c) \big| |K|^2 - 1 = (q^{deg(f)})^2 - 1$

Als Test auf Irreduzibilität: $a_{per} \neq a_0$ oder $a_{per+1} \neq a_1 \Rightarrow f$ nicht irreduzibel.

Verschiedene Möglichkeiten a_{per} zu berechnen:

- rekursiv $\Rightarrow$ Laufzeit!
- explizit mit Matrix
- mit Lucas-Kette: bestimmte Form der Rekursionsgleichung gegeben, dafür einfache Formel, die Glieder explizit auszurechnen; rechnen im Ring

Lucas-Folgen

Lineare Rekursionsgleichung $(a_n)_n$ von Grad 2

Satz

χ_c irreduzibel $\Rightarrow per(c) \big| |K|^2 - 1 = (q^{deg(f)})^2 - 1$

Als Test auf Irreduzibilität: $a_{per} \neq a_0$ oder $a_{per+1} \neq a_1 \Rightarrow f$ nicht irreduzibel.

Verschiedene Möglichkeiten a_{per} zu berechnen:

- rekursiv $\Rightarrow$ Laufzeit!
- explizit mit Matrix
- mit Lucas-Kette: bestimmte Form der Rekursionsgleichung gegeben, dafür einfache Formel, die Glieder explizit auszurechnen; rechnen im Ring $((\mathbb{Z}_q[t]/f)[s])/(s^2 - a \cdot s + b)$