Proseminar: Mathematik in Computerspielen

Delaunay-Triangulierung

16.1.2017

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 $\forall a \in \mathbb{N}$:
$a^{p-1} = 1 \text{ mod } p$

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

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

Fermat

Fermat für Polynome

Ist f irreduzibel über $\mathbb{Z}_q$, so gilt $\forall a \in \mathbb{Z}_q[x]$:
$a^{q^{deg(f)}-1} = 1 \text{ mod } f$

Miller-Rabin

- finde $s, u \in \mathbb{N}$, u ungerade mit $p - 1 = 2^s u$
- wähle a
- teste ob $a^u = 1 \bmod p$
- für $1 \leq t \leq s$, teste ob $a^{2^s u} = -1 \bmod p$

Miller-Rabin für Polynome

- finde $s, u \in \mathbb{N}, u$ ungerade mit $q^{deg(f)} - 1 = 2^s u$
- wähle a
- teste ob $a^u = 1 \mod f$
- für $1 \leq t \leq s$, teste ob $a^{2^s u} = -1 \mod f$

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, $f \nmid a$:
$(a/f)_d = a^{(|f|-1)/d} \mod f$

Reziprozitätsgesetz

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

Jacobi Symbol

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

Reziprozitätsgesetz

Seien f, g irreduzible Polynome. Dann gilt: noch einfügen!

Power-Residue Test

- Nutze Reziprozitätsgesetz, um $(a/f)_d$ zu berechnen
- vergleiche Ergebnis mit der Definition

Laufzeit

Ein Durchlauf sehr schnell; vergleichbar mit isirreducible Problem: gibt oft fälschlicherweise true aus abhängig von a

Pocklington

Inhalt...

Lucas-Folgen

Rekursiv definierte Folgen