Polynomials and Prime Numbers

Andreas Aabrandt, aabrandt@di.ku.dk

September 12, 2017

Department of Computer Science
University of Copenhagen

Overview

About me

The Problem

What you really need to know to solve the problem

About me

About me - Andreas Aabrandt

Research interests include: parallel algorithms, discrete mathematics and number theory.

Positions

- 2017-present Postdoc
  University of Copenhagen.
- 2016-2017 Data analyst
  Massive Entertainment — A Ubisoft Studio.
- 2013-2016 Ph.D. candidate
  Technical University of Denmark.

The Problem

The Problem

Find polynomials in $\mathbb{Z}_p[x]$ without linear factors.

This is interesting because we can contruct new fields using these irreducible polynomials.

The Problem - an example

Consider polynomials in $\mathbb{Z}_3[x]$. These polynomials have coefficients $0, 1$ or 2, e.g.,

$$f(x) = x^2 + 2x + 2.$$

Coefficients are added modulo 3, so $x^2 + 1 + 2x^2 + 2 = 0$ in $\mathbb{Z}_3[x]$. The polynomial f does not have any linear factors and thus **it is irreducible.**

To construct a finite field of order $3^2 = 9$ we consider

$$\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 2x + 2).$$

The Problem - an example

An element in $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+2x+2)$ is a polynomial in $\mathbb{Z}_3[x]$ with degree less than 2. We use the equivalence

$$x^2 = -2x - 2 = x + 1.$$

The elements of $\mathbb{F}_9$ are $\{0, 1, 2, x, x+1, 2x, 2x+1, 2x+2\}$.

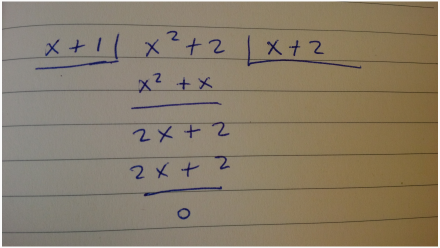
$a * b$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x+1$	2	x	$x+2$	$2x$	1
$x+2$	0	$x+2$	$2x+1$	1	x	$2x+2$	2	$x+1$	$2x$
$2x$	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$
$2x+1$	0	$2x+1$	$x+2$	2	$2x$	$x+1$	1	$2x+2$	x
$2x+2$	0	$2x+2$	$x+1$	$x+2$	1	$2x$	$2x+1$	x	2

Field extensions are only for motivational use!

What you really need to know to solve the problem

What you really need to know

Polynomial division is easy in univariate polynomial rings. Consider the polynomial $g(x) = x^2 + 2 \in \mathbb{Z}_3[x]$. If we want to divide this polynomial with, say $x + 1$, then we get that



Therefore

$$(x + 1)(x + 2) = x^2 + 2,$$

in $\mathbb{Z}_3[x]$. Also, note that $g(a) = 0$ for $a = 1, 2$.

How to solve it

Theorem

For any polynomial $f \in \mathbb{Z}_p[x]$ of degree 2 or 3, it holds that f is reducible if and only if there exists an element $a \in \mathbb{Z}_p$ such that $f(a) = 0$ in $\mathbb{Z}_p[x]$.

Step 1. Generate a large list of primes.

Step 2. For each prime p in the generated list of primes. Construct all polynomials of degree 1,2 and 3.

Step 3. Use the theorem above to check if any of the degree 2 or 3 polynomials are irreducible. Save only the irreducible ones.

Step 4. Generate polynomials of degree 4 and for each of them do polynomial division with irreducible polynomials, already known.

Step 5. Update list of irreducible polynomials and continue to polynomials of higher degrees.

Thank you for your attention

Reach me at: aabrandt@di.ku.dk