Scribe Notes for *Algorithmic Number Theory*
Class 20—June 15, 1998

Scribes: Yizhong Wang, Jeremy Rotter, and Wen Wang

Abstract

The Berlekamp and Cantor-Zassenhaus algorithms for polynomial factorization are covered in this section.

1 The Berlekamp Algorithm

Let $R = \mathbb{F}_p[x]/(f)$ where $f = f_1 f_2 \cdots f_r$. Define $\tau(x) = x^p$ for any $x \in R$, and let

$$B = \{a \in R : a^p = a\} \supseteq \mathbb{F}_p.$$

We know that

$$R \cong \mathbb{F}_p[x]/(f_1) \oplus \mathbb{F}_p[x]/(f_2) \oplus \cdots \oplus \mathbb{F}_p[x]/(f_r),$$

so let $\rho(a) = (a_1, a_2, \cdots, a_r)$ be the isomorphism between the two.

Now we will work out a polynomial factorization by using the Berlekamp algorithm.

Example 1.1. Let $p = 3$ and $f(x) = x^5 + x^2 + 2x + 1$. Then $\tau(x) = x^3$. In order to use the Berlekamp algorithm to find a factor of f, we need the linear transformation T as defined in the previous section. Using $\{1, x, x^2, x^3, x^4\}$ as the basis of $\mathbb{F}_p[x]/(f)$, it is easy to see that

$$\begin{aligned}
\tau(1) &= 1 \\
\tau(x) &= x^3 \\
\tau(x^2) &= x^6 = 2x^3 + x^2 + 2x \\
\tau(x^3) &= x^9 = 2x^4 + x^3 + x^2 + 2x + 2 \\
\tau(x^4) &= x^{12} = x^2 + 2.
\end{aligned}$$

The matrix representation of T is

$$\begin{bmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 \end{bmatrix},$$

and hence, $T - I$ is

$$\begin{bmatrix} 0 & 0 & 0 & 2 & 2 \\ 0 & 2 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 \end{bmatrix}.$$

Using row reduction on $T - I$, we get

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

From this, we can see that $B = \ker(T - I)$ is of dimension two[1] and a vector $(v_0, v_1, v_2, v_3, v_4) \in B$ if and only if $v_1 = v_2 = v_3 = -v_4$. So, we know that $a = (1, 2, 2, 2, 0) \in B$ and the corresponding polynomial representation of a is $x^4 + 2x^3 + 2x^2 + 2x$.

Next, we calculate $\gcd(a - \alpha, f)$ for every $\alpha \in \mathbb{F}_p$ and we know for sure that 2 of them will be nontrivial factors of f. The results are

$$\begin{aligned} \gcd(a - 0, f) &= 1 \\ \gcd(a - 1, f) &= x^3 + 2x + 1 \\ \gcd(a - 2, f) &= x^2 + 1. \end{aligned}$$

So, $x^3 + 2x + 1$ and $x^2 + 1$ are factors of f. The algorithm may return any of them, depending on which one it finds first.

The following are true about this process:

1. Time complexity of finding T is $O((d + \lg p) \lg^2 f)$, where d is the degree of f.
2. Time complexity of row reduction is $O(rd^2 \lg^2 p)$,where r is the rank of the matrix.
3. If f has at least two distinct monic irreducible factors, then the time complexity of the Berlekamp algorithm is $O((d + p) \lg^2 f)$ bit operation.
4. The Berlekamp algorithm is a deterministic algorithm but not a polynomial time one.

2 Cantor-Zassenhaus Algorithm

We assume that p is odd. From the previous discussion, we know that the Berlekamp algorithm is not a polynomial time algorithm. The problem is that after it finds a it checks all the elements of $\mathbb{F}_p$ to find the factor. To find the factor, we may also check whether $\gcd(a, f)$ is a nontrivial factor. If not, $a = (a_1, a_2, \cdots, a_r)$, where all a_i's are non-zero. Consequently, $a^{(p-1)/2} = (\pm 1, \pm 1, \cdots, , \pm 1)$. If there are different signs in this vector, then $\gcd(a^{(p-1)/2} - 1, f)$ is a non-trivial factor. These are the motivations behind the Cantor-Zassenhaus algorithm.

The Cantor-Zassenhaus algorithm can be implemented using the pseudocode in Figure 1.

Theorem 2.1. *The probability that CZ fails is at most* $1/2^{r-1}$. *The time complexity of CZ is* $O((dg\mathrm{f} + \lg \mathrm{p}) \lg^2 \mathrm{f})$.

Now, we do an exercise where we illustrate the Cantor-Zassenhaus algorithm.

[1] This implies that f can be factored into 2 irreducible factors.

$CZ(f)$

1 Find the linear transformation T for which $Ta = a^p$ for all $a \in R$.
2 Compute the kernel of $T - I$ and let $\{b_1, b_2, \cdots, b_r\}$ be a basis.
3 **if** $r = 1$ **then return** "f is irreducible"
4 Choose $x_1, \cdots, x_r \in \mathbb{F}_p$ uniformly at random.
5 $a \longleftarrow \sum_{i=1}^{r} x_i b_i$
6 $g \longleftarrow \gcd(a, f)$
7 **if** $0 < \deg g < \deg f$, **then return** g
8 $s \longleftarrow a^{(p-1)/2}$
9 $g \longleftarrow \gcd(s - 1, f)$
10 **if** $0 < \deg g < \deg f$, **then return** g
11 **return** "bad luck".

Figure 1: Cantor-Zassenhaus Algorithm.

Exercise 2.2. Factor $f(x) = x^3 + x^2 + x + 1$ over $\mathbb{F}_3$ using CZ.
First, we need to find the matrix representation of T.
Choose the basis $\{1, x, x^2\}$ of $\mathbb{F}_3[x]/(f)$. We can compute that

$$\begin{aligned} \tau(1) &= 1 \\ \tau(x) &= x^3 = 2x^2 + 2x + 2 \\ \tau(x^2) &= x^6 = x^2 \end{aligned}$$

The matrix representation of T is

$$\begin{bmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 2 & 1 \end{bmatrix},$$

so $T - I$ is

$$\begin{bmatrix} 0 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 0 \end{bmatrix}.$$

Now we can see that $B = \ker(T - I)$ is of dimension 2 and $\{1, x^2\}$ is a basis. Now, suppose we randomly choose $a = 2x^2+1$. By using *Mathematica*, we find that $\gcd(2x^2+1, x^3+x^2+x+1) = x+1$, so $x + 1$ is a factor. Actually, we can see that f(x) has two factors, $X + 1$ and $X^2 + 1$.

3 Next Time

Next time, we will begin to discuss lattice reduction.