Scribe Notes for *Algorithmic Number Theory*
Class 19—June 12, 1998

Scribes: Scott A. Guyer, Duxing Cai, and Degong Song

Abstract

Today's class continues with the topic of taking d-th roots in $\mathbb{F}_q^*$ including presentation of the AMM algorithm. We also begin to explore factoring polynomials.

1 Roots in $\mathbb{F}_q^*$

Let $a \in \mathbb{F}_q^*$ be an r-th power in $\mathbb{F}_q^*$ where $r \mid q-1$. Adleman, Manders, and Miller developed a generalization of Tonelli's quadratic root algorithm for d-th roots, called the AMM algorithm.
AMM(a, r)

$\triangleright$ Let $q-1 = r^s t$ where $r \not| t$.
$\triangleright$ choose $h \in \mathbb{F}_q^*$ at random
if $h^{(q-1)/r} = 1$
  then Fail
$g \leftarrow h^t$ $\triangleright$ $\langle g \rangle = C_{r^s}$
$(a_r, a_t) \leftarrow (a^t, a^{r^s})$
$e \leftarrow 0$
for $i \leftarrow 0$ **to** $s-1$
  do $\triangleright$ select $0 \le e_i < r$ such that $(ag^{-e_i r^i - e})^{r^{s-i-1}} = 1$
    $e \leftarrow e + e_i r^i r' \leftarrow r^{-1} \pmod t$
$(b_r, b_t) \leftarrow (g^{e/r}, a_t^{r'})$
$\triangleright$ choose α, β such that $\alpha t + \beta r^s = 1$
$b \leftarrow b_r^{\alpha} b_t^{\beta}$
return b

Example 1.1 Let $q = 19$, $q-1 = 23^2$, $r = 3$, $s = 2$, $t = 2$, and $a = \bar{1}1$. We will use the following table for help with computation.

$\mathbb{F}_q^*$	C_{r^s}	C_t	$\mathbb{F}_q^*$	C_{r^s}	C_t
1	1	1	10	5	18
2	4	18	11	7	1
3	9	18	12	11	18
4	16	1	13	17	18
5	6	1	14	6	18
6	17	1	15	16	18
7	11	1	16	9	1
8	7	18	17	4	1
9	5	1	18	1	18

First, we compute line 3 of the algorithm to verify we may have a generator. And indeed, $2^9 = -1$ so we can continue. We calculate $h^2 = 4$ and assign it to g. Continuing with line 6, we assign to (a_r, a_t) the value of $(11^2, 11^9)$, or $(7, 1)$. Next, we initialize e to 0 and jump into the loop.

Case $i = 0$**.**

e_0	$(a_r g^{-e_0})^r = (7 \cdot 4^{-e_0})^3$
0	1
1	11
2	7

So we select $e_0 = 0$. Hence, e remains 0.

Case $i = 1$**.**

e_0	$(7 \cdot 4^{-3e_1})$
0	7
1	1
2	11

Letting $e_1 = 1$ gives us the desired result. So e becomes $0 + (1)3$, or 3.

Continuing outside the loop, we assign $3^{-1} \pmod 2 = 1$ to r'. Computing the roots in line 11, we get $(b_r, b_t) = (4, 1)$. Choosing $\alpha = 5$ and $\beta = -1$ gives us the desired result for line 12. Finally, we compute the root b to be $4^5 \cdot 1^{-1}$ which is 17.

The analysis of the AMM algorithm is provided by Theorem 7.3.2 in [1]. It states that AMM fails with probability $1/r$, corresponding to the probability of not selecting a generator in line 2. The bit complexity of the algorithm is $O(r(\lg q)^4)$.

2 Factoring Polynomials Over Finite Fields

We will assume for the sake of simplicity that we are working with fields $\mathbb{F}_p$ where p is simply a prime. Let $f \in \mathbb{F}_p[X]$. Furthermore, assume that f is monic. The work in factoring polynomials is in finding a non-trivial factor g. In particular, we want to find a factor g such that $g \mid f$ and $\deg g$ is neither 0 nor $\deg f$. Let $f = f_1^{e_1} f_2^{e_2} \cdots f_r^{e_r}$ where each $f_i^{e_i}$ is irreducible and monic. To make this problem interesting, we will also assume that $r \geq 1$ and $e_i \geq 1$.

NOTE: Suppose some $e_i > 1$. Also assume $e_1 \geq 2$. Then take the formal derivative of f using the chain rule.

$$
\begin{aligned}
f'(X) &= \frac{df(X)}{dX} \\
&= e_1 f_1^{e-1}(X) \cdot \frac{d\, f_1(X)}{dX} \cdot f_2^{e_2}(X) \cdots f_r^{e_r}(X) \\
&\quad + f_1^{e_1}(X) \cdot \frac{d\, f_2^{e_2}(X) \cdots f_r^{e_r}(X)}{dX}
\end{aligned}
$$

So, $f_1 \mid f'$. If $f' \neq 0$, then $\gcd(f, f')$ is a non-trivial factor. Henceforth we assume that each $e_i = 1$.

We will introduce some more notation and observations to help develop ideas behind the polynomial factoring algorithm. Recall that by the second version of the CRT, we know

$$R = \mathbb{F}_p[X]/(f) \cong \mathbb{F}_p[X]/(f_1) \oplus \mathbb{F}_p[X]/(f_2) \oplus \cdots \oplus \mathbb{F}_p[X]/(f_r).$$

For some $a \in R$, we define the map $\rho : R \longrightarrow (a_1, a_2, \ldots, a_r)$ where $a_i \in \mathbb{F}_p[X]/(f_i)$. We make two observations.

1. If $b \in \mathbb{F}_p \subseteq \mathbb{F}_p[X]/(f)$, then $\rho(b) = (b_1, b_2, \ldots, b_r)$.
2. If $\rho(a) = (a_1, a_2, \ldots, a_r)$, has a non-zero component a_i, and a 0 component a_j; then $f_i \not| a$ and $f_j \not| a$. Hence, $\gcd(a, f)$ is a non-trivial factor.

2.1 Berlekamp Algebra

The (absolute) Berlekamp algebra of R is

$$B = \{a \in R : a^p = a\}.$$

Note that B is a vector space over $\mathbb{F}_p$ of dimension r and has p^r elements. Also, $\mathbb{F}_p \subseteq B$.

THEOREM 1 (Theorem 7.4.1 in [1]) *If $a \in \mathbb{F}_p[X]/(f)$, then $a \in B$ if and only if each $a_i \in \mathbb{F}_p$, for $1 \leq i \leq r$.*

Proof: $\rho(a) = (a_1, a_2, \ldots, a_r)$. We have the following equalities:

$$\rho(a)^p = \rho(a^p) = (a_1^p, a_2^p, \ldots, a_r^p).$$

If each $a_i \in \mathbb{F}_p$, then $a_i^p = a_i$. Hence, $\rho(a)^p = \rho(a)$. We conclude that $a \in B$.

Conversely, if $a \in B$, then $a^p = a$ implies that $a_i^p = a_i$ for $1 \leq i \leq r$. This implies that

$$a_i^p \equiv a_i \pmod{f_i}.$$

Hence, $f_i \mid a_i^p - a_i$. We use the following equality.

$$X^p - X = \prod_{c \in \mathbb{F}_p} (X - c)$$

Substituting, we get

$$f_i \mid \prod_{c \in \mathbb{F}_p} (a_i - c).$$

We must have $f_i \mid (a_i - c)$ for some $c \in \mathbb{F}_p$. But $\deg(a_i - c) < \deg f_i$ implies that $a_i = c \in \mathbb{F}_p$. □

Finding the Berlekamp algebra B lets us know how many irreducible factors there are in R. Along those lines, we can find out something about B using the Frobenius map $\tau : R \longrightarrow R$ ($\tau(r) = r^p$). Recall that τ is a linear function on R. Since $a^p - a = 0$ for all $a \in B$, B is the kernel of a linear map $\tau - \mathbf{1}$ (where $\mathbf{1}$ is the identity map on R). Hence, the dimension of B is r.

Now suppose that $b \in B - \mathbb{F}_p$. Let $\rho(b) = (b_1, b_2, \ldots, b_r)$. We know $b_i \in \mathbb{F}_p$ for all i, but no all b_i are equal. Then there are i, j such that $b_i \neq b_j$. Then,

$$\rho(b - b_j) = (b_1 - b_j, \ldots, b_i - b_j, \ldots, 0, \ldots, b_r - b_j).$$

Hence, $\gcd(b - b_j, f)$ is a non-trivial factor.

3 Next Time

The next class will begin with a presentation of Berlekamp's algorithm for finding non-trivial factors of a polynomial as well as an example of its execution.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, The MIT Press, Cambridge, Massachusetts, 1996.