Scribe Notes for *Algorithmic Number Theory*
Class 16—June 9, 1998

Scribes: Yizhong Wang, Wen Wang, and Jeremy Rotter

Abstract

This section covers the Euclidean algorithm and continued fractions in a field of Laurent series. The structure for $\mathbb{K}[x]/(f)$ is also discussed.

1 Euclidean Algorithm

Definition 1.1. For a polynomial f, define

$$\mathrm{dg} f = \begin{cases} 1 & \text{if } f = 0; \\ 1 + \deg f & \text{if } f \neq 0. \end{cases}$$

Theorem 1.2. *(6.2.4. from text) Given nonzero polynomials $u, v \in \mathbb{K}[x]$, the extended Euclidean algorithm returns a and b such that $au + bv = \gcd(u, v)$, using $O((\mathrm{dg}u)(\mathrm{dg}v))$ bit operations in $\mathbb{K}$. Moreover, if $\deg u > \deg v > 0$, then we have $\deg a < \deg v$ and $\deg b < \deg u$.*

2 Continued Fractions

Theorem 2.1. *(6.3.1. from text) An element $f \in \mathbb{K}((1/x))$ is rational if and only if its continued fraction expansion is finite.*

Example 2.2. Let

$$f(y) = \frac{x^4y^3 + xy + 1}{x^3y^2 + x^5}.$$

From the previous class, we know the extended Euclidean algorithm gives us

$$\begin{aligned} a_0 &= xy \\ a_1 &= x^5 + 1 \\ a_2 &= xy + x^3. \end{aligned}$$

So,

$$f(y) = a_0 + \cfrac{1}{a1 + \cfrac{1}{a_2}} = xy + \cfrac{1}{x^5 + 1 + \cfrac{1}{xy + x^3}}.$$

Theorem 2.3. *(6.3.2. from text) Let $f(x) = \sum_{i \geq 0} c_i x^{-i}$ be an element of $\mathbb{K}((1/x))$. Then f is rational if and only if the sequence $c_0, c_1, c_2, \ldots$ satisfies a linear recurrence relation.*

Proof. First suppose $f = u/v$. Write

$$\begin{aligned} u &= \sum_{j=0}^{s} u_j x^j \quad \text{where} \quad u_s \neq 0 \\ v &= \sum_{k=0}^{t} v_k x^k \quad \text{where} \quad v_t \neq 0. \end{aligned}$$

For simplicity, assume $u_j = 0$ when j is outside the range $0, \ldots, s$ and $v_k = 0$ if k is outside the range $0, \ldots, t$.

From the definition of f, we know that $t \geq s$. Now,

$$\begin{aligned} u &= \sum_{j=0}^{s} u_j x^j \\ &= vf \\ &= \sum_{i=0}^{\infty} \sum_{k=0}^{t} c_i v_k x^{k-i} \quad \text{substitute } k-i \text{ with } r \\ &= \sum_{r=-\infty}^{t} \left(\sum_{k=r}^{t} c_{k-r} v_k \right) x^r. \end{aligned}$$

So, for $r \geq 0$, we have,

$$\left.\begin{array}{lllllll} r = t, & u_t & = & c_0 v_t, & \text{so } c_0 & = & \dfrac{u_t}{v_t} \\ r = t-1, & u_{t-1} & = & c_1 v_t + c_0 v_{t-1}, & \text{so } c_1 & = & \dfrac{u_{t-1} - c_0 v_{t-1}}{v_t} \\ \vdots & \vdots & & & & \vdots & \\ r = 0, & u_0 & = & c_0 v_0 + c_1 v_1 + \cdots + c_t v_t, & \text{so } c_t & = & \dfrac{u_0 - c_0 v_0 \cdots - c_{t-1} v_{t-1}}{v_t} \end{array}\right\} \quad (*)$$

For $r < 0$ we have,

$$0 = \sum_{k=r}^{t} c_{k-r} v_k = \sum_{k=0}^{t} c_{k-r} v_k.$$

The second equality holds because $v_k = 0$ if k is outside the range $0, \ldots, t$. Then we get,

$$v_t c_{t-r} = -\sum_{k=0}^{t-1} c_{k-r} v_k$$

or

$$\begin{aligned} c_{t-r} &= \sum_{k=0}^{t-1} \left(-\frac{v_k}{v_t} \right) c_{k-r} \\ v_t &= \sum_{k=0}^{t-1} \left(-\frac{c_{k-r}}{c_{t-r}} \right) v_k. \end{aligned}$$

Making the substitution $i = t - r$ in the first equation, we get

$$c_i = \sum_{k=0}^{t-1} \left(-\frac{v_k}{v_t} \right) c_{i+k-t}.$$

Making the substitution $j = i + k - t$, we now get

$$c_i = \sum_{j=i-t}^{i-1} \left(-\frac{v_{j-i+t}}{v_t} \right) c_j,$$

so we have

$$\left.\begin{array}{rcl} c_i & = & \displaystyle\sum_{j=i-t}^{i-1} \left(-\frac{v_{j-i+t}}{v_t} \right) c_j \\ v_t & = & \displaystyle\sum_{k=0}^{t-1} \left(-\frac{c_{k-r}}{c_{t-r}} \right) v_k. \end{array}\right\} \quad (**)$$

Now we can see that if $f(x)$ is rational, $(*)$ and $(**)$ give the base case and the linear recurrence relation, respectively. On the other hand, if $(*)$ and $(**)$ hold for $f(x)$, we can find a pair of polynomials u and v from $(*)$ and $(**)$ such that $f(x) = \frac{u}{v}$, i.e., $f(x)$ is rational. □

The following example is an application of Theorem 2.3, used in pseudorandom sequence generation.

Example 2.4. Let $\mathbb{K} = \mathbb{F}_2, u = 1$ and $v = x^3 + x + 1$. Let $t = 3$ and $s = 0$.

- From $(*)$ we get $c_0 = 0$, $c_1 = 0$, $c_2 = 0$, and $c_3 = 1$.
- From $(**)$ we get the recurrence relation, for $i > 3$,

$$\begin{array}{rcl} c_i & = & \displaystyle\sum_{j=i-3} i - 1(-v_{j-i+3})c_j \\ & = & v_0 c_{i-3} + v_1 c_{i-2} + v_2 c_{i-1} \\ & = & c_{i-2} + c_{i-3}. \end{array}$$

From this relation, we can generate the pseudorandom sequence,

$$0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, \ldots$$

3 The Structure of $\mathbb{K}[x]/(f)$

Theorem 3.1 (CRT version 2). *(6.6.1. from text) Let $f_1, f_2, \ldots, f_r$ be polynomials of positive degree in $\mathbb{K}[x]$ that are pairwise relatively prime, and let f denote there product. Then*

$$\mathbb{K}[x]/(f) \cong \mathbb{K}[x]/(f_1) \oplus \mathbb{K}[x]/(f_2) \oplus \cdots \oplus \mathbb{K}[x]/(f_r).$$

Theorem 3.2 (CRT version 1). *Let f and $f_1, f_2, \ldots, f_r$ be as in the previous theorem. Then there exists a solution $a \in \mathbb{K}[x]$ to the system of congruences*

$$\begin{aligned} a &\equiv a_1 \pmod{f_1} \\ a &\equiv a_2 \pmod{f_2} \\ &\vdots \\ a &\equiv a_r \pmod{f_r}. \end{aligned}$$

Moreover, a is unique modulo f and a can be computed in $O((\lg f)^2)$ bit operations, assuming $\deg a_i < \deg f_i$.

Example 3.3. Let $\mathbb{K} = \mathbb{F}_8$ and find a such that

$$\begin{aligned} a &\equiv x^3 \pmod{y + x^6} \\ a &\equiv x^2 \pmod{y + x} \\ a &\equiv x^4 \pmod{y + x^5}. \end{aligned}$$

Here, we use the same notation we have used before with the Chinese remainder theorem:

$$\begin{array}{rclcrclcrcl} m_1 &=& y + x^6 && m_2 &=& y + x && m_3 &=& y + x^5 \\ a_1 &=& x^3 && a_2 &=& x^2 && a_3 &=& x^4. \end{array}$$

First, we solve for e_1. We start by computing

$$f_1 = m_2 m_3 = (y + x)(y + x^5) = y^2 + x^6 y + x^6.$$

Now that we have f_1, we can compute

$$\overline{f_1} = f_1 \pmod{m_1} = x^6.$$

From here, we can easily see that

$$\overline{f_1}^{-1} = x,$$

so we can compute e_1:

$$e_1 = f_1 \overline{f_1}^{-1} = xy^2 + y + 1.$$

Computing e_2 requires the same steps:

$$\begin{aligned} f_2 &= m_1 m_3 = (y + x^6)(y + x^5) = y^2 + xy + x^4 \\ \overline{f_2} &= f_2 \pmod{m_2} = x^4 \\ \overline{f_2}^{-1} &= x^3 \\ e_2 &= f_2 \overline{f_2}^{-1} = x^3 y^2 + x^4 y + 1, \end{aligned}$$

as does e_3:

$$\begin{aligned} f_3 &= m_1 m_2 = (y + x^6)(y + x) = y^2 + x^5 y + 1 \\ \overline{f_3} &= f_3 \pmod{m_3} = 1 \\ \overline{f_3}^{-1} &= 1 \\ e_3 &= f_3 \overline{f_3}^{-1} = y^2 + x^5 y + 1. \end{aligned}$$

Now, finding a is simply a matter of plugging values into the equation

$$\begin{aligned} a &= a_1e_1 + a_2e_2 + a_3e_3 \\ &= x^4y^2 + x^3y + x^3 + x^5y^2 + x^6y + x^2 + x^4y^2 + x^2y + x^4 \\ &= x^5y^2 + xy + 1. \end{aligned}$$

Theorem 3.4. *(6.6.3. from text) $\mathbb{F}_q^*$ is a cyclic group of order $q-1$ (where $q = p^n$ for some prime p).*

Proof. Let e be the smallest integer such that $x^e = 1$ for all $x \in \mathbb{F}_q^*$. Alternately,

$$e = \operatorname*{lcm}_{x \in \mathbb{F}_q^*} \operatorname{ord}(x).$$

Invoking some group theory, we know that $e \mid q-1$, since $\mathbb{F}_q^*$ must contain an element of order e. Also, $x^e - 1$ has $q-1$ roots in $\mathbb{F}_q^*$, so $e \geq q-1$. Hence $e = q-1$.

Therefore, $\mathbb{F}_q^*$ contains an element of order $q-1$ and must be cyclic of order $q-1$. □

4 Galois Theory

Definition 4.1. A polynomial $f \in \mathbb{F}_{p^n}[x]$ of degree n that is irreducible over $\mathbb{F}_p$ is *primitive* if a root x of f generates the cyclic group $\mathbb{F}_{p^n}^*$. Such a root is called a *primitive element* of $\mathbb{F}_{p^n}$.

Theorem 4.2. *The number of primitive polynomials of degree n over $\mathbb{F}_p$ is $\phi(p^n-1)/n$ and the number of primitive elements of $\mathbb{F}_{p^n}$ is $\phi(p^n-1)$.*

Proof. $\mathbb{F}_{p^n}^*$ is a cyclic group of order p^n-1. Hence it has $\phi(p^n-1)$ generators or primitive elements. Each primitive element has a minimal polynomial of degree n that is primitive. All the roots of that polynomial are primitive[1]. Hence, the number of primitive polynomials is $\phi(p^n-1)/n$. □

5 Next Time

Next time, we will begin to study chapter 7. We should cover sections 7.1 through 7.4.

[1]This statement needs to be proved by using the properties of the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$.