Scribe Notes for *Algorithmic Number Theory*
Class 15—June 8, 1998

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

Abstract

Properties of finite fields are discussed and, in particular, the relationship between the classical and more general settings of number theory is explored.

1 Classical Setting

The classical number theory setting based on the integers has the following relationship between units, integer, rationals, and reals:

$$U = \{-1, 1\} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R},$$

where as usual, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ represent the set of integers, rational numbers, and real numbers.

$\mathbb{Q}$ can be viewed as a field of fractions with the following construction:

$$\{(p, q) : p \in \mathbb{Z}, q \in \mathbb{Z} - \{0\}\}$$

modulo an equivalence relation $(p, q) \equiv (r, s)$ if $ps = qr$.

$\mathbb{R}$ can be viewed as a field of "power series" over a base b with following construction:

Choose $b \in \mathbb{Z}^+ - \{0\} - U$ as base. Any element $a \in \mathbb{Z}$ can be uniquely written as $\displaystyle\sum_{i=0}^{k} c_i b^i$ where $0 \leq c_i < b$, $c_k \neq 0$ if $a \neq 0$. If we divide a by b, we get $a = qb + r$, $0 \leq r < b$. We want $c_0 = r$ and $q = \displaystyle\sum_{i=0}^{k-1} c_{i+1} b^i$. General element in $\mathbb{R}$ is $\displaystyle\sum_{i \leq k} c_i b^i$.

Example 1.1. $b = 5, a = \frac{1}{3}$. We can use long division to get the c_i as shown in Figure 1.

$\mathbb{R}$ can be written as

$$\mathbb{R} = \{(k, (c_k, c_{k-1}, c_{k-2}, \ldots)) : k \geq 0, 0 \leq c_i < b\}.$$

It has the following properties:

1. $\mathbb{Q} \subseteq \mathbb{R}$. In particular,
$$(k, (c_k, c_{k-1}, c_{k-2}, \ldots)) \in \mathbb{Q}$$
when $c_k, c_{k-1}, c_{k-2}, \ldots$ is ultimately periodic with some period. Also, when such a sequence satisfies a linear recurrence relation, then it is a element of $\mathbb{Q}$. The following example illustrates property 1.

$$
\begin{array}{r l}
 & \;\;\;\;\;\;\;1\,3\,1\,3\,\ldots \\ \cline{2-2}
3 & \big)\, 1.\,0\,0\,0\,0\,\ldots \\
 & \;\;\;\;\;\;3 \\ \cline{2-2}
 & \;\;\;\;\;\;2\,0 \\
 & \;\;\;\;\;\;1\,4 \\ \cline{2-2}
 & \;\;\;\;\;\;\;\;\;1\,0 \\
 & \;\;\;\;\;\;\;\;\;\;\;\;3 \\ \cline{2-2}
 & \;\;\;\;\;\;\;\;\;\;\;\;2\,0 \\
 & \;\;\;\;\;\;\;\;\;\;\;\;1\,4 \\ \cline{2-2}
\end{array}
$$

Figure 1: Long division for Example 1.1

Example 1.2. $b = 5$, $a = \frac{1}{3}$. From the previous example, we can see that the following recurrence relations holds:

$$c_{-i} = c_{-i+2} \;\text{ for }\; i \geq 3,$$

or, alternatively,

$$c_{-i} = 4 - c_{-i+1} \;\text{ for }\; i \geq 2.$$

2. An alternative representation for $\mathbb{R}$ is by continued fraction:

$$[a_0, a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \ldots}}.$$

In this representation, if $a \in \mathbb{Q}$, then it has a finite continued fraction. If the continued fraction is periodic, then a corresponds to an algebraic number; otherwise, it corresponds to a transcendental number.

Algorithm analysis in the classical settings depends on the complexity of the basic operations, $+, -, \times, \div$, in $\mathbb{Z}$.

2 A More General Setting

Given any field k, we can derive a similar structure of relationships as in the classical setting.

$$k \subseteq k[X] \subseteq k(X) \subseteq k((1/X))$$

where, we will see in the following, $k[X]$ is the polynomial ring defined on k, $k(X)$ is the rational function field, and $k((1/X))$ is a field of "power series" over a base.

2.1 Euclidean Domain R

The following is a definition taken from [1]. Given any general ring R, there is a function ϕ

$$\phi : R \longrightarrow \mathbb{Z}$$

satisfying

1. $\phi(x) \geq 0$;
2. $\phi(x) = 0$ if and only if $x = 0$;
3. $\phi(xy) = \phi(x)\phi(y)$; and,
4. if $x, y \in R$ and $y \neq 0$, then there exist unique q, r such that $x = qy + r$ with r satisfying $0 \leq \phi(r) < \phi(y)$.

From condition 2, we know for a unit element e, $\phi(e) = 1$.

Example 2.1. Consider first the case where R is $\mathbb{Z}$. Then we can take $\phi(n) = |n|$. If R is $k[X]$ for some field k, then ϕ can be defined by

$$\phi(f) = \begin{cases} 0 & \text{if } f = 0, \\ 2^{\text{deg} f} & \text{otherwise.} \end{cases}$$

Now for any field k, we can define all the entities in

$$k \subseteq k[X] \subseteq k(X) \subseteq k((1/X)).$$

- $k[X]$ is the polynomial ring defined on k.
- $k(X)$ is the rational function field with following construction: The rational functions, p/q, are the set $\{(p, q)|p \in k[X], q \in k[X] - \{0\}\}$ modulo the equivalence relation $(p, q) \equiv (r, s)$ if $ps = qr$. For example,
$$\frac{X^3 + 3X + \frac{5}{7}}{-\frac{11}{12}X^7 + \frac{18}{13}X^5 + 2} \in k(X)$$
if we take k as $\mathbb{Q}$ or some other suitable field.
- $k((1/X))$ is the field of "power series" over a base b with the following construction:
Choose $b \in k[X]$ with $\phi(b) = 2$ as the base (i.e., think of $b = X$). Given $f \in k[X]$ write $f = \sum_{i=0}^{k} c_i b^i$ uniquely where $0 \leq \phi(c_i) < 2 = \phi(b)$, $c_k \neq 0$ if $a \neq 0$. If we divide a by b, we get $a = qb + r$, $0 \leq r < b$. We want $c_0 = r$ and $q = \sum_{i=0}^{k-1} c_{i+1} b^i$.

A general element of k((1/X)) has the form

$$\sum_{i \leq k} c_i X^i.$$

Example 2.2. Let $b = X$, $k = \mathbb{R}$. By virtue of the long division method, we can see the following.

$$\begin{aligned} \frac{X^2+1}{X-1} &= X + 1 + \frac{2}{X} + \frac{2}{X^2} + \frac{2}{X^3} + \cdots \text{ and,} \\ \frac{X^3+X+1}{X^2-X} &= X + 1 + \frac{2}{X} + \frac{3}{X^2} + \frac{3}{X^4} + \cdots. \end{aligned}$$

It is interesting to notice that the integral part of an element in $k((1/X))$ is the portion associated with non-negative powers of the series expansion. In the previous example, this is just $X+1$. Also, note that the rationals in $k((1/X))$ are just the elements of $k(X)$.

3 Euclidean Algorithm in the General Setting

In this section, we investigate the algorithms obtained for the classical setting as applied to the more general setting.

Definition 3.1. Fix the field k. Let $u, v \in k[X]$. Define the greatest common divisor of u and v by:

$$\gcd(u,v) = \begin{cases} 0 & \text{if } u = v = 0, \\ u' & \text{if } v = 0, u \neq 0, \text{and } u' \text{ has a certain property,} \\ v' & \text{if } u = 0, v \neq 0, \text{and } v' \text{ has a certain property,} \\ h & \textit{otherwise.} \end{cases}$$

where $h \in k[X]$ is the unique monic polynomial such that $h \mid u$, $h \mid v$, and for every d that divides both u and v, $d \mid h$. The certain property referred to for both u' and v' is that they must be the unique monic polynomial of degree equal to $\deg u$ that divides u.

Theorem 3.2. (Theorem 6.2.2, Unique division in $k[X]$.) *Let u and v be polynomials in $k[X]$, with $v \neq 0$. Then there exist unique polynomials q and r such that*

$$u = qv + r$$

where $\deg r < \deg v$. *By convention, we take* $\deg 0 = -\infty$.

Given the theorem above and the Euclidean domain, we can run the (extended) Euclidean algorithm on u, v to get $a, b \in k[X]$ such that $au + bv = \gcd(u,v)$. The algorithm is the same, though the time complexity might be different as it is relative to the complexity of the operations in the field.

Example 3.3. Let $k = \mathbb{F}_8$, and consider the following u and v in $k[Y]$:

$$\begin{aligned} u_0 = u &= (X^2+X)Y^3 + XY + 1 \\ &= X^4Y^3 + XY + 1 \\ u_1 = v &= (X+1)Y^2 + (X^2+X+1) \\ &= X^3Y^2 + X^5 \end{aligned}$$

using the table for $\mathbb{F}_8$ that was constructed in the previous class. Using long division, we get

$$\begin{aligned} u_0 &= a_0u_1 + u_2 \text{ with } a_0 = XY, u_2 = X^5Y + 1; \\ u_1 &= a_1u_2 + u_3 \text{ with } a_1 = X^5Y + 1, u_3 = X^4; \\ u_2 &= a_2u_3 + u_4 \text{ with } a_2 = XY + X^3, u_4 = 0. \end{aligned}$$

From the last equation, we get $d = \gcd(u, v) = u_3 = X^4$ and thus $n = 3$. Hence,

$$\begin{aligned} a &= (-1)^nQ_1(a_1) \\ &= -a_1 \\ &= -(X^5Y + 1) \\ &= X^5Y + 1, \end{aligned}$$

and

$$\begin{aligned} b &= (-1)^{n+1}Q_2(a_0, a_1) \\ &= a_0a + 1 \\ &= XY(X^5Y + 1) + 1 \\ &= X^6Y^2 + XY + 1. \end{aligned}$$

We can see that $au + bv = X^4$. However, to match the theorem, we would like to make the expression monic. So we multiply by X^3 which yields

$$\begin{aligned} a' &= X^3a \\ &= XY + X^3, \text{ and} \\ b' &= X^3b \\ &= X^2Y^2 + X^4Y + X^3. \end{aligned}$$

Finally, we can verify that everything is still correct by checking to see that $a'u + b'v = 1$.

References

[1] L. J. Goldstein, *Abstract Algebra*, Prentice-Hall, Englewood Cliffs, New Jersey, 1973.