ANALOGIES WITH POLYNOMIALS

KEITH CONRAD

1. The Basic Analogies

Similarities between $\mathbf{Z}$ and $F[T]$ are an important theme in number theory. The following table collects some analogous concepts in $\mathbf{Z}$ and in $F[T]$.

$\mathbf{Z}$	$F[T]$	Similarity
± 1	nonzero constants	these are the units
prime	irreducible	have only trivial factors
$\lvert n \rvert$	$\deg f$	role in division theorem
positive	monic (lead. coeff $= 1$)	standard unit multiple

A polynomial is called *monic* when it has leading coefficient 1, such as $T^2 + 7T + 3$ but not $2T^2 + 5T - 1$. Every nonzero integer has exactly one positive unit multiple, while every nonzero polynomial in $F[T]$ has exactly one monic unit multiple: just multiply through the polynomial by the inverse of the leading coefficient.

Example 1.1. In $\mathbf{Q}[T]$, the monic unit multiple of $2T^2 + 5T - 1$ is $\frac{1}{2}(2T^2 + 5T - 1) = T^2 + \frac{5}{2}T - \frac{1}{2}$. In $\mathbf{F}_7$, $2 \cdot 4 = 1$, so the monic unit multiple of $2T^2 + 5T - 1$ in $\mathbf{F}_7[T]$ is $4(2T^2 + 5T - 1) = T^2 + 6T + 3$.

Positive integers are closed under multiplication and monic polynomials are closed under multiplication. Positive integers are also closed under addition but monic polynomials are *not* generally closed under addition. This is an important difference!

The standard notation for a prime number in $\mathbf{Z}$ is p. The standard notation for an irreducible polynomial in $F[T]$ is $\pi = \pi(T)$. (This has nothing to do with $3.14159\ldots$, of course.) By definition, a prime in $\mathbf{Z}$ is a number which is not ± 1 and its only factors are ± 1 and $\pm$ itself. Similarly, a polynomial in $F[T]$ is called irreducible when it is nonconstant (that is, is not a unit) and its only factors are nonzero constants and nonzero constant multiples of itself.

Here are some analogous results in $\mathbf{Z}$ and $F[T]$:

(1) In $\mathbf{Z}$, $|mn| = |m||n|$. In $F[T]$, $\deg fg = \deg f + \deg g$.
(2) The units in $\mathbf{Z}$ have absolute value 1 (which is the smallest absolute value possible for nonzero integers) and the units in $F[T]$ have degree 0 (the smallest degree possible for nonzero polynomials).
(3) In $\mathbf{Z}$ if $a|b$ then $|a| \leq |b|$. In $F[T]$, if $f|g$ then $\deg f \leq \deg g$.
(4) If $a|b$ and $b|a$ in $\mathbf{Z}$ then $a = \pm b$, while if $f|g$ and $g|f$ in $F[T]$ then $f = cg$ for some nonzero constant c.
(5) Every integer other than 0 and ± 1 is a product of primes (allowing negative primes!), while every polynomial in $F[T]$ other than a constant is a product of irreducible polynomials.

The most important similarity between $\mathbf{Z}$ and $F[T]$ is the division theorem in both settings. We state them without proof, using similar wording.

Theorem 1.2. *For $a, b \in \mathbf{Z}$ with $b \neq 0$, there are unique q and r in $\mathbf{Z}$ such that $a = bq + r$ with $0 \leq r < |b|$.*

Theorem 1.3. *For $f, g \in F[T]$ with $g \neq 0$, there are unique q and r in $F[T]$ such that $f = gq + r$ with $r = 0$ or $\deg r < \deg g$.*

The greatest common divisor of two integers is the common divisor largest in size (so always positive). In $F[T]$, the greatest common divisor of two polynomials is the common monic polynomial factor with the largest degree. Examples will be worked out in the next section.

Two integers are called relatively prime when their only common factors are ± 1. Similarly, two polynomials in $F[T]$ are called relatively prime when their only common factors are nonzero constants. In both $\mathbf{Z}$ and $F[T]$, relative primality means the only common factors are units. Euclid's algorithm is the standard method to compute greatest common divisors in $\mathbf{Z}$ (so, in particular, to determine relative primality) while a variant of Euclid's algorithm in $F[T]$ will perform the same role for polynomials.

The standard chain of reasoning

$$\text{div. thm.} \rightsquigarrow \text{Euclid} \rightsquigarrow \text{Bezout} \rightsquigarrow \text{if } p|ab \text{ then } p|a \text{ or } p|b \rightsquigarrow \text{unique fact}^{\text{n}}$$

in $\mathbf{Z}$ carries over to $F[T]$ nearly *verbatim*, with only minor changes needed in most proofs:

$$\text{div. thm.} \rightsquigarrow \text{Euclid} \rightsquigarrow \text{Bezout} \rightsquigarrow \text{if } \pi|fg \text{ then } \pi|f \text{ or } \pi|g \rightsquigarrow \text{unique fact}^{\text{n}}.$$

There is one important *difference* between $\mathbf{Z}$ and $F[T]$. Division in $\mathbf{Z}$ involves remainders ≥ 0, so if two integers are relatively prime Euclid's algorithm will *always* have last nonzero remainder 1. But this is false with polynomials: the last nonzero remainder in Euclid's algorithm for polynomials might be a nonzero constant other than 1, so writing an $F[T]$-linear combination of relatively prime polynomials as 1 can involve some additional scaling which we don't have to do in $\mathbf{Z}$.

Example 1.4. In $\mathbf{R}[T]$, let $f(T) = T^2 + 1$ and $g(T) = T - 1$. Certainly $f(T)$ and $g(T)$ are relatively prime: they have no common factor in $\mathbf{R}[T]$ other than nonzero constants. When we carry out Euclid's algorithm on these two polynomials we find

$$\begin{aligned} T^2 + 1 &= (T-1)(T+1) + 2 \\ T - 1 &= 2\left(\frac{1}{2}T - \frac{1}{2}\right) + 0, \end{aligned}$$

so the last nonzero remainder is 2. This is a nonzero constant in $\mathbf{R}[T]$ but it is not 1. By *convention* we normalize the gcd of two polynomials to be monic, so the gcd of $T^2 + 1$ and $T - 1$ is called 1, not 2.

2. Euclid and Bezout: examples

Bezout's identity in $\mathbf{Z}$ says for a and b in $\mathbf{Z}$ that we can write

$$ax + by = (a, b)$$

for some integers x and y. Values for x and y can be found by using back-substitution into Euclid's algorithm for a and b. Similarly, Bezout's identity for $F[T]$ says for $f(T)$ and $g(T)$ in $F[T]$ that

$$f(T)u(T) + g(T)v(T) = (f, g),$$

for some $u(T)$ and $v(T)$ in $F[T]$. Here too the polynomials $u(T)$ and $v(T)$ can be found using back-susbtitution into Euclid's algorithm for $f(T)$ and $g(T)$.

Example 2.1. Let $f(T) = T^4 + T^3 + T^2 + T + 1$ and $g(T) = T^3 - 2T - 4$. We will perform Euclid's algorithm to compute a greatest common divisor of $f(T)$ and $g(T)$ in $F[T]$ for various fields F.

In $\mathbf{Q}[T]$, the gcd of $f(T)$ and $g(T)$ is found as follows:

$$\begin{aligned} T^4 + T^3 + T^2 + T + 1 &= (T^3 - 2T - 4)(T + 1) + (3T^2 + 7T + 5) \\ T^3 - 2T - 4 &= (3T^2 + 7T + 5)\left(\frac{1}{3}T - \frac{7}{9}\right) + \left(\frac{16}{9}T - \frac{1}{9}\right) \\ 3T^2 + 7T + 5 &= \left(\frac{16}{9}T - \frac{1}{9}\right)\left(\frac{27}{16}T + \frac{1035}{256}\right) + \frac{1395}{256} \\ \frac{16}{9}T - \frac{1}{9} &= \frac{1395}{256}\left(\frac{4096}{12555}T - \frac{256}{12555}\right) + 0. \end{aligned}$$

In practice, once we reach a nonzero constant as a remainder we can stop, just as we do when we get a remainder of 1 in Euclid's algorithm for $\mathbf{Z}$: the next step will definitely have a remainder of 0, so the nonzero constant remainder $\frac{1395}{256}$ will be the last nonzero remainder and there is no point in performing the next step. Since the last nonzero remainder is a nonzero constant, f and g are relatively prime in $\mathbf{Q}[T]$. Even though the last nonzero remainder is not 1, but some other nonzero constant, we still write "$(f, g) = 1$" because (f, g) denotes the *monic* greatest common divisor.

Now we will compute (f, g) in $\mathbf{F}_p[T]$ for small p, with the same $f(T)$ and $g(T)$ as above.

In $\mathbf{F}_2[T]$, $g(T) = T^3$ (the linear and constant terms in $g(T)$ are 0 in $\mathbf{F}_2$). Then Euclid's algorithm on $f(T)$ and $g(T)$ in $\mathbf{F}_2[T]$ is

$$\begin{aligned} T^4 + T^3 + T^2 + T + 1 &= (T^3)(T + 1) + (T^2 + T + 1) \\ T^3 &= (T^2 + T + 1)(T + 1) + 1, \end{aligned}$$

and we stop at the nonzero constant remainder: $(f, g) = 1$ in $\mathbf{F}_2[T]$.

In $\mathbf{F}_3[T]$, $g(T) = T^3 + T + 2$ and Euclid's algorithm on $f(T)$ and $g(T)$ is

$$\begin{aligned} T^4 + T^3 + T^2 + T + 1 &= (T^3 + T + 2)(T + 1) + (T + 2) \\ T^3 + T + 2 &= (T + 2)(T^2 + T + 2) + 1, \end{aligned}$$

so $(f, g) = 1$ in $\mathbf{F}_3[T]$.

In $\mathbf{F}_5[T]$, $g(T) = T^3 + 3T + 1$ and Euclid's algorithm on $f(T)$ and $g(T)$ is

$$\begin{aligned} T^4 + T^3 + T^2 + T + 1 &= (T^3 + 3T + 1)(T + 1) + (3T^2 + 2T) \\ T^3 + 3T + 1 &= (3T^2 + 2T)(2T + 2) + (4T + 1) \\ 3T^2 + 2T &= (4T + 1)(2T) + 0, \end{aligned}$$

so the last nonzero remainder is *not* constant: $f(T)$ and $g(T)$ have greatest common divisor $4T + 1$ in $\mathbf{F}_5[T]$, so their monic gcd is its monic scalar multiple $(f, g) = -(4T + 1) = T + 4$. We can explicitly factor out $T + 4$ from both f and g in $\mathbf{F}_5[T]$:

$$f(T) = (T + 4)(T^3 + 2T^2 + 3T + 4), \quad g(T) = (T + 4)(T^2 + T + 4).$$

In $\mathbf{F}_7[T]$, $g(T) = T^3 + 5T + 3$ and Euclid's algorithm on $f(T)$ and $g(T)$ is

$$\begin{aligned} T^4 + T^3 + T^2 + T + 1 &= (T^3 + 5T + 3)(T + 1) + (3T^2 + 5) \\ T^3 + 5T + 3 &= (3T^2 + 5)(5T) + (T + 3) \\ 3T^2 + 5 &= (T + 3)(3T + 5) + 4, \end{aligned}$$

and we stop since we have reached a nonzero constant, 4. The gcd of f and g in $\mathbf{F}_7[T]$ is 1.

The following table summarizes our computations. We list both the last nonzero remainder in Euclid's algorithm and the gcd to reinforce the fact that these need not be the same: (f,g) is the monic unit multiple of the last nonzero remainder.

$F[T]$	Last Remainder	(f,g)
$\mathbf{Q}[T]$	$1395/256$	1
$\mathbf{F}_2[T]$	1	1
$\mathbf{F}_3[T]$	1	1
$\mathbf{F}_5[T]$	$4T+1$	$T+4$
$\mathbf{F}_7[T]$	4	1

TABLE 1. $f(T)=T^4+T^3+T^2+T+1, g(T)=T^3-2T-4$

Remark 2.2. The case of $\mathbf{F}_5[T]$ sticks out: here we have a nonconstant gcd, but for the rest the gcd is 1. It turns out there is exactly one other p for which $f(T)$ and $g(T)$ are not relatively prime in $\mathbf{F}_p[T]$: in $\mathbf{F}_{31}[T]$, $f(T)$ and $g(T)$ have gcd $T-2$.

Now let's realize Bezout's identity from each of those gcd calculations. We can back-substitute into Euclid's algorithm to write the last nonzero remainder as a polynomial-linear combination of f and g.

In $\mathbf{Q}[T]$, the gcd of $f(T)$ and $g(T)$ is found as follows:

$$\begin{aligned}
\frac{1395}{256} &= (3T^2+7T+5)-\left(\frac{16}{9}T-\frac{1}{9}\right)\left(\frac{27}{16}T+\frac{1035}{256}\right)\\
&= (3T^2+7T+5)-\left((T^3-2T-4)-(3T^2+7T+5)\left(\frac{1}{3}T-\frac{7}{9}\right)\right)\left(\frac{27}{16}T+\frac{1035}{256}\right)\\
&= (3T^2+7T+5)\left(\frac{9}{16}T^2+\frac{9}{256}T-\frac{549}{256}\right)-(T^3-2T-4)\left(\frac{27}{16}T+\frac{1035}{256}\right)\\
&\vdots\\
&= f\cdot\left(\frac{9}{16}T^2+\frac{9}{256}T-\frac{549}{256}\right)+g\cdot\left(-\frac{9}{16}T^3-\frac{153}{256}T^2+\frac{27}{64}T-\frac{243}{128}\right).
\end{aligned}$$

Multiplying through by $256/1395$,

$$1=f\cdot\left(\frac{16}{155}T^2+\frac{1}{155}T-\frac{61}{155}\right)+g\cdot\left(-\frac{16}{155}T^3-\frac{17}{155}T^2+\frac{12}{155}T-\frac{54}{155}\right).$$

Remark 2.3. The common denominator 155 appearing in this equation factors as $5\cdot 31$. This is related to the special roles of 5 and 31 in Remark 2.2!

In $\mathbf{F}_2[T]$ we get by back-substitution from Euclid's algorithm

$$\begin{aligned}
1 &= g-(T^2+T+1)(T+1)\\
&= g-(f-g(T+1))(T+1))\\
&= f\cdot(T+1)+g\cdot(1+(T+1)(T+1))\\
&= f\cdot(T+1)+g\cdot T^2.
\end{aligned}$$

Using back-substitution in $\mathbf{F}_3[T]$,

$$\begin{aligned} 1 &= g-(T+2)(T^2+x+2) \\ &= g-(f-g(T+1))(T^2+T+2) \\ &= f\cdot(2T^2+2T+1)+g\cdot(1+(T+1)(T^2+T+2)) \\ &= f\cdot(2T^2+2T+1)+g\cdot(T^3+2T^2). \end{aligned}$$

In $\mathbf{F}_5[T]$,

$$\begin{aligned} 4T+1 &= g-(3T^2+2T)(2T+2) \\ &= g-(f-g(T+1)(2T+2)) \\ &= f\cdot(3T+3)+g\cdot(1+(T+1)(2T+2)) \\ &= f\cdot(3T+3)+g\cdot(2T^2+4T+3). \end{aligned}$$

The gcd we found in Euclid's algorithm, $4T+1$, is not monic. To write the monic gcd of f and g as an $\mathbf{F}_5[T]$-linear combination of f and g we simply multiply through the equations by $-1=4$:

$$T+4=f\cdot(2T+2)+g\cdot(3T^2+T+2).$$

In $\mathbf{F}_7[T]$,

$$\begin{aligned} 4 &= (3T^2+5)-(T+3)(3T+5) \\ &= (3T^2+5)-(g-(3T^2+5)(5T))(3T+5) \\ &= (3T^2+5)(1+5T(3T+5))+g(4T+2) \\ &= (3T^2+5)(T^2+4T+1)+g(4T+2) \\ &= (f-g(T+1))(T^2+4T+1)+g(4T+2) \\ &= f\cdot(T^2+4T+1)+g\cdot(6T^3+2T^2+6T+1). \end{aligned}$$

Multiplying through by $4^{-1}=2$,

$$1=f\cdot(2T^2+T+2)+g\cdot(5T^3+4T^2+5T+2).$$

We can also do back-substitution in $\mathbf{Q}[T]$. The calculations would be quite tedious to do by hand on account of the large fractions arising in Euclid's algorithm. The result will express $\frac{1395}{256}$ as a $\mathbf{Q}[T]$-linear combination of $f(T)$ and $g(T)$, and then we have to multiply through by the reciprocal $\frac{256}{1395}$ to write 1 as a $\mathbf{Q}[T]$-linear combination of $f(T)$ and $g(T)$. Omitting the intermediate details, the final result is

$$1=f\cdot\left(\frac{16}{155}T^2+\frac{1}{155}T-\frac{61}{155}\right)+g\cdot\left(-\frac{16}{155}T^3-\frac{17}{155}T^2+\frac{12}{155}T-\frac{54}{155}\right).$$

Remark 2.4. The common denominator 155 appearing in this equation factors as $5\cdot 31$. This is related to the special roles of 5 and 31 in Remark 2.2!

3. Solving simultaneous congruences: an example

In $\mathbf{Z}$, if we want to solve the pair of congruence conditions

$$x\equiv 2 \bmod 5, \quad x\equiv 11 \bmod 19,$$

we lift the first congruence to $\mathbf{Z}$ in the form $x=2+5y$ for some $y\in\mathbf{Z}$ and substitute that into the second congruence and solve for y:

$$2+5y\equiv 11 \bmod 19 \Rightarrow 5y\equiv 9 \bmod 19 \Rightarrow y\equiv 17 \bmod 19.$$

Thus $y = 17 + 19z$ for some integer z, so $x = 2 + 5(17 + 19z) = 87 + 95z$, so $x \equiv 87 \bmod 95$. Conversely, if $x \equiv 87 \bmod 95$ then $x \equiv 2 \bmod 5$ and $x \equiv 11 \bmod 19$ since 87 fits both conditions and the modulus 95 is divisible by 5 and 19. This is a special instance of the Chinese remainder theorem in $\mathbf{Z}$.

We can solve polynomial congruences in the same way. Consider in $\mathbf{F}_5[T]$ the two congruence conditions

$$f(T) \equiv 3T \bmod T^2 + 1, \quad f(T) \equiv 2T^2 + 1 \bmod T^3.$$

Here the unknown we are looking for is $f(T)$, *not* T: T is just a variable for the polynomials. We want an $f(T)$ in $\mathbf{F}_5[T]$ which fits both congruence conditions.

Lift the first congruence into $\mathbf{F}_5[T]$ by writing it as

$$f(T) = 3T + (T^2 + 1)g(T) \tag{3.1}$$

for some $g(T) \in \mathbf{F}_5[T]$. Substitute this into the second congruence:

$$3T + (T^2 + 1)g(T) \equiv 2T^2 + 1 \bmod T^3.$$

Subtracting $3T$ from both sides (note $-3T = 2T$ in $\mathbf{F}_5[T]$),

$$(T^2 + 1)g(T) \equiv 2T^2 + 2T + 1 \bmod T^3. \tag{3.2}$$

We now need to invert $T^2 + 1 \bmod T^3$. This will be done with Euclid: in $\mathbf{F}_5[T]$,

$$\begin{aligned} T^3 &= (T^2 + 1)T + 4T, \\ T^2 + 1 &= 4T(4T) + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= T^2 + 1 - 4T(4T) \\ &= T^2 + 1 - 4T(T^3 - (T^2 + 1)T) \\ &= (T^2 + 1)(4T^2 + 1) + T^3(-4T), \end{aligned}$$

so $(T^2 + 1)(4T^2 + 1) \equiv 1 \bmod T^3$. Therefore in $\mathbf{F}_5[T]$, the inverse of $T^2 + 1 \bmod T^3$ is $4T^2 + 1$, so multiplying both sides of (3.2) by $4T^2 + 1$ gives

$$\begin{aligned} g(T) &\equiv (4T^2 + 1)(2T^2 + 2T + 1) \bmod T^3 \\ &\equiv 3T^4 + 3T^3 + T^2 + 2T + 1 \bmod T^3 \\ &\equiv T^2 + 2T + 1 \bmod T^3. \end{aligned}$$

Therefore $g(T) = T^2 + 2T + 1 + T^3 h(T)$ for some $h(T) \in \mathbf{F}_5[T]$, and substituting this formula for $g(T)$ into (3.1) shows any $f(T)$ fitting the two original congruence conditions has the form

$$\begin{aligned} f(T) &= 3T + (T^2 + 1)(T^2 + 2T + 1 + T^3 h(T)) \\ &= T^4 + 2T^3 + 2T^2 + 1 + (T^2 + 1)T^3 h(T), \end{aligned}$$

so

$$f(T) \equiv T^4 + 2T^3 + 2T^2 + 1 \bmod (T^2 + 1)T^3.$$

As a check that $T^4 + 2T^3 + 2T^2 + 1$ fits the original two congruence conditions, in $\mathbf{F}_5[T]$

$$(T^4 + 2T^3 + 2T^2 + 1) - 3T = (T^2 + 1)(T + 1)$$

and

$$(T^4 + 2T^3 + 2T^2 + 1) - (2T^2 + 1) = T^3(T + 2).$$

Therefore $T^4 + 2T^3 + 2T^2 + 1$ works, and more generally any polynomial congruent to $T^4 + 2T^3 + 2T^2 + 1 \bmod (T^2 + 1)T^3$ works. This is the complete set of solutions to both congruences.