

ANALOGIES WITH POLYNOMIALS

KEITH CONRAD

Very early in our mathematical education – in fact in junior high school or in high school itself – we are introduced to polynomials. For a seemingly endless amount of time we are drilled, to the point of utter boredom, in factoring them, multiplying them, dividing them, simplifying them. Facility in factoring a quadratic becomes confused with genuine mathematical talent.

I. Herstein

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	the units
prime	irreducible	have only trivial factors
$ n $	$\deg f$	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 polynomial in $F[T]$ has exactly one monic constant multiple: just multiply through the polynomial by the inverse of the leading coefficient.

Example 1.1. In $\mathbf{Q}[T]$, the monic constant 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 constant 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!

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. Primes will be written as p and irreducible polynomials will be written as $p(T)$.¹

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 $a \mid b$ then $|a| \leq |b|$. In $F[T]$, if $f \mid g$ then $\deg f \leq \deg g$.

¹Some people write irreducible polynomials as $\pi(T)$, where that use of the letter π has nothing to do with the number 3.1415926...

- (4) If $a \mid b$ and $b \mid a$ in \mathbf{Z} then $a = \pm b$, while if $f \mid g$ and $g \mid f$ 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 $\deg r < \deg g$.*

In \mathbf{Z} , the greatest common divisor of two numbers is the common divisor largest in size (so always positive). In $F[T]$, the greatest common divisor of two polynomials is the common monic factor with 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 (± 1 in \mathbf{Z} and nonzero constants in $F[T]$). Euclid's algorithm is the standard method to compute greatest common divisors in \mathbf{Z} (so, in particular, to determine relative primality) and a variant of Euclid's algorithm in $F[T]$ will perform the same role for polynomials. Euclid's algorithm run in reverse leads to a proof of Bezout's identity in both \mathbf{Z} and $F[T]$, where Bezout's identity in \mathbf{Z} says for all integers a and b that

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

for some integers x and y , while Bezout's identity in $F[T]$ says for all $f(T)$ 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 $F[T]$.

The standard chain of reasoning in \mathbf{Z}

div. thm. \rightsquigarrow Euclid \rightsquigarrow Bezout $\rightsquigarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b \rightsquigarrow$ unique factorization,

where p is a prime number, carries over to $F[T]$ nearly *verbatim*, with only minor changes needed in most proofs: in $F[T]$,

div. thm. \rightsquigarrow Euclid \rightsquigarrow Bezout $\rightsquigarrow p(T) \mid f(T)g(T) \Rightarrow p(T) \mid f(T)$ or $p(T) \mid g(T) \rightsquigarrow$ u.f.,

where $p(T)$ is an irreducible.

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 that 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: AN EXAMPLE IN $\mathbf{Q}[T]$

We will work out Euclid's algorithm and Bezout's identity for a pair of polynomials in $\mathbf{Q}[T]$.

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 $\mathbf{Q}[T]$:

$$\begin{aligned} (2.1) \quad T^4 + T^3 + T^2 + T + 1 &= (T^3 - 2T - 4)(T + 1) + (3T^2 + 7T + 5) \\ T^3 - 2T - 4 &= (3T^2 + 7T + 5) \left(\frac{1}{3}T - \frac{7}{9} \right) + \left(\frac{16}{9}T - \frac{1}{9} \right) \\ 3T^2 + 7T + 5 &= \left(\frac{16}{9}T - \frac{1}{9} \right) \left(\frac{27}{16}T + \frac{1035}{256} \right) + \frac{1395}{256} \\ \frac{16}{9}T - \frac{1}{9} &= \frac{1395}{256} \left(\frac{4096}{12555}T - \frac{256}{12555} \right) + 0. \end{aligned}$$

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 let's obtain Bezout's identity for the f and g of Example 2.1 by back substitution into Euclid's algorithm from (2.1):

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

Multiplying through by the reciprocal $256/1395$ makes the left side 1:

$$(2.2) \quad 1 = f \cdot \left(\frac{16}{155}T^2 + \frac{1}{155}T - \frac{61}{155} \right) + g \cdot \left(-\frac{16}{155}T^3 - \frac{17}{155}T^2 + \frac{12}{155}T - \frac{54}{155} \right).$$

3. MODULAR ARITHMETIC IN $\mathbf{Q}[T]$

In \mathbf{Z} , modular arithmetic concerns the congruence relation

$$a \equiv b \pmod{m},$$

which means $m \mid (a - b)$ or $a = b + mk$ for some $k \in \mathbf{Z}$. Every integer is congruent modulo m to its remainder under division by m , and we can add and multiply modulo m without worrying about which representatives we use:

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m}, \quad ac \equiv bd \pmod{m}.$$

All of this can be adapted to polynomials in $F[T]$ for a field F : for a nonconstant $m(T) \in F[T]$, define $f(T) \equiv g(T) \pmod{m(T)}$ when $m(T) \mid (f(T) - g(T))$, or equivalently when $f(T) = g(T) + m(T)k(T)$ for some $k(T) \in F[T]$.

Example 3.1. In $\mathbf{Q}[T]$ we have $T^7 \equiv T^5 + 2T^3 \pmod{T^2 - 2}$ since

$$T^7 - (T^5 + 2T^3) = T^3(T^4 - T^2 - 2) = T^3(T^2 - 2)(T^2 + 1),$$

which is a multiple of $T^2 - 2$.

Every polynomial when divided by $T^2 - 2$ has a remainder of the form $aT + b$, so every polynomial in $\mathbf{Q}[T]$ is congruent modulo $T^2 - 2$ to a polynomial of the form $aT + b$. For example,

$$T^7 = (T^2 - 2)(T^5 + 2T^3 + 4T) + 8T \implies T^7 \equiv 8T \pmod{T^2 - 2}.$$

When $\deg m(T) = d$, every polynomial in $F[T]$ is congruent to a unique “remainder” of the form $a_0 + a_1T + \cdots + a_{d-1}T^{d-1}$.

We can carry out the calculation in the previous example more efficiently by using the fact that $m(T) \equiv 0 \pmod{m(T)}$. From $T^2 - 2 \equiv 0 \pmod{T^2 - 2}$ we have $T^2 \equiv 2 \pmod{T^2 - 2}$, so

$$\begin{aligned} T^3 &= T^2T \equiv 2T \pmod{T^2 - 2}, \\ T^4 &= T^3T \equiv (2T)T \equiv 2T^2 \equiv 2(2) \equiv 4 \pmod{T^2 - 2}, \\ T^7 &= T^3T^4 \equiv (2T)(4) \equiv 8T \pmod{T^2 - 2}. \end{aligned}$$

Example 3.2. In $\mathbf{Q}[T]$ let $f(T) = T^4 + T^3 + T^2 + T + 1$ and $g(T) = T^3 - 2T - 4$ as in Example 2.1. We found in (2.2), from Euclid’s algorithm and back-substitution (and multiplication by the reciprocal of the last nonzero remainder) that

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

Reducing both sides mod g ,

$$f \cdot \left(\frac{16}{155}T^2 + \frac{1}{155}T - \frac{61}{155} \right) \equiv 1 \pmod{g}.$$

Reducing both sides mod f ,

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

In this way we found inverses of $f \pmod{g}$ and $g \pmod{f}$.

4. SOLVING SIMULTANEOUS CONGRUENCES: AN EXAMPLE IN $\mathbf{Q}[T]$

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

$$x \equiv 2 \pmod{5}, \quad x \equiv 11 \pmod{19},$$

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 :

$$2 + 5y \equiv 11 \pmod{19} \Rightarrow 5y \equiv 9 \pmod{19} \Rightarrow y \equiv 36 \equiv 17 \pmod{19}$$

since $4 \cdot 5 \equiv 1 \pmod{19}$. Thus $y = 17 + 19z$ for some integer z , so $x = 2 + 5(17 + 19z) = 87 + 95z$, so $x \equiv 87 \pmod{95}$. Conversely, if $x \equiv 87 \pmod{95}$ then $x \equiv 2 \pmod{5}$ and $x \equiv 11 \pmod{19}$ since 87 fits both conditions and the modulus 95 is divisible by 5 and 19.

In a similar way, for all $a, b \in \mathbf{Z}$, the pair of congruences

$$x \equiv a \pmod{5}, \quad x \equiv b \pmod{19}$$

is equivalent to $x \equiv 20b - 19a \pmod{95}$.

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

$$(4.1) \quad \boxed{f(T) \equiv 3T \pmod{T^2 - 2}, \quad f(T) \equiv 2T^2 + 1 \pmod{T^3}.}$$

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 $\mathbf{Q}[T]$ that fits both congruence conditions in (4.1).

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

$$(4.2) \quad f(T) = 3T + (T^2 - 2)g(T)$$

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

$$3T + (T^2 - 2)g(T) \equiv 2T^2 + 1 \pmod{T^3}.$$

Subtracting $3T$ from both sides,

$$(4.3) \quad (T^2 - 2)g(T) \equiv 2T^2 - 3T + 1 \pmod{T^3}.$$

We now need to invert $T^2 - 2 \pmod{T^3}$. This will be done with Euclid's algorithm: in $\mathbf{Q}[T]$,

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

so

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

so dividing through by -2 gives us

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

Thus $\boxed{(T^2 - 2)(-T^2/4 - 1/2) \equiv 1 \pmod{T^3}}$. Therefore in $\mathbf{Q}[T]$, the inverse of $T^2 - 2 \pmod{T^3}$ is $-T^2/4 - 1/2$. Multiplying both sides of (4.3) by $-T^2/4 - 1/2$ gives

$$\begin{aligned} g(T) &\equiv (-T^2/4 - 1/2)(2T^2 - 3T + 1) \pmod{T^3} \\ &\equiv -T^4/2 + (3/4)T^3 - (5/4)T^2 + (3/2)T - 1/2 \pmod{T^3} \\ &\equiv (-5/4)T^2 + (3/2)T - 1/2 \pmod{T^3} \end{aligned}$$

since $T^3 \equiv 0 \pmod{T^3}$ and $T^4 \equiv 0 \pmod{T^3}$. Therefore

$$g(T) = (-5/4)T^2 + (3/2)T - 1/2 + (T^3)h(T)$$

for some $h(T) \in \mathbf{Q}[T]$, and substituting this formula for $g(T)$ into (4.2) shows an $f(T)$ fitting the two congruences in (4.1) must have the form

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

so

$$\boxed{f(T) \equiv (-5/4)T^4 + (3/2)T^3 + 2T^2 + 1 \pmod{(T^2 + 1)T^3}}.$$

As a check that $(-5/4)T^4 + (3/2)T^3 + 2T^2 + 1$ fits the original congruences in (4.1),

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

and

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

Therefore $(-5/4)T^4 + (3/2)T^3 + 2T^2 + 1$ works, and more generally any polynomial $f(T)$ in $\mathbf{Q}[T]$ such that

$$f(T) \equiv (-5/4)T^4 + (3/2)T^3 + 2T^2 + 1 \pmod{(T^2 - 2)T^3}$$

satisfies the congruences in (4.1). Such $f(T)$ form the complete set of solutions to the congruences in (4.1).

In a similar way, for all $a(T), b(T) \in \mathbf{Q}[T]$, the pair of congruences

$$f(T) \equiv a(T) \pmod{T^2 - 2}, \quad f(T) \equiv b(T) \pmod{T^3}$$

is equivalent to $f(T) \equiv (T^4/4)a(T) + (1 - T^4/4)b(T) \pmod{(T^2 - 2)T^3}$.

5. EXAMPLES IN $\mathbf{F}_p[T]$

Using the same polynomials $f(T) = T^4 + T^3 + T^2 + T + 1$ and $g(T) = T^3 - 2T - 4$ as before, now we will do calculations with them in $\mathbf{F}_p[T]$ for small p . Here think of the coefficients of f and g as integers modulo p .

Example 5.1. We'll calculate (f, g) in $\mathbf{F}_p[T]$ for $p = 2, 3, 5$, and 7 .

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

$$\begin{aligned} (5.1) \quad T^4 + T^3 + T^2 + T + 1 &= (T^3)(T + 1) + (T^2 + T + 1) \\ T^3 &= (T^2 + T + 1)(T + 1) + 1, \end{aligned}$$

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

$$(5.2) \quad \begin{aligned} T^4 + T^3 + T^2 + T + 1 &= (T^3 + T + 2)(T + 1) + (T + 2) \\ T^3 + T + 2 &= (T + 2)(T^2 + T + 2) + 1, \end{aligned}$$

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

$$(5.3) \quad \begin{aligned} T^4 + T^3 + T^2 + T + 1 &= (T^3 + 3T + 1)(T + 1) + (3T^2 + 2T) \\ T^3 + 3T + 1 &= (3T^2 + 2T)(2T + 2) + (4T + 1) \\ 3T^2 + 2T &= (4T + 1)(2T) + 0, \end{aligned}$$

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

$$(5.4) \quad \begin{aligned} T^4 + T^3 + T^2 + T + 1 &= (T^3 + 5T + 3)(T + 1) + (3T^2 + 5) \\ T^3 + 5T + 3 &= (3T^2 + 5)(5T) + (T + 3) \\ 3T^2 + 5 &= (T + 3)(3T + 5) + 4, \end{aligned}$$

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

Table 1 summarizes the last nonzero remainder in Euclid's algorithm and the monic gcd.

$F[T]$	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. Euclid's algorithm on $f(T) = T^4 + T^3 + T^2 + T + 1, g(T) = T^3 - 2T - 4$.

Remark 5.2. In $\mathbf{F}_5[T]$ there is a nonconstant gcd. There is one prime $p \neq 5$ such that $f(T)$ and $g(T)$ are not relatively prime in $\mathbf{F}_p[T]$: in $\mathbf{F}_{31}[T]$, $(f(T), g(T)) = T - 2$.

The denominator 155 in the coefficients of (2.2) factors as $5 \cdot 31$. This is related to the roles of 5 and 31 as primes where $f(T) \bmod p$ and $g(T) \bmod p$ have nonconstant gcd.

Example 5.3. Now we figure out how to write (f, g) in $\mathbf{F}_p[T]$ as a combination of $f(T) \bmod p$ and $g(T) \bmod p$ for $p = 2, 3, 5$, and 7.

In $\mathbf{F}_2[T]$ we get by back-substitution in Euclid's algorithm from (5.1)

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

Using back-substitution in $\mathbf{F}_3[T]$ from (5.2),

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

In $\mathbf{F}_5[T]$ from (5.3),

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

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 $\mathbf{F}_7[T]$ from (5.4),

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

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

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

Example 5.4. Similar to the solution of simultaneous congruences in $\mathbf{Q}[T]$ in Section 4, now consider in $\mathbf{F}_5[T]$ the two congruence conditions

$$(5.5) \quad \boxed{f(T) \equiv 3T \pmod{T^2 - 2}, \quad f(T) \equiv 2T^2 + 1 \pmod{T^3}.$$

To find $f(T)$ in $\mathbf{F}_5[T]$ fitting both congruence conditions, we carry out the same procedure as in $\mathbf{Q}[T]$, but now *all calculations are in $\mathbf{F}_5[T]$* .

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

$$(5.6) \quad f(T) = 3T + (T^2 - 2)g(T)$$

where $g(T) \in \mathbf{F}_5[T]$. Substituting this into the second congruence,

$$3T + (T^2 - 2)g(T) \equiv 2T^2 + 1 \pmod{T^3}.$$

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

$$(5.7) \quad (T^2 - 2)g(T) \equiv 2T^2 + 2T + 1 \pmod{T^3}.$$

To invert $T^2 - 2 \pmod{T^3}$ we use Euclid's algorithm in $\mathbf{F}_5[T]$:

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

so

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

Since $(-2)2 = 1$ in \mathbf{F}_5 , multiply through by 2:

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

Therefore $\boxed{(T^2 - 2)(T^2 + 2) \equiv 1 \pmod{T^3}}$, so in $\mathbf{F}_5[T]$, the inverse of $T^2 - 2 \pmod{T^3}$ is $T^2 + 2$. That tells us to multiply both sides of (5.7) by $T^2 + 2$, and we get

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

Lifting this into $\mathbf{F}_5[T]$ as $g(T) = 4T + 2 + T^3h(T)$ for $h(T) \in \mathbf{F}_5[T]$, substitute this formula for $g(T)$ into (5.6) to obtain a formula for $f(T)$: any $f(T)$ fitting the congruence conditions in (5.5) is

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

so

$$\boxed{f(T) \equiv 4T^3 + 2T^2 + 1 \pmod{(T^2 - 2)T^3}}.$$

To check that $4T^3 + 2T^2 + 1$ fits the conditions in (5.5), in $\mathbf{F}_5[T]$

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

and

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

Therefore $4T^3 + 2T^2 + 1$ works, and more generally every polynomial $f(T)$ in $\mathbf{F}_5[T]$ such that

$$f(T) \equiv 4T^3 + 2T^2 + 1 \pmod{(T^2 - 2)T^3}$$

satisfies the two congruence conditions in (5.5) and such $f(T)$ form the complete set of solutions to the two congruences in (5.5).