ANALOGIES BETWEEN Z AND F[T]: HOMEWORK 1

KEITH CONRAD

Continued fractions.
1. Express the continued fraction \([T, 1, T + 1]\) in \(F(T)\) as a standard continued fraction (that is, nonconstant \(a_n\) for \(n > 1\)). Do likewise for \([T, 1, T, T]\) and \([T, T^2, 1, T - 1]\). Conjecture?

2. Compute the degree of \(1/T^2 - 1/T^3\). Expand this rational function into a (standard) continued fraction.

Quadratic residues.
3. On \(F_3[T]\), compute \((\frac{1}{T+2T+3})\) for all \(f \mod T^2 + T + 2\). How often is the value \(1\)? \(-1\)?

4. \((p = 2)\) On Homework 0, you worked out some aspects of the quadratic residue symbol on \(F_p[T]\) for odd \(p\). Let's look at the case \(p = 2\).
   a) Let \(\pi\) be irreducible in \(F_2[T]\). Show every polynomial \(g \in F_2[T]\) is a square modulo \(\pi\). (Use Lemma 3.1 on the handout about roots and irreducible polynomials.)

   This seems to make the topic of quadratic residues in \(F_2[T]\) trivial. However, there is something interesting one can do in the case \(p = 2\). The substitute theory will revolve around the function

   \[\varphi(x) = x^2 - x = x^2 + x\]

   instead of \(x^2\). (Recall from the end of Homework 0 that \(x^2 + x + d\) is the standardized quadratic with distinct roots in \(F[x]\) when \(F\) has characteristic 2, just like \(x^2 - d\) is when the characteristic is not 2.) Be prepared for a few differences from your usual expectations with quadratic residues, but also keep in mind whatever analogies occur.

   b) Let \(A\) be a (commutative) ring of characteristic 2 (i.e., \(2 = 0\) in \(A\)), such as \(F_2[T]\) or its reduction modulo some polynomial. For \(x, y \in A\), show \(\varphi(x + y) = \varphi(x) + \varphi(y)\). When \(A\) is a field, show \(\varphi(x) = \varphi(y)\) if and only if \(y = x\) or \(y = x + 1\). What multiplicative results for squares (classically) do these additive results resemble?

   c) For irreducible \(\pi\) in \(F_2[T]\), show the number of elements of the form \(g^2 + g \mod \pi\) is \((N\pi)/2\).

   d) For irreducible \(\pi\) in \(F_2[T]\) and \(f \in F_2[T]\), the trace of \(f \mod \pi\) is defined to be

   \[\text{Tr}_\pi(f) := f + f^2 + f^4 + f^8 + \cdots + f^{(N\pi)/2} \mod \pi.\]

   Compute the trace of all polynomials in \(F_2[T]\) modulo \(T^3 + T^2 + 1\). Observations?

   e) Prove \(f \equiv \varphi(g) \mod \pi\) for some \(g \in F_2[T]\) if and only if \(\text{Tr}_\pi(f) \equiv 0 \mod \pi\). (Think about roots of the polynomial \(x + x^2 + x^4 + \cdots + x^{(N\pi)/2}\). What polynomial is this analogous to when \(p \neq 2\)?)

5. For \(f \in F_2[T]\) and irreducible \(\pi\) in \(F_2[T]\), define the symbol \([f, \pi] \in F_2\) by

   \[([f, \pi]) := \begin{cases} 0, & \text{if } f \equiv g^2 + g \mod \pi \text{ for some } g \in F_2[T], \\ 1, & \text{if } f \not\equiv g^2 + g \mod \pi \text{ for any } g \in F_2[T]. \end{cases}\]

   (The additive group \([0,1] = F_2\) is replacing the multiplicative group \(\{±1\}\) as the values of our quadratic symbol \([,\cdot]\). Do not forget: in \(F_2\), 1 is the nonidentity element of the group, so the equation \([f, \pi] = 1\) is like \((\frac{2}{p}) = -1\), not \((\frac{2}{p}) = 1\).) It is immediate from the definition that \(f_1 \equiv f_2 \mod \pi \implies [f_1, \pi] = [f_2, \pi]\).
a) Using the definition, compute \([f, T^3 + T^2 + 1]\) for all \(f \in \mathbb{F}_2[T]\) of degree less than 3. In particular, does the congruence \(x^2 + x \equiv T^2 + 1 \mod T^3 + T^2 + 1\) have a solution in \(\mathbb{F}_2[T]\)?

b) Prove
\[\begin{align*}
[f_1 + f_2, \pi] &= [f_1, \pi] + [f_2, \pi], \\
[f^2, \pi] &= [f, \pi], \\
[1, \pi] &= \deg \pi,
\end{align*}\]
where the integer \(\deg \pi\) in the third formula is viewed in \(\mathbb{F}_2\).

The square bracket on the left side of the symbol \([\cdot, \cdot]\) serves to remind us to be careful: the first coordinate does not behave multiplicatively.

c) Use part b to compute \([T^2 + T + 1, \pi]\) and to give a formula for \([c_2 T^2 + c_1 T + c_0, T^3 + T^2 + 1]\) in terms of the \(c_j \in \mathbb{F}_2\). Compare with your answers in part a.

d) Let \(\pi(T) = a_d T^d + a_{d-1} T^{d-1} + \cdots + a_0\) be irreducible of degree \(d\) in \(\mathbb{F}_2[T]\). (In particular, \(a_d = 1\), and also \(a_0 = 1\) unless \(\pi = T\).) Compute \([T, \pi]\) in terms of \(\pi\).

e) When an integer \(a \in \mathbb{Z}\) is not a perfect square, there are many \(p\) for which \((\frac{a}{p}) = -1\). There is an analogue in \(\mathbb{F}_2[T]\) with the operator \(\varphi(x) = x^2 + x\), illustrated as follows.

In \(\mathbb{F}_2[T]\), find \(g\) such that \(T^6 + T^4 + T^3 + T = \varphi(g)\). (This is an equation in \(\mathbb{F}_2[T]\), not a congruence.) On the other hand, show \(T^4 + T^3\) and \(T^5\) do not have the form \(\varphi(g)\) for any \(g\) in \(\mathbb{F}_2[T]\).

Find irreducible \(\pi\) in \(\mathbb{F}_2[T]\) such that \([T^3 + T^2 + \pi, \pi] = 1\) and then \([T^5, \pi] = 1\).

6. For every \(f \in \mathbb{F}_2[T]\), show there exist \(h, k \in \mathbb{F}_2[T]\) such that \(f = \varphi(h) + k\), where \(\deg k\) is odd or \(k\) is constant. Are \(h, k\) uniquely determined by \(f\)?

Miscellaneous.

7. Here is a nonanalogy to ponder.

a) For any prime \(p\), show \((\mathbb{Z}/p^2)^\times = U_{p^2}\) is a cyclic group.

b) Fix a prime \(p\). For any irreducible \(\pi \in \mathbb{F}_p[T]\) with \(\deg \pi > 1\), show \((\mathbb{F}_p[T]/\pi^2)^\times\) is not a cyclic group. When \(\deg \pi = 1\), show the group is cyclic.

8. Another comparison, this time between \(\mathbb{Z}[X]\) and \(\mathbb{F}_p[T][X]\).

a) For nonconstant \(f(X) \in \mathbb{Z}[X]\), show it is impossible for \(f(n)\) to be prime for all \(n \in \mathbb{Z}\).

b) For nonconstant \(f(X) \in \mathbb{Z}[X]\), show it is impossible for \(f(n)\) to be squarefree for all \(n\): for some \(n \in \mathbb{Z}\) and prime \(p\), \(f(n) \equiv 0 \mod p^2\). (Hint: Explain why, without loss of generality, we can assume \(\deg f\) is irreducible. Then show some \(\mathbb{Z}[X]\)-combination of \(f(X)\) and its derivative \(f'(X)\) is a nonzero integer, say \(c\). Find \(m\) such that \(f(m)\) has a prime factor \(p\) not dividing \(c\). Refine the congruence \(f(m) \equiv 0 \mod p\) to \(f(n) \equiv 0 \mod p^2\) where \(n \equiv m \mod p\).)

c) Working instead with \(f(X) \in \mathbb{F}_p[T][X]\), having positive \(X\)-degree, show it is impossible for \(f(g)\) to be irreducible for all \(g \in \mathbb{F}_p[T]\). In contrast with part b, though, show the polynomial \(X^p + T\) only takes squarefree values on \(\mathbb{F}_p[T]\). That is, show \(g^p + T\) is squarefree for all \(g\) in \(\mathbb{F}_p[T]\). (Hint: derivatives.)

d) Is there a simple formula for \(\mu_{\mathbb{F}_p(T)}(g^p + T)\) in terms of \(p\) and the coefficients and degree of \(g\)?

9. Read Section 1 on the handout about roots and irreducible polynomials.

a) Prove Theorem 1.1 and Corollary 1.3 in the handout.

b) Show the polynomial \(X^p - u \in \mathbb{F}_p(u)[X]\) has no roots in \(\mathbb{F}_p(u)\). Over a large enough field \(K \supset \mathbb{F}_p(u)\) where \(X^p - u\) is a product of linear factors in \(X\), how many distinct roots are there?

10. Suppose \((a(T), b(T)) \in \mathbb{F}[T]\) are relatively prime. In \(\mathbb{F}(T)\), assume the ratio \(a(T)/b(T)\) is a rational function of \(T^3\), i.e., \(a(T)/b(T) = k(T^3)\) where \(k \in \mathbb{F}(T)\). Prove \(a(T)\) and \(b(T)\) are polynomials in \(T^3\). Generalize.