ANALOGIES BETWEEN Z AND $F[T]$: HOMEWORK 3

KEITH CONRAD

Quadratic residues.

1. Use quadratic reciprocity in $\mathbf{F}_p[T]$. (All the moduli below are irreducible.)
a) In $\mathbf{F}_3[T]$, determine if T^2+T+2 is a square modulo $T^5+T^4+T^2+1$.
b) In $\mathbf{F}_5[T]$, determine if T^3+T^2+T is a square modulo $3T^5+T^4+4$.
c) In $\mathbf{F}_7[T]$, determine if $4T^2+T+5$ is a square modulo T^3+6T^2+1.

2. Does the congruence $x^2+(T^3+T)x+2T \equiv 0 \bmod T^4+2T+2$ have a solution in $\mathbf{F}_3[T]$? (The modulus is irreducible.)

3. Here is a typical kind of application of QR, in $\mathbf{Z}$ and in $\mathbf{F}_p[T]$ ($p \neq 2$).
a) Use QR on $\mathbf{Z}$ to show $(\frac{6}{p}) = 1 \Longleftrightarrow p \equiv \pm 1, \pm 5 \bmod 24$.
b) Find a congruence on monic irreducible π in $\mathbf{F}_5[T]$ which is equivalent to $(\frac{2T^3+3T+1}{\pi}) = 1$.

4. For monic irreducible π in $\mathbf{F}_7[T]$, is the condition $(\frac{T}{\pi}) = 1$ determined by a congruence on π?

5. Fix a prime $p \neq 2$. For relatively prime $F, G \in \mathbf{F}_p[T]$, with $\deg G > 0$, write $G = a\pi_1 \cdots \pi_r$ (a lies in $\mathbf{F}_p^\times$ and the irreducible π_i might be associates). Define the Jacobi symbol

$$\left(\frac{F}{G}\right) := \left(\frac{F}{\pi_1}\right) \cdots \left(\frac{F}{\pi_r}\right).$$

a) For $c \in \mathbf{F}_p$, express $(\frac{c}{G})$ in terms of the usual Legendre symbol $(\frac{c}{p})$.
b) Prove an $\mathbf{F}_p[T]$-analogue of Jacobi reciprocity.

6. ($p = 2$, continued) Let π be irreducible in $\mathbf{F}_2[T]$, of degree d, with roots $\alpha_1, \cdots, \alpha_d$ in some field containing $\mathbf{F}_2$. Prove

$$[f, \pi) = f(\alpha_1) + f(\alpha_2) + \cdots + f(\alpha_d).$$

In particular,

$$[T^m, \pi) = \alpha_1^m + \cdots + \alpha_d^m.$$

Compute $[T, \pi)$ in terms of coefficients of π, if you did not do this on Homework 1.

7. (Jacobi symbols in $\mathbf{F}_2[T]$) The symbol $[f, \pi)$ is additive in its first coordinate. Extend its meaning in the second coordinate "logarithmically" to any nonzero $g \in \mathbf{F}_2[T]$: when $g = \pi_1 \cdots \pi_r$ (the π_i's are not necessarily distinct), define

$$[f, g) := [f, \pi_1) + [f, \pi_2) + \cdots + [f, \pi_r).$$

This is a sum, not a product. For example, $[f, 1) = 0$ and $[f, T^2+T) = [f, T) + [f, T+1)$. (The second example should not be confused with $[T^2+T, \pi)$, which is 0.)

a) Check $[f, g_1g_2) = [f, g_1) + [f, g_2)$ for any nonzero g_1, g_2 in $\mathbf{F}_2[T]$. In particular, $[f, g^2) = 0$.
b) Compute $[f, T^3+T^2+T)$ and $[f, T^3+T^2)$ for all f with degree less than 3.

8. The following are three versions of the classical quadratic reciprocity law.

(1) (Euler) For any nonzero integer d and primes p, q not dividing $4d$,

$$p \equiv q \bmod 4d \Longrightarrow \left(\frac{d}{p}\right) = \left(\frac{d}{q}\right), \quad p \equiv -q \bmod 4d \Longrightarrow \left(\frac{d}{p}\right) = (\operatorname{sgn} d)\left(\frac{d}{q}\right),$$

where $\operatorname{sgn} d = \pm 1$ is the sign of d.

(2) (Legendre/Gauss) For any distinct odd primes p and q, $(\frac{q}{p}) = (-1)^{(p-1)/2\cdot(q-1)/2}(\frac{p}{q})$. Moreover, $(\frac{-1}{p}) = (-1)^{(p-1)/2}$ and $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.

(3) (Artin) For any nonzero integer d, there is a group homomorphism $f\colon (\mathbf{Z}/4d)^\times \to \{\pm 1\}$, where $f(p \bmod 4d) = (\frac{d}{p})$ for any prime p not dividing $4d$.

Prove the statements are equivalent. (At least prove the first two are equivalent. Showing (3) $\Longrightarrow$ (1) is trickier.) Since the second statement is the form of QR you are familiar with, it is of course against the rules to use this form of QR in your proof unless you are in a position to be assuming the second statement. All you can use about the Legendre symbol $(\frac{a}{p})$, to start off, is its basic definition and its multiplicativity in a.

9. Is there an analogue of question 8 in the context of QR on $\mathbf{F}_p[T]$, with p odd?

10. (n-th power reciprocity in $\mathbf{F}_p[T]$) Fix a positive integer n and a prime $p \equiv 1 \bmod n$. Since $\mathbf{F}_p^\times$ is cyclic, there are n different nth roots of unity in $\mathbf{F}_p$.

a) Let π be irreducible in $\mathbf{F}_p[T]$. For f not divisible by π, define $(\frac{f}{\pi})_n$ to be the nth root of unity ω in $\mathbf{F}_p$ such that

$$f^{(\mathrm{N}\pi-1)/n} \equiv \omega \bmod \pi.$$

Show there really is such an nth root of unity in $\mathbf{F}_p$, and that $(\frac{fg}{\pi})_n = (\frac{f}{\pi})_n(\frac{g}{\pi})_n$ for f and g not divisible by π.

b) Compute $(\frac{T}{T^3+T+1})_3$ from $\mathbf{F}_7[T]$.

c) For distinct monic irreducibles π_1 and π_2 in $\mathbf{F}_p[T]$, express $(\frac{\pi_2}{\pi_1})_n$ in terms of $(\frac{\pi_1}{\pi_2})_n$. (The case $n = 2$ is quadratic reciprocity.) Don't forget that $p \equiv 1 \bmod n$.

Continued fractions.

11. Let's compare a certain operation on continued fractions in the classical and polynomial setting.

a) Let $\alpha = [a_1, a_2, a_3, \dots] \in F((1/T))$ be a standard infinite continued fraction: $a_n \in F[T]$ and $\deg a_n \geq 1$ for $n \geq 2$. What is the continued fraction for $-\alpha$? For $c\alpha$, with $c \in F^\times$?

b) Let $\alpha = [a_1, a_2, a_3, \dots] \in \mathbf{R}$, with $a_n \in \mathbf{Z}$ and $a_n > 0$ for $n \geq 2$. What is the continued fraction for $-\alpha$?

12. Compute the first six terms in the continued fraction for $\sqrt{T^4+T^3}$ in $\mathbf{Q}((1/T))$ and in $\mathbf{F}_5((1/T))$. Then solve $u^2 - (T^4+T^3)v^2 = 1$ nontrivially in $\mathbf{F}_5[T]$.

13. In $\mathbf{F}_p((1/T))$, let $\alpha = [0, T, T^p, T^{p^2}, \dots, T^{p^n}, \dots]$. Show α is the root of a monic polynomial in $\mathbf{F}_p[T][X]$. (Hint: Compute α^p.) This is an example of an element which is algebraic over $\mathbf{F}_p(T)$ whose continued fraction entries are known to be unbounded. Classically, it is expected that every real irrational number which is algebraic over $\mathbf{Q}$ and nonquadratic has unbounded continued fraction entries, but this is not proved in any example.

Miscellaneous.

14. For nonzero $g(T) = c_nT^n + c_{n-1}T^{n-1} + \cdots + c_1T + c_0$ in $F[T]$ ($c_j \in F$, $c_n \neq 0$), define

$$g^* := \frac{g(T)}{T^{\deg g}} = c_n + \frac{c_{n-1}}{T} + \cdots + \frac{c_1}{T^{n-1}} + \frac{c_0}{T^n}.$$

In particular, $c^* = c$ for $c \in F^\times$ and $(T-1)^* = 1 - 1/T$. Note that g^* is a polynomial in $F[1/T]$.

a) If g is monic, how is this reflected in g^*?

b) Show $(g_1g_2)^* = g_1^*g_2^*$, but $g \mapsto g^*$ is not additive. What is $\deg(g^*)$? (Remember, the degree in $F(T)$ is understood to be defined relative to the parameter T, not $1/T$. Hmm, what's so special about T?)

c) For any nonzero g in $F[T]$, show g^* is a unit in the ring $F[1/T]/(1/T)^r$, $r \geq 1$. In $F[1/T]/(1/T)^5$, compute the multiplicative inverses of $(T^2+T)^*$ and $(T^2-1)^*$.

d) If π is an irreducible in $F[T]$ which is not a multiple of T, show π^* is irreducible in $F[1/T]$.

15. Pythagorean triples are solutions to the equation $a^2 + b^2 = c^2$ in (positive) integers a, b, c. Either a or b is odd. Assuming without loss of generality that a is odd, then a classical result says that when $\gcd(a, b, c) = 1$,

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

for some relatively prime integers $m > n$ with $m \not\equiv n \bmod 2$. (Conversely, this formula produces only relatively prime triples with a odd.)

Generalize a suitable proof of this classical result to describe all solutions to $f^2 + g^2 = h^2$ with $f, g, h \in F[T]$, $\gcd(f, g, h) = 1$, and at least one of f, g, and h nonconstant. Of course (why?), here we suppose F does not have characteristic 2. When F does have characteristic 2, describe all solutions to $f^2 + fg + g^2 = h^2$.

16. (Lucas). Let a, b be nonnegative integers, and p be a prime.

a) When $0 \leq n < p^k$, prove $a \equiv b \bmod p^k \implies \binom{a}{n} \equiv \binom{b}{n} \bmod p$. In particular, $\binom{p-1}{n} \equiv (-1)^n \bmod p$ when $n < p$. (Hint: $(1+T)^{a+p^k} = (1+T)^a(1+T^{p^k})$ in $\mathbf{F}_p[T]$.)

b) Write a and b in base p:

$$a = a_0 + a_1 p + \cdots + a_d p^d, \quad b = b_0 + b_1 p + \cdots + b_d p^d,$$

where $0 \leq a_i, b_i \leq p - 1$. (Some high order digits may be 0 to give the expansions equal length.)

Prove

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_d}{b_d} \bmod p.$$

c) Define the binomial coefficient polynomial $\binom{X}{n} \in \mathbf{Q}[X]$ by $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}$. For example, $\binom{X}{0} = 1, \binom{X}{1} = X$, and $\binom{X}{2} = \frac{X(X-1)}{2}$. Define $\binom{m}{n}$ for $m < 0$ as the value of $\binom{X}{n}$ at $X = m$. (This approach also recovers the usual combinatorial meaning of $\binom{m}{n}$ when $m \geq 0$.) Check $\binom{m}{n} \in \mathbf{Z}$ for all integers m. Is part a true when a or b is allowed to be negative?

17. By a change of variables, we can write $F(T)$ in the form $F(U)$ for other rational functions U. For instance,

$$F(T) = F(T+1) = F(1/T) = F(1/(T+1)) = F((T-1)/(T+1)).$$

The last choice needs $-1 \neq 1$ (why?).

a) Give a formula for T in terms of each of the following rational functions U: $T + 1$, $1/T$, $1/(T+1)$, and $(T-1)/(T+1)$ (when $-1 \neq 1$).

b) When $U = T^2/(T+1)$, prove $F(U)$ is a proper subfield of $F(T)$.

c) Prove $F[T] = F[U] \iff U = aT + b$, where $a \in F^\times$ and $b \in F$. Prove $F(T) = F(U) \iff U = (aT+b)/(cT+d)$ where $a, b, c, d \in F$ with $ad - bc \neq 0$.

d) Let $F(T) = F(U)$. We will say $f \in F(T)$ has a "real" square root with respect to U when f is a square in $F((1/U))$. Otherwise we will say f has an "imaginary" square root with respect to U (*i.e.*, there is no square root of f in $F((1/U))$.)

As an example, let $F = \mathbf{F}_5$. Then $f = 2T^2 + 1$ is not a square in $\mathbf{F}_5((1/T))$, so f has an imaginary square root with respect to T. However, taking $\widetilde{T} = 1/T$, we have $\mathbf{F}_5(T) = \mathbf{F}_5(\widetilde{T})$ and $f = (\widetilde{T}^2 + 2)/\widetilde{T}^2$, so f has a real square root with respect to $\widetilde{T}$. Compute the first few terms in the Laurent expansion of a square root of f in $\mathbf{F}_5((1/\widetilde{T}))$.

Investigate whether $3T^2 + T + 2 \in \mathbf{F}_5(T)$ has real or imaginary square roots with respect to $T, T+1, 1/T$, and $1/(T+1)$.

The notion of "real" versus "imaginary" square roots in the context of $F(T)$, unlike the context of $\mathbf{Q}$, is not completely rigid, since it depends on the choice of U to define the field $F(T) = F(U)$. There are no such choices to be made in the case of the field $\mathbf{Q}$.