ANALOGIES BETWEEN Z AND $F[T]$: HOMEWORK 4

KEITH CONRAD

Quadratic residues.

1. Use QR in $\mathbf{F}_2[T]$ to compute the symbols

$$[T^3+1, T^4+T^3+1), \quad [T^3+1, T^5+T^3+1), \quad [T^5, T^7+T^3+T^2+T+1).$$

(All moduli here are irreducible.)

2. Does the congruence $x^2 + (T^5+T^3+T)x \equiv T^8+T+1 \bmod T^{11}+T^4+T^2+T+1$ have a solution in $\mathbf{F}_2[T]$? (The modulus is irreducible.) Use QR in $\mathbf{F}_2[T]$ to answer the question.

3. (The result of this exercise is used in the proof of the quadratic reciprocity law in $\mathbf{F}_2[T]$.) Let $x_1, \ldots, x_d$ be variables and $p_m = x_1^m + \cdots + x_d^m$ be the m-th power sum, $m \geq 1$.

Consider the identity

$$(1-x_1t)(1-x_2t)\cdots(1-x_dt) = 1 - s_1t + s_2t^2 - \cdots + (-1)^d s_d t^d,$$

where s_j is the jth elementary symmetric function of the x's. Apply the operation $f(t) \mapsto f'(t)/f(t)$ to both sides, then expand them into formal power series ("generating functions") in t to prove, for $1 \leq m \leq d$, that p_m is an integral polynomial in $s_1, \ldots, s_m$. Make these formulas (also called the Newton identities) explicit for $m = 1, \ldots, 5$, over $\mathbf{Z}$ and then over $\mathbf{F}_2$.

(The significance of the operation f'/f is that it is log-like in f, converting products to sums, even if we are in characteristic p where there is no logarithm. In characteristic 0, $f'/f = (\log f)'$.)

4. By QR in $\mathbf{F}_2[T]$,

$$g_1^* \equiv g_2^* \bmod \frac{1}{T^4} \Longrightarrow [T^3, g_1) = [T^3, g_2).$$

a) Compute $[T^3, T^{12}+T^4+T^2+T+1)$. (The degree 12 polynomial is irreducible.)

b) Prepare a table which indicates when $[T^3, \pi) = 0$ in terms of congruence conditions on π^* in $\mathbf{F}_2[1/T]/(1/T)^4$.

Continued fractions.

5. Compute the continued fraction expansion of $\sqrt{1+1/T}$ in $\mathbf{F}_3((1/T))$.

6. Let F be a field with characteristic 2. We extend exercises 1 and 9 on Homework 2 to characteristic 2.

a) For $f \in F((1/T))$, prove $f = \wp(x) = x^2 + x$ for some $x \in F((1/T))$ if and only if the polynomial part of f has the form $\wp(g)$ for some *polynomial* $g \in F[T]$. (Hint: When $|y| < 1$, show $\sum_{n\geq 0} y^{2^n}$ converges in $F((1/T))$ and has $\wp$-value y. Also keep in mind, from Homework 2, that $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$ for any $x \in F((1/T))$ since F has characteristic 2.)

b) Determine which of the following rational functions has the form $\wp(g)$ for some $g \in \mathbf{F}_2((1/T))$: $T/(T+1)$, $(T^3+T+1)/(T+1)$, $T^3/(T^2+1)$.

c) For $b, c \in F[T]$ such that $b \notin F$, assume the equation $u^2 + buv + cv^2 = 1$ has a solution $u, v \in F[T]$ with $v \neq 0$. Prove $x^2 + bx + c$ has roots in $F((1/T))$ and u/v is a convergent to the continued fraction of one of these roots. (Writing "$b \notin F$" in the equivalent form "$b^2 - 4c \notin F$," as $2 = 0$, this result assumes a form *identical* to the case of characteristic $\neq 2$ on Homework 2.)

7. The polynomial $y^2 + Ty + T$ has a root in $\mathbf{F}_2((1/T))$ which begins $T + 1 + 1/T + 1/T^3 + \cdots$.

a) Find the complete Laurent expansion of this root, and also of the other root in $\mathbf{F}_2((1/T))$.

b) Find the (periodic) continued fraction expansions of these two roots.

c) If $u, v \in \mathbf{F}_2[T]$ is a solution to the Pell-type equation $u^2 + Tuv + Tv^2 = 1$ with $v \neq 0$, show that either $\deg u = \deg v$ or $\deg u = \deg v + 1$.

d) Use continued fractions to find a solution to $u^2+Tuv+Tv^2 = 1$ in $\mathbf{F}_2[T]$ with $\deg u = \deg v = 2$, and then with $\deg u = 5, \deg v = 4$. In each case, which root of y^2+Ty+T has u/v as a convergent?

8. Determine a nontrivial solution in $\mathbf{F}_2[T]$ to each of the following equations, or prove no nontrivial solution exists:

$$u^2 + (T+1)uv + T^3v^2 = 1, \quad u^2 + Tuv + (T^2+T)v^2 = 1, \quad u^2 + Tuv + (T^4+T^3+1)v^2 = 1.$$

For those equations without a nontrivial solution in $\mathbf{F}_2[T]$, can you find a nontrivial solution in $\mathbf{F}_4[T]$? (If you are not comfortable with $\mathbf{F}_4$, ignore this last part.)