# Number Theory Homework #5 *Spring 2026*

Instructor: *Chan Ieong Kuan*

Solutions by: ***Haoyu Zhu***

## 10 Equations over finite fields

1. Exercise 10.7:

*Proof.* Since partial differentialtion is linear for polynomials, we only need to prove the cases where $f$ is monic monomial, write $f = \prod_{i=0}^{n} x_i^{e_i}$ with $\sum_{i=0}^{n} e_i = m$ and $e_i \geq 1$, then in general for $g = \sum_j a_j g_j$, $g_j$ monic monomials,

$$\sum_{i=0}^{n} x_i(\partial g/\partial x_i) = \sum_j a_j \sum_{i=0}^{n} x_i(\partial g_j/\partial x_i) = \sum_j a_j m g_j = mg.$$

When $f$ is monic monomial of degree $m$, we have

$$\sum_{i=0}^{n} x_i(\partial f/\partial x_i) = \sum_{i=0}^{n} x_i e_i(x_i^{e_i-1} \prod_{j\neq i} x_j^{e_j}) = \sum_{i=0}^{n} e_i f = mf.$$

□

2. Exercise 10.8:

*Proof.* For all $\bar{a}$ at which $\partial f/\partial x_i = 0$, from Ex10.7 we know that $mf(\bar{a}) = 0$. Moreover, $m$ is prime to the characteristic, say $p$, so there exists $c_1, c_2 \in \mathbb{Z}$ such that $c_1 m + c_2 p = 1$. Therefore, $f = c_1 mf + c_2 pf = 0$ over the field of characteristic $p$.(Or from another perspective, $m$ is nonzero hence invertible in field $F_q$, thus $mf = 0$ implies $f = 0$.) □

3. Exercise 10.9:

*Proof.* For contrast, we suppose the existence of some nonzero singular points $b = (b_0, b_1, \ldots, b_n)$ such that $f(b) = 0$. By definition, $\partial f/\partial x_i = a_i m x_i^{m-1} = 0$ at $b$ for all $i$, i.e.

$$a_i m b_i^{m-1} = 0, \forall i.$$

We assume all coefficients $a_i$ nonzero and $m$ is prime to the characteristic, hence $b_i = 0$ for all $i$ over the finite field $F$ where all nonzero elements are invertible and no nilpotent element exists other than 0. Contradiction occurs and this completes the proof that the projective hypersurface of $f$. □

4. Exercise 10.23:

*Proof.* Recall that $\frac{1}{q}\sum_{\alpha\in F}\psi(\alpha(x-y)) = \delta(x-y)$. Plugging the definition of $\hat{f}$ into $\sum_s \hat{f}(s)\psi(st)$, we obtain

$$\sum_s (\frac{1}{q}\sum_u f(u)\overline{\psi(su)})\psi(st) = \sum_u f(u)(\frac{1}{q}\sum_s \psi(st-su)) = \sum_u f(u)\delta(t-u) = f(t).$$

□

## 11 The Zeta Functions

5. Exercise 11.9

*Proof.* (I sometimes write $H_f$ in place of $H_f(F_q)$ for laziness.) We should find out the number of points on the affine curve. Set $f(x,y) = y^2 - x^3 - x^2$ and $g(x,z) = z^2 - x - 1$. There is a natural map $\varphi : (x,y) \mapsto (x, y/x)$ from $H_f(F_q)$ to $H_g(F_q)$ once $x \neq 0$, and its inverse $\varphi^{-1} : (x,z) \mapsto (x, xz)$ exists everywhere. Hence the bijectivity when $x \neq 0$ and $|H_f - \{(0,0)\}| = |H_g - \{(0,1),(0,-1)\}|$. Moreover, $H_g(F_q)$ is bijective to $F_q$ by $\psi : z \mapsto (z^2 - 1, z)$ and $\psi^{-1} : (x,z) \mapsto z$ the inverse forgetting $x$. Therefore, $|H_g| = q = p^s$, so the number of points on the affine curve is $|H_f| = p^s - 1$. By definition, $Z_f(u) = (1-u)(1-pu)^{-1}$. □

6. Exercise 11.17

*Proof.* Since $P(u) = \prod(1 - \alpha u)$ with all $\alpha \neq 0$, its degree is exactly the cardinality of $S = \{(\chi_i)_{i=0}^n : x_i^m = \epsilon, x_i \neq \epsilon, \prod_{i=1}^n \chi_i = \epsilon\}$.

Multiplicative characters of $F_q$ form a cyclic group of order $q-1$ which is divided by $m$, so its cyclic subgroup $H = \{\chi : \chi^m = \epsilon\}$ has order $m$, write $H = \{\epsilon, h, h^2, \ldots, h^{m-1}\}$.

Now given $(n+1)-$tuple $(e_i)$ corresponding to $S$, we rewrite $S$ as $S_n = \{(h^{e_i})_{i=0}^{n} : e_i \neq 0, \sum_i e_i \equiv 0 \pmod m\} = \{(h^{e_i})_{i=0}^{n-1} : e_i \neq 0, \sum_i e_i \neq 0 \pmod m\}$, where $e_i \in \{1, 2, \ldots, m-1\}$. The last equation holds because $e_n$ is uniquely determined by the precedents.

Now we compute the explicit expression for $c_n = card(S_n)$ by induction on $n$. Firstly, $c_1 = card(\{e_0 : e_0 \neq 0\}) = m-1$. For $n \geq 2$, there are two cases.

If $e_0 + \cdots + e_{n-2} \neq 0$, there are $m-2$ choices for $e_{n-1}$, only requiring it not equal to 0 or $-e_0 - \cdots - e_{n-2}$, and if $e_0 + \cdots + e_{n-2} = 0$, there are $m-1$ choices for $e_{n-1}$. This gives the relation

$$\begin{aligned} d_n &= (m-2)d_{n-1} + (m-1)((m-1)^{n-1} - d_{n-1}), \\ &= (m-1)^n - d_{n-1}. \end{aligned}$$

We obtain by immediate induction

$$d_n = (m-1)^n - (m-1)^{n-1} + \cdots + (-1)^{n-1}(m-1) \qquad (n \geq 1).$$

Then

$$\begin{aligned} d_n &= (m-1)^n - (m-1)^{n-1} + \cdots + (-1)^{n-1}(m-1) \\ &= (-1)^{n-1}(m-1)\left\{[-(m-1)]^{n-1} + [-(m-1)]^{n-2} + \cdots + 1\right\} \\ &= (-1)^{n-1}(m-1)\frac{[-(m-1)]^n - 1}{-(m-1) - 1} \\ &= \frac{(-1)^n(m-1)\left\{[-(m-1)]^n - 1\right\}}{m} \\ &= \frac{(m-1)^{n+1} + (-1)^{n+1}(m-1)}{m}. \end{aligned}$$

□