E. Dummit's Math 7362 ∼ Number Theory in Function Fields, Fall 2025 ∼ Homework 1, due Oct 5th

Solve whichever problems you haven't seen before that interest you the most (suggestion: between 30 and 50 points' worth). Starred problems are especially recommended. Prepare to present 2-4 problems in class on the due date.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Sep 3)

1. [1pt] For any polynomials f, g, show $\deg(fg) = \deg(f) + \deg(g)$, $\text{sgn}(fg) = \text{sgn}(f)\text{sgn}(g)$, and $\deg(f+g) \le \max(\deg f, \deg g)$ with equality whenever $\deg f \ne \deg g$.
2. [1pt] If F is any field, then for any $f, g \in F[t]$ with $g \ne 0$, show there exist unique $q, r \in F[t]$ such that $f = qg + r$ and $\deg r < \deg g$.
3. [2pts] Determine when $\deg \gcd(f, f') = \deg f - \deg \text{rad} f$ for a polynomial f. [It is probably easier to describe when equality *doesn't* hold.]
4. [1pt] Suppose $f \in F[t]$. Show that f divides its derivative f' if and only if $f' = 0$.
5. [1pt] We gave two proofs of Fermat's Last Theorem for polynomials. Where and why do these proofs break down if we try to use them to prove Fermat's Last Theorem for integers?

0.1.2 Exercises from (Sep 8)

1. [1pt] For $|f| = q^{\deg f}$, show $|fg| = |f| \cdot |g|$ and $|f+g| \le \max(|f|, |g|)$ with equality whenever $|f| \ne |g|$.
2. [2pts*] Show that a commutative ring R with 1 has a unique maximal ideal M if and only if the set of nonunits in R forms an ideal, which is then a unique maximal ideal M. A ring with this property is called a <u>local ring</u>.
3. [2pts] Generalize proof 2 of Wilson's theorem to show that if G is a finite abelian group, then the product of all elements in g is the unique element in G of order 2 (if there is one), or is otherwise the identity.
4. [1pt] For positive integers a, b, show $\gcd(x^a - 1, x^b - 1) = x^{\gcd(a,b)} - 1$ in $F[x]$.
5. [1pt] Prove that if there are d dth roots of unity in A/pA, then d divides $|p| - 1$.

0.1.3 Exercises from (Sep 10)

1. [1pt] Show that a polynomial in $F[t]$ is separable (i.e., has no repeated factors) if and only if it is relatively prime to its derivative.
2. [1pt] For positive integers q, a, b, show that $\gcd(q^a - 1, q^b - 1) = q^{\gcd(a,b)} - 1$ in $\mathbb{Z}$. (This is almost identical to the polynomial version above.)
3. [1pt] For the Mobius μ-function $\mu(n)$, show that $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{for } n = 1 \\ 0 & \text{for } n > 1 \end{cases}$.
4. [1pt] Show that the residue of $\zeta_A(s)$ at $s = 1$ (which is to say, the value of $\lim_{s\to 1}(s-1)\zeta_A(s)$) is $1/\log q$.
5. [2pts*] For $\xi_A(s) = q^{-s}(1 - q^{-s})^{-1}\zeta_A(s)$, show the functional equation $\xi_A(s) = \xi_A(1-s)$.

0.1.4 Exercises from (Sep 15)

1. [4pts] Show the following properties of Dirichlet convolution $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$:
   (a) Dirichlet convolution is commutative, associative, and has an identity element given by $I(n) = \begin{cases} 1 & \text{for } n = 1 \\ 0 & \text{for } n > 1 \end{cases}$.
   (b) The function f has an inverse under Dirichlet convolution if and only if $f(1) \ne 0$.
   (c) If $f(1) \ne 0$ and f is multiplicative, then its Dirichlet inverse f^{-1} is also multiplicative.
   (d) If two of f, g, and $f * g$ are multiplicative, then the third is also.

2. [4pts] Show the following things about Dirichlet series for integer-valued functions:

   (a) Use $\mu * 1 = I$ to establish Mobius inversion: if $g(n) = \sum_{d|n} f(n)$ then $f(n) = \sum_{d|n} \mu(d) g(n/d)$.

   (b) For the Euler φ-function, show that $\sum_{d|n} \varphi(d) = n$.

   (c) If σ is the sum-of-divisors function $\sigma(n) = \sum_{d|n} d$, show that $D_\sigma(s) = \zeta(s)\zeta(s-1)$.

   (d) If σ_k is the sum-of-kth-powers-of-divisors function $\sigma_k(n) = \sum_{d|n} d^k$, find and prove a formula for $D_{\sigma_k}(s)$ in terms of the Riemann zeta function.

3. [1pt] If $f = p_1^{a_1} \cdots p_k^{a_k}$ show that the number of monic divisors $d(f) = (a_1+1)\cdots(a_k+1)$ and the sum of divisors analogue $\sum_{d|f \text{ monic}} |d|$ is $\sigma(f) = \dfrac{|p_1|^{a_1+1}-1}{|p_1|-1} \cdots \dfrac{|p_k|^{a_k+1}-1}{|p_k|-1}$.

4. [2pts] Show that if $\lim_{n\to\infty} \mathrm{Avg}_n(h) = \alpha$, then $\lim_{n\to\infty} \dfrac{1}{1+q+\cdots+q^n} \sum_{\deg(f)\le n} h(f) = \alpha$ as well, so it is irrelevant whether we average over degree exactly n or $\le n$.

5. [1pt] Show that the average value of σ on degree-n polynomials is $(q^{n+1}-1)/(q-1)$.

0.1.5 Exercises from (Sep 17)

1. [1pt] Show that for polynomials $a, m \in \mathbb{F}_q[t]$, if a is not relatively prime to m then there are only finitely many primes congruent to a modulo m.

2. [2pts*] If S is finite, show that its Dirichlet and natural densities are both 0.

3. [2pts] Show that the set of primes whose leading digit is 1 in base 10 has undefined natural density, but has Dirichlet density $\log_{10} 2$. (The answer works out the same if you use integers with leading digit 1; you may do that version instead.)

4. [1pt] Show that extended Dirichlet characters modulo m are the same as functions $\chi : \mathbb{Z} \to \mathbb{C}$ (or $A \to \mathbb{C}$) such that (i) $\chi(a+bm) = \chi(a)$ for all a, b, (ii) $\chi(ab) = \chi(a)\chi(b)$ for all a, b, and (iii) $\chi(a) \neq 0$ iff a is relatively prime to m.

5. [2pts] If H is a subgroup of the finite abelian group G, define $H^\perp = \{\chi \in \hat{G} : \chi(H) = 1\}$. Show that $H^\perp \cong \widehat{G/H}$ and that $\hat{G}/H^\perp \cong \hat{H}$. Use these results along with $\hat{G} \cong G$ to conclude that the subgroup lattice of G is the same when turned upside down.

6. [2pts*] Verify that the evaluation map $\varphi : G \to \hat{\hat{G}}$ with $\varphi(g) = \{\chi \mapsto \chi(g)\}$ is an isomorphism from $\hat{\hat{G}}$ to G.

0.1.6 Exercises from (Sep 22)

1. [1pt] Choose a modulus $m \in \mathbb{F}_q[t]$ and a nontrivial Dirichlet character χ, and verify explicitly that $L(s, \chi)$ is a polynomial in q^{-s}.

2. [1pt] For $a, m \in \mathbb{F}_q[t]$ with a relatively prime to m, show that the proportion of primes of degree N congruent to a (mod m) is $\dfrac{1}{\Phi(m)} + O(q^{-N/2})$, where the implied constant is independent of q and N.

0.1.7 Exercises from (Sep 24)

1. [2pts] Prove Zolotarev's lemma: the signature ± 1 of the permutation associated to multiplication by a on $(\mathbb{Z}/p\mathbb{Z})^*$ (as an element of the symmetric group S_{p-1}) equals the Legendre symbol $\left(\dfrac{a}{p}\right)$.

2. [1pt] For odd primes p, q, show that $\left(\dfrac{p^*}{q}\right) = \left(\dfrac{q}{p}\right)$ is equivalent to $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

3. [2pts] Show that for any monic polynomial m, there are $\Phi(m)/d^{\lambda(m)}$ total dth powers modulo m, where $\lambda(m)$ is the number of distinct monic irreducible factors of m.

0.1.8 Exercises from (Sep 29)

1. [2pts] Describe all monic irreducibles $p \in \mathbb{F}_q[t]$ such that t is a square modulo p for arbitrary finite fields $\mathbb{F}_q$.

0.1.9 Exercises from (Oct 1)

1. [1pt] Show that the set $\{x+y, x^2+y^2\}$ is algebraically independent in $F(x,y)$ for any field F of characteristic not 2, but is algebraically dependent if F has characteristic 2.
2. [1pt] Use Zorn's lemma to show that every field extension has a transcendence base.
3. [4pts] Show that localization commutes with sums, intersections, quotients, finite direct sums, and is exact.
4. [1pt] Show that if I is an ideal of R, then $D = R\backslash I$ is multiplicatively closed if and only if I is prime.
5. [2pts*] Show that if P is a prime ideal and $D = R\backslash P$, then $D^{-1}R$ is a local ring with unique maximal ideal $D^{-1}P = \pi(P) = e_P$, the extension of the ideal P to $D^{-1}R$.

0.2 Additional Exercises

1. [3pts] For m monic, define $\Lambda(m)$ to be $\log|p|$ if $m = p^d$ is a prime power and 0 otherwise. (This is the function-field analogue of the Carmichael Λ-function, which is often used in proofs of the prime number theorem.)
   (a) Show that $\sum_{d|m \text{ monic}} \Lambda(d) = \log|m|$.
   (b) Show that $D_\Lambda(s) = -\zeta_A'(s)/\zeta_A(s)$.
   (c) Find the average value of Λ on monic degree-n polynomials.

2. [8pts] The goal of this problem is to give a self-contained proof of quadratic reciprocity (in $\mathbb{Z}$) using Gauss sums. So let p, q be distinct odd integer primes and let $\chi_p(a) = \left(\frac{a}{p}\right)$ be the Legendre symbol modulo p. The <u>Gauss sum</u> of a multiplicative character χ is defined to be $g_a(\chi) = \sum_{t=1}^{p-1} \chi(t) e^{2\pi i a t/p} \in \mathbb{C}$.
   (a) Show that $g_a(\chi_p) = \left(\frac{a}{p}\right) g_1(\chi_p)$ for any integer a.
   (b) Let $S = \sum_{a=0}^{p-1} g_a(\chi_p) g_{-a}(\chi_p)$. Show that $S = \left(\frac{-1}{p}\right)(p-1) g_1(\chi)^2$.
   (c) Show that $\sum_{a=0}^{p-1} e^{2\pi i a(s-t)/p} = \begin{cases} p & \text{if } s \equiv t \bmod p \\ 0 & \text{if } s \not\equiv t \bmod p \end{cases}$ for any integers s and t.
   (d) Show that the sum S from part (b) is equal to $p(p-1)$.
   (e) Let $p^* = \left(\frac{-1}{p}\right) p$. Show that the Gauss sum $g_1(\chi_p)$ has $g_1(\chi_p)^2 = p^*$. Deduce that $g_1(\chi_p)$ is an element of the quadratic integer ring $\mathcal{O}_{\sqrt{p^*}}$.

   Now let p and q be distinct odd primes and let $g = g_1(\chi_p) \in \mathcal{O}_{\sqrt{p^*}}$ be the quadratic Gauss sum.

   (f) Show that $g^{q-1} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$.
   (g) Show that $g^q \equiv g_q(\chi_p) \equiv \left(\frac{q}{p}\right) g \pmod{q}$, and deduce that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$.