E. Dummit's Math 7315 ~ Number Theory in Function Fields, Fall 2021 ~ Homework 1

Problems are worth points as indicated. Solve as many problems as you can (suggestion: at least 30 points' worth). Prepare solutions to these problems so that you may present some of them in lecture on Thursday, October 7th.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Sep 9)

- [2pts] As proven in class, we have $\deg \gcd(f, f') \geq \deg f - \deg \operatorname{rad} f$, where f' is the derivative of f. Determine when equality holds.

0.1.2 Exercises from (Sep 13)

- [2pts] Recall that $|g| = q^{\deg g} = \#(A/gA)$ when $g \neq 0$. Show that $|fg| = |f| \cdot |g|$ and that $|f + g| \leq \max(|f|, |g|)$ with equality whenever $|f| \neq |g|$.
- [2pts] 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). Note that a ring with this property is called a local ring.
- [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 1.
- [3pts] Prove that for positive integers a, b, $\gcd(x^a - 1, x^b - 1) = x^{\gcd(a,b)} - 1$ where x is a variable. Show also that $\gcd(q^a - 1, q^b - 1) = q^{\gcd(a,b)} - 1$ for positive integers q, a, b.
- [2pts] Prove that if there are d dth roots of unity in A/pA, then d divides $|p| - 1$.
- [1pt] Show that a polynomial in $F[x]$ has no repeated factors if and only if it is relatively prime to its derivative.

0.1.3 Exercises from (Sep 16)

- [2pts] Show that $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{for } n = 1 \\ 0 & \text{for } n > 1 \end{cases}$.
- [3pts] Recall that the <u>zeta function</u> of A is $\zeta_A(s) = \sum_{f \in A \text{ monic}} \frac{1}{|f|^s}$ for $s \in \mathbb{C}$.
  1. 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 $1/\log q$.
  2. Show the functional equation for $\zeta_A(s)$: if we set $\xi_A(s) = q^{-s}(1 - q^{-s})^{-1}\zeta_A(s)$, then $\xi_A(s) = \xi_A(1-s)$.
- [3pts] Give a formula for the number of cubefree monic polynomials in $\mathbb{F}_q[t]$ of degree n.

0.1.4 Exercises from (Sep 20)

- [2pts each] Show the following properties of the Dirichlet convolution operator:
  1. Show that Dirichlet convolution is commutative and associative, and has an identity element given by $I(n) = \begin{cases} 1 & \text{for } n = 1 \\ 0 & \text{for } n > 1 \end{cases}$.
  2. Show that f has an inverse under Dirichlet convolution if and only if $f(1) \neq 0$.
  3. If $f(1) \neq 0$ and f is multiplicative, then its Dirichlet inverse f^{-1} is also multiplicative.
  4. Show that if two of f, g, and $f * g$ are multiplicative, then the third is also.

- [2pts each] Do the following with Dirichlet series:

    1. Use $\mu * 1 = I$ to establish Mobius inversion: if $g(n) = \sum_{d|n} f(n)$ then $f(n) = \sum_{d|n} \mu(d)g(n/d)$.
    2. 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.

- [2pts] If $f = p_1^{a_1} \cdots p_k^{a_k}$, verify that $d(f) = (a_1+1)\cdots(a_k+1)$ and $\sigma(f) = \dfrac{|p_1|^{a_1+1}-1}{|p_1|-1} \cdots \dfrac{|p_k|^{a_k+1}-1}{|p_k|-1}$.

- [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.

- [2pts] Show that the average value of σ on degree-n polynomials is $(q^{n+1}-1)/(q-1)$.

0.1.5 Exercises from (Sep 23)

- [3pts] 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 $\left(\dfrac{a}{p}\right)$.

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

- [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.

0.2 Additional Exercises

- [5pts] 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.)

    1. Show that $\sum_{d|m \text{ monic}} \Lambda(d) = \log|m|$.
    2. Show that $D_\Lambda(s) = -\zeta_A'(s)/\zeta_A(s)$.
    3. Find the average value of Λ on monic degree-n polynomials.

- [15pts] 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 $\chi_p(a) = \left(\dfrac{a}{p}\right)$ be the Legendre symbol modulo p. The Gauss sum of a multiplicative character χ is defined to be $g_a(\chi) = \sum_{t=1}^{p-1} \chi(t) e^{2\pi i a t/p} \in \mathbb{C}$.

    1. Show that $g_a(\chi_p) = \left(\dfrac{a}{p}\right) g_1(\chi_p)$ for any integer a.
    2. Let $S = \sum_{a=0}^{p-1} g_a(\chi_p) g_{-a}(\chi_p)$. Show that $S = \left(\dfrac{-1}{p}\right)(p-1) g_1(\chi)^2$.
    3. Show that if p does not divide a, then $\sum_{a=0}^{p-1} e^{2\pi i a(s-t)/p} = \begin{cases} p & \text{if } s \equiv t \text{ mod p} \\ 0 & \text{if } s \not\equiv t \text{ mod p} \end{cases}$ for any integers s and t.
    4. Show that the sum S from part (b) is equal to $p(p-1)$.
    5. Let $p^* = \left(\dfrac{-1}{p}\right) p$. 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.

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