Due: Thursday, August 3 at the beginning of class

Problems:

(1) (An application of Dirichlet’s and Kornblum’s theorem)

a) Let $m | n$ in $\mathbb{Z}$ and $M | N$ in $\mathbb{F}_p[T]$. (Here $m, n, M, N$ are all nonzero.) Use the Chinese Remainder Theorem to show the reduction maps $(\mathbb{Z}/n)^\times \to (\mathbb{Z}/m)^\times$ and $(\mathbb{F}_p[T]/N)^\times \to (\mathbb{F}_p[T]/M)^\times$ are surjective.

b) Let $m$ be a positive integer, $a$ be relatively prime to $m$, and $S$ be a finite set of primes. Use Dirichlet’s theorem and part a) to prove that $\gcd(\{ p - a : p \equiv a \mod m, p \not\in S \}) = m$

unless $m$ is odd and $a$ is odd, in which case the gcd is $2m$. Try to give a proof that works when $S$ is a possibly infinite set of primes, with a suitable constraint on $S$.

c) Let $M$ be monic in $\mathbb{F}_p[T]$, $A$ be relatively prime to $M$, and $S$ be a finite set of monic irreducible polynomials. Use Kornblum’s theorem and part a) to prove that $\gcd(\{ \pi - A : \pi \equiv A \mod M, \pi \not\in S \}) = M$

unless $p = 2$ and $M$ is relatively prime to either $T$ or $T + 1$ (or both), and then give a formula for the gcd in these cases as well. As in part b), your proof should work when $S$ is infinite with a suitable constraint.

(2) For a prime $p$, let $N_p = \# \{(x, y) \in \mathbb{Z}/p \times \mathbb{Z}/p : y^2 = x^3 - x \}$. Compute $N_p$ for $2 \leq p \leq 29$. Make some good observations, and try to prove some of them.

(What, you may ask, does this have to do with $L$-functions? Wait to find out in the solution set, or think carefully about your data and discover the connection for yourself.)

(3) Let $M$ be a nonzero polynomial in $\mathbb{F}_p[T]$, of degree $d > 1$. Let $\chi$ be a nontrivial Dirichlet character mod $M$. We know from class that $L(s, \chi)$ is a polynomial in $p^{-s}$ of degree $< d$, say $L(s, \chi) = \sum_{0 \leq n \leq d-1} a_n p^{-ns}$.

As noted in class, this equation extends the definition of $L(s, \chi)$ to all real $s$. In particular, $L(0, \chi) = \sum_{n \leq d-1} a_n$. Recalling how the coefficients $a_n$ are determined, we find

$$\sum_{n \leq d-1} a_n = \sum_{n \leq d-1} \sum_{\deg f = n} \chi(f) = \sum_{\deg f < d} \chi(f) = 0,$$
since the sum of a nontrivial character over a group is 0, the polynomials of degree less than \( d = \deg M \) (which are relatively prime to \( M \)) represent all the units of the group \((\mathbb{F}_p[T]/M)^\times\), and \( \chi(f) = 0 \) if \( f \) is a nonunit mod \( M \). Thus \( L(0, \chi) = 0 \).

Alas, this is incorrect. We’ve seen examples in class where \( L(s, \chi) = 1 \) for all \( s \), so in particular \( L(0, \chi) = 1 \). Where is the error in the above argument? (Do not give examples where the argument fails. Pinpoint the actual error in the “proof”.)

(4) Let \( p \) be an odd prime and \( \omega \) a fixed nontrivial \( p \)th root of unity in \( \mathbb{C} \), e.g., \( \cos(2\pi/p) + i\sin(2\pi/p) \). For a monic polynomial

\[
f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_0
\]

in \( \mathbb{F}_p[T] \), define \( \chi(f) = (\frac{\omega}{p})^{c_n-1} \), where \( (\frac{\cdot}{p}) \) is the Legendre symbol. (It is okay to raise \( \omega \) to an exponent taken from \( \mathbb{F}_p = \mathbb{Z}/p \) since the exponent only matters modulo \( p \) anyway.) In particular, \( \chi(1) = 1 \) and \( \chi(T + c) = (\frac{\omega}{p})^{c} \).

a) Show \( \chi(fg) = \chi(f)\chi(g) \) for any two monic \( f \) and \( g \) in \( \mathbb{F}_p[T] \).

b) Prove \( \chi \) is not periodic, i.e., there is no polynomial \( M(T) \in \mathbb{F}_p[T] \) such that \( \chi(f) = \chi(g) \) when \( f \) and \( g \) are monic with \( f \equiv g \mod M \).

c) For \( s > 1 \), define

\[
L(s, \chi) = \sum_{\text{monic } f} \frac{\chi(f)}{Nf^s}.
\]

Show that \( L(s, \chi) = 1 + a_1/p^s \), where

\[
a_1 = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \omega^j.
\]

Warning: Since \( \chi \) is not a Dirichlet character for \( \mathbb{F}_p[T] \), be careful about appealing to results from class which were only proved for \( L \)-functions of Dirichlet characters.

(5) (An \( L \)-function for a quadratic modulus)

Let \( p \) be an odd prime and fix a nontrivial \( p \)th root of unity \( \omega \). Define a function \( \chi: (\mathbb{F}_p[T]/T^2)^\times \to \mathbb{C}^\times \) by

\[
\chi(c_0 + c_1T + \cdots + c_nT^n) = \left(\frac{c_0}{p}\right) \omega^{c_n/c_0}.
\]

(The mod \( p \) division in the exponent of \( \omega \) makes sense since \( c_0 \neq 0 \) in \( \mathbb{F}_p \) for a polynomial that is a unit mod \( T^2 \).) Note \( \chi \) is defined for all units mod \( T^2 \), not just for the monic polynomials which are units mod \( T^2 \).

a) Show \( \chi(fg) = \chi(f)\chi(g) \) for any two polynomials \( f \) and \( g \) that are units mod \( T^2 \).

b) Extend \( \chi \) to the nonunits mod \( T^2 \) by setting it 0 there, and define the \( L \)-function of \( \chi \), for \( s > 1 \), by

\[
L(s, \chi) = \sum_{\text{monic } f} \frac{\chi(f)}{Nf^s}.
\]
Show \( L(s, \chi) = 1 + a_1/p^s \), where
\[
a_1 = \sum_{j=1}^{p-1} \left( \frac{j}{p} \right) \omega^j.
\]

Comparing with the previous exercise, we see that the same \( L \)-function arises from a Dirichlet character mod \( T^2 \) and from a non-Dirichlet character.

In case you haven’t seen a sum like \( a_1 \) before, it is called a Gauss sum. This Gauss sum can be used to give a proof of quadratic reciprocity which is less roundabout than the proof on the PROMYS sets, and it also arises in the more advanced study of the classical Dirichlet \( L \)-function \( L(s, (\frac{\cdot}{p})) \).

(6) (An \( L \)-function for a cubic modulus)

a) Show 2 and \( T + 1 \) generate the units of \( \mathbb{F}_3[T]/(T^3 + T) \).

b) Define a character \( \chi \) by \( \chi(2) = -1 \) and \( \chi(T + 1) = -1 \), extended by multiplicativity to other units. Compute \( L(s, \chi) \) and the associated polynomial \( P_\chi(x) \).

c) Same as part b), but let \( \chi \) be determined by \( \chi(2) = -1 \) and \( \chi(T + 1) = i \).

(7) (An \( L \)-function for a quartic modulus)

a) Show \( T^4 + T + 2 \) is irreducible in \( \mathbb{F}_3[T] \).

b) Show \( T \) generates the units of \( \mathbb{F}_3[T]/(T^4 + T + 2) \).

c) Define a character mod \( T^4 + T + 2 \) by \( \chi(T) = i \). Compute \( L(s, \chi) \) as a polynomial in \( 1/3^s \). (As a check on your work, the final answer should be a polynomial \( P_\chi(x) \) which has a root at \( x = 1 \), and the other two roots have the same absolute value.)

(8) Fix nonzero \( M \in \mathbb{F}_p[T] \) and integers \( a \) and \( b \). For \( (A, M) = 1 \), show there are infinitely many monic irreducible \( \pi \) such that both \( \pi \equiv A \mod M \) and \( \deg \pi \equiv a \mod b \). Compute a density for such \( \pi \). (Hint: In the spirit of the proof of Dirichlet’s theorem, you want to get a good formula for the sum
\[
\sum_{\substack{\pi \equiv A \mod M \\ \deg \pi \equiv a \mod b}} \frac{1}{N\pi^s},
\]
where the sum is taken over monic irreducible \( \pi \) satisfying the indicated conditions. For \( b \)th roots of unity \( \omega \), consider the characters \( \psi_\chi, \omega(f) = \omega^{\deg f} \chi(f) \) and the corresponding \( L \)-functions. Note
\[
\frac{1}{b} \sum_{\omega^d=1} \omega^{d-a} = \begin{cases} 1, & \text{if } d \equiv a \mod b, \\ 0, & \text{if } d \not\equiv a \mod b, \end{cases}
\]
so the condition of being congruent to \( a \mod b \) can be expressed via a sum of \( b \)th roots of unity.)