SOME PROBLEMS ON DIRICHLET CHARACTERS AND L-SERIES

LEONARD TOMCZAK

Contents

1. Different things on Dirichlet Series

Problem 1 (Warm-up)**.** For a function $f : \mathbb{N} \to \mathbb{C}$ denote by $L_f(s)$ the Dirichlet series $\sum_{n=1}^{\infty} f(n)n^{-s}$. For functions $f, g : \mathbb{N} \to \mathbb{C}$ the (Dirichlet) convolution $f * g : \mathbb{N} \to \mathbb{C}$ is defined by $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$, where the sum runs over the positive divisors d of n.

(1) Show that $L_f(s)L_g(s) = L_{f*g}(s)$.

(2) Show that $*$ is commutative, associative, and has ϵ as a neutral element where $\epsilon(n) = 1$ if $n = 1$ and $\epsilon(n) = 0$ otherwise.

(3) Show that if f, g are multiplicative, then so is $f * g$.

(4) If $a \in \mathbb{C}$, let $\sigma_a(n) = \sum_{d|n} d^a$. Show that $\zeta(s)\zeta(s-a) = L_{\sigma_a}(s)$.

(5) The Möbius function $\mu : \mathbb{N} \to \mathbb{C}$ is defined by $\mu(n) = 0$ if n is not squarefree and $\mu(n) = (-1)^k$ otherwise where k is the number of primes dividing n. Show that μ is multiplicative and $\mu * 1 = \epsilon$. (Hint for the last part: You can show the equality directly for all n, but since both sides are multiplicative it suffices to show it just for prime powers)

(6) Show that $L_\mu(s) = \frac{1}{\zeta(s)}$ and $L_{|\mu|}(s) = \frac{\zeta(s)}{\zeta(2s)}$.

(7) See [Mur08, 1.2], [Apo76, Chapter 2], or Wikipedia for more examples and exercises on this.

Problem 2 (Requires a bit of knowledge about $\mathbb{Z}[i]$)**.** For an integer $n \geq 1$ denote by $r(n)$ the number of tuples $(a, b) \in \mathbb{Z}^2$ with $a^2 + b^2 = n$. The goal of this exercise is to find a formula for $r(n)$.

Consider the ring $R = \mathbb{Z}[i]$. For $z \in R$ set $N(z) = z\overline{z} = |z|^2$. For $a, b \in R \setminus \{0\}$ write $a \sim b$ if a, b are associated, meaning $a = bu$ for some unit u of R. Note that the units of R are $\{\pm 1, \pm i\}$. Define

$$\zeta_R(s) = \sum_{a \in (R\setminus\{0\})/\sim} N(a)^{-s}.$$

(1) Show that this sum converges absolutely for $\operatorname{Re} s > 1$.

(2) Show that $\zeta_R(s) = \frac{1}{4}\sum_{n=1}^{\infty} r(n)n^{-s}$.

(3) Using the fact that R is a UFD, mimic the proof for $\zeta(s)$ to show that ζ_R has an Euler product:

$$\zeta_R(s) = \prod_{P/\sim}(1 - N(P)^{-s})^{-1},$$

where the product runs over all prime elements P of R up to units.

(4) Show (or look it up) that primes P of R are classified as follows. For any prime P of R there is a prime number p such that $P \mid p$ and:

(a) If $p = 2$, then $N(P) = 2$, in which case $P \sim 1 + i$,

(b) If $p \equiv 1 \bmod 4$, then $N(P) = p$ and there are two non-associated primes P with $N(P) = p$.

(c) If $p \equiv 3 \bmod 4$, then $N(P) = p^2$ and $P \sim p$.

Conversely, for every prime number p there is a prime P of R with $P \mid p$.

(5) Let χ_{-4} be the nontrivial Dirichlet character modulo 4. Using the previous parts show that

$$\zeta_R(s) = \zeta(s)L(s, \chi_{-4}).$$

(6) Deduce the formula

$$r(n) = 4\sum_{d\mid n}\chi_{-4}(d).$$

(7) What is the residue of ζ_R at $s = 1$? (There are various ways to do this, one is to use Problem 9 (5).)

Problem 3. Now let $r(n)$ denote the number of $(a, b) \in \mathbb{Z}^2$ with $a^2 + 2b^2 = n$. Adapt the previous problem to find a formula for $r(n)$ using $\mathbb{Z}[\sqrt{-2}]$.

Problem 4. Fix a non-zero square-free integer a. Let N_m denote the number of solutions $x \in \mathbb{Z}/m\mathbb{Z}$ to $x^2 \equiv a \bmod m$. Let

$$F(s) = \sum_{(n,2a)=1}^{\infty} N_n n^{-s},$$

where the sum runs over all integers $n \geq 1$ coprime to $2a$. We want to express F in terms of L-series.

(1) Show that $m \mapsto N_m$ is multiplicative and deduce that $F(s) = \prod_{p\nmid 2a}\sum_{k\geq 0} N_{p^k}p^{-ks}$.

(2) For any prime $p \nmid 2a$ compute N_{p^k} and hence determine the Euler factor of $F(s)$ at p.

(3) Show that
$$F(s) = \frac{\zeta(s)L(s,\chi_a)}{\zeta(2s)} \prod_{p|2a} (1+p^{-s})^{-1}$$
for a suitable Dirichlet character χ_a.

(4) Determine χ_a for $a = 3$ and $a = -3$.

Problem 5. Here are various proofs of non-vanishing of L-series:

(1) Show that
$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)} = \sum_{n=1}^{\infty} \frac{\sigma_a(n)\sigma_b(n)}{n^s},$$
and deduce that $\zeta(1+it) \neq 0$ for all $t \neq 0$ (apply the identity with $a = it, b = -it$, and look at what happens near $s = 1$).

(2) Generalizing the previous example, let χ be a Dirichlet character mod N and $t \in \mathbb{R}$. Let χ_0 be the trivial character mod N. Let $f(n) = \chi(n)n^{-it}$ and $g = f * 1$. Show that
$$\sum_{n=1}^{\infty} |g(n)|^2 n^{-\sigma} = \frac{\zeta(\sigma)}{L(2\sigma,\chi_0)} L(\sigma+it,\chi)L(\sigma-it,\chi^{-1}),$$
and deduce $L(1+it,\chi) \neq 0$.

(3) Let χ be a Dirichlet character mod n, and χ_0 the trivial Dirichlet character mod n. Fix $t \neq 0$. Let $F(\sigma) = L^3(\sigma,\chi_0)L^4(\sigma+it,\chi)L(\sigma+2it,\chi^2)$. Show $3 + 4\cos x + \cos(2x) \geq 0$ for all real $x \in \mathbb{R}$. Use this to show $\operatorname{Re}\log F(\sigma) \geq 0$ for all $\sigma > 1$ (here the logarithm is defined by its series expansion and the Euler products). Deduce $|F(\sigma)| \geq 1$ and $L(1+it,\chi) \neq 0$. Does this proof also work for $t = 0$? If not, under what assumption would it work?

(4) Similarly as in in the previous case, but with $F(\sigma) = L^3(\sigma,\chi_0)L^2(\sigma+it,\chi)L^2(\sigma-it,\chi^{-1})L(\sigma+2it,\chi^2)L(\sigma-2it,\chi^{-2})$ (hint: note that $\chi^{-1} = \overline{\chi}$.)

(5) Fix a positive integer N. Let $F(s) = \prod_\chi L(s,\chi)$ where the product runs over all Dirichlet characters mod N. Show that $\log F(s)$ is a Dirichlet series with nonnegative coefficients. Similarly as in the previous parts then show that $F(s)$ has no zero on $\operatorname{Re} s = 1$ and deduce that $L(s,\chi) \neq 0$ for all χ and $s \neq 1$ with $\operatorname{Re} s = 1$.

Problem 6 (Partial summation)**.** Let a_n be a sequence of complex numbers, $f : [1,\infty) \to \mathbb{C}$ a continuously differentiable function. We are often interested in estimating sums of the form $\sum_{n\leq x} a_n f(n)$ as $x \to \infty$. Let $A(x) = \sum_{n\leq x} a_n$. We have
$$\begin{aligned}\sum_{n\leq x} a_n f(n) &= a_1 f(1) + \int_1^x f(t)\mathrm{d}A(t) = a_1 f(1) + [A(t)f(t)]_1^x - \int_1^x A(t)\mathrm{d}f(t) \\ &= A(x)f(x) - \int_1^x A(t)f'(t)\mathrm{d}t.\end{aligned}$$

(1) If you don't know about the Riemann-Stieltjes integral used above, ignore the middle terms and establish the equality between the first and the last term directly.

(2) Assume that $\sum_{p\le x}\frac{\log p}{p}=\log x+O(1)$ (the sum runs over the primes $\le x$). Then show that there is a constant C such that $\sum_{p\le x}\frac{1}{p}=\log\log x+C+O(1/\log x)$.

(3) Suppose $A(x)=O(x^\delta)$. For $\operatorname{Re}s>\delta$, show that $\sum_{n=1}^\infty a_n n^{-s}=s\int_1^\infty A(x)x^{-s-1}\mathrm{d}x$ and that both sides converge.

(4) Suppose $f:[1,\infty)\to(0,\infty)$ is continuously differentiable and decreasing to 0. Show that if $\sum_{n=1}^\infty a_n f(n)$ converges, then $f(N)\sum_{n\le N}a_n\to 0$ as $N\to\infty$ (this is *Kronecker's Lemma*).

(5) Use the previous two parts to show that the abscissa of convergence of the Dirichlet series $\sum_{n=1}^\infty a_n n^{-s}$ is given by $\limsup_{x\to\infty}\frac{\log|A(x)|}{\log x}$ (for general Dirichlet series one can analogously show the abscissa of convergence to be $\limsup_{n\to\infty}\frac{\log|A(n)|}{\lambda_n}$).

2. Dirichlet's theorem for natural density

Theorem 1 (Wiener-Ikehara Tauberian Theorem)**.** *Let $f(s)=\sum_{n=1}^\infty a_n n^{-s}$ be a Dirichlet series with nonnegative real coefficients. Assume it converges for $\operatorname{Re}s>1$ and that $f(s)-\frac{r}{s-1}$ extends to a continuous function on $\operatorname{Re}s\ge 1$, where r is (necessarily) the residue of f at $s=1$. Then*

$$\sum_{n\le x}a_n=rx+o(x).$$

See [Lan94, XV §2] or [Mur08, 3.3] if you would like to see a proof of this.

Problem 7. Let a,n be coprime integers. Define $\psi(x;a,n)=\sum_{p\le x,p\equiv a\bmod n}\log p$. Use Theorem 1 and Problem 5 to show

$$\psi(x;a,n)=\frac{1}{\varphi(n)}x+o(x).$$

(Hint: Consider the Dirichlet series $\sum_{p\equiv a}(\log p)p^{-s}$ and relate it to the functions $\frac{L'(s,\chi)}{L(s,\chi)}=(\log L(s,\chi))'$, similar as in the proof of Dirichlet's theorem)

Problem 8. Let a_n be a sequence of complex numbers and $r\in\mathbb{C}$. Show that

$$\sum_{n\le x}a_n=rx+o(x)$$

is equivalent to

$$\sum_{n\le x}\frac{a_n}{\log n}=r\frac{x}{\log x}+o(x/\log x).$$

Use this and the previous problem to deduce

$$|\{p\le x: p\text{ prime and }p\equiv a\bmod n\}|\sim\frac{1}{\varphi(n)}\frac{x}{\log x},$$

whenever a,n are coprime positive integers. Note that for $a=n=1$ this is the prime number theorem.

3. Analytic continuation of the zeta function

Problem 9 (Analytic continuation of ζ and functional equation I)**.** For an integrable function $f : \mathbb{R} \to \mathbb{C}$ define its Fourier transform $\widehat{f} : \mathbb{R} \to \mathbb{C}$ by

$$\widehat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} \mathrm{d}x.$$

If f is continuous and of sufficiently rapid decay at $\pm\infty$, Poisson's summation formula states

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n).$$

(1) Show that if $f(x) = e^{-\pi x^2}$, then $\widehat{f}(\xi) = e^{-\pi\xi^2}$. Deduce that $\widehat{f_a}(\xi) = \frac{1}{\sqrt{a}} e^{-\pi\xi^2/a}$ where $f_a(x) = e^{-a\pi x^2}$ for $a > 0$. (Hint: Use contour integration and Cauchy's theorem)

(2) Define $\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau}$ for $\tau \in \mathbb{C}$ with $\operatorname{Im}\tau > 0$. Use Poisson's summation formula to show $\theta(-1/\tau) = \sqrt{-i\tau}\theta(\tau)$. Here the square root has radicand in the left half plane and we take the branch with $\sqrt{-1} = i$. (Hint: Show it for $\tau \in i\mathbb{R}_{>0}$ and then use the identity principle)

(3) Define $\xi(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$. Show that

$$\xi(s) = \frac{1}{2}\int_0^{\infty} (\theta(it) - 1) t^{s/2} \frac{\mathrm{d}t}{t}$$

for $\operatorname{Re} s > 1$. Here the Gamma function $\Gamma(s)$ is defined by $\Gamma(s) = \int_0^\infty e^{-x} x^s \frac{\mathrm{d}x}{x}$ for $\operatorname{Re} s > 0$.

(4) Use the functional equation for θ and the previous part to show that ξ extends to a meromorphic function on $\mathbb{C}$ with its only poles at $s = 0, 1$ and satisfies the functional equation

$$\xi(s) = \xi(1-s).$$

(Hint: split up the integral as $\int_0^1 + \int_1^\infty$ and then do a change of variables in the first integral.)

(5) Let $\xi_R(s) = \pi^{-s}\Gamma(s)\zeta_R(s)$ where ζ_R is from Problem 2. Show that

$$\xi_R(s) = \int_0^{\infty} (\theta^2(it) - 1) t^{s} \frac{\mathrm{d}t}{t}$$

For $\operatorname{Re} s > 1$. As in part (4) deduce that ξ_R has a meromorphic continuation to $\mathbb{C}$ and satisfies a certain functional equation.

Problem 10 (Analytic continuation of ζ and functional equation II)**.** Let $f(x) = \frac{1}{2} - \{x\}$, where $\{x\} = x - \lfloor x \rfloor$ is the fractional part of x.

(1) Show that the Fourier series of f is $\sum_{n=1}^\infty \frac{\sin(2\pi n x)}{n\pi}$.

(2) Show that $\zeta(s) = \frac{s}{s-1} + \frac{1}{2} + s\int_1^\infty \frac{f(x)}{x^{s+1}}\mathrm{d}x$ and the integral on the right converges as an improper Riemann integral for $\operatorname{Re} s > -1$. Deduce that $\zeta(s) = s\int_0^\infty \frac{f(x)}{x^{s+1}}\mathrm{d}x$ where the integral now converges as an improper Riemann integral for $-1 < \operatorname{Re} s < 0$.

(3) Show that

$$\int_0^{\infty} \frac{\sin t}{t^{s+1}} \mathrm{d}t = -\Gamma(-s)\sin\left(\frac{\pi s}{2}\right)$$

for $-1 < \operatorname{Re} s < 0$. (Hint: Write $\sin t = \frac{1}{2i}(e^{it} - e^{-it})$ and do contour integration with quarter circles).

(4) Show that we may interchange integral and sum:

$$\zeta(s) = s\int_0^\infty \frac{\sum_{n=1}^\infty \frac{\sin(2\pi nx)}{n\pi}}{x^{s+1}}\mathrm{d}x = \frac{s}{\pi}\sum_{n=1}^\infty \frac{1}{n}\int_0^\infty \frac{\sin(2\pi nx)}{x^{s+1}}\mathrm{d}x.$$

Hence, using (3) deduce that

$$\zeta(s) = 2^s\pi^{s-1}\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)\zeta(1-s)$$

for $-1 < \operatorname{Re} s < 0$, and that ζ extends to a meromorphic function in $\mathbb{C}$ with its only pole at $s = 1$ (you will need some information about Γ for the last part).

(Hint for the interchange of sum/integral: Split up the integral into $\int_0^c + \int_c^\infty$. Show you can interchange the first integral with the sum. For the second show that $\lim_{c\to\infty}\sum\int_c^\infty = 0$ by integrating by parts.)

(5) Using the duplication formula $\Gamma(z)\Gamma\left(z+\frac{1}{2}\right) = 2^{1-2z}\sqrt{\pi}\Gamma(2z)$ and the reflection formula $\Gamma(1-z)\Gamma(z) = \frac{\pi}{\sin(\pi z)}$, convince yourself that this functional equation is equivalent to the one in Problem 9.

For even more proofs of the analytic continuation and functional equation, including the classical contour integration argument, see [Tit51, Chapter II].

Problem 11 (Special values of ζ)**.** Here we provide yet another proof of analytic continuation of ζ that also gives us the values of ζ at negative integers.

(1) Show $\Gamma(s)s = \Gamma(s+1)$ for all s with $\operatorname{Re} s > 0$. Deduce that Γ as a meromorphic continuation to $\mathbb{C}$ with simple poles at integers $k \le 0$. Determine the residues $\operatorname{Res}_{s=k}\Gamma(s)$.

(2) Show

$$\Gamma(s)\zeta(s) = \int_0^\infty \frac{x^{s-1}}{e^x - 1}\frac{\mathrm{d}x}{x}$$

for $\operatorname{Re} s > 1$.

(3) Write the integral above as $I_0 + I_1$ where $I_0 = \int_0^1 \dots$ and $I_1 = \int_1^\infty \dots$. Show that I_1 converges for all $s \in \mathbb{C}$ and hence defines an entire function.

(4) The Bernoulli numbers B_n are defined through the series expansion

$$\frac{x}{e^x - 1} = \sum_{n=0}^\infty \frac{B_n}{n!}x^n.$$

What is the radius of convergence of this power series? Show that

$$I_0 = \sum_{n=0}^\infty \frac{B_n}{n!}\frac{1}{n+s-1}$$

for $\operatorname{Re} s > 1$. Show that this sum converges for all $s \in \mathbb{C} - \{1, 0, -1, -2, -3, \dots\}$ and defines a meromorphic function in $\mathbb{C}$ with simple poles at $1-k$ for integers $k \ge 0$. Compute the residue at $1-k$.

(5) Deduce that ζ has a meromorphic continuation to $\mathbb{C}$ with its only pole at $s = 1$, and that

$$\zeta(1-k) = (-1)^{k-1}\frac{B_k}{k}$$

for all $k \geq 1$. Using the functional equation in the previous problems, derive the classical formula

$$\zeta(2k) = (-1)^{k+1}\frac{B_{2k}}{2(2k)!}(2\pi)^{2k}.$$

for integers $k \geq 1$.

Problem 12 (An Euler product without analytic continuation)**.** As shown above, the zeta function can be meromorphically continued to $\mathbb{C}$. The same holds more for the Dirichlet L-functions $L(s,\chi)$, and more generally automorphic L-functions. This is a somewhat special property! Let a_p be a sequence of complex numbers, indexed by primes p, with $\sum_p |a_p| < \infty$. Let $F(s) = \prod_p \left(1 + \frac{a_p}{1-p^{-s}}\right)$.

(1) Show this converges for $\operatorname{Re} s > 0$ and defines an analytic function in this half plane.

(2) Show that there is a dense set of points s_0 on the imaginary axis for which $\lim_{s\to s_0} F(s)$ does not exist. Hence, conclude that there is no open connected subset strictly containing the right half plane to which F extends meromorphically (so the imaginary axis is a natural boundary for F).

The same argument applies to $\prod_p \left(1 + \frac{p^{-s-1}}{1-p^{-s}}\right)$ which even has number theoretical significance: The coefficients of its Dirichlet series are given by $\frac{1}{\operatorname{rad} n}$ where $\operatorname{rad}(n) = \prod_{p|n} p$ is the product of the distinct prime factors of n.

4. Sums of two squares and Quadratic Reciprocity via characters

Problem 13. Fix an odd prime p. Let χ denote the (unique) quadratic Dirichlet character mod p, i.e. the Legendre symbol $\left(\frac{\cdot}{p}\right)$. Define $\psi(D) = \sum_{m\in\mathbb{F}_p}\chi(m^2 - D)$ and $\varphi(e) = \sum_{m\in\mathbb{F}_p}\chi(m^3 + em)$.

(1) Show $\sum_{m=1}^{p-1} m^k \equiv \begin{cases} -1 \bmod p & \text{if } k \equiv 0 \bmod p-1, \\ 0 \bmod p & \text{if } k \not\equiv 0 \bmod p-1. \end{cases}$

(2) Using (1) and $\chi(x) \equiv x^{(p-1)/2} \bmod p$ show $\psi(D) \equiv -1 \bmod p$. Conclude $\psi(D) = -1$ or $p-1$.

(3) Show $\sum_{D\in\mathbb{F}_p^\times}\psi(D)$ and $\psi(p) = p-1$. Conclude $\psi(D) = -1$ for all $D \in \mathbb{F}_p^\times$. (Alternative way: Count the number of solutions (x, y) to $x^2 = y^2 - D$ in $\mathbb{F}_p$ in two different ways.)

(4) Show $\sum_{m\in\mathbb{F}_p}\chi(m^2 + bm + c) = \psi(D)$ with $D = b^2 - 4c$.

(5) Show $\varphi(et^2)^2 = \varphi(e)^2$ for any $t \in \mathbb{F}_p^\times$.

(6) Compute $S = \sum_{m\in\mathbb{F}_p}\varphi(e)^2$ in two ways:

  (a) Sum over the squares and non-squares separately and use (5) to show $S = \frac{p-1}{2}(\varphi(r)^2 + \varphi(n)^2)$ where r is a quadratic residue and n a quadratic non-residue mod p.

  (b) Use the definition of $\varphi(e)$ and (3), (4) to show $S = (1 + \chi(-1))p(p-1)$.

(7) Deduce that if $p \equiv 1 \bmod 4$, then $p = a^2 + b^2$ for some integers a, b.

The method of proof of the two square theorem in the last problem is from [Jac07].

Problem 14. Let χ be a nontrivial Dirichlet character modulo a prime number p. Define the Gauss sum $G(\chi, a) = \sum_{n=1}^{p-1} \chi(n)\zeta^{an}$ where $\zeta = e^{2\pi i/p}$ and a an integer. Denote $G(\chi) := G(\chi, 1)$.

(1) Show $G(\chi, a) = \chi(a)G(\chi)$.

(2) Show $|G(\chi)|^2 = p$. (Hint: Compute $\sum_{a=1}^{p-1} |G(\chi, a)|^2$ in two different ways.)

(3) If ψ is another nontrivial Dirichlet character modulo p, define the Jacobi sum $J(\chi, \psi) = \sum_{a+b=1} \chi(a)\psi(b)$. Show that if $\chi\psi \neq 1$, then $G(\chi)G(\psi) = G(\chi\psi)J(\chi, \psi)$. (Conceptually a Gauss sum is a Fourier transform and the Jacobi sum a convolution, and this property has to do with the Fourier transform turning convolution into products.)

(4) Deduce that if $\chi^2 \neq 1$, then $|J(\chi, \chi)| = \sqrt{p}$. (You may also want to try to prove this without Gauss sums)

(5) If $p \equiv 1 \bmod 4$, show that there exists a Dirichlet character $\chi \bmod p$ of order 4. Applying the previous part to it, deduce that $p = a^2 + b^2$ for some integers a, b.

One can also define Gauss sums for arbitrary moduli n, but then instead of assuming χ to be trivial one wants χ to be primitive, meaning it does not factor through $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ for any proper divisor $m \mid n$.

Problem 15. Let χ be a nontrivial Dirichlet character modulo a prime number p. Show

$$\begin{aligned} L(1, \chi) &= -\frac{\chi(-1)G(\chi)}{p} \sum_{m \in \mathbb{F}_p} \overline{\chi(m)} \log(1 - \zeta^m) \\ &= \begin{cases} \frac{-2G(\chi)}{p} \sum_{m=1}^{p-1} \overline{\chi(m)} \log(\sin(m\pi/p)) & \text{if } \chi(-1) = 1, \\ \frac{\pi i G(\chi)}{p^2} \sum_{m=1}^{p-1} \overline{\chi(m)} m & \text{if } \chi(-1) = -1. \end{cases} \end{aligned}$$

If $p \equiv 3 \bmod 4$ and χ is the Legendre symbol, one can show that $G(\chi) = i\sqrt{p}$. Deduce that the sum of quadratic non-residues in $[1, p-1]$ exceeds the sum of quadratic residues.

Problem 16. Let p, q be distinct odd primes. Take a splitting field of the polynomial $x^p - 1$ over $\mathbb{F}_q$. Then $x^p - 1$ has p distinct roots in that field. Let ζ be any one of them except 1, so ζ is a primitive p-th root of unity, but not in $\mathbb{C}^\times$, instead in an extension of $\mathbb{F}_q$. Let $\chi = \left(\frac{\cdot}{p}\right)$ be the quadratic Dirichlet character modulo p. We may view χ as taking values in $\mathbb{F}_q^\times$ (the values are ± 1). Define the Gauss sum $S := G(\chi) = \sum_{n=1}^{p-1} \chi(n)\zeta^n = \sum_{n \in \mathbb{F}_p^\times} \left(\frac{n}{p}\right)\zeta^n$ in the same way as in Problem 14.

(1) Show $S^2 = \left(\frac{-1}{p}\right)p$.

(2) Show $S^q = \left(\frac{q}{p}\right)S$.

(3) Combine the previous two results to evaluate S^{q-1} in two different ways and conclude the quadratic reciprocity law

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

(You will have to use $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ in the final step.)

(4) The supplementary law $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/4}$ can be proven similarly. For this let i be a primitive fourth root of unity in some extension of $\mathbb{F}_p$ (which we can take to be $\mathbb{F}_p$ itself if $p \equiv 1 \bmod 4$ and a quadratic extension otherwise). Now compute $(1+i)^{p-1}$ in two ways.

References

[Apo76] T. M. Apostol. *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[Jac07] E. Jacobsthal. "Über die Darstellung der Primzahlen der Form 4n + 1 als Summe zweier Quadrate." In: *Journal für die reine und angewandte Mathematik* 132 (1907).

[Lan94] S. Lang. *Algebraic number theory.* Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.

[Mur08] M. R. Murty. *Problems in analytic number theory.* Second. Vol. 206. Graduate Texts in Mathematics. Springer, New York, 2008.

[Tit51] E. C. Titchmarsh. *The theory of the Riemann zeta-function.* Oxford science publications. Oxford: Clarendon Press, 1951.

Department of Mathematics, Evans Hall, University of California, Berkeley, CA 94720, USA

Email address: `leonard.tomczak@berkeley.edu`