189-346/377B: Number Theory

Assignment 5

Due: Wednesday, March 27

1. Let $w = e^{2\pi i/7}$ denote on of the non-trivial complex 7th roots of unity. Show that the numbers $a = w + w^2 + w^4$ and $b = w^3 + w^5 + w^6$ are the common roots of a quadratic equation with integer coefficients, by directly computing $a + b$ and ab. Deduce a simpler expression for the values of a and b from this argument.

2. Show that there is a field extension of $\mathbf{Z}/p\mathbf{Z}$ which also contains a non-trivial 7-th root of unity w. Show that the elements $a = w + w^2 + w^4$ and $b = w^3 + w^5 + w^6$, which are "modulo p avatars" of the complex numbers denoted by the same symbols in question 1, continue to satisfy the same algebraic relations. Use this to show, as done in class, that the function on primes given by $p \mapsto (\frac{-7}{p})$ depends only on the residue class of p modulo 7, and to give an explicit rule for calculating this Legendre symbol. (Note that you are not allowed to use the law of quadratic reciprocity shown in class, to treat this question: this would be cheating, as the goal here is to derive a special case of quadratic reciprocity from more basic principles.)

3. The law of quadratic reciprocity gives a simple recipe in terms of a prime p for determining whether the polynomial $x^2 - a \in \mathbf{Z}[x]$ has roots when viewed in $\mathbf{Z}/p\mathbf{Z}[x]$. One might ask whether a simple pattern also emerges for polynomials of larger degree. Try answering this question independently for the cubic polynomials $f(x) = x^3 - 2$ and $g(x) = x^3 + x^2 - 2x - 1$, by tabulating the number of roots of each of these polynomials modulo p, for all primes $p \leq 1000$. Write down all the patterns you observe, and try proving as many of these as you can. (In running your experiment in Pari, the commands `polrootsmod` and `forprime` might be useful.)

4. An integer n is said to be *square-free* if its prime factorisation is of the form

$$n = p_1 p_2 \cdots p_r,$$

where $p_1, \ldots, p_r$ are *distinct* primes. Show that for all real $s > 1$,

$$\frac{\zeta(s)}{\zeta(2s)} = \sum_{n \in S} \frac{1}{n^s},$$

where

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

is the Riemann zeta function, and S is the set of positive square free integers.

5. Let q be a fixed prime. Show that any integer which is *not* a quadratic residue modulo q always has a prime divisor with the same property. Use this to prove that there are infinitely many primes p satisfying $\left(\frac{p}{q}\right) = -1$.

6. Let q be a prime. Show that any prime $p \neq q$ which divides the integer

$$n^{q-1} + n^{q-2} + \cdots + 1$$

($n \in \mathbf{Z}$) is necessarily congruent to 1 modulo q. Use this to show that there are infinitely many primes which are congruent to 1 modulo q, and a fortiori that there are infinitely many primes that are quadratic residues modulo q. (Hint: assume otherwise, and study the asymptotics of $\#\{n^{q-1} + \cdots + n + 1, \quad n \leq x^{1/d}\}$ as $x \longrightarrow \infty$ in two different ways to derive a contradiction.)

7. Using the functions `binomial` and `factor` in PARI, give the prime factorisations of the middle binomial coefficient $\binom{2n}{n}$, for $n = 20$ and 50. What do you observe? Explain.