Lecture 10 Exercises

This exercise will walk through a proof that the process of modular inversion is "random."

(a) Let $p = 17$ and for $a = 1, 2, \ldots, 16$, compute $\bar{a} \in \mathbb{Z}/p$ so that $a\bar{a} \equiv 1 (\mathrm{mod}\, p)$. Plot the pairs $(\frac{a}{p}, \frac{\bar{a}}{p})$ in the unit square.

Our goal will be to prove what you're (hopefully) seeing with this example. What should it mean to say that these points equidistribute? The proportion of these points in any region should be the area of the region. To capture this, fix a smooth "test function" $f \in C^\infty([0,1] \times [0,1])$ (think of f as the indicator function of some fixed region – of course that's not smooth, so approximate it). We claim that

$$\frac{1}{p-1} \sideset{}{'}\sum_{a(p)} f\left(\frac{a}{p}, \frac{\bar{a}}{p}\right) \to \int_0^1 \int_0^1 f, \tag{1}$$

as $p \to \infty$ in the primes. The "prime" notation over the Sigma restricts to a coprime to p. (There's nothing special about primes, but it makes this exercise easier.)

Break f into its Fourier series,

$$f(x,y) = \sum_{n,m \in \mathbb{Z}} \widehat{f}(n,m) e(nx + my). \tag{2}$$

(b) As before, show that $\widehat{f}$ decays super polynomially, that is, for any $A, B > 0$,

$$|\widehat{f}(n,m)| \ll_{A,B} 1/((|n|^A + 1)(|m|^B + 1)).$$

(c) Next insert (2) into the left hand side of (1) to get

$$LHS(1) = \sum_{n,m \in \mathbb{Z}} \widehat{f}(n,m) \frac{1}{p-1} S_p(n,m),$$

where S_p is the "Kloosterman sum":

$$S_p(n,m) := \sideset{}{'}\sum_{a(p)} e_p(na + m\bar{a}).$$

Observe that the contribution when $n = m = 0$ is $\widehat{f}(0,0) = \int_0^1 \int_0^1 f$, that is, the right hand side of 1 and (supposedly) the main term. So we need cancellation in the other terms as p grows. Notice that we have the "trivial" bound $|S_p(n,m)| \leq p - 1$, which is what we'll need to beat. Kloosterman managed to improve on this by a whole power of p; here's how.

He considered an L^4 norm on the *coefficients*: Let

$$\mathcal{U} := \sum_{k,\ell(p)} |S_p(k,\ell)|^4 .$$

(d) Open the fourth power and show that

$$\mathcal{U} = \sum_{a_1,a_2,a_3,a_4 (p)}{}' \sum_{k,\ell (p)} e_p(k(a_1+a_2-a_3-a_4)+\ell(\bar{a}_1+\bar{a}_2-\bar{a}_3-\bar{a}_4)).$$

The sums on k, ℓ vanish unless their coefficients are both zero, in which case they contribute p^2.

(e) Count how often this happens (in the a_j's) to deduce that

$$\mathcal{U} \ll p^4.$$

Now note simply by positivity that, for our particular values $k = n$ and $\ell = m$, we get $|S_p(n,m)|^4 \leq \mathcal{U} \ll p^4$. This just fails to give something non-trivial. But! Kloosterman noticed that, then for any $s \in (\mathbb{Z}/p)^\times$, we have that $|S_p(n,m)| = |S_p(sn, \bar{s}m)|$.

(f) Prove this fact.

Thus, if $(n,m) \neq (0,0)$, then these other values all contribute the same amount to $\mathcal{U}$. Therefore, if $(n,m) \neq (0,0) (\mathrm{mod}\, p)$, then

$$(p-1)|S_p(n,m)|^4 \ll p^4,$$

implying the "Kloosterman bound":

$$|S_p(n,m)| \ll p^{3/4}.$$

(g) Now complete the proof of (1).

(h)*: Look up how Selberg used this fact to prove "expansion" (though he likely wouldn't have recognized the term) in the mod p Cayley graphs for any set generating all of $\mathrm{SL}_2(\mathbb{Z})$.

(i)*:** Prove the better ("Weil") bound:

$$|S_p(n,m)| \leq 2p^{1/2}.$$

(See, e.g., Iwaniec-Kowalski.)

Problem 2: Consider the set $M(X;p)$ of matrices $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ in an archimedean ball of size X (say all entries bounded by X) so that $\gamma \equiv I (\mathrm{mod}\, p)$. With your "bare hands" (no spectral theory of automorphic forms), prove that

$$\#M(X;p) \ \ll_\varepsilon \ X^\varepsilon \left(\frac{X^2}{p^3} + \frac{X}{p} + 1 \right),$$

for any $\varepsilon > 0$. [Big hint: you won't get this quality of an estimate by considering things mod p alone. First prove that $\mathrm{tr}(\gamma) \equiv 2 (\mathrm{mod}\, p^2)$!...] See the use of this in Sarnak-Xue to give an even softer proof of expansion than Selberg's...