Honors 1: Undergraduate Math Lab*

Peter Sarnak†, Steven Miller‡, Alex Barnett§

October 23rd, 2002

Courant Institute of Mathematical Sciences
New York University
New York, NY

Abstract

Multipliative Functions, Kloosterman Sums and Bounds, p-adic Numbers. Review of the Three Problems (Germain Primes, Randomness of $x \to \overline{x}$ mod p, Random Graphs). Lecture by Peter Sarnak; notes by Steven Miller.

1 Multiplicative Functions, Kloosterman and p-adic Numbers

1.1 Multiplicative Functions

Definition 1.1 (Multiplicative Functions). *Let f be defined on the positive integers $\mathbb{N}$. f is multiplicative if*

$$f(mn) \;=\; f(m)f(n) \quad \text{if } m \text{ and } n \text{ are relatively prime.} \tag{1}$$

This is the same as

*Homepage: `http://www.math.nyu.edu/~millerj/`
†E-mail: `sarnak@math.princeton.edu`
‡E-mail: `millerj@cims.nyu.edu` or `sjmiller@math.princeton.edu`
§E-mail: `barnett@nmr.mgh.harvard.edu`

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} \;=\; \prod_p \Big(1 + f(p)p^{-s} + f(p^2)p^{-2s} + \cdots\Big). \tag{2}$$

We call the above an **Euler Product**. The standard example is the **Riemann Zeta Function**,

$$\zeta(s) \;=\; \sum_{n=1}^{\infty} \frac{1}{n^s} \;=\; \prod_p \frac{1}{1-p^{-s}}. \tag{3}$$

There are many multiplicative functions (some, like Dirichlet Characters, do not even require m and n to be relatively prime).

The Kloosterman sums are *not* multiplicative.

1.2 Kloosterman Sums

If c_1 and c_2 are relatively prime,

$$K(a,b,c_1c_2) \;=\; K(*,*,c_1) \cdot K(*,*,c_2), \tag{4}$$

where the $*$s are functions of a, b, c_1 and c_2.

Say we show $|K(a,b,p)| \ll p^{\nu}$, where ν does not depend on a or b or p.

Then, if $c = \prod_i p_i^{r_i}$, we have

$$K\Big(a,b,\prod_i p_i^{r_i}\Big) \;=\; \prod_i K(*,*,p_i^{r_i}). \tag{5}$$

Thus, we just need to get bounds over prime powers to bound a general Kloosterman sum.

Theorem 1.2 (Salie). *If $\alpha \geq 2$,*

$$K(a,b,p^{\alpha}) \;\leq\; 2p^{\frac{\alpha}{2}}. \tag{6}$$

Proof: elementary.

$$\sum_{x \bmod p^2} \;=\; \sum_{x_1=0}^{p-1}\sum_{x_2=0}^{p-1}, \tag{7}$$

where $x = x_1 + x_2 p$ and $x_1, x_2 \in \{0, 1, \ldots, p-1\}$.

Thus, when we encounter terms like $e\left(\frac{\overline{x_1+px_2}}{p^2}\right)$, we need the inverse of $\overline{x_1+px_2}$.

Let x_1^{-1} be the inverse of x_1 mod p. Then

$$(x_1+px_2)^{-1} \quad = \quad x_1^{-1}(1+x_1^{-1}x_2p)^{-1}. \tag{8}$$

Note that

$$(1-pb)^{-1} \;=\; 1+pb+O(p^2). \tag{9}$$

Say we want the inverse mod p^2 of $(1-bp)$. Try multiplying by $(1+bp)$. We get

$$(1-pb)(1+pb) \;=\; 1-b^2p^2 \;\equiv\; 1 \bmod p^2. \tag{10}$$

The above arguments is Hensel's Lemma.

1.3 p-adic numbers

We define the p-adic norm of a rational $\alpha = \frac{a}{b}$, a and b relatively prime, by

$$||\alpha||_p \;=\; p^{-m}, \text{ where } \frac{a}{b} = p^m l, \, (p,l)=1. \tag{11}$$

Note that numbers that are highly divisible by p are small p-adically.

We have the rationals $\mathbb{Q}$ and the p-adic norm $||*||_p$. Similar to completing the rationals $\mathbb{Q}$ with the usual norm to get $\mathbb{R}$, we can complete the rationals with respect to this norm. The resulting field is called the p-adic numbers, $\mathbb{Q}_p$.

$\mathbb{Q} \subset \mathbb{R}$, and $\mathbb{Q}$ is dense in $\mathbb{R}$. Similarly $\mathbb{Q} \subset \mathbb{Q}_p$ and $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Let $x \in \mathbb{Q}_p$. Then

$$x \;=\; \frac{a_{-m}}{p^m} + \frac{a_{-m+1}}{p^{m-1}} + \cdots + a_0 + a_1p + a_2p^2 + \cdots, \tag{12}$$

where $0 \le a_i \le p-1$.

Suppose we have a solution $f(x_0) \equiv 0 \bmod p$. We then try and find x_1 such that $f(x_0+px_1) \equiv 0 \bmod p^2$. Hensel noted that all we need to find x_1 is some knowledge of the derivative at the previous stage.

2 Germain Primes

$p-1=2q$, p and q prime. What are the statistics? How many are there up to x? Do they know about each other? What are their correlations? What about $p-3$?

The Circle Method is a way of trying to solve additive equations (Waring's Problem, Goldbach's Problem $p_1+p_2 = 2n$, Vinogradov's Three Primes Theorem $p_1+p_2+p_3 = 2n+1$, Twin Primes $p_2-p_1 = 2$).

Definition 2.1 (Germain Primes). *If p is prime and $p-1 = 2q$ for some prime q, we say p is a Germain Prime.*

Definition 2.2 ($\pi_G(x)$). *Recall $\pi(x)$ is the number of primes at most x. Then $\pi(x) \sim \frac{x}{\log x}$. Let $\pi_G(x)$ be the number of Germain primes at most x. If the probability of getting a prime is $\log x$, then we might expect that*

$$\pi_G(x) \quad = \quad \sum_{\substack{p\leq x \\ p-1=2q}} 1 \quad \sim \quad \text{Const} \cdot \frac{x}{\log^2 x}. \tag{13}$$

Using the circle method, we will try and estimate the above constant, and hope the minor arcs *do not contribute to the main term.*

Major McMahan (from the army, friendly with Hardy and Littlewood) made tables of primes to the *millions.* He checked, and Hardy and Littlewood's constant (for twin primes) was correct and Sylvester (who made a probabilistic argument) was shown to be slightly off.

See Hardy and Littlewood, Acta Mathematica, v44, 1923, Partitio numerorum. III: *On the expression of a number as a sum of primes.*

We will then investigate the nearest neighbor and k^{th}-nearest neighbor spacings.

Also look at Robert Vaughn, *The Hardy Littlewood Method.*

3 Randomness of $x \to \overline{x}$

Given a prime p, look at $x \to \overline{x}$. How do we compute $\overline{x}$?

One can compute $\overline{x}$ by using the Euclidean Algorithm (very fast, $\log p$ steps). Recall the Euclidean Algorithm gives a and b such that $ax+bp = 1$. Thus, mod p, $ax \equiv 1$, or $a = \overline{x}$ mod p.

We now study the spacings between $\overline{x}$ as x ranges in some interval mod p. If the interval is very small, we don't expect randomness. What if we take an interval of length $\sqrt{p}$. Do we see Poissonian Behavior there for a fixed prime?

Now, fix a number a. Look at $\frac{a \bmod p}{p}$ as you vary p.

Theorem 3.1 (Duke-Iwaniec). *Suppose $p \equiv 1$ mod 4. There is a square root of -1 mod p; ie, $\exists x$ such that $x^2 \equiv 1$ mod p. Now we can take $1 \leq x \leq \frac{p-1}{2}$, so $\frac{x}{p} \in \left[0, \frac{1}{2}\right]$. Then $\frac{x}{p}$, as we vary p, is equi-distributed.*

One can also look at the longest increasing sub-sequence.

Knuth, volume 2 of the Art of Computer Programming. Look at the stuff on generating random numbers.

4 Random Graphs / Ramanujan Graphs

Bollobas, *Random Graphs*: he will have a model of the random 3-regular graphs (what it means, how to generate, how many are there). *Very* hard if you don't distinguish between isomorphic graphs (which have the same spectrum).

Look at the distribution of the second largest eigenvalue λ_1 of the random 3-regular graph. Find the mean and the variance, graph.

Professor Sarnak will give a lecture on the Tracy-Widom distribution (which is the distribution of the biggest eigenvalue in some random ensemble – will we see the same distribution here)?

What is the scale for normalizing?

Take an interval, see how many eigenvalues in it, slide the interval down, and see how the number varies.