INTRODUCTORY LECTURES COURSE NOTES, 2015

STEVE LESTER AND ZEÉV RUDNICK

1. About this course

The goal of the course is to study some problems in the theory of primes and the effect of prime factorization on the distribution of various sequences of integers.The name "sieve theory" suggests a collection of techniques and ideas which have a distinct flavor than other methods in analytic number theory, such as the theory of L-functions, but they are often applied together with other techniques.

Rather than try to *define* what are sieve methods, I will describe some of the problems that we shall study.

1.1. **PNT.**

The Prime Number Theorem says that the number $\pi(x)$ of primes up to x is asymptotically $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \sim x/\log x$. We shall not prove this, which some will have seen in other courses, but will give weak substitutes which shall suffice for the first half of the course.

1.2. **Twin primes.**

This is the statement that for any even $h > 0$, there are infinitely many integers n so that both n and $n + h$ are prime. This is currently open. A quantitative conjecture asserts that

$$\#\{n \le x : n, n+h \text{ prime}\} \sim \mathfrak{S}(h) \frac{x}{(\log x)^2}$$

for a certain constant $\mathfrak{S}(h)$, which is positive if $h > 0$ is even.

While this is vastly open (no lower bounds), sieve theory provides upper bounds of the correct order of magnitude (Brun, Selberg). We will see how to achive this.

1.3. **Bounded gaps.**

An alternative formulation of the twin prime conjecture for $h = 2$ is that there are infinitely n so that $[n, n + 2]$ contains two primes. A major result due to Yitang Zhang in 2013 is that there are infinitely many n so that $[n, n+10^7]$ contains two primes; this is called "bounded gaps". The number 10^7 has subsequently been improved, the current record being 246. A few months later, James Maynard, using a different idea, improved this to say that given any m, there is some $H_m < \infty$ so that there are infinitely many n's so that the interval $[n, n + H_m]$ contains at least $m + 1$ primes (so $H_1 = 246$).

Date: March 30, 2015.

1.4. Primes and squarefrees represented by polynomials.

A very ambitious problem is to show that every reasonable polynomial represents infinitely many primes, for instance to show that there are infinitely many primes of the form $n^2 + 1$.

Instead, one can ask about representing squarefrees. The density of squarefrees is (as we shall see) $1/\zeta(2)$ so it is easier to be squarefree than it is to be prime. One can ask, given a reasonable polynomial $f(x)$, if there are infinitely many n so that $f(n)$ is squarefree. We shall show (Ricci, 1930's) that this is true for quadratic polynomials such as $f(x) = x^2 + 1$. Hooley in the 1960's dealt with the cubic case $\deg f = 3$, and beyond that nothing is known to date.

1.5. Function field analogues.

Several of these problems make sense for the ring $\mathbb{F}_q[x]$ of polynomials over a finite field $\mathbb{F}_q$, and it turns out that some of these problems are more tractable there. We will spend some time discussing this circle of ideas.

2. Arithmetic functions

2.1. Definition and examples of arithmetic functions.

An arithmetic function is a complex-valued function on the positive integers $\alpha : \mathbb{N}_{\geq 1} \to \mathbb{C}$.

Here are some examples:

- the constant function $\mathbf{1}(n) = 1$, $\forall n \geq 1$;
- The delta function $\delta(n) = \begin{cases} 1, n = 1 \\ 0, n > 1 \end{cases}$
- The Möbius function μ, defined for square-free integers $n = p_1 \cdot \ldots \cdot p_k$ to be $(-1)^k$, and is zero otherwise. In particular $\mu(1) = 1$.
- The divisor function, giving the number of divisors of an integer:
$$\tau(n) = \{(a,b) : a, b \geq 1, a \cdot b = n\} = \sum_{d|n} 1$$
More generally, we have higher divisor functions, for integer $r \geq 2$, defined as
$$\tau_r(n) := \{(a_1, \ldots, a_r) : a_j \geq 1, a_1 \cdot \ldots \cdot a_r = n\}$$
- The power functions n^s
- Sum of divisors: If $s \in \mathbb{C}$ then set $\sigma_s(n) = \sum_{d|n} d^s$.
- The von Mangoldt function $\Lambda(n) = \begin{cases} \log p, & n = p^k, k \geq 1 \\ 0, & \text{otherwise} \end{cases}$

The set of $\mathcal{A} = \mathbb{C}[\mathbb{N}_{\geq 1}]$ of all arithmetic functions form an algebra over $\mathbb{C}$ under addition and pointwise multiplication.

2.2. **Dirichlet convolution.** Another useful binary operation is called Dirichlet convolution: If $\alpha, \beta \in \mathcal{A}$, their convolution is defined as

$$\alpha * \beta(n) := \sum_{ab=n} \alpha(a)\beta(b) = \sum_{d|n} \alpha(d)\beta(\frac{n}{d}) \ .$$

Here and elsewhere, the notation $\sum_{d|n}$ denotes the sum over all positive divisors of n.

Some elementary properties of Dirichlet convolution are

- Commutativity: $\alpha * \beta = \beta * \alpha$
- Associativity $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$.
- The delta function is the neutral element for convolution: $\delta * \alpha = \alpha$, $\forall \alpha \in \mathcal{A}$.

Using Dirichlet convolution, we can express some of the arithmetic functions we have just seen in terms of others. For instance, by definition

$$\tau = \mathbf{1} * \mathbf{1}$$

and more generally, for $r \geq 2$ (assuming $\tau_1 = \mathbf{1}$)

$$\tau_r = \tau_{r-1} * \mathbf{1} \ ,$$

and the sum of divisors functions are given by

$$\sigma_s = \mathbf{1} * n^s \ .$$

Exercise 1. *Show that* $\log = \Lambda * \mathbf{1}$*, that is*

$$\sum_{d|n} \Lambda(d) = \log n \ .$$

2.3. **Multiplicative functions.** An arithmetic function α is *multiplicative* if it satisfies $\alpha(1) = 1$ and for any coprime integers m, n,

$$\alpha(mn) = \alpha(m)\alpha(n), \quad \gcd(m,n) = 1 \ . \tag{1}$$

A function is *completely multiplicative* if $\alpha(mn) = \alpha(m)\alpha(n)$ for any (not necessarily coprime) integers $m, n \geq 1$.

Note: Sometimes one defines a multiplicative function as any function which is not identically zero, and satisfies the relation (1); one then shows that necessarily $\alpha(1) = 1$.

Examples:

- The power functions n^s and the constant function $\mathbf{1}$ are strongly multiplicative.
- The delta function δ is strongly multiplicative.
- μ is multiplicative by its definition.

It is clear from the definition that a multiplicative function is determined by its values on prime powers, since by induction if $n = \prod_j p_j^{e_j}$ is the prime factorization of n, then

$$\alpha(n) = \prod_j \alpha(p_j^{e_j}) \ . \tag{2}$$

The basic property that we need it that convolution preserves multiplicativity:

Proposition 2.1. *If $\alpha, \beta \in \mathcal{A}$ are multiplicative, then so is $\alpha * \beta$.*

Proof. Suppose $\gcd(m,n)=1$. Then we claim there is a bijection

$$\{\text{divisors } D \mid n\} \leftrightarrow \{\text{ordered pairs of coprime integers } (c,d), \quad c \mid m,\ d \mid n\}$$

where the maps take $(c,d) \mapsto c\cdot d =: D$ which is a divisor of mn, and given a divisor D of $m\cdot n$, it can be uniquely written as $D = c\cdot d$ where $c \mid m$ and $d \mid n$. This is seen by taking the prime factorization $m = \prod_i p^{a_i}$, $n = \prod_j q_j^{b_j}$ where since m,n are coprime, $p_i \neq q_j$. Then if $D = \prod_i p_i^{u_i} \prod_j q_j^{v_j}$ is the factorization of D, where necessarily $u_i \le a_i$, $v_j \le b_j$ then take $c = \prod_i p_i^{u_i}$ and $d = \prod_j q_j^{v_j}$.

Then we compute

$$\begin{aligned}\alpha * \beta(mn) &= \sum_{D\mid mn} \alpha(D)\beta(\frac{mn}{D})\\ &= \sum_{c\mid m}\sum_{d\mid n} \alpha(cd)\beta(\frac{mn}{cd})\end{aligned}$$

Since c, d are coprime, $\alpha(cd) = \alpha(c)\alpha(d)$. Since m, n are coprime, so are m/c and n/d and hence $\beta(\frac{mn}{cd}) = \beta(\frac{m}{c})\beta(\frac{n}{d})$. Hence we find

$$\begin{aligned}(\alpha * \beta)(mn) &= \sum_{c\mid m}\sum_{d\mid n} \alpha(c)\alpha(d)\beta(\frac{m}{c})\beta(\frac{n}{d})\\ &= \sum_{c\mid m}\alpha(c)\beta(\frac{m}{c})\sum_{d\mid n}\alpha(d)\beta(\frac{n}{d}) = (\alpha*\beta)(m)\cdot(\alpha*\beta)(n)\end{aligned}$$

proving multiplicativity, after noting that $\alpha * \beta(1) = \alpha(1)\beta(1) = 1$. □

As a corollary, we immediately see that the divisor function $\tau = \mathbf{1} * \mathbf{1}$ is multiplicative, and by induction so are the higher divisor functions $\tau_r = \tau_{r-1} * 1$.

We can now use the above to prove a fundamental property of the Möbius function:

Proposition 2.2. *$\mu * \mathbf{1} = \delta$, that is*

$$\sum_{d\mid n}\mu(d) = \begin{cases}1, & n=1\\ 0, & n>1\end{cases}$$

Proof. Since μ and $\mathbf{1}$ are multiplicative, so is $\mu * 1$; and so is δ. Hence it suffices to prove the identity on prime powers. So for a prime power p^e, $e \ge 1$, the divisors are $\{1, p, \dots, p^e\}$ and then

$$(\mu * \mathbf{1})(p^e) = \sum_{j=0}^{e}\mu(p^j)$$

Since $\mu(p^j) = 0$ for $j \geq 2$, and $e \geq 1$, we are left with

$$\mu * \mathbf{1}(p^e) = \mu(1) + \mu(p) = 1 - 1 = 0 = \delta(p^e)$$

as claimed. □

As a corollary we get the Möbius inversion formula: If $\alpha, \beta \in \mathcal{A}$ satisfy

$$\alpha(n) = \sum_{d|n} \beta(d)$$

then we can recover β from α by

$$\beta(n) = \sum_{d|n} \mu(d)\alpha(\frac{n}{d})$$

Indeed, the first relation says that $\alpha = \beta * \mathbf{1}$. Hence

$$\alpha * \mu = (\beta * \mathbf{1}) * \mu = \beta * (\mathbf{1} * \mu) = \beta * \delta = \beta$$

2.4. **Dirichlet series.** An arithmetic function $\alpha \in \mathcal{A}$ has *polynomial growth* if there is some $A \geq 0$ so that $|\alpha(n)| \ll n^A$, for all $n \gg 1$.

For such an arithmetic function α of polynomial growth, we define an associated Dirichlet series $D_\alpha(s)$ by

$$D_\alpha(s) := \sum_{n=1}^{\infty} \frac{\alpha(n)}{n^s}$$

This converges for all complex $s \in \mathbb{C}$ with $\Re(s) > A + 1$, and hence defines an analytic function in that half-plane.

Examples

- The Dirichlet series of δ is $D_\delta(s) = 1$.
- The constant function $\mathbf{1}$ gives the Riemann zeta function

$$D_\delta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s), \quad \Re(s) > 1$$

Lemma 2.3. *If $\alpha, \beta \in \mathcal{A}$ have polynomial growth, then so does their convolution $\alpha * \beta$ and the corresponding Dirichlet series is the product*

$$D_{\alpha*\beta}(s) = D_\alpha(s) D_\beta(s), \quad \Re(s) \gg 1$$

Proof. For $\Re(s) \gg 1$,

$$\begin{aligned} D_\alpha(s) D_\beta(s) &= \sum \frac{\alpha(m)}{m^s} \sum_n \frac{\beta(n)}{n^s} \\ &= \sum_{m,n \geq 1} \frac{\alpha(m)\beta(n)}{(nm)^s} \\ &= \sum_{N=1}^{\infty} \frac{1}{N^s} \sum_{\substack{m,n \geq 1 \\ m \cdot n = N}} \alpha(m)\beta(n) \\ &= \sum_{N=1}^{\infty} \frac{1}{N^s} \alpha * \beta(N) = D_{\alpha * \beta}(s) \end{aligned}$$

□

As a corollary we see that the Dirichlet series associated to the Möbius function is $1/\zeta(s)$:

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}, \quad \Re(s) > 1 \tag{3}$$

Indeed, by Möbius inversion,

$$1 = D_\delta(s) = D_{\mu * \mathbf{1}}(s) = D_\mu(s) \cdot D_{\mathbf{1}}(s)$$

and since $D_{\mathbf{1}}(s) = \zeta(s)$ we are done.

An important property of the Dirichlet series associated to *multiplicative* functions is having an Euler product:

Proposition 2.4. *If α is a multiplicative function of polynomial growth, then*

$$D_\alpha(s) = \prod_{p \text{ prime}} \sum_{j=0}^{\infty} \frac{\alpha(p^j)}{p^{js}}, \quad \Re(s) \gg 1$$

As an example, we obtain Euler's product for the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}, \quad \Re(s) > 1 \, .$$

3. Application: The density of squarefree integers

As a first application of the material of Section 2, we use a very simple sieve to find the density of squarefree integers.

An integer n is *squarefree* if it has no square factors, that is if there is no $d > 1$ so that $d^2 \mid n$. Every integer $n \geq 1$ can be uniquely written in the form

$$n = f s^2, \quad f \text{ squarefree}$$

and n is squarefree if and only if $s = 1$; we will write $s = s(n)$.

Proposition 3.1. *The number $F(x)$ of squarefree integers up to x is*

$$\#\{n \leq x : n \text{ squarefree}\} = \frac{x}{\zeta(2)} + O(\sqrt{x})$$

Denote the indicator function of squarefrees by μ_2:

$$\mu_2(n) = \begin{cases} 1, & n \text{ squarefree} \\ 0, & \text{otherwise} \end{cases}$$

We need a representation of μ_2 using the Möbius function:

Lemma 3.2.

$$\mu_2(n) = \sum_{d^2|n} \mu(d)$$

Proof. We use the decomposition $n = f(n)s(n)^2$ with $f(n)$ squarefree. Since n is squarefree if and only if $s(n) = 1$, we can write (recall $\sum_{d|s} \mu(d) = 0$ if $s > 1$)

$$\mu_2(n) = \delta(s(n)) = \sum_{d|s(n)} \mu(d)$$

Now $d \mid s(n)$ if and only if $d^2 \mid s(n)^2$, and since $f(n)$ is squarefree, this happens if and only if $d^2 \mid n$. Thus

$$\sum_{d|s(n)} \mu(d) = \sum_{d^2|n} \mu(d)$$

which proves our claim. □

Proof of Proposition 3.1. Using Lemma 3.2 , we write

$$F(x) = \sum_{n \leq x} \mu_2(n) = \sum_{n \leq x} \sum_{d^2|n} \mu(d) \ .$$

Now we switch order of summation, noting that the d's will range up to $\sqrt{x}$:

$$F(x) = \sum_{d \leq \sqrt{x}} \sum_{\substack{n \leq x \\ d^2|n}} \mu(d)$$

The number of $n \leq x$, such that $d^2 \mid n$ is

$$\lfloor \frac{x}{d^2} \rfloor = \frac{x}{d^2} + O(1)$$

and hence we find

$$\begin{aligned} F(x) &= \sum_{d \leq \sqrt{x}} \mu(d) \left(\frac{x}{d^2} + O(1) \right) \\ &= x \sum_{d \leq \sqrt{x}} \frac{\mu(d)}{d^2} + O(\sum_{d \leq \sqrt{x}} 1) \end{aligned}$$

The series above is given by

$$\sum_{d\le\sqrt{x}} \frac{\mu(d)}{d^2} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O\left(\sum_{d>\sqrt{x}} \frac{1}{d^2}\right)$$

where we have used $|\mu(d)| \le 1$. The infinite sum is, by (3)

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)}$$

and thus we find

$$F(x) = \frac{x}{\zeta(2)} + O(\sqrt{x})$$

as claimed. □

Exercise 2. *Let $k \ge 2$. An integer n is k-free if $d^k \nmid n$ for all $d > 1$. Show that the number of k-free integers up to x is $x/\zeta(k) + O(x^{1/k})$.*