Math 229x - Introduction to Analytic Number Theory

Taught by Héctor Pastén
Notes by Dongryul Kim

Spring 2017

This course was taught by Héctor Pastén, and we met on MWF 11-12 in Science Center 411. We followed *Problems in Analytic Number Theory* by Ram Murty during the first half of the semester. There were 4 undergraduates and 4 graduate students, and the grading was based on weekly problem sets, a in-class midterm, and a take-home final. There was no course assistant.

Contents

1 January 23, 2017

1.1 Logistics

The purpose of this course is to expose you to fundamental methods, results, and problems of analytic number theory. This is not a research course, so we will not go for the sharpest results. Office hours are Thursdays from 10:00 am to 11:59 am. The text book is Ram Murty, *Problems in analytic number theory.* For some more advanced material, Iwaniec, Kowalski, *Analytic number theory* is a good reference. We will be covering:

- some elementary methods
- prime numbers: prime number theorem, primes in arithmetic progressions
- Dirichlet L-functions
- sieves: Brun's sieve and Selberg's Λ^2 sieve
- additive problems: Schnirelman's method and the circle method

There will be weekly assignments, due each monday, an in-class midterm, and a take-home final.

1.2 Playing with sums

You will need to get some practice in changing order of sums and partial summation.

Lemma 1.1. *Let $a_1, a_2, \dots$ be complex numbers and $x > 1$ be a real number. Let $f : [1, x] \to \mathbb{C}$ be a $C^1_{\mathbb{C}}$ function. Then*

$$\sum_{n \le x} a_n f(n) = \Big(\sum_{n \le x} a_n\Big) f(x) - \int_1^x \Big(\sum_{n \le t} a_n\Big) f'(t) dt.$$

Proof. Exercise. □

Example 1.2. Define $T(x) = \sum_{n \le x} \log n$. Then

$$\begin{aligned} T(x) &= \Big(\sum_{n \le x} 1\Big) \log x - \int_1^x \Big(\sum_{n \le t} 1\Big) \frac{dt}{t} \\ &= x \log x - \int_1^x \frac{t - \{t\}}{t} dt = (x + O(1)) \log x - (x - 1) + O(\log x) \\ &= x \log x - x + O(\log x). \end{aligned}$$

Example 1.3. Write $d(n) = \#$ of divisors of n. Then

$$\sum_{n \le x} d(n) = \sum_{n \le x} \sum_{a \cdot b = n} 1.$$

The picture is that we are counting points in a region bounded by two lines and a hyperbola. The big error is coming from the tail. So what Dirichlet did is to add up to $\sqrt{n}$ and then multiply by 2 using symmetry. So

$$\begin{aligned}\sum_{n\le x} d(n) &= 2\sum_{a\le x^{1/2}} \lfloor \frac{x}{a} \rfloor - (x + O(\sqrt{x})) = 2\sum_{a\le x^{1/2}} \Big(\frac{x}{a} + O(1)\Big) - x + O(\sqrt{x}) \\ &= 2x \sum_{a\le x^{1/2}} \frac{1}{a} - x + O(\sqrt{x}) \\ &= 2x(\log x^{1/2} + \gamma + O(x^{-1/2})) - x + O(\sqrt{x}) \\ &= x\log x + (2\gamma - 1)x + O(\sqrt{x}).\end{aligned}$$

Example 1.4. Write $\phi(n) = \#\{a \bmod n \text{ is invertible}\}$. Also define

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square-free,} \\ (-1)^{\#\text{prime factors on } n} & \text{if } n \text{ is square-free.}\end{cases}$$

Then

$$\phi(n) = n\sum_{d\mid n} \frac{\mu(d)}{d}.$$

The sum of $\phi(n)$ can be computed as

$$\begin{aligned}\sum_{n\le x}\phi(n) &= \sum_{n\le x} n \sum_{d\mid n}\frac{\mu(d)}{d} = \sum_{d\le x}\frac{\mu(d)}{d}\sum_{e\le x/d} de \\ &= \sum_{d\le x}\mu(d)\sum_{e\le x/d} e = \sum_{d\le x}\mu(d)\Big(\frac{1}{2}\Big(\frac{x}{d}\Big)^2 + O\Big(\frac{x}{d}\Big)\Big) \\ &= \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2} + O\Big(x\sum_{d\le x}\frac{1}{d}\Big) \\ &= \frac{x^2}{2}\Big(\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2} + O(x^{-1})\Big) + O(x\log x) = c\cdot x^2 + O(x\log x),\end{aligned}$$

where $c = 1/2\zeta(2) = 3/\pi^2$ by a problem in the homework.

2 January 25, 2017

Today we will count primes using Chebyshev's method. I am going to introduce a few functions. The **von Mangoldt function** is defined as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^\alpha \text{ for } \alpha \geq 1 \text{ and } p \text{ prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Higher prime powers don't contribute too much, so essentially we are counting primes. There are the prime counting functions

$$\begin{aligned} \pi(x) &= \#\{p \leq x : p \text{ is prime}\}, \\ \theta(x) &= \sum_{p \leq x} \log p, \\ \psi(x) &= \sum_{n \leq x} \Lambda(n). \end{aligned}$$

Clearly $\psi(x) \geq \theta(x)$ and $\pi(x) \log x \geq \theta(x)$. We can also write

$$\begin{aligned} \psi(x) &= \theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \cdots \\ &= \theta(x) + O(\theta(\sqrt{x}) \log x) = \theta(x) + O(x^{1/2} (\log x)^2) \end{aligned}$$

because trivially $\theta(x) \leq x \log x$.

2.1 Chebyshev's method

Recall that

$$T(x) = \sum_{n \leq x} \log n = \log(\lfloor x \rfloor !) = x \log x - x + (\log x).$$

It follows that

$$T(x) - 2T\Big(\frac{x}{2}\Big) = (\log x)x + O(\log x).$$

The reason we are doing this is because T and Λ can be related in a direct way. Recall that

$$\nu_p(n!) = \Big\lfloor \frac{n}{p} \Big\rfloor + \Big\lfloor \frac{n}{p^2} \Big\rfloor + \Big\lfloor \frac{n}{p^3} \Big\rfloor + \cdots .$$

Then

$$\begin{aligned} \sum_{k \geq 1} \psi\big(\frac{x}{k}\big) &= \sum_{k \geq 1} \sum_{n \leq x/k} \Lambda(n) = \sum_{n \leq x} \Lambda(n) \Big\lfloor \frac{x}{n} \Big\rfloor \\ &= \sum_{n \leq \lfloor x \rfloor} \Lambda(n) \Bigg\lfloor \frac{\lfloor x \rfloor}{n} \Bigg\rfloor = \sum_p \Bigg(\Bigg\lfloor \frac{\lfloor x \rfloor}{p} \Bigg\rfloor + \Bigg\lfloor \frac{\lfloor x \rfloor}{p^2} \Bigg\rfloor + \cdots \Bigg) \log p \\ &= \sum_p \nu_p(\lfloor x \rfloor !) \log p = \log(\lfloor x \rfloor !) = T(x). \end{aligned}$$

It follows that

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) + \psi\Big(\frac{x}{3}\Big) - \cdots = T(x) - 2T(x/2) = (\log 2)x + O(\log x).$$

So because ψ is increasing,

$$\psi(x) \geq (\log 2)x + O(\log x).$$

Corollary 2.1. *$\psi(x) \sim \theta(x)$.*

Similarly, we have $\psi(x) + \psi(x/2) \leq (\log 2)x + O(\log x)$ and so adding up this inequality for $x/2^s$, we get

$$\psi(x) \leq 2(\log 2)x + O((\log x)^2).$$

Corollary 2.2. *There are constants $a, A > 0$ such that $ax < \psi(x) < Ax$ for $x \gg 1$. That is, $\psi(x) \asymp x$. Hence $\theta(x) \asymp x$.*

Because $\theta(x) \leq \pi(x)\log x$, we have $\pi(x) \gg x/\log x$.

For the upper bound, we divide the interval into two and compute it separately.

$$\begin{aligned}\pi(x) &= \pi\Big(\frac{x}{(\log x)^2}\Big) + \#\{p : x/(\log x)^2 < p \leq x\} \\ &\leq \frac{x}{(\log x)^2} + \frac{\theta(x)}{\log(x/(\log x)^2)} \ll \frac{x}{(\log x)^2} + \frac{x}{\log x}.\end{aligned}$$

Corollary 2.3. *$\pi(x) \asymp x/\log x$.*

Corollary 2.4. *For $x \gg 1$, there exists a prime between x and $3x$.*

Proof. We have the estimate $(\log 2 - \epsilon)x < \psi(x) < 2(\log 2 + \epsilon)x$. □

What's missing in this picture is the asymptotic relation between θ (or ψ) and π. Recall that $\pi(x)\log x \geq \theta(x)$. In the other direction,

$$\theta(x) = \sum_{p \leq x} \log p = \pi(x)\log x - \int_2^x \pi(t)\frac{dt}{t}$$

and

$$\begin{aligned}\int_2^x \pi(t)\frac{dt}{t} &= \int_2^x \frac{t}{\log t}\frac{dt}{t} = \int_2^{x/\log x} \frac{dt}{\log t} + \int_{x/\log x}^x \frac{dt}{\log t} \\ &\ll 1 \cdot \frac{x}{\log x} + \frac{1}{\log x} \cdot x \ll \frac{x}{\log x}.\end{aligned}$$

It follows that

$$\theta(x) \sim \pi(x)\log x.$$

Theorem 2.5. *We have:*

(1) $\pi(x)\log x \sim \psi(x) \sim \theta(x)$

(2) $\pi(x) \asymp x/\log x$, $\psi(x) \asymp x$, $\theta(x) \asymp x$.

This is pretty much it for elementary methods.

2.2 The Riemann zeta function

This is not actually Riemann's function; it is Euler's. Euler defined

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \Big(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots \Big) = \prod_p \Big(1 - \frac{1}{p^s}\Big)^{-1}$$

which converges absolutely for $\Re(s) > 1$. It follows that there are infinitely many primes, because $\sum n^{-1} = 1$.

Now this function is defined only on the half-plane, but I want to do analytic continuation. For $\Re(s) > 1$, we have

$$\begin{aligned} \zeta(s) &= \lim_{x \to \infty} \sum_{n \leq x} \frac{1}{n^s} = \lim_{x \to \infty} \left(\lfloor x \rfloor \cdot \frac{1}{x^s} + s \int_1^x \frac{\lfloor t \rfloor}{t^{s+1}} dt \right) \\ &= s \int_1^\infty \frac{\lfloor t \rfloor}{t^{s+1}} dt = s \int_1^\infty \frac{dt}{t^s} - s \int_1^\infty \frac{\{t\} dt}{t^{s+1}} = \frac{s}{s-1} - s \int_1^\infty \frac{\{t\} dt}{t^{s+1}}. \end{aligned}$$

Note that the fractional part is bounded by 1 and so the integral on the right hand side makes sense for $\Re(s) > 0$ and is analytic on that region. And by complex analysis, if there is a meromorphic continuation, then it is unique.

Proposition 2.6. *$\zeta(s)$ has a meromorphic continuation to $\Re(s) > 0$ with a unique pole at $s = 1$. Moreover, the residue is $\operatorname{Res}_{s=1} \zeta(s) = 1$.*

Next time we will talk about L-functions.

3 January 27, 2017

Last time we discussed Chebyshev's method for counting primes and defined the Riemann ζ function. We also showed that $\zeta(s)$ has an analytic continuation for $\Re(s) > 0$.

3.1 Dirichlet series

Definition 3.1. A **Dirichlet series** is a series of form

$$D(s) = \sum_{n\geq 1} \frac{a_n}{n^s}, \quad a_n \in \mathbb{C}.$$

Proposition 3.2. *If $D(s)$ converges for $s = s_0 \in \mathbb{C}$, then for every $0 < \alpha < \pi/2$, $D(s)$ converges* uniformly *on the region $\{z \in \mathbb{C} : \Re(z - s_0) \geq 0, |\arg(z - s_0)| \leq \alpha\}$.*

Proof. Without loss of generality we may set $s_0 = 0$. This is because we may make a substitution. Now $\sum_{n\geq 1} a_n$ converges. We want for every $M > 0$ that $D(s)$ converges uniformly on $\{s \in \mathbb{C} : \Re(s) > 0, |s| \leq M\Re(s)\}$.

We have for $l > k$,

$$\sum_{n=k}^{l} \frac{a_n}{n^s} = \Big(\sum_{n=k}^{l} a_n\Big)\frac{1}{l^s} + \sum_{n=k}^{l-1}\Big(\sum_{j=k}^{n} a_j\Big)\Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big).$$

Let $\epsilon > 0$. Take N_ϵ such that for every $l > k > N_\epsilon$, $|\sum_{n=l}^{k} a_n| < \epsilon$. Then for s in the region,

$$\Big|\sum_{n=k}^{l} \frac{a_n}{n^s}\Big| < \epsilon\Big(1 + \sum_{n=k}^{l-1}\Big|\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big|\Big).$$

We now have the estimate

$$\Big|\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big| = \Big|s\int_{\log n}^{\log(n+1)} e^{-st}dt\Big| \leq |s|\int_{\log n}^{\log(n+1)} e^{-\Re(s)t}dt$$
$$= \frac{|s|}{\Re(s)}\Big(\frac{1}{n^{\Re(s)}} - \frac{1}{(n+1)^{\Re(s)}}\Big).$$

Because s is in the region,

$$\Big|\sum_{n=k}^{l} \frac{a_n}{n^s}\Big| < \epsilon\Big(1 + M\Big(\frac{1}{k^{\Re(s)}} - \frac{1}{l^{\Re(s)}}\Big)\Big) < \epsilon(1 + M). \qquad \square$$

Corollary 3.3. *There exist $\sigma_a, \sigma_c \in [-\infty, \infty]$ such that $D(s)$ converges (absolutely) for $\Re(s) > \sigma_c$ ($\Re(s) > \sigma_a$) and does not converge (absolutely) for $\Re(s) < \sigma_c$ ($\Re(s) < \sigma_a$). (Obviously $\sigma_c \leq \sigma_a$.)*

Corollary 3.4. *The Dirichlet series is $D(s) \equiv 0$ if and only if $a_n = 0$ for all n.*

Proof. By uniform convergence,

$$0 = \lim_{\sigma \to \infty} D(\sigma) = \lim_{\sigma \to \infty} \sum_n \frac{a_n}{n^\sigma} = \sum_n \lim_{\sigma \to \infty} \frac{a_n}{n^\sigma} = a_1.$$

Multiply by 2^s and repeat this process. □

Theorem 3.5 (Landau)**.** *Suppose that $a_n \geq 0$. Suppose also that:*

(1) $D(s)$ converges for $\Re(s) > \sigma$, where $\sigma \in \mathbb{R}$,

(2) there is a neighborhood of $s = \sigma$ where $D(s)$ has analytic continuation.

Then there exists an $\epsilon > 0$ such that $D(s)$ converges for $\Re(s) > \sigma - \epsilon$.

Note that this theorem cannot be applied to the Riemann zeta function because it has a pole at $s = 1$.

Proof. Without loss of generality let $\sigma = 0$. Let $\epsilon > 0$ such that $D(s)$ has analytic continuation to $|z - 1| \leq 1 + \epsilon$. By uniform absolute converge near 1, we have

$$D^{(k)}(1) = (-1)^k \sum_{n \geq 1} \frac{a_n (\log n)^k}{n}.$$

So we have

$$D(s) = \sum_{k \geq 0} \frac{(-1)^k}{k!} \left(\sum_{n \geq 1} \frac{a_n (\log n)^k}{n} \right) (s - 1)^k.$$

for $|s - 1| \leq 1 + \epsilon$. Then

$$\begin{aligned} D(-\epsilon) &= \sum_{k \geq 0} \frac{(-1)^k}{k!} \left(\sum_{n \geq 1} \frac{a_n (\log n)^k}{n} \right) (-1 - \epsilon)^k \\ &= \sum_{k \geq 0} \frac{1}{k!} \left(\sum_{n \geq 1} \frac{a_n (\log n)^k}{n} \right) (1 + \epsilon) \\ &= \sum_{n \geq 1} \frac{a_n}{n} \exp((\log n)(1 + \epsilon)) = \sum_{n \geq 1} \frac{a_n}{n^{-\epsilon}}. \end{aligned}$$

That is, the series converge. This shows that it converges for $\Re(s) > -\epsilon$. □

4 January 30, 2017

If you have two Dirichlet series

$$D(\{a_n\}_n, s) = \sum_{n\geq 1} \frac{a_n}{n^s}, \quad D(\{b_n\}_n, s) = \sum_{n\geq 1} \frac{b_n}{n^s},$$

that converge for $\Re(s) > \sigma$, then

$$D(\{a_n\}_n, s)D(\{b_n\}_n, s) = D(\{(a*b)_n\}_n, s)$$

where $(a*b)_n = \sum_{d|n} a_d b_{n/d}$ for $\Re(s) > \sigma$.

4.1 Dirichlet L-functions

Let $N \geq 1$ be an integer and let $G_N = (\mathbb{Z}/N\mathbb{Z})^\times$ be the multiplicative group. Define

$$\hat{G}_N = \{\chi : G_N \to \mathbb{C}^\times \text{ group morph.}\}.$$

By representation theory of abelian groups, we have a non-canonical isomorphic $\hat{G}_N \cong G_N$. There are orthogonality relations

$$\sum_{a \in G_N} \chi(a)\overline{\psi(a)} = \begin{cases} \phi(N), & \text{if } \chi = \psi \in \hat{G}_N \\ 0 & \text{otherwise,} \end{cases}$$

$$\sum_{\chi \in \hat{G}_N} \chi(a) \cdot \overline{\chi(b)} = \begin{cases} \phi(N) & \text{if } a = b \in G_N, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 4.1. Extend $\chi \in \hat{G}_N$ to $\mathbb{Z}$ by 0. Then define the **Dirichlet L-function** of the **Dirichlet character** χ as

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}.$$

The series converges absolutely in the region $\Re(s) > 1$. We also have a presentation

$$L(s, \chi) = \prod_p \Big(1 - \frac{\chi(p)}{p^s}\Big)^{-1}$$

which also converges absolutely in $\Re(s) > 1$.

Example 4.2. In the case $N = 4$, there is the principal character $\chi_0 =$ trivial and $\chi \neq \chi_0$. We have

$$L(s, \chi_0) = 1 + \frac{0}{2^s} + \frac{1}{3^s} + \cdots = \Big(1 - \frac{1}{2^s}\Big)\zeta(s).$$

There are some junk here, and this leads to the notion of primitive characters. The other L-function is

$$L(s, \chi) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots .$$

4.2 Analytic continuation

The first case is $\chi = \chi_0$. We have

$$L(s, \chi_0) = \prod_{p|N} \Big(1 - \frac{1}{p^s}\Big) \zeta(s)$$

and this implies that $L(s, \chi_0)$ has meromorphic continuation to $\Re(s) > 0$. The unique pole is at $s = 1$ of order 1 and $\operatorname{Res}_{s=1} L(s, \chi_0) = \phi(N)/N$.

Now let us look at the case $\chi \neq \chi_0$. In this case

$$\Big|\sum_{n \le t} \chi(n)\Big| \le \phi(N),$$

because there is cancellation on every interval of length N. Then by partial summation, for $\Re(s) > 1$

$$\sum_{n \le x} \frac{\chi(n)}{n^s} = \Big(\sum_{n \le x} \chi(n)\Big) \frac{1}{x^s} + s \int_1^x \Big(\sum_{n \le t} \chi(n)\Big) \frac{dt}{t^{s+1}}.$$

So we get for $\Re(s) > 1$,

$$L(s, \chi) = s \int_1^\infty \Big(\sum_{n \le t} \chi(n)\Big) \frac{dt}{t^{s+1}}.$$

But the right hand side converges absolutely for $\Re(s) > 0$. This gives analytic continuation and there is no pole. We moreover have:

Proposition 4.3. *The series $\sum_{n \ge 1} \chi(n)/n^s$ converges for $\Re(s) > 0$, and $L(s, \chi)$ is analytic for $\Re(s) > 0$.*

The question here is what is $L(1, \chi)$? If it doesn't go to infinity, what will it be? For $N = 4$ and $\chi \neq \chi_0$, we have

$$L(1, \chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \arctan(1) = \frac{\pi}{4}.$$

4.3 Nonvanishing of the L-function at 1

Fix $N > 1$. We want to show that if $\chi \neq \chi_0$ then $L(1, \chi) \neq 0$.

Lemma 4.4. *Let $p \nmid N$ and let $f(p) = \#\langle p \rangle$ in G_N and let $g(p) = \#(G_N/\langle p \rangle)$. Then*

$$\prod_{\chi \in \tilde{G}_N} (1 - \chi(p)T) = (1 - T^{f(p)})^{g(p)}.$$

Proof. We have

$$\prod_{\chi \in \hat{G}_N} (1 - \chi(p)T) = \prod_{\epsilon \in \mu_{f(p)}} \prod_{\chi(p) = \epsilon} (1 - \epsilon T) = (1 - T^{f(p)})^{g(p)}. \qquad \square$$

Define

$$F_N(s) = \prod_{\chi \in \hat{G}_N} L(s, \chi).$$

Lemma 4.5. *F_N is meromorphic on $\Re(s) > 0$. The only possible pole is at $s = 1$. If some $\chi \neq \chi_0$ satisfies $L(1, \chi) = 0$, then $F_N(s)$ is analytic on $\Re(s) > 0$.*

Proof. Obvious. □

Lemma 4.6. *$F_N(s)$ can be expressed as a Dirichlet series for $\Re(s) > 1$, in the form $F_N(s) = \sum_{n \geq 1} a_n / n^s$ with $a_n \geq 0$. Furthermore, the Dirichlet series does not converge at $s = 1/\phi(N)$.*

Proof. Look at the Euler factors. Then

$$F_N(s) = \prod_{p \nmid N} (1 - p^{-sf(p)})^{-g(p)} = \prod_{p \nmid N} (1 + f^{-f(p)s} + f^{-2f(p)s} + \cdots)^{g(p)}.$$

This immediately proves the first part. Now for $s \in \mathbb{R}$, the Euler factor is greater than $1 + p^{-\phi(N)s} + p^{-2\phi(N)s} + \cdots$. A comparison with the zeta function shows that this cannot converge. □

If $F_N(s)$ has no pole on $\Re(s) > 0$, then Landau imply convergence on $\Re(s) > 0$. But we have seen that the Dirichlet series does not converge at $s = 1/\phi(N)$. Thus there exists a pole.

Theorem 4.7. *For $\chi \neq \chi_0$, $L(1, \chi) \neq 0$.*

5 February 1, 2017

Last time we showed that if we take the character $\chi \neq \chi_0$ then $L(1, \chi) \neq 0$. This looks like a random fact, but it has a deeper meaning.

5.1 Primes in arithmetic progressions

Lemma 5.1. *Let $\chi \in \hat{G}_N$ be any character. Then for all $s \in \mathbb{C}$ with $\Re(s) > 1$, we have $L(s, \chi) \neq 0$.*

Proof. Look at the Euler product. □

Using this fact we can define $\log L(s, \chi)$ for $\Re(s) > 1$ with the condition that $\log 1 = 0$. In other words, we want $\lim_{\sigma \to +\infty} \log L(\sigma, \chi) = 0$.

Lemma 5.2. *Let $\chi \in \hat{G}_N$. There is $g_\chi(s)$ holomorphic on $\Re(s) > 1/2$ such that for all s with $\Re(s) > 1$,*

$$\log L(s, \chi) = \sum_p \frac{\chi(p)}{p^s} + g_\chi(s).$$

Proof. Define

$$g_\chi(s) = \sum_p \sum_{k \geq 2} \frac{1}{k} \frac{\chi(p^k)}{p^{ks}}.$$

This is holomorphic on $\Re(s) > 1/2$. Now

$$\log L(s, \chi) = \sum_p -\log\Big(1 - \frac{\chi(p)}{p^s}\Big) = \sum_p \sum_{k \geq 1} \frac{1}{k} \frac{\chi(p^k)}{p^{ks}}$$

for $\Re(s) > 1$ because Taylor expansion works in the region. □

Corollary 5.3. *Let $\chi \in \hat{G}_N$.*
(1) If $\chi = \chi_0$ then $\sum_p \chi_0(p)/p^s \sim -\log(s-1)$ as $s \to 1^+$.
(2) If $\chi \neq \chi_0$ then there exists a $B_\chi \in \mathbb{C}$ such that

$$\lim_{s \to 1^+} \sum_p \frac{\chi(p)}{p^s} = B_\chi.$$

Proof. (1) Look at the pole.

(2) Take $B_\chi = \log L(1, \chi) - g_\chi(1)$. (This works because $L(1, \chi) \neq 0$.) □

Theorem 5.4 (Dirichlet). *Let $N \geq 1$ and $(a, N) = 1$. There are infinitely many primes $p \equiv a \pmod{N}$. Furthermore, they have* ***analytic density*** *$1/\phi(N)$:*

$$\lim_{s \to 1^+} \frac{\sum_{p \equiv a\,(N)} p^{-s}}{\sum_p p^{-s}} = \frac{1}{\phi(N)}.$$

Proof. We have

$$\begin{aligned}\frac{1}{\phi(N)}\sum_{\chi\in\hat{G}_N}\overline{\chi(a)}\sum_p\frac{\chi(p)}{p^s}&=\sum_p\frac{1}{p^s}\frac{1}{\phi(N)}\sum_\chi\chi(p)\overline{\chi(a)}\\&=\sum_{p\equiv a\ (N)}\frac{1}{p^s}\end{aligned}$$

by orthogonality. Now we know the behavior of the sums $\sum_p\chi(p)/p^s$. □

5.2 Tauberian theorems

In general, the statements look like this. You have some weak convergence of sum sum or integral. And you have some analytic property. From this you show that you have strong convergence. Or you have some estimate for sums with weights and have some analytic property and get estimates without weights.

Theorem 5.5 (Newman's simple Tauberian theorem)**.** *Let $F:[0,\infty)\to\mathbb{C}$ be bounded an locally integrable. For $\Re(s)>0$ define*

$$G(s)=\int_0^\infty F(t)e^{-st}dt.$$

(Note that $G(s)$ is analytic on $\Re(s)>0$.) Suppose $G(s)$ has analytic continuation to a domain containing $\{s\in\mathbb{C}:\Re(s)\geq 0\}$. Then the improper integral $\int_0^\infty F(t)dt$ converges and its value is $G(0)$.

Proof. For $T>0$ let

$$G_T(s)=\int_0^T F(t)e^{-st}dt.$$

Note $G_T(s)$ converges for every $s\in\mathbb{C}$ and it is entire. We want to show that $\lim_{T\to\infty}G_T(0)=G(0)$.

For an arbitrary $R>0$ let $\delta=\delta_R>0$ such that $\{s\in\mathbb{C}:\Re(s)\geq-\delta,|\Im(s)|\leq R\}$ is contained in the domain of analytic extension of $G(s)$. Let

$$\mathscr{C}=\partial\{s\in\mathbb{C}:\Re(s)\geq-\delta,|s|\leq R\}.$$

Also let $\mathscr{C}^+=\mathscr{C}\cap\{\Re(s)>0\}$, $\mathscr{C}^-=\mathscr{C}\cap\{\Re(s)<0\}$. Write

$$G(0)-G_T(0)=\frac{1}{2\pi i}\int_{\mathscr{C}}(G(s)-G_T(s))e^{sT}\Big(1+\frac{s^2}{R^2}\Big)\frac{ds}{s}.$$

We will show that for R fixed, this is "small" as $T\to\infty$.

On $\mathscr{C}^+$ let $B=\|F\|_\infty$. For $\Re(s)>0$

$$|G(s)-G_T(s)|=\left|\int_T^\infty F(t)e^{-st}dt\right|\leq B\int_T^\infty|e^{-st}|dt=\frac{Be^{-\Re(s)T}}{\Re(s)}.$$

Note that for $w \in S^1$, $|1+w^2| = 2|\Re(w)|$. So, for $s \in \mathscr{C}^+$,

$$\left|e^{sT}\Big(1+\Big(\frac{s}{R}\Big)^2\Big)\frac{1}{s}\right| = \frac{2\Re(s)e^{\Re(s)T}}{R^2}.$$

So

$$\left|\frac{1}{2\pi i}\int_{\mathscr{C}^+}\cdots\right| \leq \frac{1}{2\pi}\ell(\mathscr{C}^+)\frac{2B}{R^2} = \frac{B}{R}.$$

The estimate on $\mathscr{C}^-$ is more complicated. Look at G and G^T separately. Because G_T is entire, we have $\int_{\mathscr{C}^-} G_T = \int_\gamma G_T$ where $\gamma = \{\Re(s) < 0, |s| = R\}$. For $s \in \gamma$,

$$|G_T(s)| = \left|\int_0^T F(t)e^{-st}dt\right| \leq B\int_0^T |e^{-st}|dt \leq \frac{Be^{-\Re(s)T}}{|\Re(s)|}.$$

The bound for the other factor is given by $2|\Re(s)|e^{\Re(s)}T/R^2$ and so we get

$$\left|\frac{1}{2\pi i}\int_{\mathscr{C}^-} G_T(s)(\cdots)\right| \leq \frac{B}{R}.$$

I will do the other estimate next time. □

6 February 3, 2017

Proof of Theorem 5.5. We showed

$$\begin{aligned}|G(0)-G_T(0)| &\le \frac{1}{2\pi}\bigg\{\bigg|\int_{\mathscr{C}+}(\cdots)\bigg| + \bigg|\int_{\mathscr{C}-} G_T(s)\cdot(\cdots)\bigg| + \bigg|\int_{\mathscr{C}-} G(s)\cdot(\cdots)\bigg|\bigg\} \\ &\le \frac{B}{R}+\frac{B}{R}+\frac{1}{2\pi}\bigg|\int_{\mathscr{C}-} G(s)e^{sT}\Big(1+\frac{s^2}{R^2}\Big)\frac{ds}{s}\bigg|.\end{aligned}$$

We now have to estimate this integral.

Note that on $\mathscr{C}^-$,

$$\Big|G(s)\Big(1+\frac{s^2}{R^2}\Big)\frac{1}{s}\Big| = O_R(1)$$

as $T\to\infty$, i.e., does not depend on T and is actually bounded. Thus

$$\frac{1}{2\pi}\bigg|\int_{\mathscr{C}-} G(s)e^{sT}\Big(1+\frac{s^2}{R^2}\Big)\frac{ds}{s}\bigg| \ll_R \int_{\mathscr{C}-} e^{\Re(s)T}|ds|.$$

As $T\to\infty$, the right hand side converges to 0, when R is fixed.

Adding the inequalities up, we get

$$\limsup_{T\to\infty}|G(0)-G_T(0)| \le \frac{2B}{R}$$

for any fixed $R>0$. Thus $\lim_{T\to\infty} G_T(0) = G(0)$. □

With this theorem our next goal is the prime number theorem.

6.1 The Riemann zeta on $\Re(s) = 1$

Lemma 6.1. *Let $0<\delta<1$ and $w\in\mathbb{C}$ with $|w|=1$. Then*

$$|(1-\delta)^{-3}(1-\delta w)^{-4}(1-\delta w^2)^{-1}| \ge 1.$$

Proof. Since δ is small we can use the Taylor series of $-\log(1-x)$. Then

$$\log|\cdots| = \Re\sum_{k\ge1}\frac{\delta^k}{k}(3+4w^k+w^{2k}) = \Re\sum_{k\ge1}\frac{\delta^k}{k}((2+w^k)^2-1)\ge 0. \qquad \square$$

This has a deep meaning as you will see later.

Corollary 6.2. *Let $\sigma>1$ and $t\in\mathbb{R}$. Then $|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)|\ge 1$.*

Proof. Look at the Euler factors for each p. □

Theorem 6.3. *$\zeta(s)$ does not vanish on $\Re(s)=1$.*

Proof. Suppose $\zeta(1+it_0)=0$. Certainly $t_0\ne 0$ and so $2t_0\ne t_0$. Let $\alpha = \mathrm{ord}_{1+it_0}\zeta(s)\ge 1$ and $\beta = \mathrm{ord}_{1+2it_0}\zeta(s)\ge 0$. Let $\sigma\to 1^+$ in the expression $\zeta(\sigma)^3\zeta(\sigma+it_0)^4\zeta(\sigma+2it_0)$. The limit is 0 because $-3+4\alpha+\beta\ge 1$. This is a contradiction. □

6.2 Prime number theorem

We want $\psi(x)/x \to 1$. This will show $\pi(x) \sim x/\log x$. Recall that

$$\psi(x) = \sum_{n \le x} \Lambda(n) \asymp x, \quad \sum_{n \ge 1} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)} \quad \text{for } \Re(s) > 1.$$

Note that for $\Re(s) > 1$,

$$\sum \frac{\Lambda(n)}{n^s} = s \int_1^\infty \psi(s) x^{-(s+1)} dx$$

by partial summation.

Theorem 6.4. *The integral* $\displaystyle\int_1^\infty \Big(\frac{\psi(x)}{x} - 1\Big)\frac{dx}{x}$ *converges.*

Proof. Define

$$G(s) = \int_1^\infty \Big(\frac{\psi(x)}{x} - 1\Big) x^{-s} \frac{dx}{x} = \int_0^\infty (\psi(e^t)e^{-t} - 1) e^{-st} dt.$$

Note that $F(t) = \psi(e^t)e^{-t} - 1$ is a bounded function and clearly locally integrable. Also for $\Re(s) > 0$,

$$G(s) = \int_1^\infty \psi(x) x^{-(s+2)} dx - \int_1^\infty x^{-(s+1)} dx = -\frac{1}{s+1} \frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{1}{s}.$$

This has analytic continuation to $\Re(s+1) = 1$. □

7 February 6, 2017

The midterm will be on Friday, March 3.

Our goal is to show $\pi(x) \sim \pi/\log x$, or equivalently, $\psi(x) \sim x$. Together with the Tauberian theorem and $\zeta(1+it) \neq 0$, we showed that

$$\int_1^\infty \Big(\frac{\psi(x)}{x} - 1\Big)\frac{dx}{x}$$

converges.

Theorem 7.1 (Prime number theorem)**.** *$\psi(x) \sim x$.*

Proof. Suppose not. Then one of the following holds:

I. There exists $\lambda > 1$ and infinitely many $T \to \infty$ such that $\psi(T) > \lambda T$. In such a case, since ψ is non-decreasing

$$\int_T^{\lambda T} \Big(\frac{\psi(x)}{x} - 1\Big)\frac{dx}{x} > \int_T^{\lambda T} \Big(\frac{\lambda T}{x} - 1\Big)\frac{dx}{x} = c^+(\lambda) > 0.$$

This contradicts the convergence of the integral.

II. There exists $0 \le \lambda < 1$ and infinitely many $T \to \infty$ with $\psi(T) < \lambda T$. You do the same thing. We have

$$\int_{\lambda T}^{T} \Big(\frac{\psi(x)}{x} - 1\Big)\frac{dx}{x} < \int_{\lambda T}^{T} \Big(\frac{\lambda T}{x} - 1\Big)\frac{dx}{x} = c^-(\lambda) < 0.$$

This again is a contradiction. □

The more you understand the behavior of the L-functions to the left, you know more about primes.

7.1 Poisson summation

Let's recall some Fourier analysis. Let $F : \mathbb{R} \to \mathbb{C}$ be $L^1([0,1])$ and 1-periodic. Define

$$c_k(F) = \int_0^1 F(t)e^{-2\pi ikt}dt.$$

Theorem 7.2. *If F is continuous and $\sum_{k\in\mathbb{Z}}|c_k(F)| < \infty$, then F equals its Fourier series pointwise:*

$$F(x) = \sum_k c_k(F)e^{2\pi ikx}.$$

Now start with a function $f : \mathbb{R} \to \mathbb{C}$ in $L^1(\mathbb{R})$. We define its **Fourier transform**

$$\hat{f}(t) = \int_{\mathbb{R}} f(x)e^{-2\pi ixt}dx.$$

Example 7.3. The Fourier transform of $f(x) = e^{-\pi x^2}$ is $\hat{f}(y) = e^{-\pi y^2}$.

Theorem 7.4 (Poisson summation formula)**.** *Suppose $f : \mathbb{R} \to \mathbb{C}$ is continuous, and there exists a $\delta > 0$ such that $|f(x)|, |\hat{f}(x)| \ll (1+|x|)^{-1-\delta}$. Then for every $y \in \mathbb{R}$,*

$$\sum_{n\in\mathbb{Z}} f(n+y) = \sum_{k\in\mathbb{Z}} \hat{f}(k)e^{2\pi iky}.$$

In particular, $\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n)$.

Proof. Define $F(y) = \sum_n f(n+y)$. The bound on $f(x)$ implies uniform absolute convergence. Thus F is continuous. This is a 1-periodic function. So we can compute its Fourier coefficients. By uniform and absolute convergence,

$$\begin{aligned} c_k(F) &= \int_0^1 F(x)e^{-2\pi ikx}dx = \int_0^1 \sum_n f(n+x)e^{-2\pi ikx}dx \\ &= \sum_n \int_0^1 f(n+x)e^{-2\pi ikx}dx = \sum_n \int_n^{n+1} f(x)e^{-2\pi ikx}dx = \hat{f}(k). \end{aligned}$$

Now analyze F. □

Here are some examples of f and $\hat{f}$ with $f, \hat{f} \ll (1+|x|)^{1+\delta}$.

$f(t)$	$e^{-\pi t^2}$	$e^{-\pi(t+c)^2}$	$e^{-\pi(t/r+c)^2}$
$\hat{f}(t)$	$e^{-\pi t^2}$	$e^{-\pi t^2+2\pi it}$	$re^{-\pi(rt)^2+2\pi icrt}$

Table 1: Some examples of Fourier transformation

Theorem 7.5. *Let $\alpha \in \mathbb{R}$. For $x > 0$ we have*

$$\sum_n e^{-\pi(n+\alpha)^2/x} = x^{1/2} \sum_n e^{-\pi n^2 x} e^{2\pi i\alpha n},$$

and in particular,

$$\sum_n e^{-\pi n^2/x} = x^{1/2} \sum_n e^{-\pi n^2 x}.$$

Proof. Take $f(t) = e^{-\pi(t+\alpha)^2/x}$. □

Define

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi in^2 z}$$

for $\Im(z) > 0$. Then we have just proved

$$\theta(i/x) = x^{1/2}\theta(ix)$$

for $x > 0$.

8 February 8, 2017

We defined $\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}$ for z in the upper half plane. We showed that $\theta(ix)$ satisfies a functional equation $\theta(i/x) = x^{1/2}\theta(ix)$ for $x > 0$. So we see that

$$\theta\Big(-\frac{1}{z}\Big) = (-iz)^{1/2}\theta(z)$$

for all z in the upper half plane, because both sides are holomorphic.

8.1 The Γ-function

Recall that

$$\Gamma(s) = \int_0^\infty e^{-x}x^s\frac{dx}{x}$$

for $\Re(s) > 0$. The reason we have a shift is because we are working in the Haar measure. The space $\mathbb{R}_{>0}$ has a structure of a multiplicative Lie group, and it has a locally additive structure. We are in some sense putting these together.

We have a functional equation $\Gamma(s+1) = s\Gamma(s)$ for $\Re(s) > 0$. Using this equation, you can inductively extend Γ to the whole complex plane and get a meromorphic function on $\mathbb{C}$. Here are some facts:

- $\Gamma(s)$ is holomorphic for $\Re(s) > 0$.
- $\Gamma(n) = (n-1)!$ for $n \in \mathbb{Z}_{>0}$.
- $\Gamma(s)$ has simple poles at $s = 0, -1, -2, \dots$.

I will post some additional material on $\Gamma(s)$ on the webpage.

8.2 Functional equation of $\zeta(s)$

We have

$$\begin{aligned}\Gamma\Big(\frac{s}{2}\Big) &= \int_0^\infty e^{-t}t^{s/2}\frac{dt}{t} = \int_0^\infty e^{-\pi n^2 x}(\pi n^2 x)^{s/2}\frac{dx}{x} \\ &= \pi^{s/2}n^s\int_0^\infty x^{s/2}e^{-\pi n^2 x}\frac{dx}{x}.\end{aligned}$$

So we see the zeta function arising here. We can write for $\Re(s) > 1$,

$$\begin{aligned}\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\zeta(s) &= \sum_{n\geq 1}\int_0^\infty x^{s/2}e^{-\pi n^2 x}\frac{dx}{x} \\ &= \int_0^\infty x^{s/2}\bigg(\sum_{n\geq 1}e^{-\pi n^2 x}\bigg)\frac{dx}{x} = \int_0^\infty x^{s/2}W(x)\frac{dx}{x}\end{aligned}$$

because of absolute convergence, where

$$W(x) = \sum_{n\geq 1} e^{-\pi n^2 x} = \frac{1}{2}(\theta(ix) - 1).$$

Now we are going to use the functional equation for θ, but there is a fixed point of the involution, 1. So

$$\begin{aligned}\int_0^\infty x^{s/2} W(x)\frac{dx}{x} &= \int_1^\infty x^{s/2}x^{s/2}W(x)\frac{dx}{x}W(x) + \int_0^1 x^{s/2}W(x)\frac{dx}{x} \\ &= \int_1^\infty x^{s/2}W(s)\frac{dx}{x} + \int_1^\infty x^{-s/2}W(x^{-1})\frac{dx}{x}.\end{aligned}$$

We have

$$W(x^{-1}) = \frac{1}{2}(\theta(i/x) - 1) = \frac{1}{2}(x^{1/2}\theta(ix) - 1) = x^{1/2}W(x) + \frac{1}{2}(x^{1/2} - 1).$$

Hence

$$\begin{aligned}\int_0^\infty x^{s/2}W(x)\frac{dx}{x} &= \int_1^\infty (x^{s/2} + x^{(1-s)/2})W(x)\frac{dx}{x} + \frac{1}{2}\int_1^\infty x^{-s/2}(x^{1/2} - 1)\frac{dx}{x} \\ &= \frac{1}{s(s-1)} + \int_1^\infty (x^{s/2} + x^{(1-s)/2})W(x)\frac{dx}{x}.\end{aligned}$$

Let us define

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\zeta(s).$$

Theorem 8.1 (Riemann)**.** *For $\Re(s) > 1$,*

$$\xi(s) = 1 + s(s-1)\int_1^\infty (x^{s/2} + x^{(1-s)/2})W(x)\frac{dx}{x}.$$

Corollary 8.2. *$\xi(s)$ extends to an entire function. In particular, $\zeta(s)$ extends to a meromorphic function on $\mathbb{C}$.*

Corollary 8.3. *$\xi(1-s) = \xi(s)$. This also gives a functional equation for $\zeta(s)$.*

Example 8.4. Let us compute $\zeta(0) = 1 + 1 + \cdots$. We have

$$s(s-1)\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\zeta(s) = 1 + s(s-1)(\text{entire}) = 1$$

at $s = 0$. The left hand side is $2(s-1)\pi^{-s/2}\Gamma(s/2+1)\zeta(s)$. So we can plug in $s = 0$ and get $\zeta(0) = -1/2$.

Example 8.5 (Trivial zeros)**.** Let $n \geq 1$ be a positive integer. Put $s = -2n$. Then

$$\xi(-2n) = 1 + 2n(2n+1)\int_1^\infty (\text{positive})\frac{dx}{x} > 0.$$

On the left hand side,

$$s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$$

is a product of a nonzero number and a simple pole and $\zeta(s)$. So we see that $\zeta(s)$ as a simple zero at $s=-2n$.

9 February 10, 2017

9.1 Primitive characters

For a $d \mid N$ there is a projection $\pi_d : G_N \to G_d$ because we have $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$. Then taking the dual gives

$$\pi_d^* : \hat{G}_d \to \hat{G}_N.$$

For any coprime a, d, there exists an r such that $(a + rd, N) = 1$, because for each prime factor $p \mid N$ you can locally find r such that $p \nmid a + rd$. So $G_N \to G_d$ is surjective and $\pi_d^* : \hat{G}_d \to \hat{G}_N$ is injective.

Definition 9.1. $\chi \in \hat{G}_N$ is **imprimitive** if there exists a proper divisor $d \mid N$ such that $\chi \in \operatorname{im}(\pi_d^*)$. Otherwise χ is called **primitive**.

Lemma 9.2. *Let $\chi \in \hat{G}_N$ and $d \mid N$. Then the following are equivalent:*

(i) $\chi \in \operatorname{im}(\pi_d^*)$.

(ii) for any $a \equiv 1 \pmod{d}$, if $(a, N) = 1$ then $\chi(a) = 1$.

Proof. Both (i) and (ii) are equivalent to: for every a, b, if $a \equiv b \pmod{d}$ and $(a, N) = (b, N) = 1$, then $\chi(a) = \chi(b)$. □

Definition 9.3. The **conductor** $\operatorname{cond}(\chi)$ of χ is the least Q such that $\chi \in \operatorname{im}(\pi_Q^*)$.

Lemma 9.4. *Let $\chi \in \hat{G}_N$. If for some $d \mid N$ we have $\chi \in \operatorname{im}(\pi_d^*)$, then* $\operatorname{cond}(\chi) \mid d$.

Proof. Write $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where $\alpha_i \geq 1$ and p_i are distinct primes. The Chinese remainder theorem says that there exist $\chi_j \in \hat{G}_{p_j^{\alpha_j}}$ such that $\chi = \prod_{j=1}^r \pi^*_{p_j^{\alpha_j}}(\chi_j)$. Now the result is clear for χ_j because the divisibility ordering for prime powers is the same as the usual ordering.

Note that for all $d \mid N$ such that $\chi \in \operatorname{im}(\pi_d^*)$, we have $Q = \prod_{j=1}^r \operatorname{cond}(\chi_j) \mid d$. Moreover, $\chi \in \operatorname{im}(\pi_Q^*)$. So by minimality, we have $Q = \operatorname{cond}(\chi)$. □

9.2 Gauss sums

Let $\chi \in \hat{G}_N$. The **Gauss sum** of χ is defined as

$$\tau(\chi) = \sum_{h=1}^{N} \chi(h) e\Big(\frac{h}{N}\Big), \quad e(x) = e^{2\pi i x}.$$

This is kind of a discrete version of Γ because it is the sum of something multiplicative and additive.

Proposition 9.5. *Let $\chi \in \hat{G}_N$. If $(n,N)=1$, then*

$$\chi(n)\tau(\bar{\chi}) = \sum_{h=1}^{N} \overline{\chi(h)} e\Big(\frac{nh}{N}\Big).$$

Moreover, if χ is primitive, then the condition $(n,N)=1$ can be dropped.

Proof. For $(n,N)=1$,

$$\chi(n)\tau(\bar{\chi}) = \sum_{k=1}^{N} \chi(n)\overline{\chi(k)} e\Big(\frac{k}{n}\Big) = \sum_{h=1}^{N} \overline{\chi(h)} e\Big(\frac{nh}{N}\Big).$$

For χ primitive, we only need to consider $(n,N)=q>1$. Write $N=qM$ and $n=qm$. Note that $\chi(n)\tau(\bar{\chi})=0$. So we have to show that the right hand side is zero. We have

$$\sum_{h=1}^{N} \overline{\chi(h)} e\Big(\frac{hm}{M}\Big) = \sum_{b=1}^{M} e\Big(\frac{bm}{M}\Big) \sum_{a=0}^{q-1} \bar{\chi}(aM+b) = \sum_{b=1}^{M} e\Big(\frac{bm}{M}\Big),$$

where $S(b)=\sum_{a=0}^{q-1}\bar{\chi}(aM+b)$. It suffices to show that $S(b)=0$ for all b.

Note that S is M-periodic. Since χ is primitive and $M \mid N$, there exist $t\equiv 1 \pmod{M}$ with $(t,N)=1$ and $\chi(t)\neq 1$. Write $t=cM+1$. Then

$$\bar{\chi}(t)S(b) = \sum_{a=0}^{q-1} \bar{\chi}(taM+cbM+b) = \sum_{a=0}^{q-1} \bar{\chi}(aM+cbM+b) = S(b).$$

Because $\bar{\chi}(t)\neq 1$, we get $S(b)=0$. □

Theorem 9.6. *Let $\chi \in \hat{G}_N$ be primitive. Then $|\tau(\chi)|=\sqrt{N}$.*

Proof. For every n

$$|\chi(n)|^2|\tau(\chi)|^2 = \bar{\chi}(n)\tau(\chi)\overline{\bar{\chi}(n)\tau(\chi)} = \sum_{k=1}^{N}\sum_{h=1}^{N} \chi(h)\bar{\chi}(k) e\Big(\frac{n(h-k)}{N}\Big).$$

Averaging over n gives

$$\phi(N)|\tau(\chi)|^2 = \sum_{n=1}^{N} |\chi(h)|^2 N = \phi(N)N.$$

□

The reason we are doing all this is because we want to give a functional equation for $L(s,\chi)$. If we define $\theta_0(z,\chi)=\sum_n \chi(n)e^{-\pi n^2 z}$, then this becomes 0 if $\chi(-1)=-1$. Anyways, the Poisson summation doesn't really apply directly. The Gauss sums give way to make this work.

10 February 13, 2017

For χ a primitive character, we proved a formula for $\chi(n)\tau(\bar{\chi})$ and also proved that $|\tau(\chi)| = N^{1/2}$.

10.1 Twisted θ-functions

Let $\chi \in \hat{G}_N$ be a primitive character. We have to distinguish two cases: when χ is **even**, i.e., $\chi(-1) = 1$, and when χ is **odd**, i.e., $\chi(-1) = -1$. Suppose now that χ is even. For $\Im(z) > 0$, we define

$$\theta_0(z, \chi) = \sum_{n \in \mathbb{Z}} \chi(n) e^{i\pi n^2 z/N}.$$

The condition χ even ensures that θ_0 does not vanish. Since χ is primitive,

$$\begin{aligned}\tau(\bar{\chi})\theta_0(z, \chi) &= \sum_n \chi(n)\tau(\bar{\chi}) e^{i\pi n^2 z/N} = \sum_n \sum_{h=1}^N \bar{\chi}(h) e^{i\pi n^2 z/N} e^{2\pi i h n/N} \\ &= \sum_{h=1}^N \bar{\chi}(h) \sum_n e^{i\pi n^2 z/N} e^{2\pi i h n/N}.\end{aligned}$$

For $x > 0$, we get

$$\begin{aligned}\tau(\bar{\chi})\theta_0(ix, \chi) &= \sum_{h=1}^N \bar{\chi}(h) e^{-\pi n^2 x/N} e^{2\pi i n h/N} \\ &= \left(\frac{N}{x}\right)^{1/2} \sum_{h=1}^N \bar{\chi}(h) \sum_n e^{-\pi(n+h/N)^2 N/x} \\ &= \left(\frac{N}{x}\right)^{1/2} \sum_{h=1}^N \bar{\chi}(h) \sum_n e^{-\pi(Nn+h)^2/(xN)} \\ &= \left(\frac{N}{x}\right)^{1/2} \sum_m \bar{\chi}(m) e^{-\pi m^2/xN} = \left(\frac{N}{x}\right)^{1/2} \theta_0(i/x, \bar{\chi}).\end{aligned}$$

We get a $\bar{\chi}$ but that is fine.

Theorem 10.1. *Let $\chi \in \hat{G}_n$ be primitive and even. Then*

$$\theta_0(i/x, \bar{\chi}) = \frac{\tau(\bar{\chi})}{N^{1/2}} x^{1/2} \theta_0(ix, \chi).$$

Again, the property of analytic continuation shows that this actually holds on the whole upper half plane.

Theorem 10.2. *Let $N > 1$, and let $\chi \in \hat{G}_N$ be primitive and even. Define*

$$\xi_0(s, \chi) = \left(\frac{N}{\pi}\right)^{s/2} \Gamma\left(\frac{s}{2}\right) L(s, \chi).$$

Then $\xi_0(s,\chi)$ extends to an entire function. It satisfies the functional equation

$$\xi_0(s,\chi) = w_0(\chi)\xi_0(1-s,\bar{\chi}) \quad \textit{with } w_0(\chi) = \frac{\tau(\chi)}{N^{1/2}}.$$

Let us now look at the case when χ is odd. For $\Im(z) > 0$, we define

$$\theta_1(z,\chi) = \sum_n \chi(n) n e^{i\pi n^2 z/N}.$$

To get a functional equation, we need the Poisson summation formula for $ne^{i\pi n^2 z/N}$. Recall that

$$\sum_n e^{-\pi n^2 y} e^{2\pi i n\zeta} = y^{-1/2} \sum_n e^{-\pi(n+\alpha)^2/y}.$$

By uniform convergence (on α), we can differentiate:

$$2\pi i \sum_n n e^{-\pi n^2 y} e^{2\pi i n\alpha} = -2\pi y^{-3/2} \sum_n (n+\alpha) e^{-\pi(n+\alpha)^2/y}.$$

For $h = 1, \dots, N$, choose $\alpha = h/N$ and $y = x/N$. Then

$$\begin{aligned}\sum_n n e^{-\pi n^2 x/N} e^{2\pi i n h/N} &= i\Big(\frac{N}{x}\Big)^{3/2} \sum_n \Big(n + \frac{h}{N}\Big) e^{-\pi(Nn+h)^2/xN} \\ &= iN^{1/2} \frac{1}{x^{3/2}} \sum_n (Nn+h) e^{-\pi(Nn+h)^2/xN}.\end{aligned}$$

After doing the exactly same thing, we get the following theorem.

Theorem 10.3. *Let $\chi \in \hat{G}_N$ be a odd primitive character. Then for all $x > 0$,*

$$\theta_1(i/x,\bar{\chi}) = \frac{\tau(\bar{\chi})}{iN^{1/2}} x^{3/2} \theta_1(ix,\chi).$$

Because the exponent of x is shifted by 1, we get a slightly different functional equation.

Theorem 10.4. *Let $\chi \in \hat{G}^N$ be odd and primitive. Define*

$$\xi_1(s,\chi) = \Big(\frac{N}{\pi}\Big)^{(s+1)/2} \Gamma\Big(\frac{s+1}{2}\Big) L(s,\chi).$$

Then $\xi_1(s,\chi)$ extends to an entire function and satisfies:

$$\xi_1(s,\chi) = w_1(\chi)\xi_1(1-s,\bar{\chi}) \quad \textit{with } w_1(\chi) = \frac{\tau(\chi)}{iN^{1/2}}.$$

In Murty's book there is a misprint in the formula.

Theorem 10.5. *Let $N > 1$ and $\chi \in \hat{G}_N$ primitive. Define $a_\chi = a = (1 - \chi(-1))/2$. Then*

$$\xi_a(s,\chi) = \Big(\frac{N}{\pi}\Big)^{(s+a)/2} \Gamma\Big(\frac{s+a}{2}\Big) L(s,\chi)$$

is entire and satisfies

$$\xi_a(1-s,\bar{\chi}) = \epsilon_a(\chi)\xi_a(s,\chi) \quad \textit{with } \epsilon_a(\chi) = i^a N^{1/2}/\tau(\chi).$$

11 February 15, 2017

11.1 Growth and zeros of $\xi(s)$

Recall that

$$\begin{aligned}\xi(s) &= s(s-1)\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\zeta(s)\\ &= 1 + s(s-1)\int_1^\infty \bigg(\sum_{n\geq 1} e^{-\pi n^2 x}\bigg)(x^{s/2} + x^{(1-s)/2})\frac{dx}{x}.\end{aligned}$$

This satisfies the functional equation $\xi(1-s) = \xi(s)$. So we are going to focus on $\Re(s) \geq 1/2$. On this region, we have

(1) $|s(s-1)\pi^{-s/2}| \ll \exp(c_1|s|)$.

(2) $\displaystyle \Big|\Gamma\Big(\frac{s}{2}\Big)\Big| = \bigg|\int_0^\infty e^{-t}t^{s/2-1}dt\bigg| \leq \int_0^\infty e^{-t}t^{\sigma/2-1}dt < \exp(c_2|s|(\log|\sigma|+1))$.

(3) $\displaystyle \zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt$, and so on the region $\Re(s) \geq 1/2$ and $|s| > 2$, we have $|\zeta(s)| \ll c_3 + c_4|s|$.

This all shows that

$$|\xi(s)| < \exp(c_5(|s|+1)\log(|s|+1))$$

for all $s \in \mathbb{C}$. This looks like a crude bound, but this is actually is optimal up to c_5, because it is sharp on the real line.

Corollary 11.1. *$\xi(s)$ has order 1. So $\xi(s)$ has infinitely many zeros.*

Proof. If $\xi(s)$ does not have infinitely many zeros, then $\xi(s)$ has to be a polynomial times e^{A+Bs}. But the lower bound does not match this growth. □

Theorem 11.2. *$\xi(s)$ and $\zeta(s)$ have the same zeroes in the critical strip $0 \leq \sigma \leq 1$, and there are infinitely many zeros, and the other zeros of $\zeta(s)$ are the trivial ones $s = -2n$.*

11.2 Hadamard factorization

In the case of order 1, we have the following factorization:

$$\xi(s) = e^{A+Bs}\prod_\rho \Big(1 - \frac{s}{\rho}\Big)e^{s/\rho},$$

where ρ runs over the zeros of ξ, repeated according to multiplicities. (Here we are using $\xi(0) = 1$.) We know that $1 = e^A$, and so we can take $A = 0$. The constant B has a deeper meaning.

Lemma 11.3. *We have:*

(i) $\frac{\xi'}{\xi}(1-s) = -\frac{\xi'}{\xi}(s)$.

(ii) $\frac{\xi'}{\xi}(s) = \frac{\zeta'}{\zeta}(s) + \frac{1}{s-1} - \frac{1}{2}\log\pi + \frac{1}{2}\frac{\Gamma'}{\Gamma}\Big(\frac{s}{2}+1\Big)$.

(iii) $\frac{\xi'}{\xi}(s) = B + \sum_\rho \Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big)$ *uniformly and absolutely in every large disc on* $\mathbb{C}$.

Proof. The only thing you need to check is that the Hadamard product is uniformly and absolutely convergent. This is the whole point of the Hadamard product. □

Corollary 11.4. $B = -\text{p.v.}\sum_\rho \frac{1}{\rho}$, *where the principal value means that you add them for* $|\Im\rho| < N$ *and let* $N \to \infty$.

Proof. This follows from (i) and (iii). □

Also, from (ii) and (iii), we get

$$B = -\frac{1}{2}\gamma - 1 + \frac{1}{2}\log(4\pi) \approx -0.02.$$

Theorem 11.5. *For* $s \in \mathbb{C}$,

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s-1} - B - \frac{1}{2}\log\pi + \frac{1}{2}\frac{\Gamma'}{\Gamma}\Big(\frac{s}{2}+1\Big) - \sum_\rho\Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big),$$

where ρ *runs over the nontrivial zeros of* $\zeta(s)$.

For $\sigma > 1$ and $s = \sigma + it$,

$$\Re\Big(-\frac{\zeta'}{\zeta}(s)\Big) = \sum_{n\ge 1}\frac{\Lambda(n)}{n^\sigma}\cos(t\log n).$$

Using the 3-4-1 bound, we get

$$3\Re\Big(-\frac{\zeta'}{\zeta}(\sigma)\Big) + 4\Re\Big(-\frac{\zeta'}{\zeta}(\sigma+it)\Big) + \Re\Big(-\frac{\zeta'}{\zeta}(\sigma+2it)\Big) \ge 0.$$

Lemma 11.6. *For* $\sigma > 1$, $-\frac{\zeta'}{\zeta}(\sigma) < \frac{1}{\sigma-1} + A_1$.

Lemma 11.7. *Let* $I \subseteq \mathbb{R}_{>0}$ *be a compact interval. Then for* $\sigma \in I$,

$$\Big|\Re\frac{\Gamma'}{\Gamma}(\sigma+it)\Big| \ll_I \log(|t|+2).$$

12 February 17, 2017

12.1 Zero-free region for $\zeta(s)$

Last time we discussed some consequences of the Hadamard product expansion. There is the "partial fraction formula"

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s-1} - B - \frac{1}{2}\log\pi + \frac{1}{2}\frac{\Gamma'}{\Gamma}\Big(\frac{s}{2}+1\Big) - \sum_\rho \Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big).$$

We also had the 3-4-1 bound

$$3\Big(-\frac{\zeta'}{\zeta}(\sigma)\Big) + 4\Re\Big(-\frac{\zeta'}{\zeta}(\sigma+it)\Big) + \Re\Big(-\frac{\zeta'}{\zeta}(\sigma+2it)\Big) \geq 0.$$

Lemma 12.1. *Let $I \subseteq \mathbb{R}_{>0}$ be a compact interval. Then for $\sigma \in I$,*

$$\Big|\Re\frac{\Gamma'}{\Gamma}(\sigma+it)\Big| \ll_I \log(|t|+2).$$

Proof. Taking the logarithmic derivative of the Weierstrass formula for Γ, we get

$$\Re\frac{\Gamma'}{\Gamma}(s+1) = -\gamma + \sum_{n\geq 1}\Re\Big(\frac{1}{n} - \frac{1}{s+n}\Big) = -\gamma + \sum_{n\geq 1}\frac{\sigma n + \sigma^2 + t^2}{n|s+n|^2}.$$

We have

$$\frac{\sigma n + \sigma^2 + t^2}{n|s+n|^2} \ll_I \begin{cases} 1/n^2 & |t|^2 < n \\ t^2/nt^2 = 1/n & |t|^2 \geq n. \end{cases}$$

Then the tail is bounded by a constant, and the case when $n \leq |t|^2$ is small is bounded by $\log|t|^2$. □

For $1 < \sigma < 2$, and $|t| > 1$, the partial fraction formula and Lemma 12.1 give

$$\Re\Big(-\frac{\zeta'}{\zeta}(s)\Big) \leq A_2 + A_3 + A_4\log(|t|+2) - \sum_\rho \Re\Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big).$$

Here,

$$\Re\Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big) = \frac{\sigma-\beta}{|s-\rho|^2} + \frac{\beta}{|\rho|^2} > 0,$$

where $\rho = \beta + i\tau$.

We are now going to use the 3-4-1 inequality. We look do the same thing we did for the non-vanishing of ζ on $\Re(s) = 1$. Let us write $\mathscr{L}(t) = \log(|t|+2)$.

Lemma 12.2. *For $1 < \sigma < 2$ and $|t| \geq 1$, we have*

$$\Re\Big(-\frac{\zeta'}{\zeta}(s)\Big) \leq A_5 + A_4 \mathscr{L}(t).$$

Let $\rho_0 = \beta_0 + i\tau_0$ be a non-trivial zero. Choosing $s = \sigma + i\tau_0$, we get:

Lemma 12.3. *We have for $1 < \sigma < 2$,*

$$\Re\Big(-\frac{\zeta'}{\zeta}(\sigma + i\tau_0)\Big) \leq A_5 + A_4 \mathscr{L}(\tau_0) - \frac{1}{\sigma - \beta_0}.$$

From the 3-4-1 inequality and Lemma 11.6, Lemma 12.2, Lemma 12.3, for $1 < \sigma < 2$,

$$0 \leq \frac{3}{\sigma - 1} + A_6 + A_4 \mathscr{L}(\tau_0) - \frac{4}{\sigma - \beta_0} + A_4 \mathscr{L}(2\tau_0),$$

for any nontrivial $\beta_0 + i\tau_0$ with $|\tau_0| \geq 1$. So we have

$$\frac{4}{\sigma - \beta_0} < \frac{3}{\sigma - 1} + A_6 + A_7 \mathcal{L}(\tau_0).$$

Choosing $\sigma = 1 + \delta/(\mathscr{L}(\tau_0))$ gives

$$\beta_0 < 1 - \frac{c}{\mathscr{L}(\tau_0)}$$

for some absolute constant c.

Theorem 12.4. *Let $\rho_0 = \beta_0 + i\tau_0$ be a non-trivial zero of ζ. Then $\beta_0 < 1 - c/\mathscr{L}(\tau_0)$ where $\mathscr{L}(t) = \log(|t| + 2)$.*

13 February 22, 2017

We are going to do the same thing for Dirichlet L-functions. In doing this, we may assume that the characters are primitive, because the two L-functions only differ by a finite number of Euler factors.

13.1 Zero-free region for $L(s, \chi)$

Assume that $\chi \in \hat{G}_N$ is primitive and $N > 1$. Let $a = a_\chi$. We have

$$\xi_a(s, \chi) = e^{A_\chi + B_\chi s} \prod_\rho \Big(1 - \frac{s}{\rho}\Big) e^{s/\rho},$$

because $\xi_a(s, \chi)$ has order 1 as you proved in the assignment and the only zeros are in the critical strip with $\rho \neq 0$ (since $L(1, \bar{\chi}) \neq 0$).

Recall

$$\xi_a(s, \chi) = \Big(\frac{N}{\pi}\Big)^{(s+a)/2} \Gamma\Big(\frac{s+a}{2}\Big) L(s, \chi).$$

Theorem 13.1 (Partial fraction)**.**

$$-\frac{L'}{L}(s, \chi) = -B_\chi + \frac{1}{2}\log\Big(\frac{N}{\pi}\Big) + \frac{1}{2}\frac{\Gamma'}{\Gamma}\Big(\frac{s+a}{2}\Big) - \sum_\rho \Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big),$$

where ρ runs over the nontrivial zeros of $L(s, \chi)$.

From the functional equation and $L(s, \bar{\chi}) = \overline{L(\bar{s}, \chi)}$, we get

$$\Re(B_\chi) = -\frac{1}{2}\sum_\rho \Big(\frac{1}{\rho} + \frac{1}{\bar{\rho}}\Big) = -\sum_\rho \Re\Big(\frac{1}{\rho}\Big).$$

Therefore, for $1 < \sigma < 2$,

$$\Re\Big(-\frac{L'}{L}(s, \chi)\Big) \leq c_1 \log N + c_2 \log(|t| + 2) - [\text{p.v}] \sum_\rho \frac{\sigma - \beta}{|s - \rho|^2}.$$

(We are using the notation $\rho = \beta + i\tau$.) These constants c_1 and c_2 do not depend on N. It will be convenient to write $\mathscr{L}(N, t) = \log(N(|t| + 2))$. Then

$$\Re\Big(-\frac{L'}{L}(s, \chi)\Big) \leq c_3 \mathscr{L}(N, t) - [\text{p.v}] \sum_\rho \frac{\sigma - \beta}{|s - \rho|^2}.$$

Here the standard 3-4-1 trick doesn't work, because there is a χ factor. For any (possibly non-primitive) $\psi \in \hat{G}_N$, we have

$$\Re\Big(-\frac{L'}{L}(s, \psi))\Big) = \sum_{(n,N)=1} \frac{\Lambda(n)}{n^\sigma} \Re(\psi(n) e^{-it\log n}).$$

So what we have is

$$3\Re\Big(-\frac{L'}{L}(\sigma,\chi_0)\Big)+4\Re\Big(-\frac{L'}{L}(\sigma+it,\chi)\Big)+\Re\Big(-\frac{L'}{L}(\sigma+2it,\chi^2)\Big)\geq 0.$$

Now here is a problem. If χ^2 is not principal, then we can just use this inequality, but if χ^2 is principal, then the third term introduces another pole. This was not a problem in the case of the Riemann zeta function because we can just work away from $s=1$ and check manually afterwards. But we cannot check this conceptually for all $L(s,\chi)$. This is an open problem today.

For first term, we have

$$\Big|\frac{\zeta'}{\zeta}(\sigma)-\frac{L'}{L}(\sigma,\chi_0)\Big|\leq\sum_{p\mid N}\log p\Big(\frac{1}{p^\sigma}+\frac{1}{p^{2\sigma}}+\cdots\Big)\leq\log N.$$

So we are happy as it can be absorbed into $\mathscr{L}$. We also have $\Re(-(\zeta'/\zeta)(\sigma))<1/(\sigma-1)+c_4$. So

$$\Re\Big(-\frac{L'}{L}(\sigma,\chi_0)\Big)<\frac{1}{\sigma-1}+c_5\log N.$$

For the second term, we again pick a single zero ρ_0. Taking $t=\tau_0$, we have

$$\Re\Big(-\frac{L'}{L}(\sigma+i\tau_0,\chi)\Big)<c_3\mathscr{L}(N,\tau_0)-\frac{1}{\sigma-\beta_0}.$$

Therefore:

Lemma 13.2. *Let $1<\sigma<2$, and $\rho_0=\beta_0+i\tau_0$ be some nontrivial zero of $L(s,\chi)$ where $\chi\in\hat{G}_N$ is primitive with $N>1$. Then*

$$\frac{4}{\sigma-\beta_0}<\frac{3}{\sigma-1}+c_6\mathscr{L}(N,\tau_0)+\Re\Big(-\frac{L'}{L}(\sigma+2i\tau_0,\chi^2)\Big).$$

There are two cases: when χ is non-real and when χ is quadratic.

Let us look at the case when χ is non-real. Note that χ^2 might be imprimitive. Let $N_1=\operatorname{cond}(\chi^2)$ where clearly $N-1\mid N$ and let χ^2 come from the primitive ψ. For $1<\sigma<2$,

$$\Big|\frac{L'}{L}(s,\chi^2)-\frac{L'}{L}(s,\psi)\Big|\leq\sum_{p\mid N}\log p\Big(\frac{1}{p^\sigma}+\cdots\Big)\leq\log N.$$

Thus we can use the bound we know:

$$\Re\Big(-\frac{L'}{L}(\sigma+2it,\chi^2)\Big)\leq-\log N+c_3\mathscr{L}(N_1,2t)<c_7\mathscr{L}(N,\tau_0).$$

Hence

$$\frac{4}{\sigma-\beta_0}<\frac{3}{\sigma-1}+c_8\mathscr{L}(N,\tau_0).$$

Doing the same thing we did for the zeta function, we get

$$\beta_0>1-\frac{c}{\mathscr{L}(N,\tau_0)}.$$

This is what we get for a non-real primitive character χ.

14 February 24, 2017

Last time we were discussing zero-free regions of $L(s,\chi)$, and we have finished the case of the non-quadratic characters.

14.1 Dealing with quadratic characters

Lemma 14.1. *Let $1 < \sigma < 2$, and $\rho_0 = \beta_0 + i\tau_0$ be a non-trivial zero of $L(s,\chi)$, with $\chi \in \hat{G}_N$ primitive and $N > 1$. Then*

$$\frac{4}{\sigma - \beta_0} < \frac{3}{\sigma - 1} + c_1 \mathscr{L}(N,\tau_0) + \Re\Big(-\frac{L'}{L}(\sigma + 2i\tau_0, \chi^2)\Big).$$

We now look at the case when χ is quadratic. Then $\chi^2 = \chi_0$, so for $1 < \sigma < 2$,

$$\begin{aligned}\Re\Big(-\frac{L'}{L}(\sigma + i\tau, \xi_0)\Big) &\leq \Re\Big(-\frac{\zeta'}{\zeta}(\sigma + it)\Big) + \log N \\ &\leq \Re\Big(\frac{1}{s-1}\Big) + c_2 \mathcal{L}(N,t),\end{aligned}$$

by the partial fraction decomposition. Now people don't know what to do when the imaginary part of s is too small.

Consider a small absolute constant $\delta > 0$, which we will figure our later. Assume that $|\tau_0| \geq \delta/\log N$. Choose

$$\sigma = 1 + \frac{\delta}{\mathscr{L}(n,\tau_0)}.$$

Then

$$\Re\Big(\frac{1}{\sigma + 2i\tau_0 - 1}\Big) \leq \Big|\frac{1}{(\sigma - 1) + 2i\tau_0}\Big| \leq \mathscr{L}(N,\tau_0)\frac{1}{\delta\sqrt{5}}.$$

The constant $1/\sqrt{5}$ is smaller than 1 and this is why everything works out. Now by the previous bound and the lemma, we get

$$\begin{aligned}\frac{4}{\sigma - \beta_0} &< \frac{3}{\sigma - 1} + c_3 \mathscr{L}(N,\tau_0) + \frac{1}{\delta\sqrt{5}}\mathscr{L}(N,\tau_0) \\ &= \mathscr{L}(N,\tau_0)\Big(\frac{3}{\delta} + \frac{1}{\delta\sqrt{5}} + c_3\Big).\end{aligned}$$

So we get

$$\begin{aligned}1 - \beta_0 &< -\frac{\delta}{\mathscr{L}(N,\tau_0)} + \delta\Big(\frac{3}{4} + \frac{1}{4\sqrt{5}} + \frac{\delta c_3}{4}\Big)^{-1}\frac{1}{\mathscr{L}(N,\tau_0)} \\ &= \frac{\delta}{\mathscr{L}(N,\tau_0)}\Big(\Big(\frac{3}{4} + \frac{1}{4\sqrt{5}} + \frac{\delta c_3}{4}\Big)^{-1} - 1\Big).\end{aligned}$$

Choosing a very small delta gives the bound we want.

14.2 Siegel zeros

What if τ_0 is too small? For some $0 < \delta \ll 1$, suppose that $|\tau_0| < \delta/\log N$. Then there actually is a pole contribution and there is nothing we can do about it.

Proposition 14.2. *Let $\chi \in \hat{G}_N$ with $N > 1$ be primitive quadratic. For an absolute constant $\delta^{\mathrm{II}} > 0$ (independent of N and χ) $L(s,\chi)$ can have at most one nontrivial zero in the region*

$$\beta_0 \geq 1 - \frac{\delta^{\mathrm{II}}}{\mathscr{L}(N,\tau)}.$$

If such a zero exists, then it is real and simple (and is not 1).

Such a zero, if exists, is called a **Siegel zero**, or a **Siegel–Landau zero**. A character χ such that $L(s,\chi)$ has a Siegel zero is called **exceptional**. This is not a very well-defined notion since δ^{II} is not given. But we can take δ^{II} to be small and assume that there are no Siegel zeros of infinitely many.

Proof. We only need to consider $|\tau_0| < \delta/\log N$. For $1 < \sigma < 2$, we have

$$-\frac{L'}{L}(\sigma,\chi) < c_6 \log N - [\text{p.v}] \sum_{\rho} \frac{1}{\sigma - \rho}.$$

Let $\rho_1 = \beta_1 + i\tau_1$ and $\rho_2 = \beta_2 + i\tau_2$ be two non-trivial zeros (possibly the same if ρ_1 is multiple). It is enough to consider:

(a) ρ_1 is non-real and $\rho_2 = \bar{\rho}_1$,

(b) ρ_1 and ρ_2 real.

If we can prove that they cannot be both in the region, we are done.

We will do (a) first. We end up with

$$-\frac{L'}{L}(\sigma,\chi) < c_6 \log N - \Big(\frac{1}{\sigma-\rho_1} + \frac{1}{\sigma-\bar{\rho}_1}\Big) = c_6 \log N - \frac{2(\sigma-\beta_1)}{(\sigma-\beta_1)^2 + \tau_1^2}.$$

Taking $\sigma = 1 + 2\delta/\log N$, we get

$$|\tau_1| < \frac{\delta}{\log N} = \frac{1}{2}(\sigma - 1) \leq \frac{1}{2}(\sigma - \beta_1).$$

So we have

$$-\frac{L'}{L}(\sigma,\chi) \leq c_6 \log N - \frac{8}{5}\frac{1}{\sigma-\beta_1}.$$

On the other hand, we have

$$-\frac{L'}{L}(\sigma,\chi) = \sum_n \frac{\Lambda(n)}{n^\sigma}\chi(n) > -\sum_n \frac{\Lambda(n)}{n^\sigma} = \frac{\zeta'}{\zeta}(\sigma) > -\frac{1}{\sigma-1} - c_7.$$

So we get

$$-\frac{1}{2\delta}\log N < c_8 \log N - \frac{8}{5}\frac{1}{\sigma - \beta_1}$$

and hence

$$1 - \beta_1 + \frac{2\delta}{\log N} < \frac{8}{5}\Big(c_8 + \frac{1}{2\delta}\Big)^{-1}\frac{1}{\log N}.$$

So taking δ small, we get the desired bound, because $8/5 > 1$.

The case (b) can be done very similarly. □

15 February 27, 2017

Here is the theorem we got so far.

Theorem 15.1. *Let $\chi \in \hat{G}_N$ be primitive with $N > 1$. There is an absolute constant $\delta > 0$ (effective, independent of χ and N) such that if χ is non-real, every nontrivial zero $\rho_0 = \beta_0 + i\tau_0$ of $L(s, \chi)$ satisfies*

$$\beta_0 < 1 - \frac{\delta}{\mathscr{L}(n, \tau_0)}, \quad \mathscr{L}(N, t) = \log(N(|t| + 2)). \tag{$*$}$$

Moreover, when χ is quadratic, $(*)$ also holds, except perhaps for at most one ρ_0. If such a ρ_0 exists for $L(s, \chi)$ then it is real and simple.

For now on up to spring break, we are going to only focus on the Riemann zeta function. There is nothing really interesting happening for Dirichlet L-functions, and I don't want to go into too much details in an introductory course.

We are now going to talk about counting zeros of $\zeta(s)$, explicit formula for $\psi(x)$, and the prime number theorem with error terms.

15.1 Counting zeros of $\zeta(s)$

We are going to denote

$$N(T) = \begin{pmatrix} \text{\# of zeros (with multiplicity) of } \zeta(s) \\ \text{in the region } 0 < \sigma < 1 \text{ and } 0 < t < T. \end{pmatrix}$$

Because we are going to do a contour integral, we assume that there is no zero at exactly height T. In other words, we don't take $T = \tau_0$ for ρ_0 a non-trivial zero of $\zeta(s)$. The zeros for $t < 0$ are conjugates.

Consider two contours

$$R : 2 \to 2 + iT \to -1 + iT \to -1 \to 2, \quad R' : 2 \to 2 + iT \to \frac{1}{2} + iT.$$

Then clearly

$$2\pi N(T) = \Delta_R \arg \zeta(s) = \Delta_R \xi(s).$$

Now note that $\overline{\xi(1 - \sigma + it)} = \xi(1 - \sigma + it) = \xi(\sigma + it)$. So the bottom line of ξ cancels out and the top two halves are equal. Hence

$$\pi N(T) = \Delta_{R'} \arg \xi(s).$$

Recall

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\zeta(s) = 2(s-1)\pi^{-s/2}\Gamma\Big(\frac{s}{2} + 1\Big)\zeta(s)$$

So the variation of the argument is the sum of three variations of each component. We can analyze each component as:

(i) $\Delta_{R'} \arg(s-1) = \pi/2 + O(1/T)$,

(ii) $\Delta_{R'} \arg(\pi^{-s/2}) = -T\log\pi/2$,

(iii) by Stirling's approximation,

$$\begin{aligned}\Delta_{R'} \arg\Gamma\Big(\frac{s}{2}+1\Big) &= \Im\log\Gamma\Big(\frac{5}{4}+\frac{iT}{2}\Big)\\ &= \Im\Big\{\Big(\frac{3}{4}+\frac{iT}{2}\Big)\log\Big(\frac{5}{4}+\frac{iT}{2}\Big)-\frac{iT}{2}-\frac{5}{4}+\frac{1}{2}\log(2\pi)+O(T^{-1})\Big\}\\ &= \frac{T}{2}\log\Big(\frac{T}{2}\Big)-\frac{T}{2}+\frac{3\pi}{8}+O(T^{-1}).\end{aligned}$$

We then immediately obtain

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi}-\frac{T}{2\pi}+O(1)+\frac{1}{\pi}\Delta_{R'}\arg\zeta(s).$$

We are now going to estimate the variation of $\zeta(s)$, which is erratic. This is the bound obtained a century ago and hasn't been improved.

Lemma 15.2. *For $T\to\infty$ and ρ over non-trivial zeros,*

$$\sum_\rho \frac{1}{1+(T-\tau)^2} \ll \log T.$$

Proof. For $t\geq 2$ and $1<\sigma<3$, we have

$$\Re\Big(-\frac{\zeta'}{\zeta}(s)\Big) < c_1\log t - \sum_\rho \Re\Big(\frac{1}{s-\rho}+\frac{1}{\rho}\Big).$$

Take $\sigma=2$ and $t=T$. Then $|(\zeta'/\zeta)(s)|\ll 1$. This immediately implies

$$\sum_\rho \Re\Big(\frac{1}{s-\rho}\Big)\leq c_2\log t.$$

Then

$$\Re\frac{1}{s-\rho} = \frac{2-\beta}{(2-\beta)^2+(T-\tau)^2} \geq \frac{1}{4+(T-\tau)^2}. \qquad \square$$

Corollary 15.3. *For T large:*

(1) There are $\ll\log T$ zeros ρ of $\zeta(s)$ with $|T-\tau|<1$.

(2) $\sum_{\rho,|T-\tau|\geq 1}(T-\tau)^{-2}\ll\log T$.

Lemma 15.4. *Let $\epsilon>0$. In the region $|s|>1$ and $|\arg(s)|<\pi-\epsilon$, we have*

$$\frac{\Gamma'}{\Gamma}(s) = \log s + O_\epsilon(|s|^{-1}).$$

Lemma 15.5. *For large T and $-1 \leq \sigma \leq 2$,*

$$\frac{\zeta'}{\zeta}(\sigma + iT) = \sum_{\rho, |T-\tau|<1} \frac{1}{s-\rho} + O(\log T).$$

Proof. We can write

$$\begin{aligned}\frac{\zeta'}{\zeta}(\sigma + iT) &= \frac{\zeta'}{\zeta}(\sigma + iT) - \frac{\zeta'}{\zeta}(2 + iT) + O(1) \\ &= O(\log T) + \sum_{\rho} \Big(\frac{1}{\sigma + iT - \rho} - \frac{1}{2 + iT - \rho} \Big),\end{aligned}$$

by partial fraction and Lemma 15.4. For ρ with $|T - \tau| \geq 1$, we have

$$\Big| \frac{1}{s-\rho} - \frac{1}{2+iT-\rho} \Big| = \frac{2-\sigma}{|(\sigma + iT - \rho)(2 + iT - \rho)|} \leq \frac{3}{|T-\tau|^2}.$$

Then the corollary implies that these terms contribute at most $\log T$. The other part is

$$\sum_{\rho, |T-\tau|<1} \Big(\frac{1}{s-\rho} - \frac{1}{2+iT-\rho} \Big) = \sum_{\rho, |T-\tau|<1} \frac{1}{s-\rho} + O(\log T),$$

by the corollary. □

16 March 1, 2017

Last time we had an equation

$$N(t) = \frac{T}{2\pi}\log\Big(\frac{T}{2\pi}\Big) - \frac{T}{2\pi} + O(1) + \frac{1}{\pi}\Delta_{R'}\arg\zeta(s).$$

Theorem 16.1. *For $T \to \infty$, we have*

$$N(T) = \frac{T}{2\pi}\log\Big(\frac{T}{2\pi}\Big) - \frac{T}{2\pi} + O(\log T).$$

Proof. It suffices to show that $\Delta_{R'}\arg\zeta(s) = O(\log T)$. Let us consider another contour $Q : 1/2 + iT \to 1 + iT$. We first note that

$$|\zeta(2+it) - 1| < \zeta(2) - 1 = \frac{\pi^2}{6} - 1 < 1.$$

So $\Delta_{R'}\arg\zeta(s) = O(1) - \Delta_Q \arg\zeta(s)$. We also have

$$\begin{aligned}\Delta_Q \arg\zeta(s) &= \Im\int_{1/2+iT}^{2+iT}\frac{\zeta'}{\zeta}(s)ds = \Im\int_{1/2+iT}^{2+iT}\Big(\sum_{|T-\tau|<1}\frac{1}{s-\rho}\Big)ds + O(\log T)\\ &= O(\log T) + \int_{|T-\tau|<1}\Delta_Q\arg(s-\rho)\\ &= O(\log T) + \pi O(\log T) = O(\log T).\end{aligned}$$

□

Corollary 16.2. *Let us label the nontrivial zeros of $\zeta(s)$ with $\tau > 0$ as $\rho_1, \rho_2, \dots$ such that the imaginary parts are nondecreasing (with multiplicities). Then*

$$\tau_n \sim \frac{2\pi n}{\log n}.$$

16.1 Integral approximation of ψ

The goal is to approximate

$$\psi_0(x) = \begin{cases}\psi(x) & \text{if } x > 2 \text{ is not a prime power}\\ \psi(x) - \frac{1}{2}\Lambda(x) & \text{if } x > 2 \text{ is a prime power}\end{cases}$$

in terms of the nontrivial zeros of $\zeta(s)$.

Theorem 16.3 (Perron's formula)**.** *Let*

$$\delta(y) = \begin{cases}0 & 0 < y < 1\\ 1/2 & y = 1\\ 1 & y > 1.\end{cases}$$

Define the function

$$I(y,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s} ds, \quad y > 0, c > 0, T > 0.$$

Then

$$|\delta(y) - I(y,T)| < \begin{cases} y^c \min\{1, 1/(T|\log y|)\} & y \neq 1, \\ c/T & y = 1. \end{cases}$$

Proof. Let us first consider the case $0 < y < 1$ so that $\delta(y) = 0$. Because $y < 1$, Cauchy give

$$I(y,T) = \Big(-\frac{1}{2\pi i}\int_{c+iT}^{\infty+iT} + \frac{1}{2\pi i}\int_{c-iT}^{\infty-iT}\Big)\frac{y^s}{s}ds.$$

Then we can estimate

$$\bigg|\int_{c+iT}^{\infty+iT} \frac{y^s ds}{s}\bigg| \leq \frac{1}{T}\int_c^\infty y^\sigma d\sigma = \frac{y^c}{T|\log y|}.$$

We also have the contour γ lying on the circle $R^2 = c^2 + T^2$. Then

$$|I(y,T)| \leq \frac{1}{2\pi}\bigg|\int_\gamma \frac{y^s ds}{s}\bigg| \leq \frac{1}{2\pi R} y^c \pi R < y^c.$$

For $y > 1$, you can do the same thing but use the rectangle going to the left.

Let us now consider the case $y = 1$. We have

$$I(1,T) = \frac{1}{2\pi i}\int_{-T}^{T} \frac{1}{c+it} i dt = \frac{1}{2\pi}\int_{-T}^{T} \frac{c - it}{c^2 + t^2} dt = \frac{1}{\pi}\int_0^T \frac{c}{c^2+t^2}dt.$$

You can just compute this. □

Corollary 16.4. *For $T > 0$, $c > 1$, and $x > 2$,*

$$\begin{aligned} &\bigg|\psi_0(x) - \frac{1}{2\pi i}\int_{c-iT}^{c+iT}\Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s ds}{s}\bigg| \\ &\quad = \bigg|\sum_{n\geq 1}\Lambda(n)\delta\Big(\frac{x}{n}\Big) - \sum_{n \geq 1}\Lambda(n)\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{(x/n)^s ds}{s}\bigg| \\ &\quad \leq \sum_{n\geq 1, n\neq x}\Lambda(n)\Big(\frac{x}{n}\Big)^c \min\Big\{1, \frac{1}{T|\log(x/n)|}\Big\} + \frac{c}{T}\Lambda(x). \end{aligned}$$

Let $c = c_x = 1 + 1/\log x$. With this choice, define

$$J(x,T) = \frac{1}{2\pi i}\int_{c_x - iT}^{c_x + iT}\Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s}{s}ds.$$

We are going to prove next time that for $x > 2$ and $T > 1$,

$$|\psi_0(x) - J(x,T)| \ll \frac{x(\log x)^2}{T} + (\log x)\min\Big\{1, \frac{x}{\langle x\rangle T}\Big\},$$

where $\langle x\rangle$ is its distance to the nearest prime power different to x.

17 March 6, 2017

For $x \geq e$, we let $c_x = 1 + (\log x)^{-1}$ (so that $x^{c_x} = ex$). We defined

$$J(x,T) = \frac{1}{2\pi i} \int_{c_x - iT}^{c_x + iT} \Bigl(-\frac{\zeta'}{\zeta}(s)\Bigr) \frac{x^s}{s} dx$$

for $T > 0$.

Theorem 17.1. *For $x \geq e$ and $T > 1$ we have*

$$|\psi_0(x) - J(x,T)| \ll \frac{x(\log x)^2}{T} + (\log x) \min\Bigl\{1, \frac{x}{\langle x \rangle T}\Bigr\}.$$

Proof. We had from Perron's formula,

$$|\psi_0(x) - J(x,T)| \leq \sum_{n=1, n\neq x} \Lambda(n) \Bigl(\frac{x}{n}\Bigr)^{c_x} \min\Bigl\{1, \frac{1}{T \log|x/n|}\Bigr\} + c_x \Lambda(x)/T.$$

Note that $c_x \Lambda(x)/T \ll \log x/T$. For the series, we consider the range $n \leq 3x/4$ or $n \geq 5x/4$. In this range, the series is bounded by

$$\sum \ll \sum_{n \geq 1} \Lambda(n) \frac{x}{n^{c_x}} \frac{1}{T} = \frac{x}{T} \Bigl(-\frac{\zeta'}{\zeta}(c_x)\Bigr) \ll \frac{x \log x}{T}.$$

Now we look at the range $3x/4 < n < x$. Let k be the larges prime power less than x. (Without loss of generality we may assume $3x/4 < k < x$.) We have

$$\log \frac{x}{k} = -\log \frac{k}{x} = -\log\Bigl(1 - \frac{x-k}{x}\Bigr) \geq \frac{x-k}{x} \geq \frac{\langle x \rangle}{x}.$$

So the term at $n = k$ is bounded by

$$\begin{aligned} &\ll \Lambda(k) \frac{x}{T\langle x \rangle} \ll \frac{x \log x}{T \langle x \rangle}, \quad \text{or} \\ &\ll \Lambda(k) \ll \log x. \end{aligned}$$

The other numbers n in this this range is $n = k - j$ for $0 < j < n/4$. The sum then can be bounded as

$$\sum \ll \frac{\log x}{T} \sum_{j < x/4} \frac{1}{|\log(x/(k-j))|} \ll \frac{\log x}{T} \sum_{j < 4/x} \frac{x}{j} \ll \frac{x(\log x)^2}{T}.$$

The other range $x < k < 5x/4$ can be treated similarly. □

So

$$\psi_0(x) = \frac{1}{2\pi i} \int_{c_x - iT}^{c_x + iT} \Bigl(-\frac{\zeta'}{\zeta}(s)\Bigr) \frac{x^s}{s} dx + (\text{Error term}),$$

where the error term goes to 0 as $T \to \infty$. It is very tempting to shift the integral.

17.1 Explicit formula for ψ_0

The goal is to prove that for $x \geq e$ (and $1 < c_x \leq 2$),

$$\psi_0(x) = x - \sum_{\rho}^{\text{p.v.}} \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2}\log\Big(1 - \frac{1}{x^2}\Big).$$

This looks like a random formula, but it is not. Consider a rectangle $-U-iT \to c_x - iT \to c_x + iT \to -U + iT \to -U - iT$. If we assume that the integrals on the top, bottom, left vanish as U and T go to infinity, there is only the contributions of the residues. The poles are at the zeros of ζ, the pole of ζ, and $s = 0$. The sum of these residues formally is exactly the right hand side.

When we do the contour integral, we would want to stay away from the poles. So we need some technical assumptions.

- We will take $U \geq 3$ an odd integer.
- We will take $T \geq 2$ such that if $\rho = \beta + i\tau$ is any zero of ζ, then $|T - \tau| \gg 1/\log T$. $(**)$

The second condition can be satisfied because there are at most $\log T$ possible τ in $[T-1, T+1]$.

Let us start working. We are going to split the horizontal contours to $-U + iT \to -1 + iT$ and $-1 + iT \to c_x + iT$.

Lemma 17.2. $\displaystyle\int_{-1+iT}^{c_x+iT} \Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s}{s} ds \ll \frac{x(\log T)^2}{T \log x}$*, and similarly for the conjugate path.*

Proof. We have

$$\left|\int_{-1+iT}^{c_x+iT} \Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s}{s} ds\right| \ll \frac{(\log T)^2}{T} \int_{-1}^{c_x} x^\sigma d\sigma.$$

This is because

$$-\frac{\zeta'}{\zeta}(s) = \sum_{|T-\tau|<1} \frac{1}{s-\rho} + O(\log T)$$

and we assume $(**)$. □

Lemma 17.3. *For* $\Re(s) \leq -1$ *we have*

$$\left|\frac{\zeta'}{\zeta}(s)\right| \ll \log(2|s|).$$

away from radius $1/2$ *from the trivial zeros* $s = -2, -4, \ldots$.

Proof. The functional equation gives you

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\cos\Bigl(\frac{\pi s}{2}\Bigr)\Gamma(s)\zeta(s).$$

Then taking the logarithmic derivative gives

$$-\frac{\zeta'}{\zeta}(1-s) = O(1) - \frac{\pi}{2}\tan\Bigl(\frac{\pi s}{2}\Bigr) + \frac{\Gamma'}{\Gamma}(s) + \frac{\zeta'}{\zeta}(s)$$

for $\Re(s) \geq 2$. Now ζ'/ζ is bounded for $\Re(s) \geq 2$. □

18 March 8, 2017

We are trying to estimate the integral. Let us write

$S : -1 + iT \to c_x + iT, \quad H : -U + iT \to -1 + iT, \quad V : -U - iT \to -U + iT.$

Last time we proved

$$\left|\int_S \Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s}{s}ds\right| \ll \frac{x(\log T)^2}{T\log x}$$

for $x \geq e$, $T \geq 2$, and under hypothesis $(**)$. There was also the estimate

$$\left|\frac{\zeta'}{\zeta}(s)\right| \ll \log(2|s|)$$

for $\Re(s) \leq -1$ away from the points $-2, -4, \dots$ by distance $1/2$. Because of this, we let U be an odd integer.

Using this estimate, we have

$$\left|\int_H \Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s ds}{s}\right| \ll \frac{\log(2T)}{T}\int_1^U x^{-\sigma}d\sigma \ll \frac{\log T}{T}\frac{1}{x\log x}$$

because $\log(2|s|)/|s|$ is decreasing in $|s|$.

The same argument gives

$$\left|\int_V \Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s}{s}ds\right| \ll \frac{\log U}{U}\int_{-T}^T x^{-U}dt \ll \frac{\log U}{U}Tx^{-U}.$$

If I collect all my bounds,

$$\frac{1}{2\pi i}\int_{c_x-iT}^{c_x+iT}\Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s ds}{s} = (\text{residues}) + O\Big(\frac{x(\log T)^2}{T\log x} + \frac{\log U}{U}Tx^{-U}\Big).$$

I can make this sum of residues explicit:

$$(\text{residues}) = x - \sum_{|\tau|<T}\frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) + \sum_{1\leq n<U/2}\frac{x^{-2n}}{2n}.$$

Letting $U \to \infty$, we get

$$\frac{1}{2\pi i}\int_{c_x-iT}^{c_x+iT}\Big(-\frac{\zeta'}{\zeta}(s)\Big)\frac{x^s ds}{s} = x - \sum_{|\tau|<T}\frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \log\Big(1 - \frac{1}{x^2}\Big) + O\Big(\frac{x(\log T)^2}{T\log x}\Big).$$

We can now use the integral approximation for $\psi_0(x)$.

Theorem 18.1 (Explicit formula)**.** *For $x \geq e$ and $T \geq 3$ under $(**)$,*

$$\psi_0(x) = x - \sum_{|\tau|<T}\frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \log\Big(1 - \frac{1}{x^2}\Big) + E(x,T),$$

where

$$|E(x,T)| \ll \frac{x(\log T)^2}{T\log x} + \frac{x(\log x)^2}{T} + (\log x)\min\Big\{1, \frac{x}{\langle x\rangle T}\Big\}.$$

In particular, as $T \to \infty$,

$$\psi_0(x) = x - \sum_{\rho}^{\text{p.v.}} \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \log\Big(1 - \frac{1}{x^2}\Big).$$

18.1 Prime number theorem revisited

Let us estimate the $\psi(x)$ for $x \geq 3$ an integer. The first thing to notice is that

$$\psi(x) = \psi_0(x) + O(\log x) = x - \sum_{|\tau|<T} \frac{x^\rho}{\rho} + O(\log x) + E(x,T).$$

This $O(\log x)$ is a pretty small error. Also,

$$|E(x,T)| \ll \frac{x}{T}(\log(xT))^2.$$

Now the goal is to estimate the sum of x^ρ/ρ for T as large as possible. We have

$$\bigg|\sum_{0<\tau<T} \frac{x^\rho}{\rho}\bigg| \leq x^{\beta_T} \sum_{0<\tau<T} \frac{1}{|\rho|} \ll x^{1-\delta/\log T}(\log T)^2,$$

because we know how to count zeros, and

$$\beta_T = \max\{\Re(\rho) : 0 < \tau < T\} \leq x^{1-\delta/\log T}.$$

from the zero-free region. I now claim that $T = \exp(\sqrt{\log x})$ is a good choice. You plug things in and you get the following theorem.

Theorem 18.2. $\psi(x) = x + O(x \exp^{-c\sqrt{\log x}})$. *So for any $A > 1$,*

$$\psi(x) = x + O_A\Big(\frac{x}{(\log x)^A}\Big).$$

19 March 10, 2017

19.1 Riemann hypothesis

Conjecture 19.1 (Riemann hypothesis)**.** *All nontrivial zeros of $\zeta(s)$ have real part $1/2$.*

Conjecture 19.2 (δ-Riemann hypothesis)**.** *For a real number $0 < \delta \leq 1/2$, every non-trivial zero ρ of $\zeta(s)$ have $\Re(\rho) \leq 1 - \delta$.*

Conjecture 19.3 (Quasi-Riemann hypothesis)**.** *The δ-Riemann hypothesis holds for some $0 < \delta \leq 1/2$.*

The explicit formula says that, for $x \geq 3$ and $T \geq 3$ under hypothesis $(**)$,

$$\psi(x) = x - \sum_{|\tau|<T} \frac{x^\rho}{\rho} + O\Big(\log x + \frac{x}{T}\{(\log x)^2 + (\log T)^2\}\Big).$$

Let us assume the δ-Riemann hypothesis for some fixed $\delta \in (0, 1/2]$. Then

$$\left| \sum_{0 \leq \tau < T} \frac{x^\rho}{\rho} \right| \leq x^{1-\delta} \sum_{0<\tau<T} \ll x^{1-\delta}(\log T)^2.$$

Take $T = x^\delta + O(1)$, where $O(1)$ is there to make T satisfy $(**)$. We get the following theorem.

Theorem 19.4. *The δ-Riemann hypothesis implies that*

$$\psi(x) = x + O_\delta(x^{1-\delta}(\log x)^2).$$

Theorem 19.5. *Suppose that for some $\delta > 0$ we have*

$$\psi(x) = x + O_\epsilon(x^{1-\delta+\epsilon})$$

for each $\epsilon > 0$. Then the δ-Riemann hypothesis holds (for the same δ).

Proof. Write $E(t) = \psi(x) - x$. Our hypothesis is that $|E(t)| \ll_\epsilon t^{1-\delta+\epsilon}$. For $\Re(s) > 1$,

$$-\frac{\zeta'}{\zeta}(s) = \sum_{n\geq 1} \frac{\Lambda(n)}{n^s} = s\int_1^\infty \frac{\psi(x)dx}{x^{s+1}} = \frac{s}{s-1} + s\int_1^\infty E(t)\frac{dt}{t^{s+1}}.$$

The integral is holomorphic for $\Re(s) > 1 - \delta$. This shows that ζ'/ζ only has a pole at $s = 1$ in $\Re(s) > 1 - \delta$. □

Corollary 19.6. *The error term $\psi(x) \sim x$ cannot be $O(x^\alpha)$ for any $\alpha < 1/2$.*

Corollary 19.7. *Suppose that for some $\delta > 0$ we have*

$$\psi(x) = x + O_\epsilon(x^{1-\delta}(\log x)^2).$$

Then $\psi(x) + O(x^{1-\delta}(\log x)^2)$.

What is the best zero-free region? Vinogradov and Korobov proved in 1958 that

$$\sigma > 1 - \frac{\delta_\alpha}{(\log(|t|+2))^\alpha},$$

for any fixed $\alpha > 2/3$ and $\delta_\alpha > 0$. This 2/3 hasn't been improved since.

19.2 Lindelöf hypothesis

How large is $\zeta(s)$ on the critical strip? An easy exercise is that for $0 < \sigma < 1$ and $t > 1$,

$$|\zeta(s)| \ll t.$$

Conjecture 19.8 (Lindelöf hypothesis)**.** *For any $\epsilon > 0$,*

$$\left|\zeta\left(\frac{1}{2} + it\right)\right| \ll_\epsilon |t|^\epsilon.$$

Theorem 19.9. *The Riemann hypothesis implies the Lindelöf hypothesis.*

Theorem 19.10 (Lindelöf)**.** *For $\sigma \in \mathbb{R}$ define*

$$\mu(\sigma) = \inf\{\alpha : |\zeta(\sigma + it)| \ll_{\sigma,\alpha} |t|^\alpha \textit{ for } |t| > 1\}.$$

Then $\mu : \mathbb{R} \to \mathbb{R}$ is convex (hence continuous).

The proof follows from the Phragmén–Lindelöf principle. Note that $\mu(\sigma) = 0$ for $\sigma \geq 1$. By the functional equation

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

we get $\mu(\sigma) = 1/2 - \sigma$ for $\sigma \leq 0$. The convexitiy will give

$$\mu(\sigma) \leq \frac{1-\sigma}{2}$$

for $0 \leq \sigma \leq 1$. Lindelöf hypothesis is telling you that $\mu(\sigma) = 0$ for $\sigma \geq 1/2$ and $\mu(\sigma) = 1/2 - \sigma$ for $\sigma \leq 1/2$.

The best subconvexity bound was proved by Bourgain in 2017:

$$\mu(1/2) \leq \frac{13}{84} \approx 0.154.$$

20 March 20, 2017

20.1 Introduction to sieves

Let me start with the concrete problem before going to the general theory. We want to estimate the number of primes $\pi(x)$. There is a combinatorial way of getting primes. Starting from 2, you circle 2 and scar out all multiples of 2. Then circle 3 and scar out all multiples of 3. You can do this up to some z, and this gives an upper bound of $\pi(x)$. Formally, we define

$$\pi(x,z) = \#\{n \leq x : p \nmid n \text{ for all } p \leq z\}.$$

Here are some obvious facts:

- $\pi(x) \leq \pi(z) + \pi(x,z)$
- $\pi(x) = \pi(\sqrt{x}) + \pi(x,\sqrt{x}) = \pi(x,\sqrt{x}) + O(\sqrt{x})$

Let us define

$$P_z = \prod_{p \leq z} p, \quad \delta(m) = \begin{cases} 1 & m = 1, \\ 0 & m \neq 1. \end{cases}$$

Then

$$\pi(x,z) = \sum_{n \leq x} \delta(\gcd(n, P_z)).$$

There is the **combinatorial sieve**, that uses

$$\sum_{d \mid n} \mu(d) = \delta(n).$$

Then we have

$$\begin{aligned} \pi(x,z) &= \sum_{n \leq x} \sum_{d \mid (n,P_z)} \mu(d) = \sum_{d \mid P_z} \mu(d) \sum_{n \leq x, d \mid n} 1 = \sum_{d \mid P_z} \mu(d) \Big(\frac{x}{d} + O(1) \Big) \\ &= x \sum_{d \mid P_z} \frac{\mu(d)}{d} + O\Big(\sum_{d \mid P_z} 1 \Big) = x \prod_{p \leq z} \Big(1 - \frac{1}{p} \Big) + O(2^{\pi(z)}). \end{aligned}$$

Proposition 20.1. $\pi(x,z) = x \prod_{p \leq x} \Big(1 - \frac{1}{p} \Big) + O(2^{\pi(z)})$.

How good is this? From Chebyshev's bound we have

$$\prod_{p \leq z} \Big(1 - \frac{1}{p} \Big) = \frac{c}{\log z} + O\Big(\frac{1}{(\log z)^2} \Big),$$

and we also have $2^{\pi(z)} \leq 2^z$. So

$$\pi(x, z) = \frac{cx}{\log z} + O\Big(\frac{x}{(\log z)^2} + 2^z\Big).$$

The best we can do for π is

$$\pi(x) \leq O(\log x) + \frac{cx}{\log \log x} + O\Big(\frac{x}{(\log \log x)^2}\Big).$$

This is worse than Chebyshev, but it can be good for estimating $\pi(x, \log x)$. Maybe we can find another sieve that works well for other problems.

20.2 Selberg sieve for counting primes

Let $\lambda_1, \lambda_2, \dots$ be any sequence of real numbers. Then trivially

$$\delta(m) \leq \Big(\sum_{d|m} \lambda_d\Big)^2.$$

As we go along, we can impose conditions on (λ_j). For technical reasons, we want the following conditions.

(S1) $\lambda_1 = 1$.

(S2) $\lambda_d = 0$ for $d > z$ or d not square-free.

(S3) $|\lambda_d| \leq 1$ for all δ.

Under these conditions,

$$\pi(x, z) \leq \sum_{n \leq x} \Big(\sum_{d|(n, P_z)} \lambda_d\Big)^2 = \sum_{n \leq x} \sum_{d_1, d_2 | (n, P_z)} \lambda_{d_1}\lambda_{d_2} = \sum_{d_1, d_2 | P_z} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{n \leq x, \\ d_1, d_2 | n}} 1.$$

The point is that (S2) tells us that d_1, d_2 just ranges up to z and square-free. Then

$$\pi(x, z) \leq \sum_{d_1, d_2 \leq z}{}^{b} \lambda_{d_1}\lambda_{d_2}\Big(\frac{x}{[d_1, d_2]} + O(1)\Big) = x\Big(\sum_{d_1, d_2 \leq z}{}^{b} \frac{\lambda_{d_1}\lambda_{d_2}}{[d_1, d_2]}\Big) + O(z^2),$$

where Σ^b means that the we are summing over square-free numbers. Now the main problem is finding λ_d so that the quadratic form is minimized. We will call that quadratic form $Q(\lambda_d)$.

Let us first diagonalize Q. We have

$$\begin{aligned} Q &= \sum_{d_1, d_2 \leq z}{}^{2} \frac{\lambda_{d_1}\lambda_{d_2}}{d_1 d_2}(d_1, d_2) = \sum_{d_1, d_2 \leq z}{}^{b} \frac{\lambda_{d_1}\lambda_{d_2}}{d_1 d_2} \sum_{k|(d_1, d_2)} \phi(k) \\ &= \sum_{k \leq z}{}^{b} \phi(k) \sum_{\substack{d_1, d_2 \leq z \\ k | d_1, d_2}}{}^{b} \frac{\lambda_{d_1}}{d_2}\frac{\lambda_{d_2}}{d_2} = \sum_{k \leq z}{}^{b} \phi(k)\alpha_k^2, \end{aligned}$$

where $\alpha_k = \sum_{d\le z, k|d}{}^b \lambda_d/d$. This is the diagonalization and the inverse transform is given by $\lambda_d = d\sum_{d|k}\mu(k/d)\alpha_k$ for $d,k\le z$ square-free. Note that (S1) is equivalent to

$$1 = \sum_{k\le z}{}^b \mu(k)\alpha_k.$$

We want to minimize $\sum_{k\le z}{}^b \phi(k)\alpha_k^2$ under this condition.

Lagrange's multipliers tells us that for the optimal value ξ, we need

$$2\phi(k)\alpha_k = \mu(k)\xi.$$

Then $\alpha_k = \xi\mu(k)/(2\phi(k))$. To find ξ, we use (S1) to get $1 = \sum_{k\le z}{}^b \frac{1}{2\phi(k)}\xi$. This finally leads us to the choice

$$\alpha_k = \frac{1}{\sum_{l\le z}{}^b \frac{1}{\phi(l)}}\frac{\mu(k)}{\phi(k)}.$$

The conditions (S1) and (S2) are satisfied automatically. We now check (S3). We have, where we write $V = \sum_{k\le z}{}^b 1/\phi(k)$,

$$\begin{aligned}\lambda_d = d\sum_{d|k}\alpha_k &= \frac{d}{V}\sum_{d|k,k\le z}{}^b \frac{\mu(k/d)\mu(k)}{\phi(k)} = \frac{d\mu(d)}{V}\sum_{d|k,k\le z}{}^b \frac{1}{\phi(k)}\\ &= \frac{d\mu(d)}{\phi(d)V}\sum_{\substack{r\le z/d\\(d,r)=1}}{}^b \frac{1}{\phi(r)} = \frac{\mu(d)}{V}\sum_{l|d}\frac{1}{\phi(l)}\sum_{\substack{r\le z/d\\(d,r)=1}}{}^b \frac{1}{\phi(r)}.\end{aligned}$$

This shows that $|\lambda_d| \le 1$.

Using this choice, we can compute $Q(\text{our choice}) = 1/V$. Then we get:

Proposition 20.2. $\pi(x,z) \le \dfrac{x}{V(z)} + O(z^2)$, *where* $V(z) = \sum_{k\le z}{}^b 1/\phi(k)$.

Furthermore, choosing $z = x^{1/3}$ gives $\pi(x) \ll x/\log x$.

21 March 22, 2017

Last time we considered the problem of estimating

$$\pi(x,z) = \#\{n \leq z : \gcd(n, P_z) = 1\}, \quad P_z = \prod_{p \leq z} p.$$

This is a good upper bound on the prime counting function.

21.1 Selberg sieve

The basic principle for the Selberg sieve is

$$\delta(m) \leq \Big(\sum_{d|m} \lambda_d\Big)^2,$$

where $\lambda_d \in \mathbb{R}$ and $\lambda_1 = 1$. You can use more variables than just two. Maynard proved bounded gaps using a multidimensional Selberg sieve.

We consider a fixed sequence sequence of integers $a_1, a_2, \dots$ and count

$$N(x,z) = \#\{n \leq x : (a_n, P_z) = 1\}.$$

We will need to use the data of

$$N_d(x) = \#\{n \leq x : d \mid a_n\}.$$

Last time we used $a_n = n$ and $N_d(x) = x/d + O(1)$. We are also going to assume that there are arithmetic functions $f(n)$, $R(n)$, and a set of primes S, such that

(1) f and R are $\mathbb{R}_{>0}$-valued,

(2) f is multiplicative,

(3) $f(p) > 1$ for any $p \notin S$,

(4) for $\gcd(d, S) = 1$, $|N_d(x) - x/f(d)| \leq R(d)$,

(5) for $\gcd(d, S) \neq 1$, $N_d(x) \leq R(d)$.

We are going to define $g = f * \mu$,

$$f(n) = \sum_{d|n} g(d).$$

For $p \notin S$, we have $g(p) = f(p) - f(1) = f(p) - 1 > 0$. Because g is also multiplicative, $g(n) > 0$ for $\gcd(n, S) = 1$ with n square-free. Using the notation $\sum_n^S = \sum_{(n,S)=1}$, we also define

$$U(z) = \sum_{n \leq z}^{S}{}^{b} \frac{1}{g(n)} \geq 1.$$

This is extremely hard to compute. It is useful to have the following estimate.

Lemma 21.1. *Let h be the completely multiplicative function defined by $h(p) = f(p)$. Then*

$$U(z) \geq \sum_{n\leq z}^{S} \frac{1}{h(n)}.$$

Proof. For n square-free with $(n, S) = 1$,

$$\frac{h(n)}{g(n)} = \frac{f(n)}{g(n)} = \prod_{p|n} \frac{f(p)}{f(p)-1} = \prod_{p|n}\Big(1 + \frac{1}{f(p)} + \frac{1}{f(p)^2} + \cdots\Big) = \sum_{p|k\Rightarrow p|n} \frac{1}{h(k)}.$$

Then

$$U(z) = \sum_{n\leq z}^{s}{}^{b} \frac{1}{g(n)} \geq \sum_{m\leq z}^{S} \frac{1}{h(m)}. \qquad \square$$

Theorem 21.2. *With the previous notation and conditions relative to the sequence $a_1, a_2, \ldots$, we have*

$$N(x, z) \leq \frac{x}{U(z)} + \sum_{d_1,d_2\leq z}{}^{b} R([d_1, d_2]) \leq \frac{x}{\sum_{n\leq z}^{S} \frac{1}{h(n)}} + \sum_{d_1,d_2\leq z} R([d_1, d_2]).$$

Proof. We are going to pick $\lambda_1, \lambda_2, \ldots \in \mathbb{R}$ satisfying

(1) $\lambda_1 = 1$,

(2) $\lambda_d = 0$ if $d > z$ or d is not square-free or $(d, S) \neq 1$,

(3) $|\lambda_d| \leq 1$.

Then we have

$$\begin{aligned}
N(x, z) &\leq \sum_{n\leq x}\Big(\sum_{d|(a_n,P_z)} \lambda_d\Big)^2 = \sum_{d_1,d_2\leq z}{}^{b} \lambda_{d_1}\lambda_{d_2}\Big(\sum_{\substack{d_1,d_2|a_n\\ n\leq x}} 1\Big) \\
&= \sum_{d_1,d_2\leq z}{}^{b} \lambda_{d_1}\lambda_{d_2} N_{[d_1,d_2]}(x) \\
&\leq \sum_{d_1,d_2\leq z}^{S}{}^{b} \lambda_{d_1}\lambda_{d_2} \frac{x}{f([d_1,d_2])} + \sum_{d_1,d_2\leq z}{}^{b} R([d_1, d_2]) \\
&= x \sum_{d_1,d_2\leq z}^{S}{}^{b} \frac{\lambda_1\lambda_2}{f([d_1,d_2])} + \sum_{d_1,d_2\leq z}{}^{b} R([d_1, d_2]).
\end{aligned}$$

We now have to analyze the quadratic function. We have

$$\begin{aligned}
Q &= \sum_{d_1,d_2\leq z}^{S}{}^{b} \frac{\lambda_{d_1}\lambda_{d_2}}{f(d_1)f(d_2)} f((d_1, d_2)) \\
&= \sum_{d_1,d_2\leq z}^{S}{}^{b} \frac{\lambda_{d_1}\lambda_{d_2}}{f(d_1)f(d_2)} \sum_{k|(d_1,d_2)} g(k) = \sum_{k\leq z}^{S}{}^{b} g(k)\alpha_k^2,
\end{aligned}$$

where

$$\alpha_k = \sideset{}{^{b}}\sum_{k|d\leq z}^{S} \frac{\lambda_d}{f(d)}, \quad \lambda_d = f(d) \sideset{}{^{b}}\sum_{d|k\leq z}^{S} \mu(k/d)\alpha_k.$$

Both α and λ are 0 unless the indices are at most z, square-free, and coprime to S.

We are going to choose

$$\alpha_k = \frac{1}{U(z)} \frac{\mu(k)}{g(k)}$$

in the support. You can check that $|\lambda_d| \leq 1$ is satisfied for this choice. This gives

$$Q(z) = \sideset{}{^{b}}\sum_{k\leq z}^{S} g(k) \frac{1}{U(z)^2} \frac{1}{g(k)^2} = \frac{1}{U(z)^2} \sideset{}{^{b}}\sum_{k\leq z}^{S} \frac{1}{g(k)} = \frac{1}{U(z)}.$$

This finishes the proof. □

Here is an interesting case you can apply this theorem. Consider $a_n = n(n+2)$. Let

$$\pi_2(x) = \#\{p \leq x : p+2 \text{ is prime}\}.$$

This is an upper bound sieve, so we can't prove that there are infinitely many prime. You have $\pi_2(z) \leq z + N(x,z)$ for any z.

22 March 24, 2017

Today I want to discuss the application of counting twin primes.

22.1 Application: Counting twin primes

We count the know the size of

$$\pi_2(x) = \#\{p \subseteq x : p+2 \text{ is prime }\}.$$

Heuristically, for $n \le x$ the probability that n is prime is around $1/\log x$, and similarly for $n+2$. If the two events are "nearly independent", then we can expect

$$\pi_2(x) \asymp \frac{x}{(\log x)^2}.$$

The lower bound seems out of reach, but we can prove the upper bound.

Theorem 22.1 (Selberg, after Brun)**.** $\pi_2(x) \ll \dfrac{x}{(\log x)^2}$.

Brun got with an additional $(\log\log x)^2$ factor, but this is enough to show that the reciprocal converges.

Proof. We are going to apply Selberg's sieve to the sequence $a_n = n(n+2)$. For this choice,

$$\pi_2(x) \le N(x,z) + \pi_2(z) \le z + N(x,z).$$

We need estimates on $N_d(x)$. Let me introduce

$$\rho(d) = \#\{r \bmod d : r(r+2) \equiv 0 \pmod{d}\}.$$

Then we have

$$\Big| N_d(x) - \frac{\rho(d)}{d} x \Big| \le \rho(d).$$

Also $\rho(d)$ is multiplicative. So we can choose $S = \emptyset$, $f(d) = d/\rho(d)$, and $R(n) = \rho(n)$.

We can now apply Selberg's sieve. We get

$$N(x,z) \le \frac{x}{U(z)} + \sum_{d_1,d_2 \le z}^{b} R([d_1,d_2]), \qquad \text{where } U(z) = \sum_{k \le z}^{b} \frac{1}{g(z)} \ge \sum_{n \le z} \frac{1}{h(n)}.$$

For n square-free, we claim that $\rho(n) \ll_\epsilon n^\epsilon$. This is because

$$\rho(n) = \prod_{p \mid n} \rho(p) \le d(n).$$

Therefore

$$\sum_{d_1,d_2 \le z}^{b} R([d_1,d_2]) \ll_\epsilon z^{2+\epsilon}.$$

For $U(z)$, we get

$$\frac{1}{h(n)} = \frac{2^{\Omega(n)-\nu_2(n)}}{n},$$

where $\Omega(n)$ is the number of prime factors of n counting repetitions. Then

$$\begin{aligned} U(z) &\geq \sum_{n\leq z} \frac{1}{h(n)} = \sum_{2\nmid n\leq z} \frac{2^{\Omega(n)}}{n} \geq \sum_{2\nmid n\leq z} \frac{d(n)}{n} \\ &= \Big(\sum_{2\nmid n\leq z} d(n)\Big)\frac{1}{z} + \int_1^z \Big(\sum_{2\nmid n\leq t} d(n)\Big)\frac{dt}{t^2} \gg \int_1^z \frac{\log t}{t} dt \gg (\log z)^2. \end{aligned}$$

Therefore

$$N(x,z) \ll_\epsilon \frac{x}{(\log z)^2} + z^{2+\epsilon}.$$

Take $\epsilon = 1$ and $z = x^{1/4}$. □

Corollary 22.2 (Brun's theorem, 1919)**.** *The (possibly finite) series*

$$\Big(\frac{1}{3}+\frac{1}{5}\Big)+\Big(\frac{1}{5}+\frac{1}{7}\Big)+\Big(\frac{1}{11}+\frac{1}{13}\Big)+\cdots$$

is convergent.

23 March 27, 2017

There will be no lecture this Wednesday.

The purpose of the large sieve is to give an upper bound on the size of a set with restrictions on the reduction modulo p. For a set $A \subseteq [1, x]$, we get a estimate on $\#A$ given $\#A \bmod p$. It is useful when we remove very few residue classes.

Problem. *How large is the least n such that $n \bmod p$ is not a quadratic residue?*

A trivial bound is $p/2$, because there are $p/2$ quadratic residues. A non-trivial bound is $\sqrt{p}\log p$, because the quadratic character is a character and consecutive sums of a character cannot exceed this. (Pólya–Vinogradov inequality).

Conjecture 23.1. *The least non-quadratic number is $\ll_\epsilon p^\epsilon$.*

23.1 Analytic large sieve inequality

Proposition 23.2. *Let $f : \mathbb{R} \to \mathbb{C}$ be C^1 and 1-periodic. Then for any $z \geq 1$,*

$$\sum_{d \leq z} \sum_{\substack{1 \leq a \leq d \\ (a,d)=1}} \Big| f\Big(\frac{a}{d}\Big) \Big| \leq z^2 \int_0^1 |f(t)| dt + \int_0^1 |f'(t)| dt.$$

Proof. Given any such a/d and $t > a/d$,

$$f(t) - f\Big(\frac{a}{d}\Big) = \int_{a/d}^{x} f'(t) dx.$$

Then

$$\Big| f\Big(\frac{a}{d}\Big) \Big| \leq |f(t)| + \int_{a/d}^{t} |f'(x)| dx.$$

Let $\delta = z^{-2}$ and $I(a/d) = [a/d, a/d + \delta)$. These intervals are disjoint for a/d, and so integrating over t gives

$$\begin{aligned} \delta \Big| f\Big(\frac{a}{d}\Big) \Big| &\leq \int_{I(a/d)} |f(t)| dt + \int_{I(a/d)} \int_{a/d}^{t} |f'(x)| dx \\ &\leq \int_{I(a/d)} |f(t)| dt + \delta \int_{I(a/d)} |f'(x)| dx. \end{aligned}$$

Adding over d/a gives the desired inequality. □

Theorem 23.3 (Analytic large sieve inequality)**.** *Let $a_1, a_2, \dots$ be a sequence in $\mathbb{C}$. For $x \geq 1$ define*

$$S_x(t) = \sum_{n \leq x} a_n e(nt), \quad e(\alpha) = e^{2\pi i \alpha}.$$

Then for $z \geq 1$,

$$\sum_{d \leq z} \sum_{\substack{1 \leq a \leq d \\ (a,d)=1}} \left| S_x\left(\frac{a}{d}\right) \right|^2 \leq (z^2 + 4\pi x) \sum_{n \leq x} |a_n|^2.$$

Proof. We use the previous proposition with $S_x(t)^2$. The left hand side is perfect. Then

$$(\text{LHS}) \leq z^2 \int_0^1 |S_x(t)|^2 dt + 2 \int_0^1 |S_x'(t) S_x(t)| dt.$$

The first term is just $z^2 \sum_{n \leq x} |a_n|^2$. For the second term, applying Cauchy gives us

$$\int_0^1 |S_x'(t) S_x(t)| dt \leq \left(\int_0^1 |S_\alpha(t)|^2 dt \right)^{1/2} \left(\int_0^1 |S_\alpha'(t)|^2 dt \right)^{1/2} \leq 4\pi^2 x^2 \sum_{n \leq x} |a_n|^2.$$

□

This has a huge number of applications. For instance, you can show that the average error term for the number of primes in arithmetic progressions is very small.

23.2 Ramanujan sums

Definition 23.4. For d a positive integer and $n \in \mathbb{Z}$, the **Ramanujan sum** is given by

$$c_d(n) = \sum_{\substack{1 \leq a \leq d \\ (a,d)=1}} e\left(\frac{na}{d}\right).$$

Lemma 23.5. *$c_d(n)$ is d-periodic on n.*

Lemma 23.6. *For n fixed, $c_d(n)$ is multiplicative on d.*

Lemma 23.7. $c_d(n) = \displaystyle\sum_{r \mid (n,d)} \mu(d/r) r.$

Proof. We have

$$\begin{aligned} c_d(n) &= \sum_{1 \leq a \leq d} e\left(\frac{na}{d}\right) \sum_{k \mid (a,d)} \mu(k) = \sum_{k \mid d} \mu(k) \sum_{1 \leq b \leq d/k} e\left(\frac{nkb}{d}\right) \\ &= \sum_{k \mid d} \mu(k) \sum_{1 \leq b \leq d/k} e\left(\frac{nb}{d/k}\right) = \sum_{r \mid d} \mu(d/r) \sum_{r \mid n} r. \end{aligned}$$

□

Corollary 23.8. *For $d \geq 1$ an integer,*

(1) $c_d(n) \in \mathbb{Z}$.

(2) if $(d,n) = 1$ *then* $c_d(n) = \mu(d)$.

These Ramanujan sums can be thought of as some kind of a base for Fourier series. It is periodic on n and it is multiplicative on d. Here are some examples of Ramanujan–Fourier series.

$$\sigma_1(n) = \frac{\pi^2}{6} n \sum_{d=1}^{\infty} \frac{1}{d^2} c_d(n).$$

Define $\phi_2(n) = n^2 \prod_{p|n}(1 - p^{-2})$. Then

$$\phi(n) = \frac{\pi^2}{6} n \sum_{d=1}^{\infty} \frac{\mu(d)}{\phi_2(d)} c_d(n).$$

The formula

$$0 = \sum_{d=1}^{\infty} \frac{1}{d} c_d(n)$$

is equivalent to the prime number theorem. Also Hardy proved

$$\Lambda(n) = \frac{n}{\phi(n)} \sum_{d=1}^{\infty} \frac{\mu(d)}{\phi(d)} c_d(n).$$

24 March 31, 2017

Last time we discussed the analytic version of the large sieve.

24.1 Arithmetic large sieve

For each prime p, let $\Omega_p \subseteq \mathbb{Z}/p\mathbb{Z}$ be a set of "forbidden" residue classes. Let us write $\omega(p) = \#\Omega_p$. For $x, z \geq 1$, define

$$S(x,z) = \#\{n \leq x : \text{for every } p \leq z, n \pmod{p} \notin \Omega_p\}.$$

You can even set $\Omega_p = \emptyset$ if you want. But you wouldn't want to set $\Omega_p = \mathbb{Z}/p\mathbb{Z}$. The question is how large $S(x,z)$ is.

Theorem 24.1. *Write*

$$L(z) = \sum_{d \leq z}^{b} \prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)}.$$

Then

$$S(x,z) \leq \frac{z^2 + 4\pi x}{L(z)}.$$

Proof. Extend ω multiplicatively. By the Chinese remainder theorem, we get a forbidden set $\Omega_d \subseteq \mathbb{Z}/d\mathbb{Z}$ for each square-free d, such that $\Omega_d/p = \Omega_p$ for all $p \mid d$ and $\#\Omega_d = \omega(d)$.

Let $n \leq x$ such that for every $p \leq z$, $n \pmod{p} \notin \Omega_p$. (We call this condition "$*$".) For $d \leq z$ square-free,

$$\mu(d) = c_d(n-u) = \sum_{\substack{1 \leq a \leq d \\ (a,d)=1}} e\Big(\frac{a(n-u)}{d}\Big),$$

provided that $(u,d) = 1$. This is satisfied if $u \in \Omega_d \subseteq \{1, \dots, d\}$.

Add this over n under $(*)$ and $u \in \Omega_d$:

$$\mu(d) S(x,z) \omega(d) = \sum_{\substack{1 \leq a \leq d \\ (a,d)=1}} \sum_{u \in \Omega_d} e\Big(\frac{-au}{d}\Big) \sum_{n \leq x}^{(*)} e\Big(\frac{au}{d}\Big).$$

By Cauchy–Schwarz,

$$S(x,z)^2 \omega(d)^2 \leq \Bigg(\sum_{\substack{1 \leq a \leq d \\ (a,d)=1}} \Big| \sum_{u \in \Omega_d} e\Big(\frac{-au}{d}\Big) \Big|^2 \Bigg) \Bigg(\sum_{\substack{1 \leq a \leq d \\ (a,d)=1}} \Big| \sum_{n \leq x}^{(*)} e\Big(\frac{an}{d}\Big) \Big|^2 \Bigg) = T \cdot S.$$

We can simplify the sums as

$$\begin{aligned}T &= \sum_{\substack{1\le a\le d\\(a,d)=1}}\sum_{u,v\in\Omega_d} e\Big(\frac{a(u-v)}{d}\Big) = \sum_{u,v\in\Omega_d}\sum_{\substack{1\le a\le d\\(a,d)=1}} e\Big(\frac{a(u-v)}{d}\Big)\\ &= \sum_{u,v\in\Omega_d} c_d(u-v) = \sum_{u,v\in\Omega_d}\sum_{k\mid(d,u-v)}\mu(d/k)k = \sum_{k\mid d}k\mu(d/k)\sum_{u\in\Omega_d}\sum_{\substack{v\in\Omega_d\\k\mid u-v}}1\\ &= \sum_{k\mid d}k\mu(d/k)\omega(d)\omega(d/k) = d\omega(d)\sum_{r\mid d}\frac{\mu(r)\omega(r)}{r} = d\omega(d)\prod_{p\mid d}\Big(1-\frac{\omega(p)}{p}\Big).\end{aligned}$$

Therefore adding over $d \le z$ square-free, we end up with

$$S(x,z)^2L(z) = S(x,z)^2\sum_{d\le z}^{b}\prod_{p\mid d}\frac{p-\omega(p)}{\omega(p)} \le \sum_{d\le z}^{b}\sum_{\substack{1\le a\le d\\(a,d)=1}}\Big|\sum_{n\le x}^{(*)}e\Big(\frac{an}{d}\Big)\Big|^2.$$

The right hand side looks like we can apply the analytic large sieve inequality with

$$a_n = \begin{cases}1 & \text{if } (*) \text{ holds,}\\ 0 & \text{otherwise.}\end{cases}$$

The inequality gives us

$$S(x,z)^2L(z) \le (z^2+4\pi x)\sum_{n\le x}|a_n|^2 = (z^2+4\pi x)S(x,z).$$

This finishes the proof. □

Example 24.2. Here is a useless example. Let us count $n \le x$, with $\Omega_p = \emptyset$ and $L(z) = 1$. Then

$$S(x,z) \le \frac{z^2+4\pi x}{1}.$$

Taking $z = 0$ gives $S(x,z) \le 4\pi x$. Actually you can replace $4\pi x$ in all the large sieves, but this takes more work.

Theorem 24.3 (Linnik). *Let $\epsilon > 0$. As $x \to \infty$,*

$$\#\{p \le x : n_p > n^\epsilon\} \ll_\epsilon 1,$$

where $n_p \ge 1$ is the least quadratic non-residue mod p.

Proof. Define

$$\Omega_p = \begin{cases}\emptyset & \text{if there exists } n \le x^\epsilon \text{ such that } (\frac{n}{p}) = -1,\\ \{r \bmod p : (\frac{r}{p}) = -1\} & \text{otherwise.}\end{cases}$$

Then $\omega(p) = 0$ or $(p-1)/2$ depending on the condition. Take $z = \sqrt{x}$. Then we get

$$S(x,z) \le \frac{14x}{L(\sqrt{x})},$$

and

$$L(\sqrt{x}) = \sum_{d \le z}^{b} \prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)} \ge \frac{1}{2} \sum_{\substack{p \le z \text{ exceptional} \\ \omega(p) \ne 0}} \Big(1 - \frac{1}{p}\Big) > \frac{1}{4} \sum_{\substack{p \le z \text{ exc.} \\ \omega(p) \ne 0}} 1.$$

Now let us give a lower bound on $S(x,z)$. We claim that if $n \le x$ is x^ϵ-smooth, then n is counted in $S(x,z)$. Also, you can prove in an elementary way that

$$\#\{n \le x : n \text{ is } x^\epsilon\text{-smooth}\} \gg_\epsilon x.$$

This shows that $L(\sqrt{x}) \ll_\epsilon 1$. □

Conjecture 24.4 (Strong conjecture)**.** $n_p \ll (\log p)^2$.

25 April 3, 2017

We are going to start a new topic. We can discuss sieve for a whole semester, but this is an introductory course.

25.1 Additive problems

Let $\mathbb{N} = \{0, 1, \ldots\}$ and $\mathscr{A} \subseteq \mathbb{N}$. Define $\mathscr{A}[n] = \mathscr{A} \cap [1, n]$. We are setting $\mathscr{A}[0] = \emptyset$ even if $0 \in \mathscr{A}$.

Suppose we are given sets $\mathscr{A}_1, \ldots, \mathscr{A}_k \subseteq \mathbb{N}$. The question is, can every $n \in \mathbb{N}$ be written as $n = a_1 + \cdots + a_k$ with $a_i \in \mathscr{A}_i$? This is sometimes too strong, so maybe we ask this for $n \gg 1$. Or maybe we can give some congruence conditions.

Example 25.1. Here are some examples.

(1) Lagrange's theorem: Every $n \geq 0$ is the some of 4 squares.

(2) Waring's problem: Let $k \geq 2$. Is every $n \geq 1$ the sum of at most $G(k)$ k-th powers for a uniform $G(k)$?

(2′) Get the best $G(k)$, up to finitely many n; we call the bound $g(k)$.

(3) Goldbach conjecture: Is every even integer $\gg 1$ the sum of two prime?

(4) Ternary Goldbach: Is every odd integer $\gg 1$ the sum of three primes?

(2) was solved by Hilbert in 1909. Hardy and Littlewood worked on $g(k)$. (3) is open so far. Yitang Zhang's method gives something on linear relations between primes, but it is not strong enough. (4) was solved by Vinogradov. What Helfgott proved in 2012 is that (4) is true for every odd integer ≥ 7.

In the remaining part of this course, we will study these problems. We will consider two methods:

(1) Schnirelmann's density method (with a sieve)

(2) The circle method (invented by Ramanujan; advertised by Hardy and Littlewood; refined by Vinogradov)

We are not going to see this in a very abstract setting, because it is not really helpful. The motivating problems will be:

(1) Every $n \gg 1$ is the sum of a bounded number of primes.

(2) Waring's problem.

25.2 Schnirelmann's density

Here is the heuristic. If $\mathscr{A}, \mathscr{B} \subseteq \mathbb{N}$ has "positive density", then we expect that $\mathscr{A} + \mathscr{B}$ has larger density. But this fails in general. If $\mathscr{A} = \mathscr{B} = 2\mathbb{N}$ this does not seem to work. But maybe the even numbers is not 1/2.

Definition 25.2. Let $\mathscr{A} \subseteq \mathbb{N} = \{0, 1, \ldots\}$. We define the **Schnirelmann density** of $\mathscr{A}$ as

$$\delta(\mathscr{A}) = \inf_{n \geq 1} \frac{\#\mathscr{A}[n]}{n}.$$

Under this definition $\delta(\mathbb{N}) = 1$ and $\delta(2\mathbb{N}) = 0$. We also have $\delta(2\mathbb{N}+1) = 1/2$. We have $\delta(\text{primes}) = 0$ and $\delta(k\text{-th powers}) = 0$ if $k \geq 2$.

Lemma 25.3. *Let $\mathscr{A}, \mathscr{B} \subseteq \mathbb{N}$ and assume that $0 \in \mathscr{A}, \mathscr{B}$. Let $n \geq 1$. If*

$$\#\mathscr{A}[n] + \#\mathscr{B}[n] \geq n$$

then $n \in \mathscr{A} + \mathscr{B}$.

Proof. If $n \in \mathscr{A} + \mathscr{B}$, write $n = n + 0$. If not, then $\mathscr{A}[n] = \mathscr{A}[n-1]$ and $\mathscr{B}[n] = \mathscr{B}[n-1]$. So $\mathscr{A}[n]$ and $n - \mathscr{B}[n]$ are both contained in $[1, n-1]$, and thus have an intersection. □

Corollary 25.4. *Let $\mathscr{A} \subseteq \mathbb{N}$ with $0 \in \mathscr{A}$ and $\delta(\mathscr{A}) \geq 1/2$. Then $\mathscr{A} + \mathscr{A} = \mathbb{N}$.*

Proof. For $n \geq 1$,

$$\#\mathscr{A}[n] + \#\mathscr{A}[n] \geq \delta(A)n + \delta(A)n \geq n.$$ □

Here are some useful remarks we will use without thinking.

(1) $1 \notin \mathscr{A}$ implies $\delta(A) = 0$.

(2) For all $n \geq 1$, $\#\mathscr{A}[n] \geq \delta(A)n$.

(3) If $\#\mathscr{A}[n] \geq cn$ for all $n \geq 1$ then $\delta(A) \geq c$.

(4) $\delta(\mathscr{A})$ always exists and is in $[0, 1]$.

Lemma 25.5. *Let $\mathscr{A}, \mathscr{B} \subseteq \mathbb{N}$ with $0 \in \mathscr{A}, \mathscr{B}$. Then*

$$\delta(\mathscr{A} + \mathscr{B}) \geq \delta(\mathscr{A}) + \delta(\mathscr{B}) - \delta(\mathscr{A})\delta(\mathscr{B}).$$

Proof. Let $n \geq 1$ and $r = \#\mathscr{A}[n]$. We can assume $\delta(\mathscr{A}), \delta(\mathscr{B}) > 0$, and so $1 \in \mathscr{A}, \mathscr{B}$. Let us write

$$\mathscr{A}[n] = \{1 = a_1 < a_2 < \ldots < a_r\}.$$

Let $g_j = a_{j+1} - a_j - 1$ for $j = 1, 2, \ldots, r-1$. We know $\mathscr{A} \subseteq \mathscr{A} + \mathscr{B}$. We now want to focus on what else is there.

We get at least $\#\mathscr{B}[g_j]$ elements between a_j and a_{j+1}, and $\mathscr{B}[n - a_r]$ at the end of $[1, n]$. Now we count

$$\begin{aligned} \#(\mathscr{A} + \mathscr{B})[n] &\geq r + \sum_{j=1}^{r-1} \#\mathscr{B}[g_j] + \#\mathscr{B}[n - a_r] \\ &\geq r + \sum_{j=1}^{r-1} \delta(\mathscr{B}) g_j + \delta(\mathscr{B})(n - a_r) \\ &= n(\delta(\mathscr{A}) + \delta(\mathscr{B}) - \delta(\mathscr{A})\delta(\mathscr{B})). \end{aligned}$$

This finishes the proof. □

26 April 5, 2017

Last time we defined Schnirelmann's density as

$$\delta(\mathscr{A}) = \inf_{n\geq 1} \frac{\#\mathscr{A}[n]}{n}, \quad \mathscr{A}[n] = \mathscr{A} \cap [1,n].$$

Let us denote $h \cdot \mathscr{A} = \mathscr{A} + \cdots + \mathscr{A}$ where there are h sums.

Corollary 26.1. *If $\delta(\mathscr{A}) \geq 1/2$ and $0 \in \mathscr{A}$ then $2 \cdot \mathscr{A} = \mathbb{N}$.*

Lemma 26.2. *Let $\mathscr{A}, \mathscr{B} \subseteq \mathbb{N}$ with $0 \in \mathscr{A} \cap \mathscr{B}$. Then*

$$\delta(\mathscr{A} + \mathscr{B}) \geq \delta(\mathscr{A}) + \delta(\mathscr{B}) - \delta(\mathscr{A})\delta(\mathscr{B}).$$

Corollary 26.3. *Let $\mathscr{A}_1, \dots, \mathscr{A}_n \subseteq \mathbb{N}$ with $0 \in \mathscr{A}_i$ for all i. Then*

$$\delta(\mathscr{A}_1 + \cdots + \mathscr{A}_n) \geq 1 - \prod_{i=1}^{n} (1 - \delta(\mathscr{A}_j)).$$

Proof. This follows from the lemma by induction. □

Definition 26.4. A set $\mathscr{A} \subseteq \mathbb{N}$ is a **basis of finite order** if there exists an h such that $h \cdot \mathscr{A} = \mathbb{N}$.

Theorem 26.5. *Let $\mathscr{A} \subseteq \mathbb{N}$. Suppose $0 \in \mathscr{A}$. If $\delta(\mathscr{A}) > 0$. Then $\mathscr{A}$ is a basis of finite order.*

Proof. Use Corollary 26.1 and Corollary 26.3. □

26.1 Using Schnirelmann's density

In the case we are interested in, like Waring's problem or the Goldbach problem, the set has density zero.

Given a set $\mathscr{A} \subseteq \mathbb{N}$, we would first need to define $\mathscr{A}^* = \mathscr{A} \cup \{0, 1\}$ and work with $\mathscr{A}^*$ instead. Adding 0 in is not much of a problem, because we are looking at at most h sums, rather than exactly h sums. Adding 1 in is something we need to take are later on.

Lemma 26.6. *Let $\mathscr{A} \subseteq \mathbb{N}$. We have $\delta(\mathscr{A}) > 0$ if and only if*

(i) $1 \in \mathscr{A}$,

(ii) $\liminf \#\mathscr{A}[n]/n > 0$, *i.e, there exists a $c > 0$ such that $\#\mathscr{A}[x] \geq cx$ for $x \gg 1$.*

In most cases, $\mathscr{A}$ is too thin to have positive natural density. But maybe the set $2 \cdot \mathscr{A}$ is not too thin. Here is a way to check this.

Lemma 26.7 (2nd moment trick)**.** *Let $\mathscr{A} \subseteq \mathbb{N}$. Define*

$$r_{\mathscr{A}}(n) = \{(a,b) \in \mathscr{A}^2 : a + b = n\}.$$

For $x \geq 1$,

$$\left(\sum_{1 \leq x \leq n} r_{\mathscr{A}}(n) \right)^2 \leq (\#(2 \cdot \mathscr{A})[x]) \sum_{1 \leq n \leq x} r_{\mathscr{A}}(n)^2.$$

26.2 Sums of primes (weak Goldbach)

Let $\mathscr{P}$ be the set of primes. Here are some issues: $0 \notin \mathscr{P}$, $1 \notin \mathscr{P}$, and $\#\mathscr{P}[x] = o(x)$. The plan is to work with $\mathscr{P}^*$ instead. Then inflate $\mathscr{P}$ to $2 \cdot \mathscr{P}$.

Let us write $\gamma(n) = r_{\mathscr{P}}(n)$.

Lemma 26.8. *For $x \gg 1$,*

$$\sum_{n \le x} \gamma(n) \gg \frac{x^2}{(\log x)^2}.$$

Proof. Just look at the primes $p, q \le x/2$ so that $p + q \le x$. Then apply Chebyshev. □

In the assignment, using sieves, you showed

Lemma 26.9. $\gamma(n) \ll \dfrac{n}{(\log n)^2} \displaystyle\prod_{p|n}\Big(1 + \frac{1}{p}\Big).$

Lemma 26.10. $\displaystyle\sum_{n \le x} \gamma(x)^2 \ll \frac{x^3}{(\log x)^4}.$

Proof. By the previous lemma,

$$\sum_{n \le x} \gamma(n)^2 \ll \frac{x^2}{(\log x)^4} \sum_{n \le x} \bigg(\prod_{p|n}\Big(1 + \frac{1}{p}\Big)\bigg)^2.$$

We have

$$\sum_{n \le x} \bigg(\prod_{p|n}\Big(1 + \frac{1}{p}\Big)\bigg)^2 = \sum_{n \le x}\bigg(\sum_{d|n}\frac{1}{d}\bigg)^2 = \sum_{n \le x}\sum_{d_1,d_2|n}\frac{1}{d_1 d_2}$$
$$= \sum_{d_1,d_2 \le x}\frac{1}{d_1 d_2}\Big\lfloor\frac{x}{[d_1,d_2]}\Big\rfloor \le x \sum_{d_1,d_2 \le x}\frac{1}{d_1 d_2\sqrt{d_1 d_2}} \le x \cdot \zeta(3/2)^2.$$

This proves the proof. □

Theorem 26.11. *For $x \gg 1$, $\#(2 \cdot \mathscr{P})[x] \gg x$.*

Proof. This follows from the second moment lemma. □

Theorem 26.12. *There exists an h such that every integer $n \ge 2$ is the sum of at most h primes.*

Proof. The previous theorem and Schnirelmann's theory show that there exists a k such that $k \cdot \mathscr{P}^* = \mathbb{N}$. We need to get rid of 1.

So given n we can write

$$n = p_1 + \cdots + p_r + 1 + \cdots + 1 = p_1 + \cdots + p_r + \ell,$$

where $r + \ell \leq k$.

If $\ell = 0$, then we are good. If $\ell > 1$, then we are also good, because then ℓ can be written as a sum of 2 and 3.

What if $\ell = 1$? Look at $n - 2$. Then $n - 2$ is good and so $n = (n-2) + 2$ or $n - 2$ uses one 1 and so $n = (n-3) + 3$. □

27 April 7, 2017

We are going to start on the last section of this course, which is the circle method.

27.1 Introduction to the circle method

Let $\mathscr{A} \subseteq \mathbb{N}$, and consider $s \geq 1$ an integer. We can consider the function

$$f(z) = f_{\mathscr{A}}(z) = \sum_{n \in \mathscr{A}} z^n.$$

We can work with the formal power series, but we see that this is analytic on $D^0 = \{z \in \mathbb{C} : |z| < 1\}$.

Define

$$r_s(n) = r_{s,\mathscr{A}}(n) = \#\Big\{\underline{a} \in \mathscr{A}^s : \sum_{i=1}^{s} a_i = n\Big\}.$$

The key observation is that

$$f(z)^s = \sum_{n \geq 0} r_s(n) z^n.$$

The whole point of the circle method is to recover $r_s(n)$ from $f(z)^s$ by analytic means. For $\gamma \in D^0$ a contour around 0, we have

$$r_s(N) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)^s}{z^{N+1}} dz.$$

Now we have an analytic thing on the right had side and we hope this can be approximated. The idea of Ramanujan was

(1) approximate near “heave” singularities on S^1,

(2) bound the integral away from those singularities,

(3) choose γ in such a that (1) and (2) work.

The main complication is choosing γ. We want to avoid singularities but stay close to the circle on other parts. In fact, Rademacher used a very complicated fractal contour to give an exact formula for the partition function. Choosing the contour really depends on how skillful you are.

This was the Hardy–Littlewood version of Ramanujan’s circle method. Vinogradov make technical modifications and proved the following theorem.

Theorem 27.1. *Every $N \gg 1$, odd, can be written as sum of 3 primes (and an asymptotic formula for $r_{3,\mathcal{P}}(N)$ can be found).*

What is this technical modification? Let N be fixed. The key observation is that to compute (or approximate) $r_s(N)$, we don't need the whole series $f(z) = \sum_{n\in\mathscr{A}} z^n$. Instead, we only need $f_N(z) = \sum_{n\in\mathscr{A}, n\le N} z^n$. This is a polynomial and hence entire. So again,

$$r_s(N) = \frac{1}{2\pi i}\int_\gamma \frac{f_N(z)^s}{z^{N+1}}dz. \tag{1}$$

Now $\gamma = S^1$ is allowed, and we can let $z = e(\alpha)$. Then

$$r_s(N) = \int_0^1 \tilde{f}_N(\alpha)^s e(-N\alpha)d\alpha, \quad \text{where } \tilde{F}_N(\alpha) = \sum_{n\in\mathscr{A}, n\le N} e(n\alpha). \tag{2}$$

Now the question is how to estimate the right hand side of (2). For α near a rational number of small denominator we cannot expect cancellation in $\tilde{F}_N(\alpha)$. In this case, we are going to evaluate (estimate with main term) and otherwise we are going to bound.

Here is a standard process. Fix some N. (Still, all implicit constants in the arguments should be uniform on N.) We are going to choose two parameters $Q = Q(N)$ a positive integer and $\delta = \delta(N) > 0$ a small real number.

Definition 27.2. For $1 \le q \le Q$ and $0 \le a \le q$ with $(a, q) = 1$, define

$$\mathfrak{M}(a,q) = \left\{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \le \delta\right\}.$$

Then define the **major arcs** as the union

$$\mathfrak{M} = \bigcup_{1\le q\le Q} \bigcup_{\substack{0\le a\le q\\(a,q)=1}} \mathfrak{M}(a,q).$$

The **minor arcs** is $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$.

Often, (in practice, always) we choose δ so small that the major arcs are disjoint, and it is also very common that $\mu(\mathfrak{M}) \to 0$ as $N \to \infty$.

The first step is to bound $\int_\mathfrak{m}$ using bounds for exponential sums. Recall that

$$\tilde{f}_N(\alpha) = \sum_{n\in\mathscr{A}, n\le N} e(n\alpha).$$

We need to estimate the s-th moment of this function. You might have better cancellation when looking at the s-th moment, and this is the motivation for using stuff like Weyl's inequality, Hua's inequality, or Vinogradov's inequality.

Then there is the question of how to evaluate the sum on the major arcs. Near $\alpha = a/q$, write the integrand as

$$(\text{arithmetic sum}) \cdot (\text{analytic sum}) + (\text{error}),$$

integrate, add over a, q and get

$$\mathfrak{S}(N) \cdot (\text{“analytic” function})(N) + (\text{error}).$$

Here $\mathfrak{S}(N)$ is called the singular series, and this is going to detect the local obstructions. For instance, there aren't many ways to write an even number as a sum of three odd primes.

After all this, you need to get a clean formula for the analytic part of the main term, and bound $\mathfrak{S}(N)$ away from 0 (if possible under local conditions).

This is the outline of the method. Next week, we are going to try to get bounds on exponential sums. Then we are going to jump into Waring's problem.

28 April 10, 2017

28.1 Bounds for exponential sums

We write $x = \lfloor x \rfloor + \{x\}$, and we write $\|x\| = \min_{n\in\mathbb{Z}}|x-n|$.

Lemma 28.1 (Dirichlet)**.** *Let $\alpha \in \mathbb{R}$ and $x \geq 1$ real. Then there exists a rational number $a/q \in \mathbb{Q}$ with $(a,q) = 1$, $1 \leq q \leq x$, such that*

$$\Big|\alpha - \frac{a}{q}\Big| \leq \frac{1}{qx} \leq \frac{1}{q^2}.$$

Proof. This is a classical application of the box principle. □

Lemma 28.2 ("Technical bound")**.** *Let $x, y, \alpha \in \mathbb{R}$. Assume $x, y \geq 1$. Consider a rational approximation*

$$\Big|\alpha - \frac{a}{q}\Big| \leq \frac{1}{q^2}, \quad (a,q) = 1, \quad 1 \leq q.$$

Then

$$\sum_{n\leq x} \min\Big\{\frac{xy}{n}, \frac{1}{\|\alpha n\|}\Big\} \ll xy\Big(\frac{1}{q} + \frac{1}{y} + \frac{q}{xy}\Big)\log(2xq).$$

Proof. We write $n = jq + r$ with $j \geq 0$ and $1 \leq r \leq q$. Then the left hand side is bound by

$$\text{(LHS)} \leq \sum_{0\leq j\leq x/q}\sum_{r=1}^{q} \min\Big\{\frac{xy}{jq+r}, \frac{1}{\|\alpha(jq+r)\|}\Big\}. \tag{0}$$

Write $\alpha - a/q = \theta/q^2$ with $|\theta| \leq 1$. Let us also focus on $y_j = \lfloor \alpha j q^2 \rfloor$. Then

$$\frac{y_j + ar}{q} + \frac{\{\alpha j q^2\}}{q} + \frac{\theta r}{q^2} = \frac{\alpha j q^2 + ar}{q} + \Big(\alpha - \frac{a}{q}\Big) r = \alpha(jq+r). \tag{1}$$

Now we can start to estimate $\|\alpha(qj+r)\|$.

Fix a $j \geq 0$. Then for all r with at most 10 exceptions,

$$\|\alpha(jq+r)\| \geq \Big\|\frac{y_j+ar}{q}\Big\| - \frac{2}{q} \geq_{\text{exc}} \frac{1}{2}\Big\|\frac{y_j+ar}{q}\Big\| > 0. \tag{2}$$

For those exceptions, we will want that $qj + r \gg q(j+1)$ so that we can estimate the other term easily. This is true if $j > 0$ and also if $j = 0$ and $r > q/2$. In the other case ($j = 0$ and $1 \leq r \leq q$) we need something better than (2) without exceptions. Indeed, we have

$$\|\alpha(jq+r)\| \geq \Big\|\frac{ar}{q}\Big\| - \frac{1}{2q} \geq \frac{1}{2}\Big\|\frac{ar}{q}\Big\| > 0 \tag{3}$$

without exceptions in that case.

So by (0),

$$\begin{aligned}
(\text{LHS}) &\le \sum_{0\le j\le x/q}\sum_{r=1}^{q}\min\Big\{\frac{xy}{jq+r},\frac{1}{\|\alpha(jq+r)\|}\Big\} \\
&\le \sum_{1\le r\le q/2}\frac{2}{\|ar/q\|}+\sum_{0\le j\le x/q}\sum_{\substack{1\le r\le q\\ \text{unless } j=0\\ q/2<r\le q}}\min\Big\{\frac{xy}{jq+r},\frac{1}{\|\alpha(jq+r)\|}\Big\} \\
&\ll q\log(2q)+\sum_{0\le j\le x/q}\left(\frac{xy}{q(j+1)}+\sum_{\substack{1\le r\le q\\ q\nmid y_j+ar}}\frac{1}{\|(y_j+ar)/q\|}\right) \\
&\ll q\log(2q)+\frac{xy}{q}\log(2x)+\frac{x}{q}q\log(2q)\ll \log(2xq)xy\Big(\frac{q}{xy}+\frac{1}{q}+\frac{1}{y}\Big).
\end{aligned}$$

This finishes the proof. □

The reason we are interested in this is that this shows up in the estimation. When we deal we exponential sums like

$$\sum_{n\in I}e(\alpha p(n))$$

for $\alpha\in\mathbb{R}$ and $p(x)\in\mathbb{R}[x]$. Weyl's differencing method relies on the fact that the forward differences of p have smaller degree.

For a real number $\beta_j\in\mathbb{R}$ and $\phi:\mathbb{R}\to\mathbb{R}$, we define the difference operators

$$\begin{aligned}
\Delta_1(\phi(x);\beta)&=\phi(x+\beta)-\phi(x),\\
\Delta_{j+1}(\phi(x);\beta_1,\dots,\beta_{j+1})&=\Delta_1(\Delta_j(\phi(x);\beta_1,\dots,\beta_j);\beta_{j+1}).
\end{aligned}$$

Example 28.3. For $\phi(x)=x^2$,

$$\Delta_1(\phi(x);1)=(x+1)^2-x^2=2x+1,\quad \Delta_2(\phi(x);1,1)=2.$$

Lemma 28.4 (Weyl's differencing bound)**.** *Let $Q\in\mathbb{Z}_{\ge1}$, $\phi:\mathbb{R}\to\mathbb{R}$. Let*

$$T(\phi)=\sum_{x=1}^{Q}e(\phi(x)).$$

Then for all $j\ge1$,

$$|T(\phi)|^{2^j}\le(2Q)^{2^j-j-1}\Bigg|\sum_{|h_1|<Q}\cdots\sum_{|h_j|<Q}T_j\Bigg|,$$

where

$$T_j=\sum_{x\in I_j}e(\Delta_j(\phi(x);h_1,\dots,h_j))$$

and $I_j=I_j(h_1,\dots,h_j)$ are intervals (possibly empty) satisfying

$$I_1(h_1)\subseteq[1,Q],\quad I_j(h_1,\dots,h_j)\subseteq I_{j-1}(h_1,\dots,h_{j-1}).$$

Proof. We use induction on j. In the case $j \geq 1$, we have

$$\begin{aligned}|T(\phi)|^2 = T(\phi)\overline{T(\phi)} &= \sum_{x=1}^{Q} \sum_{h_1=1-x}^{Q-x} e(\phi(x+h_1) - \phi(x)) \\ &= \sum_{x=1}^{Q} \sum_{h_1=1-x}^{Q-x} e(\Delta_1(x)) = \sum_{h_1=1-Q}^{Q-1} \sum_{x \in I_1(h_1)} e(\Delta_1(x)),\end{aligned}$$

where $I_1(h_1) = [1, Q] \cap [1 - h_1, Q - h_1]$. □

Next time we will do the inductive step.

29 April 12, 2017

We were proving Weyl's differencing bound.

Lemma 29.1 (Weyl's differencing bound). *Let $Q \in \mathbb{Z}_{\geq 1}$ and $\phi : \mathbb{R} \to \mathbb{R}$. Let*

$$T(\phi) = \sum_{n \leq Q} e(\phi(n)).$$

Then for all $j \geq 1$,

$$|T(\phi)|^{2^j} \leq (2Q)^{2^j - j - 1} \sum_{|h_1| < Q} \cdots \sum_{|h_j| < Q} T_j,$$

where

$$T_j = \sum_{x \in I_j(\underline{h})} e(\Delta_j(\phi(x); \underline{h}))$$

and $I_j(h)$ are intervals satisfying $I_1(h_1) \subseteq [1, Q]$ and $I_j(\underline{h}) \subseteq I_{j-1}(h_1, \ldots, h_{j-1})$.

Proof. Induct on $j \geq 1$. We did the case $j = 1$ last time. Assume case j for some $j \geq 1$. Then

$$|T(\phi)|^2 \leq \left| (2Q)^{2^j - j - 1} \sum_{|h_1| < Q} \cdots \sum_{|h_j| < Q} T_j \right|^2 \leq (2Q)^{2^{j+1} - 2j - 2} (2Q)^j \sum_{|h_i| < Q} |T_j|^2.$$

We note that

$$|T_j|^2 = \sum_{|h| < Q} \sum_{x \in I_{j+1}(h_1, \ldots, h_j, h)} e(\Delta_j(\phi(x+h); \underline{h}) - \Delta_j(\phi(x); \underline{h})),$$

with

$$I_{j+1}(\underline{h}, h) = I_j(\underline{h}) \cap (I_j(\underline{h}) - h).$$

So we get the inequality. □

29.1 Weyl's inequality

Theorem 29.2 (Weyl's inequality). *Let $\phi(x) = \alpha x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k \in \mathbb{R}[x]$ with $k \geq 2$. Consider a rational approximation $|\alpha - a/q| \leq q^{-2}$ with $(a, q) = 1$ and $q \geq 1$. For $Q \geq 1$ an integer, let*

$$T(\phi) = \sum_{n=1}^{Q} e(\phi(n)).$$

Then for every $\epsilon > 0$,

$$|T(\phi)| \ll_{k,\epsilon} Q^{1+\epsilon} \Big(\frac{1}{q} + \frac{1}{Q} + \frac{q}{Q^k} \Big)^{1/2^{k-1}}.$$

Proof. Lemma 29.1 with $j = k-1$ gives

$$|T(\phi)|^{2^{k-1}} \leq (2Q)^{2^{k-1}-k} \sum_{|h_1|<Q} \cdots \sum_{|h_{k-1}|<Q} \sum_{n\in I_{k-1}(\underline{h})} e(h_1\cdots h_{k-1}P(n;\underline{h}),$$

where

$$P(x;\underline{h}) = k!\alpha\Big(x + \frac{1}{2}(h_1+\cdots+h_{k-1})\Big) + (k-1)!\alpha_1.$$

Since $I_{k-1}(\underline{h}) \subseteq [1,Q]$, there are k sums with range of length $\leq 2Q$ each. So the trivial bound will give $\ll_k Q^k$ terms. We need to divide cases, when the trivial bound is correct, namely when the thing in e is equal to zero, and when it is not zero, in which we can expect some saving.

The contribution for the sum of terms with $h_1\cdots h_{k-1}p(n;\underline{h}) = 0$ is $\ll_k Q^{k-1}$, because either one of h_i is zero or $p(n;\underline{h}) = 0$ has at most one solution.

Now we estimate the remaining part of the sum. If we denote $d_t(r) = \#\{(h_1,\dots,h_t) : h_1\cdots h_t = r\}$,

$$\Bigg|\sum_{\substack{|h_1|<Q\\ h_1\neq 0}} \cdots \sum_{\substack{|h_{k-1}|<Q\\ h_{k-1}\neq 0}} \sum_{n\in I_{k-1}(\underline{h})} e(h_1\cdots h_{k-1}P(n;h))\Bigg|$$

$$\ll_k \sum_{r=1}^{k!Q^{k-1}} d_{k-1}(r) \max_{1\leq R\leq Q}\Big|\sum_{n=1}^{R} e(\alpha r n)\Big| \ll_{\epsilon,k} Q^{\epsilon} \sum_{r=1}^{k!Q^{k-1}} \min\Big\{Q, \frac{1}{\|\alpha r\|}\Big\}.$$

For $r \leq k!Q^{k-1}$, we have $Q \leq k!Q^{k-1}Q/r$. This allows us to use the technical Lemma 28.2 with $X = k!Q^{k-1}$ and $Y = Q$. This gives the bound

$$Q^{\epsilon}\sum_{r=1}^{k!Q^{k-1}} \min\Big\{\frac{k!Q^{k-1}Q}{r}, \frac{1}{\|\alpha r\|}\Big\} \ll_{k,\epsilon} Q^{2\epsilon}Q^k\Big(\frac{1}{q} + \frac{1}{Q} + \frac{q}{Q^k}\Big).$$

Therefore

$$\|T(\phi)\|^{2^{k-1}} \ll_{\epsilon,k} Q^{2^{k-1}-k}\Big(Q^{k-1}+Q^{k+\epsilon}\Big(\frac{1}{q}+\frac{1}{Q}+\frac{q}{Q^k}\Big)\Big) \ll Q^{2^{k-1}+\epsilon}\Big(\frac{1}{q}+\frac{1}{Q}+\frac{q}{Q^k}\Big).$$

This finishes the proof. □

30 April 14, 2017

30.1 Hua's lemma

For $Q \geq 1$ an integer, $k \geq 2$ a fixed integer, we define

$$f(\alpha) = f_{Q,k}(\alpha) = \sum_{n=1}^{Q} e(\alpha n^k).$$

Theorem 30.1 (Hua's lemma)**.** *Let $1 \leq j \leq k$, with the previous notation. Then for any $\epsilon > 0$,*

$$\int_0^1 |f(\alpha)|^{2^j}\, d\alpha \ll_\epsilon Q^{2^j - j + \epsilon}.$$

Proof. We use induction. For $j = 1$, we have

$$\int_0^1 |f(\alpha)|^2 d\alpha = Q.$$

Now the inductive step. Assume it for some $1 \leq j \leq k-1$ and we prove it for $j+1$. By Weyl's differencing lemma (Lemma 29.1),

$$|f(\alpha)|^{2^j} \leq (2Q)^{2^j - j - 1} \sum_{|h_1|<Q} \cdots \sum_{|h_j|<Q} \sum_{n \in I_j(\underline{h})} e(\alpha h_1 \cdots h_j p(n; \underline{h})),$$

where $p(x; \underline{h}) \in \mathbb{Z}[x]$ for any $\underline{h} \in \mathbb{Z}^j$ and $\deg p(x; \underline{h}) = k - j$. It's now important that the right hand side is a positive real number, because it came from the square modulus of some complex number.

We have to play the same game, but more carefully. For $r \in \mathbb{Z}$, let

$$c_r = \#\left\{ (n, \underline{h}) \in \mathbb{Z}^{1+j} : \begin{array}{c} |h_i| < Q \text{ for all } i \text{ and } n \in I_j(\underline{h}) \\ h_1 \cdots h_r p(n; \underline{h}) = r \end{array} \right\}.$$

So we have

$$|f(\alpha)|^{2^j} \leq (2Q)^{2^j - j - 1} \sum_r c_r e(\alpha r).$$

Last time we had the estimates $c_0 \ll_k Q^j$ and for $r \neq 0$, $c_r \ll_{k,\epsilon} Q^\epsilon$.

But let us analyze $|f(\alpha)|^{2^j}$ in a different (trivial) way:

$$|f(\alpha)|^{2^{j-1}} = f(\alpha)^{2^{j-1}} f(-\alpha)^{2^{j-1}} = \sum_r b_r e(-\alpha r),$$

where

$$b_r = \#\left\{ (\underline{x}, \underline{y}) \in \mathbb{Z}^{2^{j-1} + 2^{j-1}} : \begin{array}{c} 0 < x_i, y_i \leq Q \text{ for all } i \\ r = \sum_{i=1}^{2^{j-1}} x_i^k - \sum_{i=1}^{2^{j-1}} y_i^k \end{array} \right\}.$$

Finally,

$$\begin{aligned}\int_0^1 |f(\alpha)|^{2^{j+1}} &= \int_0^1 |f(\alpha)|^{2^j} \sum_r b_r e(-\alpha r) d\alpha \\ &= (2Q)^{2^j-j-1} \int_0^1 \biggl(\sum_s c_s e(\alpha s)\biggr)\biggl(\sum_r b_r e(-\alpha r)\biggr) d\alpha \\ &= (2Q)^{2^j-j-1} \sum_r b_r c_r = (2Q)^{2^j-j-1}\biggl(b_0 c_0 + \sum_{r\neq 0} c_r b_r\biggr).\end{aligned}$$

About the b_r, we know that

$$\sum_r b_r |f(0)|^{2^j} = Q^{2^j},$$

and

$$b_0 = \int_0^1 \sum_r b_r e(\alpha r) d\alpha = \int_0^1 |f(\alpha)|^{2^j} d\alpha \ll_{k,\epsilon} Q^{2^j-j+\epsilon}$$

by induction. So

$$\int_0^1 |f(\alpha)|^{2^{j+1}} d\alpha \ll_{k,\epsilon} Q^{2^j-j-1}(Q^{2^j-j+\epsilon}Q^j + Q^\epsilon Q^{2^j}).$$

This finishes the proof. □

30.2 Setup for Waring's problem

Let $k \geq 2$ be an integer. This is the exponent for Waring's problem. Let s be a positive integer, which is the number of k-th powers we add. We will need $s > 2^k$. Then $N \gg_{k,s} 1$ is the integer that we want to write as $x_1^k + \cdots + x_s^k$. Let $\nu = 0.01$ and $\delta = \delta(k) > 0$ such that $\delta \ll_k 1$. Define $P = \lfloor \sqrt[k]{N} \rfloor$ and we are going to use the exponential sum

$$f(\alpha) = \sum_{n=1}^P e(\alpha n^k).$$

The number that we care about is

$$r(N) = r_{k,s}(N) = \#\{\underline{n} \in \mathbb{Z}_{\geq 1}^s : N = n_1^k + \cdots + n_s^k\}.$$

The circle method is based on the equality

$$r(N) = \int_0^1 f(\alpha)^s e(-\alpha N) d\alpha.$$

But then there is half an interval near 0 and the other half near 1. This is annoying and so we will shift it a little bit.

The major arcs are, for $1 \leq a \leq q \leq P^{\nu}$ with $(a,q)=1$,

$$\mathfrak{M}(a,q) = \left\{\alpha \in \mathbb{R} : \left|\alpha - \frac{a}{q}\right| < \frac{1}{P^{k-\nu}}\right\}, \quad \mathfrak{M} = \bigcup \mathfrak{M}(a,q).$$

Then

$$\mathfrak{M} \subseteq U = \left(\frac{1}{P^{k-\nu}}, 1 + \frac{1}{P^{k-\nu}}\right]$$

and it can be checked that $\mathfrak{M}(a,q)$ are disjoint. The minor arcs are $\mathfrak{m} = U \setminus \mathfrak{M}$.

31 April 17, 2017

Today we are going to deal with the minor arcs. We keep our previous notations

31.1 Minor arcs

Proposition 31.1 (Bound on $\mathfrak{m}$). *If $s \geq 2^k + 1$, then*

$$\int_{\mathfrak{m}} |f(\alpha)|^s d\alpha \ll_{k,s} N^{s/k-1-\delta}.$$

Note that because $f(\alpha)$ is the sum of P exponentials, the trivial bound is $\ll P^s \asymp N^{s/k}$.

Proof. We start with Hua's lemma. We have

$$\begin{aligned}\int_{\mathfrak{m}} |f(\alpha)|^s d\alpha &\leq \Big(\sup_{\alpha\in\mathfrak{m}}|f(\alpha)|\Big)^{s-2^k} \int_0^1 |f(\alpha)|^{2^k} d\alpha \\ &\ll_{k,\epsilon} \Big(\sup_{\alpha\in\mathfrak{m}}|f(\alpha)|\Big)^{s-2^k} P^{2^k-k+\epsilon} \leq \Big(\sup_{\alpha\in\mathfrak{m}}|f(\alpha)|\Big)^{s-2^k} N^{2^k/k-1+\epsilon}.\end{aligned}$$

Now we estimate the supremum. By Dirichlet, there exists $(a,q)=1$ such that $1 \leq q \leq p^{k-\nu}$ such that

$$\Big|\alpha - \frac{a}{q}\Big| \leq \frac{1}{qP^{k-\nu}}.$$

Because $\alpha \in \mathfrak{m} \subseteq U$, we have $1 \leq a \leq q$. But since $\alpha \notin \mathfrak{M}$, we get $q > P^\nu$. Weyl's inequality gives

$$\sup_{\alpha\in\mathfrak{m}}|f(\alpha)| \ll_{k,\epsilon} P^{1+\epsilon}\Big(\frac{1}{q} + \frac{1}{P} + \frac{q}{P^k}\Big)^{2^{1-k}} \ll P^{1+\epsilon-\nu/2^{k-1}} \leq N^{1/k+\epsilon-\nu/k2^{n-1}}.$$

Then

$$\int_{\mathfrak{m}} |f(\alpha)|^s d\alpha \ll_{k,s,\epsilon} N^{\frac{s}{k}+2\epsilon-1-\frac{\nu}{k2^{k-1}}}.$$

□

31.2 Major arcs

The goal is to analyze $f(\alpha)$ for $\alpha \in \mathfrak{M}(a,q) \subseteq \mathfrak{M}$. Here we really need an asymptotic expression. To understand it better, we introduce two functions:

- analytic local factor

$$v(\beta) = \sum_{n=1}^{N} \frac{1}{k} n^{\frac{1}{k}-1} e(\beta n), \quad \beta \in \mathbb{R},$$

- arithmetic local factor

$$S(a,q) = \sum_{n=1}^{q} e\Big(\frac{a}{q} n^k\Big).$$

Lemma 31.2 (local factorization)**.** *Let $1 \le a \le q \le P^\nu$ with $(a,q)=1$. Let $\alpha \in \mathfrak{M}(a,q)$. Then*

$$f(\alpha) = \frac{1}{q} S(a,q)\nu(\beta) + O_k(P^{2\nu}),$$

where $\beta = \alpha - a/q$.

Proof. For $t \ge 1$ let $T = t^k$. The partial sums are

$$\sum_{n \le T} \frac{1}{n} n^{1/k-1} = \int_1^T \frac{1}{k} x^{1/k-1} dx + O(1) = t + O(1).$$

Also

$$\sum_{n\le t} e\Big(\frac{a}{q} n^k\Big) = \sum_{r=1}^{q} e\Big(\frac{a}{q} r^k\Big) \sum_{\substack{n \le t \\ n \equiv r\ (q)}} 1 = \frac{t}{q} S(a,q) + O(q).$$

The difference that we want to bound is

$$\begin{aligned} f(\alpha) - \frac{1}{q}S(a,q)\nu(\beta) &= \sum_{n \le P} e(\alpha n^k) - \frac{1}{q} S(a,q) \sum_{m=1}^{N} \frac{1}{k} n^{1/k-1} e(\beta m) \\ &= \sum_{m=1}^{N} c_m e(\beta m), \end{aligned}$$

where

$$c_m = \begin{cases} e(\frac{am}{q}) - \frac{1}{q} S(a,q) \frac{1}{k} m^{1/k-1} & \text{if } m \text{ is } k\text{th power,} \\ -\frac{1}{q} S(a,q)\frac{1}{k} m^{1/k-1} & \text{otherwise.} \end{cases}$$

We are going to do partial summation, and for this we need control over $\sum_{m \le T} c_m$. We have

$$\begin{aligned} \sum_{m \le T} c_m &= \sum_{n \le t} e\Big(\frac{an^k}{q}\Big) - \frac{1}{q} S(a,q) \sum_{m \le T} \frac{1}{k} m^{1/k-1} \\ &= \sum_{n\le t} e\Big(\frac{a}{q} n^k\Big) - \Big(\frac{1}{t} \sum_{n \le t} e\Big(\frac{a}{q} n^k\Big) + O\Big(\frac{q}{t}\Big)\Big)(t + O(1)) \\ &= O\Big(q + \frac{q}{t} + 1 \cdot 1\Big) = O(q). \end{aligned}$$

So by partial summation,

$$|(\text{difference})| \le q \cdot 1 + \int_1^N q|\beta| 1 dx \ll q(1 + |\beta| N).$$

But remember that $|\beta| < P^{-k+\nu}$ because $\alpha \in \mathfrak{M}(a,q)$ and $q < P^\nu$. So We vet

$$|(\text{difference})| \ll P^\nu \Big(1 + \frac{N}{P^{k-\nu}}\Big) \ll P^{2\nu}. \qquad \square$$

Let us define

$$V(a,q;\alpha) = \frac{1}{q} S(a,q) v\Big(\alpha - \frac{a}{q}\Big).$$

This is the good approximation for $f(\alpha)$. Explicitly, for $\alpha \in \mathfrak{M}(a,q)$,

$$|f(\alpha)^s - V^s| \ll_{s,k} |f(\alpha) - V| P^{s-1} \ll_{s,k} P^{s-1+2\nu}.$$

So:

$$\sum_{q \le P^\nu} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} \int_{\mathfrak{M}(a,q)} |f(\alpha)^s - V^s| d\alpha \ll_{s,k} P^{s-k-1+5\nu}.$$

32 April 19, 2017

Last time we had the local factorization: if we define

$$V(a,q;\alpha) = \frac{1}{q}S(a,q)v\Big(\alpha - \frac{a}{q}\Big)$$

for $\alpha \in \mathfrak{M}(a,q)$ then

$$|f(\alpha)^s - V^s| \ll_{s,k} P^{s-1+2\nu}.$$

So we had

$$\sum_{q \le P^\nu} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} \int_{\mathfrak{M}(a,q)} |f(\alpha)^2 - V^s| d\alpha \ll_{s,k} P^{s-k-1+5\nu}.$$

32.1 Global factorization

We have

$$\int_{\mathfrak{M}} f(\alpha)^s e(-\alpha N) d\alpha = \sum_{q \le P^\nu} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} \int_{\mathfrak{M}(a,q)} V(a,q;\alpha)^s e(-\alpha N) d\alpha \\ + O_{s,k}(N^{s/k-1-\delta}).$$

Let us just define this as

$$r^*(N) = \sum_{q \le P^\nu} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} \int_{\mathfrak{M}(a,q)} V(a,q;\alpha)^s e(-\alpha N) d\alpha.$$

Here we have the factorization, and the integrals are the same integrals, with some shifts. This motivates defining

$$\mathfrak{S}(N,Q) = \sum_{q \le Q} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} \int_{\mathfrak{M}(a,q)} \Big(\frac{1}{q}S(a,q)\Big)^s e\Big(-\frac{a}{q}N\Big)$$

$$J^*(N) = \int_{-p^{\nu-k}}^{p^{\nu-k}} v(\beta)^s e(-\beta N) d\beta.$$

Then it is immediate that

$$r^*(N) = \mathscr{S}(N, P^\nu) \cdot J^*(N).$$

We also note that $\mathfrak{S} = \mathfrak{S}_{s,k}$ and $J^* = J^*_{s,k}$.

Proposition 32.1 (Global factorization)**.**

$$r(N) = \mathfrak{S}(N, P^\nu) J^*(N) + O_{k,s}(N^{s/k-1-\delta})$$

Proof. Use the previous analysis on $\mathfrak{M}$ and the analysis on $\mathfrak{m}$. □

32.2 Main formula for $r(N)$

This $\mathfrak{S}(N,Q)$ is not a really well-behaved arithmetic function so what we are going to do is to let $Q \to \infty$ and then analyze the function.

Define

$$S(q) = \sum_{\substack{1\le a\le q\\(a,q)=1}} \Big(\frac{1}{q}S(a,q)\Big)^s e\Big(-\frac{a}{q}N\Big)$$

so that $\mathfrak{S}(N,Q) = \sum_{q\le Q} S(q)$.

Lemma 32.2. $|S(q)| \ll_{k,s} q^{-1-2^{-k}}$.

Proof. For $(a,q)=1$ we use Weyl's bound for the rational approximation $a/q = a/q$:

$$|S(a,q)| \ll_{k,\epsilon} q^{1+\epsilon}\Big(\frac{1}{q}+\frac{1}{q}+\frac{q}{q^k}\Big)^{2^{1-k}} \ll_{k,\epsilon} q^{1+\epsilon-2^{1-k}}.$$

With $\epsilon > 0$ small,

$$|S(q)| \ll_{s,k,\epsilon} qq^{(\epsilon-2^{1-k})s} \ll q^{1-(2^{1-k}-\epsilon)(2^k+1)} \ll_{s,k,\epsilon} q^{-1+\epsilon(2^k+1)-2^{1-k}}. \qquad \square$$

Define the **singular series**

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} S(q)$$

which converges absolutely by the lemma. Moreover,

(1) $|\mathfrak{S}(N)| \ll_{s,k} 1$,
(2) $|\mathfrak{S}(N,P^\nu) - \mathfrak{S}(N)| \ll_{s,k} N^{-\delta}$.

So we get

$$r(N) = (\mathfrak{S}(N) + O_{k,s}(N^{-\delta}))J^*(N) + O_{k,s}(N^{s/k-1-\delta}).$$

Now we go to the second part. Recall

$$J^*(N) = \int_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-\beta N)\,d\beta.$$

Lemma 32.3. *For* $|\beta| \le 1/2$,

$$|v(\beta)| \ll_k \min\Big\{N^{1/k}, \frac{1}{|\beta|^{1/k}}\Big\}.$$

Proof. Recall that $v(\beta) = \sum_{n=1}^N k^{-1}n^{1/k-1}e(\beta n)$. In the case $|\beta| < N^{-1}$,

$$|v(\beta)| \le \sum_{n=1}^N \frac{1}{k}n^{1/k-1} = N^{1/k} + O_k(1).$$

In the case $1/N \le |\beta| \le 1/2$, observe that $\|\beta\| = |\beta|$. Write $X = \lfloor 1/|\beta| \rfloor < N$. We will have

$$\Big|\sum_{n\le X} \frac{1}{k} n^{1/k-1} e(\beta n)\Big| \le X^{1/k} + O_k(1) \ll \frac{1}{|\beta|^{1/k}}.$$

On the other interval, we do partial summation and get

$$\begin{aligned}\sum_{X<n\le N} \frac{1}{k} n^{1/k-1} e(\beta n) &= \Big(\sum_{X<n\le N} e(\beta n)\Big)\frac{1}{k}N^{1/k-1} \\ &\qquad + \frac{1}{k}\Big(1-\frac{1}{k}\Big)\int_X^N \Big(\sum_{X<n\le t} e(\beta n)\Big)\frac{dt}{t^{2-1/k}} \\ &\ll_k \frac{1}{|\beta|}N^{1/k-1} + \frac{1}{|\beta|}X^{1/k-1} \ll_k \frac{1}{|\beta|^{1/k}} + \frac{1}{|\beta|^{1/k}}. \qquad \square\end{aligned}$$

Therefore we define the **singular integral**

$$J(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta N)\, d\beta,$$

for $s \ge 2^k + 1 > k$. Then

(1) $|J(N)| \ll_{s,k} \int_0^\infty \min\Big\{N^{s/k}, \frac{1}{\beta^{s/k}}\Big\} d\beta \ll_{s,k} N^{s/k-1}$,

(2) $|J^*(N) - J(N)| \ll_{s,k} \int_{P^{\nu-k}}^\infty \frac{1}{\beta^{s/k}} d\beta \ll_{s,k} N^{s/k-1-\delta}$.

Theorem 32.4. *Assume $s \ge 2^k + 1$. Then*

$$r(N) = \mathfrak{S}(N)J(N) + O_{k,s}(N^{s/k-1-\delta}).$$

In the remaining lectures, we are going to show that the main term is not too small.

33 April 21, 2017

Last time we have the main formula: for $n \geq 2^k + 1$,

$$r(N) = \mathfrak{S}(N)J(N) + O_{k,s}(N^{s/k-1-\delta}).$$

A better notation would be $r_{k,s}$, $\mathfrak{S}_{k,s}$, $J_{k,s}$, but these are fixed.

33.1 Evaluation of $J(N)$

Recall that

$$v(\beta) = \sum_{1 \leq n \leq N} \frac{1}{k} n^{1/k-1} e(\beta n)$$

and

$$J(N) = J_{k,s}(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta N) d\beta.$$

The reward for having integration over a unit interval is

$$J_{k,s}(N) = \sum_{n_1+\cdots+n_s=N} \frac{1}{k^s}(n_1 \cdots n_s)^{1/k-1}.$$

Lemma 33.1. *Let $0 < a \leq b$ with $a \leq 1$. Then for $Q \in \mathbb{Z}_{\geq 1}$ we have*

$$\sum_{1 \leq n < Q} n^{a-1}(Q-n)^{b-1} = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} Q^{a+b-1} + O_{a,b}(Q^{b-1}).$$

Proof. Let $h(x) = x^{a-1}(Q-x)^{b-1}$ on $(0, Q)$. You can estimate the error terms and get

$$\begin{aligned}\sum_{1 \leq n < Q} h(n) &= \int_0^Q h(x)dx + O_{a,b}(Q^{a+b-2} + Q^{b-1}) \\ &= Q^{a+b-1} \int_0^1 t^{a-1}(1-t)^{b-1} dt + O_{a,b}(Q^{b-1}).\end{aligned}$$

Now the integral is the beta function. □

Theorem 33.2. *Suppose $s \geq 2$. Then*

$$J_{k,s}(N) = \Gamma\Big(1 + \frac{1}{k}\Big)^s \Gamma\Big(\frac{s}{k}\Big)^{-1} N^{s/k-1} + O_{k,s}(N^{s/k-1-1/k}).$$

Proof. We use induction on $s \geq 2$. In the case $s = 2$,

$$\begin{aligned}J_{k,s}(N) &= \sum_{n=1}^{N-1} \frac{1}{k^2}(n(N-n))^{1/k-1} \\ &= \frac{\Gamma(1/k)\Gamma(1/k)}{\Gamma(2/k)} \frac{1}{k^2} N^{2/k-1} + O_k(N^{2/k-1-1/k}).\end{aligned}$$

In the inductive step, we have

$$\begin{aligned}
J_{k,s+1}(N) &= \sum_{n=1}^{N-1} \frac{1}{k} n^{1/k-1} J_{k,s}(N-n) \\
&= \Gamma\Big(1+\frac{1}{k}\Big)^s \Gamma\Big(\frac{s}{k}\Big)^{-1} \frac{1}{k} \sum_{n=1}^{N-1} n^{1/k-1}(N-n)^{s/k-1} \\
&\quad + O_{k,s}\Big(\sum_{n=1}^{N-1} n^{1/k-1}(N-n)^{(s-1)/k-1}\Big) \\
&= \Gamma\Big(1+\frac{1}{k}\Big)^s \Gamma\Big(\frac{s}{k}\Big)^{-1} \frac{1}{k} \Big[\frac{\Gamma(1/k)\Gamma(s/k)}{\Gamma((s+1)/k)} N^{(s+1)/k-1} \\
&\quad + O_{k,s}(N^{s/k-1})\Big] + O_{k,s}(N^{s/k}-1) \\
&= \Gamma\Big(1+\frac{1}{k}\Big)^{s+1} \Gamma\Big(\frac{s+1}{k}\Big)^{-1} N^{(s+1)/k-1} + O_{k,s}(N^{(s+1)/k-1-1/k}).
\end{aligned}$$

This finishes the proof. □

Theorem 33.3. *Assume $s \geq 2^k + 1$. Then*

$$r_{k,s}(N) = \mathfrak{S}(N)\Gamma\Big(1+\frac{1}{k}\Big)^s \Gamma\Big(\frac{s}{k}\Big)^{-1} N^{s/k-1} + O_{k,s}(N^{s/k-1-\delta}).$$

Moreover, $|\mathfrak{S}_{k,s}(N)| \ll_{k,s} 1$.

We need some finer analysis on the singular series.

33.2 $S(a,q)$ and $S(q)$ revisited

Recall that

$$S(a,q) = \sum_{n=1}^{q} e\Big(\frac{a}{q} n^k\Big), \quad S(q) = \sum_{\substack{1\leq a\leq q \\ (a,q)=1}} \Big(\frac{1}{q} S(a,q)\Big)^s e\Big(-\frac{a}{q} N\Big).$$

By definition,

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} S(q)$$

which converges for $s \geq 2^k + 1$, because in that case we have the estimate $|S(q)| \ll_{k,s} q^{-1-2^{-k}}$ uniformly on N.

Lemma 33.4. *Let $(a,q) = (b,r) = (q,r) = 1$. Then*

$$S(ar+bq, qr) = S(a,q)S(b,r).$$

Proof. Expand the right hand side and use the Chinese remainder theorem. □

Lemma 33.5. *$S(q)$ is a multiplicative function.*

Proof. Taking $(q,r)=1$, the previous lemma gives

$$S(q)S(r) = \Big(\sum_{\substack{1\le a\le q\\(a,q)=1}} \Big(\frac{1}{q}S(a,q)\Big)^s e\Big(-\frac{a}{q}N\Big)\Big)\Big(\sum_{\substack{1\le b\le r\\(b,r)=1}} \Big(\frac{1}{r}S(b,r)\Big)^s e\Big(-\frac{b}{r}N\Big)\Big)$$
$$= \sum_{\substack{1\le a\le q\\(a,q)=1}}\sum_{\substack{1\le b\le r\\(b,r)=1}} \frac{1}{(qr)^s}S(ar+bq,qr)^s e\Big(-\frac{ar+bq}{rq}N\Big) = S(qr) \qquad \square$$

Then

$$\mathfrak{S}_{k,s}(N) = \sum_{q\ge 1} S(q).$$

can be factored into Euler factors, by absolute convergence. For $s \ge 2^k+1$ and p a prime number, define

$$T(p) = \sum_{m\ge 0} S(p^m),$$

which converges absolutely.

Proposition 33.6. *For $s\ge 2^k+1$, we have*

$$\mathfrak{S}(N) = \prod_p T(p),$$

and the convergence is absolute.

In fact, $T(p)$ is a real number, because each $S(q)$ is a real number:

$$\overline{S(q)} = \sum_{\substack{1\le a\le q\\(a,q)=1}} \overline{\Big(\frac{1}{q}S(a,q)\Big)^s e\Big(-\frac{a}{q}N\Big)}$$
$$= \sum_{\substack{1\le a\le q\\(a,q)=1}} \Big(\frac{1}{q}\sum_{n=1}^{q} e\Big(\frac{-a}{q}n^k\Big)\Big)^s e\Big(-\frac{-a}{q}N\Big) = S(q).$$

Corollary 33.7. *For $p \gg_{k,s} 1$, $T(p)>0$.*

Furthermore, there exists a constant $C_{k,s}$, independent of N, such that for $p > C_{k,s}$, $T(p)>0$ and $\prod_{p>C_{k,s}} T(p) \in [1/2,3/2]$. The remaining lectures will be about bounding $T(p)$.

34 April 24, 2017

Last time we have
$$\mathfrak{S}(N) = \prod_p T(p)$$
for $s \geq 2^k + 1$, where $T(p) = \sum_{k \geq 0} S(p^k)$. This converges absolutely and uniformly on N, because S is multiplicative on q and $|S(q)| \ll_{s,k} q^{-1-2^{-k}}$.

Today we analyze $T(p)$.

34.1 Formula for $T(p)$

We are only going to consider $s \geq 2^k + 1$, because otherwise the series might not even converge.

Definition 34.1. We define
$$M(q) = \#\{\underline{x} \in (\mathbb{Z}/q\mathbb{Z})^s : x_1^k + \cdots + x_s^k \equiv N \pmod q\}.$$

Lemma 34.2. $\displaystyle\sum_{d|q} S(d) = \frac{1}{q^{s-1}} M(q)$.

Proof. We have
$$M(q) = \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} \frac{1}{q} \sum_{r=1}^{q} e\Big(\frac{r}{q}(x_1^k + \cdots + x_s^k - N)\Big).$$

For each r, let $d = (r, q)$ and $a = r/d$. Then
$$\begin{aligned} qM_q &= \sum_{d|q} \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \Big(\frac{q}{d}\Big)^s \sum_{n_1=1}^{d} \cdots \sum_{n_s=1}^{d} e\Big(\frac{a}{d}(n_1^k + \cdots + n_s^k - N)\Big) \\ &= q^s \sum_{d|q} \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \Big(\frac{1}{d} \sum_{n=1}^{d} e\Big(\frac{a}{d} n^k\Big)\Big)^s e\Big(-\frac{a}{d} N\Big). \end{aligned}$$

The right hand side can be identified as the sum of $S(d)$. □

Now for $q = p^h$ with $h \to \infty$, the sum converges to $T(p)$.

Lemma 34.3. *For $s \geq 2^k + 1$,*
$$T(p) = \lim_{h \to \infty} \frac{1}{p^{h(s-1)}} M(p^h).$$

Corollary 34.4. $T(p) \geq 0$.

The goal now is to produce enough solutions of $x_1^k + \cdots + x_s^k \equiv N \pmod{p^h}$ so that we can give a lower bound for $T(p)$, of course, uniformly on N.

The naïve thing you would do is to find solutions modulo p and then lift the solutions. But you need a little bit of care: 3 is a square modulo 2 but not modulo 4.

Definition 34.5. Define $\tau(p) = \nu_p(k)$.

Lemma 34.6. *The number of invertible kth powers modulo p^t ($t \geq 0$) is:*

(1) $\varphi(p^t)/(k, \varphi(p^t))$ if $p > 2$ or $t = 1$ or k is odd,

(2) $2^{t-2}/(k, 2^{t-2})$ if $p = 2$ and k is even and $t > 1$.

Define

$$\gamma(p) = \begin{cases} \tau(p) + 1 & \text{if } p > 2 \text{ or } k \text{ is odd or } \tau = 0, \\ \tau(p) + 2 & \text{if } p = 2 \text{ and } k \text{ is even and } \tau > 0. \end{cases}$$

Lemma 34.7. *The number of invertible kth powers mod $p^{\gamma(p)}$ is*

$$\varphi(p^{\tau(p)+1})/(k, \varphi(p^{\tau(p)+1})).$$

Lemma 34.8. *Let $a \in \mathbb{Z}$ be coprime to p. The number of solutions to the congruence $x^k \equiv a \pmod{p^{\gamma(p)}}$ is either 0 or $p^{\gamma-\tau-1}(k, \varphi(p^{\tau(p)} + 1))$.*

Lemma 34.9. *Let $a \in \mathbb{Z}$ be coprime to p. If a is a kth power mod $p^{\gamma(p)}$ then it is so mod p^t for all t.*

Proof. For $t \leq \gamma(p)$, it is clear. For $t > \gamma(p)$, the lift of solutions follows from the previous lemmas by counting. □

Define

$$M^*(q) = \#\{\underline{x} \in (\mathbb{Z}/q\mathbb{Z})^s : x_1^k + \cdots + x_s^k \equiv N \pmod{q}, (q, x_1) = 1\}.$$

Obviously, $M(q) \geq M^*(q)$.

Lemma 34.10. *Suppose $t \geq \gamma(p)$ and that $M^*(p^\gamma) > 0$. Then $M(p^t) \geq p^{(t-\gamma)(s-1)}$.*

Proof. Let $a_1, \ldots, a_s \in \mathbb{Z}$ be a solution of $x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma}$ with $(a_1, p) = 1$. Then consider

$$x_1^k \equiv N - (x_2^k + \cdots + x_s^k) \pmod{p^t}$$

for $t \geq \gamma$. Then any lifting for $x_2, \ldots, x_s$ from p^γ to p^t is admissible by the previous lemma, since modulo p^γ the right hand side is a kth power.

So any solution counted in $M^*(p^\gamma)$ gives the lower bound for $M^*(p^t)$. □

The remaining problem is, is $M^*(p^\gamma) > 0$? We go back to the idea of densities.

Theorem 34.11 (Cauchy–Davenport)**.** *Let $q > 1$, and let $\mathscr{A}, \mathscr{B} \subseteq \mathbb{Z}/q\mathbb{Z}$. Suppose:*

(1) $a = \#\mathscr{A} > 0$ *and* $b = \#\mathscr{B}$*,*

(2) $0 \in \mathscr{B}$ *and* $\mathscr{B} \setminus \{0\} \in (\mathbb{Z}/q\mathbb{Z})^\times$*.*

Then $\#(\mathscr{A} + \mathscr{B}) \geq \min\{a + b - 1, q\}$*.*

35 April 26, 2017

Last time we had the question of bounding

$$M^*(q) = \#\{\underline{x} \in (\mathbb{Z}/q\mathbb{Z})^s : x_1^k + \cdots + x_s^k \equiv N\ (q),\ (x_1, q) = 1\}.$$

We still need to check that for $s \geq 2^k + 1$, $M^*(p^{\gamma(p)}) > 0$ for all p.

35.1 Local Waring's problem

Theorem 35.1 (Cauchy–Davenport). *Let $q \geq 1$ and let $\mathscr{A}, \mathscr{B} \subseteq \mathbb{Z}/q\mathbb{Z}$, such that*

(1) $a = \#\mathscr{A} > 0$, $b = \#\mathscr{B}$,

(2) $0 \in \mathscr{B}$ and $\mathscr{B} \setminus \{0\} \subseteq (\mathbb{Z}/q\mathbb{Z})^\times$.

Then $\#(\mathscr{A} + \mathscr{B}) \geq \min\{q, a + b - 1\}$.

Proof. We can assume that $a + b - 1 \leq q$. Otherwise, remove $b - (q - a + q)$ non-zero elements from $\mathscr{B}$. Now induct on b. For $b = 1$, we have $\mathscr{B} = \{0\}$ and this is trivial.

Now let $b \geq 2$, in particular, 0 is not the only element. Assume all cases with $\#\mathscr{B}' < b$. We claim that there exist $\alpha_0 \in \mathscr{A}$ and $\beta_0 \in \mathscr{B}$ such that $\alpha_0 + \beta_0 \in \mathscr{A}$. Otherwise, given any $\beta_0 \in \mathscr{B}$ we would have

$$\sum_{\alpha \in \mathscr{A}} (\alpha + \beta_0) \equiv \sum_{\alpha \in \mathscr{A}} \alpha \pmod q$$

and then $a\beta_0 \equiv 0 \pmod q$. This is not possible because $\mathscr{B}$ has invertible elements.

Let α_0 be as in the claim. Let $X = \{\beta \in \mathscr{B} : \alpha_0 + \beta \notin \mathscr{A}$. Then $\emptyset \neq X \subset \mathscr{B}$. Let $\mathscr{A}' = \mathscr{A} \cup (\alpha_0 + X)$ and $\mathscr{B}' = \mathscr{B} \setminus X$. If $x = \#X$, then $\#\mathscr{A}' = a + x$ and $\#\mathscr{B}' = b - x$ and $x \neq 0$. So by induction,

$$\#(\mathscr{A}' + \mathscr{B}') \geq \min\{q, (a + x) + (b - x) - 1\} = \min\{q, a + b - 1\}.$$

But note that $\mathscr{A}' + \mathscr{B}' \subseteq \mathscr{A} + \mathscr{B}$. □

Proposition 35.2. *Let $s \geq 2^k + 1$. Then for every prime p we have $M^*(p^{\gamma(p)}) > 0$.*

Proof. We always consider $p \nmid x_1$. Recall that

$$\tau(p) = \nu_p(k), \quad \gamma(p) = \begin{cases} \tau + 1 & p \geq 3 \text{ or } k \text{ odd}, \\ \tau + 2 & p = 2 \text{ and } k \text{ even}. \end{cases}$$

For $p = 2$ and $k = 2$, we have $s \geq 5$ and you can check that $x_1^2 + \cdots + x_5^2 \equiv * \pmod 8$ has a solution. For $p = 2$ and $k = 3$, we have $s \geq 9$, and it is easier that $x_1^3 + \cdots + x_9^3 \equiv * \pmod 2$ has a solution.

For $p \geq 3$ and $k = 2$, we have $\gamma = 1$. Let $\mathscr{A} = ((\mathbb{Z}/p\mathbb{Z})^\times)^2$ and $\mathscr{B} = \mathscr{A} \cup \{0\}$. Then either $\mathscr{A} + (s-1)\mathscr{B} = \mathbb{Z}/p\mathbb{Z}$ or

$$\#(\mathscr{A} + (s-1)\mathscr{B}) \geq a + (s-1)(a+1) - (s-1) = sa \geq 5(p-1)/2 > p,$$

which is not possible.

For $p \geq 3$ and $k \geq 4$, $\gamma = \tau + 1 = \nu_p(k) + 1$. So $p^\gamma \leq pk$. Let $\mathscr{A} = ((\mathbb{Z}/p^\gamma\mathbb{Z})^\times)^2$ and $\mathscr{B} = \{0\} \cup \mathscr{A}$. Then

$$a = \#\mathscr{A} = \frac{\varphi(p^\gamma)}{(k, \varphi(p^\gamma))} = \frac{p^{\tau+1} - p^\tau}{(k, p^{\tau+1} - p^\tau)} = \frac{p-1}{(k, p-1)} \geq \frac{p-1}{k}.$$

Either $\mathscr{A} + (s-1)\mathscr{B} = \mathbb{Z}/p^\gamma\mathbb{Z}$ or it has size at least

$$a + (s-1)(a+1) - (s-1) = sa \geq (2^k + 1)\frac{p-1}{k}.$$

We need $(2^k + 1)/k^2 \geq p/(p-1)$, and this can be checked.

For $k = 3$, you can check. □

So what do we get?

Corollary 35.3. $T(p) = \lim\limits_{h \to \infty} \dfrac{1}{p^{h(s-1)}} M(p^h) \geq \dfrac{1}{p^\gamma}$.

Therefore

$$\mathfrak{S}_{s,k}(N) \geq \frac{1}{2} \prod_{p \leq C_{k,s}} T(p) \geq \frac{1}{2} \prod_{p \leq C_{k,s}} \frac{1}{p^{\gamma(p)}}.$$

So the singular series is $\mathfrak{S}_{s,k}(N) \gg_{s,k} 1$ uniformly on N. Finally,

Theorem 35.4. *For $s \geq 2^k + 1$, we have*

$$r_{s,k}(N) = \kappa_{k,s} \mathfrak{S}_{k,s}(N) N^{s/k - 1} + O_{k,s}(N^{s/k-1-\delta}),$$

where

(1) $0 < \delta \ll_k 1$,

(2) $\kappa_{k,s} = \Gamma\Big(1 + \dfrac{1}{k}\Big)^s \Gamma\Big(\dfrac{s}{k}\Big)^{-1} \asymp_{k,s} 1$,

(3) $\mathfrak{S}_{k,s}(N)$ *is the singular series defined before,*

(4) $\mathfrak{S}_{k,s} \asymp_{k,s} 1$.

In particular, for $N \gg_{k,s} 1$, $r_{s,k}(N) > 0$.

Index