Cor 6.4 (PNT in arithmetic progressions)

Let $a \in (\mathbb{Z}/q\mathbb{Z})^{\times}$. Then,

$$\#\{p \le x \mid p \equiv a \bmod q\} \sim \frac{1}{\varphi(q)} \cdot \#\{p \le x\} \text{ for } x \to \infty.$$

Pf Let
$$g(s) := \sum_{\chi} \left(-\frac{L'(s,\chi)}{L(s,\chi)}\right) \cdot \frac{1}{\chi(a)}$$
$$= \sum_{n=p^k} \frac{\sum_{\chi} \chi(\frac{n}{a}) \log p}{n^s}$$
$$= \sum_{\substack{n=p^k: \\ n \equiv a \bmod q}} \frac{\varphi(q) \log p}{n^s}$$

It is hol. in $\{\mathrm{Re}(s) \ge 1\}$ except for a simple pole at $s=1$ with residue 1 (coming from $-\frac{L'(s,\chi_0)}{L(s,\chi_0)}$, which comes from the simple pole of $L(s,\chi_0)$ at $s=1$).

Wiener - Ikehara $\Rightarrow$
$$\sum_{\substack{n=p^k \le x: \\ n \equiv a \bmod q}} \varphi(q) \log p \sim x.$$
$$\parallel$$
$$\varphi(q) \sum_{\substack{p \le x: \\ p \equiv a \bmod q}} \log p + O(x^{1/2} (\log x)^2)$$

Proceed as for the PNT (cf. Problem 3 on Pset 1). $\square$

Cor 6.5

Let $S = \{x^2+y^2 \mid x,y \in \mathbb{Z}\}$.

We have $\#\{n \in S \mid n \le x\} \sim C \cdot \frac{x}{\sqrt{\log x}}$

for some constant $C>0$.

Pf Algebraic NT tells us that $1 \le n \in S$ if and only

if n is divisible by each prime $p \equiv 3 \bmod 4$ an even number of times.

$$\Rightarrow D(\mathbb{1}_S, s) = \prod_{p \not\equiv 3 \bmod 4} \underbrace{\frac{1}{1-\frac{1}{p^s}}}_{1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots} \cdot \prod_{p \equiv 3 \bmod 4} \underbrace{\frac{1}{1-\frac{1}{p^{2s}}}}_{1+\frac{0}{p^s}+\frac{1}{p^{2s}}+\dots}$$

Let χ_1 be the nontriv. character mod 4.

$$\chi_1(x) = \begin{cases} 1, & x \equiv 1 \bmod 4, \\ -1, & x \equiv 3 \bmod 4. \end{cases}$$

$$L(s,\chi_0) \cdot L(s,\chi_1) = \prod_{p \equiv 1 \bmod 4} \frac{1}{\left(1-\frac{1}{p^s}\right)^2} \cdot \prod_{p \equiv 3 \bmod 4} \frac{1}{\left(1-\frac{1}{p^s}\right)\left(1+\frac{1}{p^s}\right)}$$

$$= \prod_{p \equiv 1} \frac{1}{\left(1-\frac{1}{p^s}\right)^2} \cdot \prod_{p \equiv 3} \frac{1}{1-\frac{1}{p^{2s}}} .$$

$$\Rightarrow \frac{D(\mathbb{1}_S, s)^2}{L(s,\chi_0)L(s,\chi_1)} = \frac{1}{\left(1-\frac{1}{2^s}\right)^2} \cdot \prod_{p\equiv 1} 1 \cdot \prod_{p \equiv 3} \frac{1}{1-\frac{1}{p^{2s}}},$$

which converges for $\mathrm{Re}(s) > \frac{1}{2}$.

$\Rightarrow$ $D(\mathbb{1}_S, s)^2$ is hol. in $\{\mathrm{Re}(s) \geq 1\}$ except for a simple pole at $s = 1$.

The result follows from Kato's extension of Wiener–Ikehara. $\square$

7. Functional equations

We'll generalise the fct. eq. for $\zeta(s)$ to fct. eq. for $L(s,\chi)$.

First, Poisson summation with a twist:

Lemma 7.1 Let $c : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be any function and let $f \in \mathcal{S}(\mathbb{R})$ (for example). Then,

$$q \cdot \sum_{x \in \mathbb{Z}} c(x \bmod q)\, f(x) = \sum_{t \in \mathbb{Z}} \hat{c}(t \bmod q)\, \hat{f}\left(\frac{t}{q}\right)$$

with $\hat{c} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ the discrete Fourier transform given by $\hat{c}(t) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} c(x)\, e^{2\pi i x t/q}$.

Ex

$$c(x) = 1 \ \forall x \Rightarrow \hat{c}(t) = \begin{cases} 1, & t \equiv 0 \bmod q, \\ 0, & \text{otherwise.} \end{cases}$$

$\rightsquigarrow$ Claim = Poisson summation.

Pf By linearity, it suffices to consider $c = \mathbb{1}_{\{a \bmod q\}}$.

Then, $\mathrm{LHS} = q \sum_{x \equiv a \bmod q} f(x) \underset{x = qy + a}{=} q \cdot \sum_{y \in \mathbb{Z}} g(y)$

with $g(y) = f(qy + a)$.

Poisson summation: $q \sum_{y} g(y) = q \sum_{t \in \mathbb{Z}} \hat{g}(t) = \sum_{t \in \mathbb{Z}} e^{2\pi i a t/q}\, \hat{f}\left(\frac{t}{q}\right)$

$= \mathrm{RHS}$. □

Rmk $\hat{\hat{c}}(x) = q \cdot c(-x)$.

Lemma 7.2 Let χ be a primitive character mod q, extended to $\mathbb{Z}/q\mathbb{Z}$ by 0 (outside $(\mathbb{Z}/q\mathbb{Z})^\times$). Its discrete Fourier transform $\hat{\chi}$ satisfies $\hat{\chi}(t) = \overline{\chi(t)} \cdot \hat{\chi}(1)$ for all $t \in \mathbb{Z}/q\mathbb{Z}$. (So the d.F.T. of χ is essentially its complex conjugate.)

Def We write $\tau(\chi) := \hat{\chi}(1) = \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^\times} \chi(x) e^{2\pi i x/q}$.
This is called a *Gauß sum*.

Pf Case 1: $t \in (\mathbb{Z}/q\mathbb{Z})^\times$

$$\text{LHS} = \sum_{x \bmod q} \chi(x) e^{2\pi i x t/q} \underset{xt=y}{=} \sum_{y \bmod q} \underbrace{\chi\left(\frac{y}{t}\right)}_{= \frac{\chi(y)}{\chi(t)} = \overline{\chi(t)} \cdot \chi(y)} e^{2\pi i y/q}$$

$$= \overline{\chi(t)} \cdot \sum_{y \bmod q} \chi(y) e^{2\pi i y \cdot 1/q} = \text{RHS}.$$

Case 2: $t \notin (\mathbb{Z}/q\mathbb{Z})^\times$

Let $d = \gcd(t, q)$, $t' = \frac{t}{d}$, $q' = \frac{q}{d}$.

$$\Rightarrow \text{LHS} = \sum_{x \bmod q} \chi(x) e^{2\pi i x t'/q'}$$

$$= \sum_{x' \bmod q'} \Big(\sum_{\substack{x \bmod q: \\ x \equiv x' \bmod q'}} \chi(x) \Big) e^{2\pi i x' t'/q'}$$

$$= 0 = \text{RHS}$$ according to the following Lemma. $\square$

Lemma 7.3 Let χ be a ~~[illegible]~~ character mod q, let $q' \mid q$ ~~[illegible]~~. Then,

$$\sum_{\substack{x \bmod q: \\ x \equiv x' \bmod q'}} \chi(x) = 0 \qquad \text{for all } x' \in \mathbb{Z}/q'\mathbb{Z}.$$

Pf This is clear if $x' \notin (\mathbb{Z}/q'\mathbb{Z})^\times$.

~~[illegible]~~

Otherwise, take any $x_0 \in (\mathbb{Z}/q\mathbb{Z})^\times$ with $x \equiv 1 \bmod q'$.

Mult. by x_0 permutes the summands.

The claim follows, unless $\chi(x_0) = 1$ for all x_0 as above.

But in that case, $\chi(x_1) = \chi(x_2)$ for any $x_1 \equiv x_2 \bmod q'$, which implies that χ is induced by a char. of q', hence not primitive. $\square$

Cor 7.4 $|\tau(\chi)| = \sqrt{q}$ for any primitive character χ mod q.

Pf $\hat{\chi}(t) = \tau(\chi) \cdot \overline{\chi}(t) \quad \forall t$

$$\Rightarrow \underset{\substack{\| \\ q \cdot \chi(-x)}}{\hat{\hat{\chi}}(x)} = \tau(\chi) \cdot \hat{\overline{\chi}}(x) = \tau(\chi) \cdot \overline{\hat{\chi}}(-x)$$

$$= \underbrace{\tau(\chi) \cdot \overline{\tau(\chi)}}_{|\tau(\chi)|^2} \cdot \underbrace{\overline{\overline{\chi}}(-x)}_{\chi(-x)}. \qquad \square$$