The Correction Factors in Artin Type Problems

Milad Fakhari

Alberta Number Theory Days XIII

November 6, 2021

History

- Gauss; The largest period of the decimal expansion of $1/p$.

Example

$1/7$ has period length 6: $\frac{1}{7} = 0.142857\ 142857...$
$1/11$ has period length of only 2: $\frac{1}{11} = 0.09\ 09...$

- The largest period occurs if and only if 10 has order $p-1$ mod p.
- We may study primes p such that a given integer a is a primitive root mod p i.e., $\langle a \bmod p\rangle = \mathbb{F}_p^\times$.

History

- In 1927, Emil Artin conjectured that for a non-zero integer $a \neq \pm 1$, the density of primes p such that a is a primitive root modulo p is

$$A_a = \prod_{q \text{ prime}} \left(1 - \frac{1}{[K_q : \mathbb{Q}]}\right).$$

  Here $K_q = \mathbb{Q}(\zeta_q, \sqrt[q]{a})$.
- Unexpected results appeared in calculations done by D. H. Lehmer and E. Lehmer in 1957.

- To deal with the discrepancies, Artin introduced a correction factor.

Conjecture (Emil Artin)

The conjectured density is $\delta_a = E(D) \cdot A_a$ *with*

$$E(D) = 1 - \mu(|D|) \prod_{q|2D} \frac{1}{[K_q : \mathbb{Q}] - 1},$$

when $D = \mathrm{disc}(K_2/\mathbb{Q}) \equiv 1 \pmod 4$. *Otherwise* $E(D) = 1$.

History

Lemma

The integer a is a primitive root modulo p if and only if p does not split completely in K_q for all primes $q \mid p-1$.

- In 1967, by the Chebotarev density theorem, Hooley proved under GRH

$$\delta_a = \sum_{n=1}^{\infty} \frac{\mu(n)}{[K_n : \mathbb{Q}]}.$$

- We call a problem an *Artin type problem* if we can tackle it by Hooley's method.

Artin Type Problems

Cyclicity Problem (Serre)

Find an asymptotic formula for the number of primes $p \leq x$ for which the group of rational points modulo p of a given elliptic curve is cyclic.

- In 1976, J. P. Serre proved, under GRH,

$$\delta_E = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]}.$$

Artin Type Problems

Titchmarsh Divisor Problem attached to a family of Kummer fields:

- $\tau_a(p) := \#\{n \in \mathbb{N}; p \text{ splits completely in } K_n = \mathbb{Q}(\zeta_n, a^{1/n})\}$.

Theorem (A. Felix and R. Murty, 2012)

Under GRH, we have

$$\sum_{p \le x} \tau_a(p) \sim \left(\sum_{n \ge 1} \frac{1}{[K_n : \mathbb{Q}]} \right) \cdot \mathrm{li}(x),$$

as $x \to \infty$.

- We can consider primes p lie in a given arithmetic progression.

Goals

- The goal of this talk is to construct a method to find the product formula for the summations appear in the Artin type problems.
- We first study the character sums method introduced by Lenstra, Moree, Stevenhagen.
- Modify this method in an effective way to cover more Artin type problems such as Titchmarsh Divisor problem and Titchmarsh Divisor problem for primes in a given arithmetic progression.

Character Sums Method

Lenstra, Moree, Stevenhagen (2014).

- Let $G = \varprojlim G(n)$ and $A = \varprojlim A(n)$ with the exact sequence

$$1 \longrightarrow G \xrightarrow{r} A \xrightarrow{\chi} \mu_2 \longrightarrow 1.$$

- Let $A = \prod_p A_p$, where $A_p = \varprojlim A(p^i)$.
- A is equipped with a normalized Haar measure $\nu_A = \prod_p \nu_{A_p}$.
- Suppose S_p has positive measure in A_p and $S = \prod_p S_p \subset A$.

Theorem (Lenstra-Moree-Stevenhagen, 2014)

$$\frac{\nu_A(G \cap S)}{\nu_A(G)} = \left(1 + \frac{1}{\nu_A(S)} \int_S \chi d\nu_A\right) \frac{\nu_A(S)}{\nu_A(A)}.$$

Modified Character Sums Method

- Let $G = \varprojlim G(n)$ and $A = \varprojlim A(n)$ with the exact sequence

$$1 \longrightarrow G \xrightarrow{r} A \xrightarrow{\chi} \mu_m \longrightarrow 1.$$

- Finding the product form of an absolutely convergence summation

$$\sum_{n \geq 1} \frac{g(n)}{\# G(n)},$$

where $g(n)$ is a real multiplicative function.

Theorem (F.)

$$\sum_{n \geq 1} \frac{g(n)}{\# G(n)} = \sum_{i=0}^{m-1} \int_A \tilde{g} \chi^i d\nu_A,$$

where $\tilde{g} = \sum_{n \geq 1} g(n) 1_{\ker \varphi_{A,n}}$ *with* $\varphi_{A,n} : A \to A(n)$.

Modified Character Sums Method

Corollary (F.)

Let g be multiplicative, $A \cong \prod_p A_p$, where $A_p = \varprojlim A(p^i)$. Assume $\chi = \prod_p \chi_p$, where $\chi_p : A_p \to \mu_m$. Let

$$\tilde{g}_p = \sum_{k \geq 0} g(p^k) 1_{\ker \varphi_{p^k}},$$

where $\varphi_{p^k} : A_p \to A(p^k)$, such that $\tilde{g} = \prod_p \tilde{g}_p$. If $\int_A \tilde{g}\, d\nu_A \neq 0$, then

$$\sum_{n=1}^{\infty} \frac{g(n)}{\# G(n)} = \left(1 + \sum_{i=1}^{m-1} \prod_p \frac{\int_{A_p} \tilde{g}_p \chi_p^i d\nu_{A_p}}{\int_{A_p} \tilde{g}_p d\nu_{A_p}}\right) \prod_p \int_{A_p} \tilde{g}_p d\nu_{A_p}.$$

Modified Character Sums Method

Next, we set some conditions on G and A such that as a result we get an explicit character χ.

- Let $G = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$.
- Let $\zeta_n \in K_n$ and $K_2 \supset K$, where K is a quadratic field.
- Let

  $$A \xrightarrow{\gamma} \hat{\mathbb{Z}}^{\times} \qquad \text{and} \qquad A \xrightarrow{\psi} \mu_2$$

  with commutative diagrams:

$$\begin{tikzcd} G \arrow[r] \arrow[d, "r"'] & \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) \arrow[d, "\cong"] \\ A \arrow[r, "\gamma"] & \hat{\mathbb{Z}}^{\times} \end{tikzcd} \qquad \text{and} \qquad \begin{tikzcd} G \arrow[rr] \arrow[d, "r"'] & & \mathrm{Gal}(K/\mathbb{Q}) \arrow[d, "\simeq"] \\ A \arrow[rr, "\psi"] \arrow[dr] & & \mu_2 \\ & A(2) \arrow[ur] & \end{tikzcd}$$

Modified Character Sums Method

Theorem (F.)

There exists a non-trivial quadratic character $\chi : A \to \mu_2$ such that:
(i) $r(G) \subset \ker \chi$.
(ii) $\chi = \prod_p \chi_p$, *where* χ_p *is a certain quadratic character of* A_p.
Let $\varphi_{p^k} : A_p \to A(p^k)$ *and* $D = \mathrm{disc}_{\mathbb{Q}}(K)$. *Then,*
(iii) For odd primes $p \nmid D$, $\chi_p = 1_{A_p}$.
(iv) If $p \mid D$ *and* p *is odd, then* $\chi_p \neq 1_{A_p}$ *and* $\chi_p|_{\ker \varphi_{p^k}} = 1_{\ker \varphi_{p^k}}$ *for all* $k \geq 1$.
(v) If D *is odd, then* $\chi_2 \neq 1_{A_2}$ *and* $\chi_2|_{\ker \varphi_{2^k}} = 1_{\ker \varphi_{2^k}}$ *for all* $k \geq 1$.
(vi) If $4 \parallel D$ *and* $\zeta_4 = i \notin K_2$, *then* $\chi_2 \neq 1_{A_2}$, $\chi_2|_{\ker \varphi_2} \neq 1_{\ker \varphi_2}$, *and* $\chi_2|_{\ker \varphi_{2^k}} = 1_{\ker \varphi_{2^k}}$ *for all* $k \geq 2$.
(vii) If $8 \parallel D$ *and* $\zeta_8 \notin K_4$, *then* $\chi_2 \neq 1_{A_2}$, $\chi_2|_{\ker \varphi_{2^k}} \neq 1_{\ker \varphi_{2^k}}$ *for* $k = 1, 2$, *and* $\chi_2|_{\ker \varphi_{2^k}} = 1_{\ker \varphi_{2^k}}$ *for all* $k \geq 3$.

Modified Character Sums Method

Recall:

Corollary (F.)

Let g be multiplicative, $A \cong \prod_p A_p$, where $A_p = \varprojlim A(p^i)$. Assume $\chi = \prod_p \chi_p$, where $\chi_p : A_p \to \mu_m$. Let

$$\tilde{g}_p = \sum_{k \geq 0} g(p^k) 1_{\ker \varphi_{p^k}},$$

where $\varphi_{p^k} : A_p \to A(p^k)$, such that $\tilde{g} = \prod_p \tilde{g}_p$. If $\int_A \tilde{g} \, d\nu_A \neq 0$, then

$$\sum_{n=1}^{\infty} \frac{g(n)}{\# G(n)} = \left(1 + \sum_{i=1}^{m-1} \prod_p \frac{\int_{A_p} \tilde{g}_p \chi_p^i \, d\nu_{A_p}}{\int_{A_p} \tilde{g}_p \, d\nu_{A_p}}\right) \prod_p \int_{A_p} \tilde{g}_p \, d\nu_{A_p}.$$

Modified Character Sums Method

Corollary (F.)

With assumptions of the above corollary, let G and A be as described above. If $m = 2$, $\zeta_4 \notin K_2$, $\zeta_8 \notin K_4$, and $\int_A \tilde{g}\, d\nu_A \neq 0$, then

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} =$$

$$\left(1 + \prod_{p|2D} \frac{\sum_{k\geq \ell} g(p^k)/\#A(p^k)}{1+\sum_{k\geq 1} g(p^k)/\#A(p^k)}\right) \prod_{p} \left(1 + \sum_{k\geq 1} \frac{g(p^k)}{\#A(p^k)}\right),$$

where in the product on primes dividing $2D$, we have $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

- Let $K_n = \mathbb{Q}(\sqrt[n]{a}, \zeta_n)$, where $|a|$ is not a perfect power.
- Let
$$r : G \to A = \left\{ \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} ;\ b \in \hat{\mathbb{Z}} \text{ and } d \in \hat{\mathbb{Z}}^{\times} \right\}.$$

Thus,

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} =$$
$$\left(1 + \prod_{p \mid 2D} \frac{\sum_{k \geq \ell} g(p^k)/p^{2k-1}(p-1)}{1 + \sum_{k \geq 1} g(p^k)/p^{2k-1}(p-1)}\right) \prod_p \left(1 + \sum_{k \geq 1} \frac{g(p^k)}{p^{2k-1}(p-1)}\right),$$

where $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

Serre Family

- Let $K_n = \mathbb{Q}(E[n])$ be the n-division field of an elliptic curve E.
- Let
$$\rho_E : \mathrm{Gal}(\mathbb{Q}^{\mathrm{tor}}/\mathbb{Q}) \to \mathrm{GL}_2(\hat{\mathbb{Z}}) = \varprojlim \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$
- We name an elliptic curve a *Serre curve* if $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{Img}\,\rho_E] = 2$.

Therefore, for a Serre curve, we have

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \left(1 + \prod_{p|2D} \frac{\sum_{k\geq\ell} g(p^k)/p^{4k-3}(p^2-1)(p-1)}{1+\sum_{k\geq1} g(p^k)/p^{4k-3}(p^2-1)(p-1)}\right) \prod_{p}\left(1 + \sum_{k\geq 1} \frac{g(p^k)}{p^{4k-3}(p^2-1)(p-1)}\right),$$

where $\ell = 1$ for odd primes and for prime 2 we have $\ell = 1$ if D is odd, $\ell = 2$ if $4 \parallel D$, and $\ell = 3$ if $8 \parallel D$.

Generalization

- $B = \varprojlim B(n) \cong \prod_p B_p$ with a surjective homomorphism from A to B.

Theorem (F.)

Let $\chi : A \to \mu_2$ be a surjective continuous homomorphism. Let $H \subset B$ and $H(n)$ be the projection of H in $B(n)$. Let $\tilde{g} = \sum_{n\geq 1} g(n) 1_{\varphi_{A,n}^{-1}(H(n))}$ where $\varphi_{A,n} : A \to B(n)$. If g is real multiplicative, $A \cong \prod_p A_p$, $\chi = \prod_p \chi_p$, $\tilde{g} = \prod_p \tilde{g}_p$, and $\int_A \tilde{g}\, d\nu_A \neq 0$, then

$$\frac{1}{\nu_A(\ker\chi)} \sum_{n\geq 1} g(n)\nu_A(\varphi_{A,n}^{-1}(H(n)) \cap \ker\chi) = \left(\prod_p \int_{A_p} \tilde{g}_p\, d\nu_{A_p}\right)\left(1 + \prod_p \frac{\int_{A_p} \tilde{g}_p \chi_p\, d\nu_{A_p}}{\int_{A_p} \tilde{g}_p\, d\nu_{A_p}}\right),$$

where $\tilde{g}_p = \sum_{k\geq 0} g(p^k) 1_{\varphi_{p^k}^{-1}(H(p^k))}$.

Application

- In the Titchmarsh Divisor Problem attached to a Kummer family for primes in a given arithmetic progression ($p \equiv \ell \pmod{f}$), we have

$$\sum_{p \leq x} \tau_{a,f,\ell}(p) \sim \sum_{n \geq 1} \frac{c_\ell(n)}{[K_n(\zeta_f) : \mathbb{Q}]} \cdot \mathrm{li}(x)$$

as $x \to \infty$, where

$$c_\ell(n) = \begin{cases} 1 & \sigma_\ell\big|_{K_n \cap \mathbb{Q}(\zeta_f)} = \mathrm{Id}_{K_n \cap \mathbb{Q}(\zeta_f)}, \\ 0 & \text{otherwise.} \end{cases}$$

- To apply the generalization, define the homomorphisms

$$\varphi_{A,n} : A \to A(n) \times (\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times,$$

and let

$$H(n) = \{(\mathcal{I}_{2\times 2}(\mathbb{Z}/n\mathbb{Z}), \bar{\ell})\} \subset A(n) \times (\hat{\mathbb{Z}}/f\hat{\mathbb{Z}})^\times.$$

Thank You

The Galois elements in $G(n)$ are identified by their actions on the multiplicative group $R_n = \{\alpha \in \bar{\mathbb{Q}}^\times;\ \alpha^n \in \langle a \rangle\}$. This yields the injective homomorphisms

$$r_n : G(n) \to A(n) := \mathrm{Aut}_{\mathbb{Q}^\times \cap R_n}(R_n).$$

Thus, we have the injective homomorphism

$$r : G = \varprojlim G(n) \to A = \varprojlim A(n).$$