C3.10 Additive and Combinatorial NT
Lecture 5: Gauss sums and integrals

Joni Teräväinen

Mathematical Institute

Circle method

Recall we need to prove three things to solve Waring's problem:

Prop. 3.2.1 (Major arcs)

Let $s \geq 2k+1$, $X = \{n^k : \ n \leq N^{1/k}\}$. Then,

$$\int_{\mathfrak{M}} \widehat{1_X}(\theta)^s e(N\theta)\, d\theta = \mathfrak{S}_{k,s}(N) N^{s/k-1} + o(N^{s/k-1}).$$

Prop. 3.2.2 (Minor arcs)

Let $s \geq 100^k$. Then,

$$\int_{\mathfrak{m}} \widehat{1_X}(\theta)^s e(N\theta)\, d\theta = o(N^{s/k-1}).$$

Prop. 3.1.1 (Singular series)

Let $s \geq k^4$. Then $1 \ll \mathfrak{S}_{k,s}(N) \ll 1$ (i.e., $\mathfrak{S}_{k,s}(N) \asymp 1$).

Gauss sums

We now begin to study $\widehat{1_X}(\theta)$ for $\theta \in \mathfrak{M}$. For $\theta = a/q$, we have

$$\widehat{1_X}(\theta) = \sum_{n \le N^{1/k}} e(-an^k/q) = \frac{N^{1/k}}{q} \sum_{b \in \mathbb{Z}/q\mathbb{Z}} e(-ab^k/q) + O(q).$$

Thus, we are lead to study

Definition (Gauss sum)

For $a \in \mathbb{Z}/q\mathbb{Z}$, define

$$G_{a,q} = \frac{1}{q} \sum_{b \in \mathbb{Z}/q\mathbb{Z}} e(-ab^k/q).$$

Trivial bound: $|G_{a,q}| \le 1$. For $a \in (\mathbb{Z}/q\mathbb{Z})^*$, expect cancellation.

Prop. 5.0.1 (Pointwise bound for Gauss sums)

Let $a \in (\mathbb{Z}/q\mathbb{Z})^*$. Then $|G_{a,q}| \ll q^{-1/k+o(1)}$.

This is optimal up to the $o(1)$ in the exponent (Sheet 2).

Multiplicativity of Gauss sums

The first step in proving Prop. 5.0.1 is a multiplicativity relation.

Lemma 5.1.1

Let $q_1, q_2 \geq 1$ be coprime and $a_i \in (\mathbb{Z}/q_i\mathbb{Z})^*$. Then

$$G_{a_1,q_1} G_{a_2,q_2} = G_{a_1 q_2 + a_2 q_1, q_1 q_2}.$$

Proof. By making the changes of variables $x_1' = q_2 x_1$, $x_2' = q_1 x_2$,

$$G_{a_1,q_1} G_{a_2,q_2} = \frac{1}{q_1 q_2} \sum_{x_1' \in \mathbb{Z}/q_1\mathbb{Z}} \sum_{x_2' \in \mathbb{Z}/q_2\mathbb{Z}} e(-\frac{a_1}{q_1}(q_2 x_1')^k - \frac{a_2}{q_2} \cdot (q_1 x_2')^k).$$

By the binomial theorem,

$$\frac{a_1}{q_1}(q_2 x_1')^k + \frac{a_2}{q_2} \cdot (q_1 x_2')^k \equiv \left(\frac{a_1}{q_1} + \frac{a_2}{q_2}\right)(q_2 x_1' + q_1 x_2')^k \pmod 1$$

$$\Rightarrow G_{a_1,q_1} G_{a_2,q_2} = \frac{1}{q_1 q_2} \sum_{x_1' \in \mathbb{Z}/q_1\mathbb{Z}} \sum_{x_2' \in \mathbb{Z}/q_2\mathbb{Z}} e(-\frac{a_1 q_2 + a_2 q_1}{q_1 q_2}(q_2 x_1' + q_1 x_2')^k).$$

Since each element of $\mathbb{Z}/(q_1 q_2\mathbb{Z})$ has a unique representation as $q_2 x_1' + q_1 x_2'$, the RHS is $G_{a_1 q_2 + a_2 q_1, q_1 q_2}$. □

Reduction to prime power moduli

We now claim that it suffices to prove

Lemma 5.1.2 (prime power case)

Let q be a prime power and $a \in (\mathbb{Z}/q\mathbb{Z})^*$. Then

$$|G_{a,q}| \leq 6kq^{-1/k}. \tag{1}$$

Proof that Lemma 5.1.2 implies Prop. 5.0.1: By the multiplicativity relation and (1), for any q and a coprime to q,

$$|G_{a,q}| \leq (6k)^{\omega(q)} q^{-1/k},$$

where $\omega(q)$ is the number of distinct prime factors of q. If $\omega(q) = o(\log q)$, we are done. Note that for any $C \geq 2$ we have

$$C^{\omega(q)-C} \leq q,$$

so $\omega(q) \leq C + (\log q)/(\log C)$. Then let $C \to \infty$. $\square$

The prime power case

We first need a few lemmas about the number of solutions to congruences in $\mathbb{Z}/q\mathbb{Z}$.

Lemma 5.3.2

If q is an odd prime power, there are $\leq k$ kth roots of unity in $(\mathbb{Z}/q\mathbb{Z})^*$. If q is a power of two, there are $\leq 2k$ kth roots of unity in $(\mathbb{Z}/q\mathbb{Z})^*$

Proof. By [Part A NT], if q is an odd prime power then $(\mathbb{Z}/q\mathbb{Z})^*$ is cyclic. Note that in a cyclic group $\mathbb{Z}/m\mathbb{Z}$ there are $\leq k$ solutions to $kx = 0$.

If $q = 2^\nu$ is a power of two, then by [Part A NT] $(\mathbb{Z}/q\mathbb{Z})^*$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\nu-2}\mathbb{Z})$, so there are $\leq 2k$ kth roots of unity. □

The prime power case

The second lemma we need is

Lemma 5.3.3

Let $k \geq 3$, and let q be a prime power. Then the number of solutions to $x^k = y^k$ in $\mathbb{Z}/q\mathbb{Z}$ is $\leq 8kq^{2(1-1/k)}$.

Proof. Let $x = p^\lambda t$, $y = p^\mu u$, $0 < t < p^{\nu-\lambda}$, $0 < u < p^{\nu-\mu}$, where t, u are coprime to p. Then, either (1) $\lambda = \mu$ and the congruence reduces to $t^k \equiv u^k \pmod{p^{\nu-k\lambda}}$, or (2) $\mu, \lambda \geq \nu/k$.

The number of solutions satisfying (2) is $\leq p^{2\nu(1-1/k)}$.

Let $N_{t,\lambda}$ be the number of solutions satisfying (1) with fixed t and λ. By Lemma 5.3.2, there are $\leq 2k$ choices for $u \pmod{p^{\nu-k\lambda}}$. Thus $N_{t,\lambda} \leq 2kp^{(k-1)\lambda}$. Summing over t, we get $\sum_t N_{t,\lambda} \leq 2kp^{\nu+(k-2)\lambda}$. Then sum over $\lambda < \nu/k$ (geometric series) to get

$$\sum_{t,\lambda} N_{t,\lambda} \leq 4kp^{\nu+(k-2)\nu/k} = 4kp^{2\nu(1-1/k)}. \qquad \square$$

The prime power case

Proof of Lemma 5.1.2 As in the Weyl sum estimate, we square out the sum to get a simpler expression.

Case 1: $k = 2$. Then, substituting $y = x + h$,

$$|G_{a,q}|^2 = \frac{1}{q^2} \sum_{x,y \in \mathbb{Z}/q\mathbb{Z}} e(\frac{a(y^2 - x^2)}{q}) = \frac{1}{q^2} \sum_{h \in \mathbb{Z}/q\mathbb{Z}} e(\frac{ah^2}{q}) \sum_{x \in \mathbb{Z}/q\mathbb{Z}} e(\frac{2ahx}{q}).$$

Apply orthogonality to the inner sum and the triangle inequality to the outer one to get

$$|G_{a,q}|^2 \leq \frac{1}{q} \sum_{h \in \mathbb{Z}/q\mathbb{Z}} 1_{2ah \equiv 0 \pmod{q}} \leq \frac{2}{q},$$

since a is coprime to q.

The prime power case

Case 2: $k \geq 3$. Let $q = p^\nu$. Note that $G_{a,q} = G_{ab^k,q}$ for b coprime to q. Also note that any $x \in (\mathbb{Z}/q\mathbb{Z})^*$ has $\leq 2k$ representations as ab^k (Lemma 5.3.2).Hence,

$$p^{\nu-1}(p-1)|G_{a,p^\nu}|^2 = \sum_{b \in (\mathbb{Z}/p^\nu\mathbb{Z})^*} |G_{ab^k,p^\nu}|^2 \leq 2k \sum_{r \in \mathbb{Z}/p^\nu\mathbb{Z}} |G_{r,p^\nu}|^2.$$

The RHS expands out as

$$\frac{2k}{p^{2\nu}} \sum_{x,y} \sum_{r} e(-r(x^k - y^k)/p^\nu) = \frac{2k}{p^\nu} |\{(x,y) \in (\mathbb{Z}/p^\nu\mathbb{Z}) : \ x^k = y^k\}|,$$

and by Lemma 5.1.2 this is $\leq 2k \cdot 8kp^{\nu-2\nu/k}$ .Since $\frac{1}{2}p \leq p-1$, we get

$$\frac{1}{2}p^\nu |G_{a,p^\nu}|^2 \leq 16k^2 p^{\nu-2\nu/k},$$

and taking square roots the claim follows. □

Integrals

Gauss sums are p-adic analogues of $\widehat{1_X}(\theta)$. We will also need to bound the Archimedean analogues of $\widehat{1_X}(\theta)$:

Definition

$$I(t) := \int_0^{N^{1/k}} e(-tx^k)\, dx.$$

Lemma 5.4.1

We have $|I(t)| \ll |t|^{-1/k}$.

Proof. By symmetry, can assume $t > 0$. Substitute $w = tx^k$, $dx = (1/k)w^{1/k-1}t^{-1/k}$ to get

$$I(t) = \frac{1}{k} t^{-1/k} \int_0^{Nt} e(-w) w^{-1+1/k}\, dw.$$

Now, suffices to show that uniformly for $Z > 0$ we have

$$\left| \int_0^{Z} e(-w) w^{-1+1/k}\, dw \right| = O(1).$$

This is true by integration by parts. □

Waring's problem (mod p)

We apply Gauss sums to prove

Lemma 5.2.2

Let $p \geq k^4$. Then for any N there exist $x_1, x_2, x_3 \in \mathbb{Z}/p\mathbb{Z}$, not all zero, such that $N \equiv x_1^k + x_2^k + x_3^k \pmod{p}$.

Proof. Let T be the number of such triples (x_1, x_2, x_3). Then by orthogonality

$$T = \frac{1}{p} \sum_{a, x_1, x_2, x_3 \in \mathbb{Z}/p\mathbb{Z}} e(a(x_1^k + x_2^k + x_3^k - N)/p) = p^2 \sum_a G_{a,p}^3 e(aN/p).$$

Separating the contribution of $a = 0$, we get

$$T \geq p^2 - p^2 \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} |G_{a,p}|^3.$$

Waring's problem (mod p)

We now have

$$T \geq p^2 - p^2 \sum_{(a \in \mathbb{Z}/p\mathbb{Z})^*} |G_{a,p}|^3.$$

In the case where p is a prime, we have the sharper bound $|G_{a,p}| \leq kp^{-1/2}$ (Lemma 5.2.1), so

$$\begin{aligned}
\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} |G_{a,p}|^3 &\leq \frac{k}{\sqrt{p}} \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} |G_{a,p}|^2 \\
&= \frac{k}{\sqrt{p}} \left(\frac{1}{p} |\{(x,y) : \ x^k \equiv y^k \pmod{p}\}| - 1 \right) \\
&\leq \frac{k(k-1)}{p^{1/2}}.
\end{aligned}$$

Thus, $T \geq p^2 - k(k-1)p^{3/2}$, and this is ≥ 2 for $p \geq k^4$. $\square$