A LEMMA IN ANALYTIC NUMBER THEORY

PENG GAO

Let p be a prime number and $q = p^n$. In Trevor's talk, the following theorem is proved:

Theorem 0.1. *Let E be an elliptic curve over $\mathbb{K}$, $[\mathbb{K} : \mathbb{Q}] = d$, and let $P \in E(\mathbb{K})$ be a point of order q. Then*

$$q \leq 2(5^d + 1) \cdot 129(3d)^6. \tag{0.1}$$

In order to prove the above theorem, he needs the following lemma(Lemma 5.2, [3]):

Lemma 0.1. *Let A, B be two intervals of $\{1, \cdots, q-1\}$, if*

$$|A| \cdot |B| \geq C_p \cdot p^{3n/2},$$

where $C_2 = 8\sqrt{2}$ and $C_p = 8, p > 2$. Then there exists $y \in A, z \in B$ such that $yz \equiv -1(modq)$.

We now present a proof of the following weaker result of Parent(Lemma 7, [2]), we note here this weaker result allows us to prove Theorem 0.1 with the constant 129 in (0.1) being replaced by C^2 where C is defined below(see also Corollary 6, [2]).

Lemma 0.2. *Let A, B be two intervals of $\{1, \cdots, q-1\}$, if*

1. $|A|, |B| \geq \max\{11, 2p+1\}$,
2. $(|A| - 11) \cdot (|B| - 11) > 144 + (C/8) \cdot p^{3n/2}$,

where $C = (4096 \cdot \pi^2)/(2\sqrt{2} - 1)$, then there exists $y \in A, z \in B$ such that $yz \equiv -1(modq)$.

Proof. Our proof follows that of [2]. It suffices to prove the assertion for $A' = \{a+1, a+2, \cdots, a+2K\}, B' = \{b+1, b+2, \cdots, b+2K'\}$ with $K = [|A|/2], K' = [|B|/2]$, where $[x]$ denotes the largest integer not exceeding x. Define $\Psi_{A'}, \Psi_{B'} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Q}$ such that

$$\Psi_{A'}(a+k) = \Psi_{A'}(a+2K+1-k) = k/K, 1 \leq k \leq K; \quad \Psi_{A'} = 0 \text{ otherwise};$$
$$\Psi_{B'}(b+k) = \Psi_{B'}(a+2K'+1-k) = k/K', 1 \leq k \leq K'; \quad \Psi_{B'} = 0 \text{ otherwise}.$$

Thus it suffices to show

$$S = \sum_{r(q)}^{*} \Psi_{A'}(r) \cdot \Psi_{B'}(\bar{r}) > 0.$$

Here $\sum^*$ denotes the sum over reduced classes mod q and $\bar{r}r \equiv -1(q)$.

Using the finite Fourier transformation, we get

$$\begin{aligned} S &= \sum_{r(q)}^{*} \left(\frac{1}{q} \sum_{h(q)} \tilde{\Psi}_{A'}(h) e_q(-hr)\right) \cdot \left(\frac{1}{q} \sum_{h'(q)} \tilde{\Psi}_{B'}(h') e_q(-h'\bar{r})\right) \\ &= \frac{1}{q^2} \sum_{h(q)} \sum_{h'(q)} \tilde{\Psi}_{A'}(h) \tilde{\Psi}_{B'}(h') S(-h, -h'; q). \end{aligned} \tag{0.2}$$

Here $e_q(x) = e^{2\pi i x/q}$, $\sum$ denotes the sum over complete classes mod q and

$$\tilde{\Psi}_{A'}(h) = \sum_{m(q)} \Psi_{A'}(m) e_q(mh), \tilde{\Psi}_{B'}(h') = \sum_{m(q)} \Psi_{b'}(m) e_q(mh').$$

Also, $S(-h, -h'; q)$ is the Kloosterman sum,

$$S(-h, -h'; q) = \sum_{r(q)}^{*} e_q(-hr - h'\bar{r}).$$

Date: April 20, 2004.

We note here that $S(0,0;q)=\phi(q)=p^n-p^{n-1}$,

$$S(-h\neq 0,0;q)=\sum_{r=0}^{p^n-1}(e_{p^n}(-hr)-e_{p^{n-1}}(-hr))=\begin{cases}-p^{n-1} & \text{if } h\equiv 0(p^{n-1})\\ 0 & \text{otherwise}\end{cases}$$

In general, one has(see [1])

$$|S(-h\neq 0,-h'\neq 0;q)|\leq 2\sqrt{2}(-h,-h',q)^{1/2}\cdot\sqrt{q},$$

where $(-h,-h',q)$ denotes the largest common divisor of $-h,-h'$ and q.

We now calculate the main term($h=h'=0$) in (0.2) as

$$S_1=\frac{1}{q^2}\tilde{\Psi}_{A'}(0)\tilde{\Psi}_{B'}(0)S(0,0;q)=(1-p^{-1})p^{-n}(K+1)(K'+1)\geq(K+1)(K'+1)/(2q).$$

The contribution in (0.2) of the term $h\neq 0,h'=0$ can be estimated as

$$\begin{aligned}S_2 &= \tilde{\Psi}_{B'}(0)\frac{1}{q^2}\sum_{h(q)}\tilde{\Psi}_{A'}(h)S(-h,0;q)\\ &= -p^{-n-1}(K'+1)\sum_{m(q)}\Psi'_A(m)\sum_{l(p)}{}^{*}e_p(lm).\end{aligned}$$

Here the inner sum is $p-1$ if $m\equiv 0(p)$ and -1 otherwise. Hence the double sum above is

$$-\sum_{m(q)}\Psi'_A(m)+p\sum_{p|m}\Psi'_A(m)\leq -(K+1)+p((2/K)\sum_{i=0}^{[K/p]}(K-ip)).$$

A simple calculation shows this is $\leq p(2+(p/K))-1$. Since $K=[|A|/2]\geq p$, this implies

$$S_2\geq -p^{-n-1}(K'+1)(3p-1)\geq -3q^{-1}(K'+1).$$

Similarly, the contribution in (0.2) of the term $h=0,h'\neq 0$ can be estimated as

$$S'_2\geq -3q^{-1}(K+1).$$

It now remains to estimate the contribution S_3 of the terms $h\neq 0,h'\neq 0$ in (0.2). We have

$$|S_3|=\frac{1}{q^2}\sum_{h=1}^{q-1}\sum_{h'=1}^{q-1}\tilde{\Psi}_{A'}(h)\tilde{\Psi}_{B'}(h')S(-h,-h';q)\leq\frac{2\sqrt{2}q^{1/2}}{q^2}\sum_{h=1}^{q-1}\sum_{h'=1}^{q-1}|\tilde{\Psi}_{A'}(h)\tilde{\Psi}_{B'}(h')|(h,h',q)^{1/2}$$

Direct computation shows

$$|\tilde{\Psi}_{A'}(h)|=\frac{1}{K}\frac{|\sin(\pi hK/q)\cdot\sin(\pi h(K+1)/q)|}{|\sin(\pi h/q)|^2}.$$

We note that for $x\in(0,\pi/2]$, $\sin x\geq 2x/\pi$. Moreover, for $x\in(0,1]$, $|\sin x/x|\leq 1\leq 2/(x+1)$ and for $x\in(1,\infty),|\sin x/x|\leq 1/x\leq 2/(x+1)$. Hence $|\sin x/x|\leq 2/(x+1)$ for $x\in(0,\infty)$. So we get

$$|\frac{\sin(Kx)}{\sin x}|\leq K\frac{\pi}{2}|\frac{\sin(Kx)}{Kx}|\leq\frac{\pi K}{Kx+1},x\in(0,\pi/2].$$

Thus for $0\leq h\leq[q/2]$,

$$|\tilde{\Psi}_{A'}(h)|\leq\frac{1}{K}\frac{\pi}{\pi h/q+K^{-1}}\cdot\frac{\pi}{\pi h/q+(K+1)^{-1}}\leq\frac{1}{K}(\frac{\pi}{\pi h/q+(K+1)^{-1}})^2.$$

Further note $\tilde{\Psi}_{A'}(h), \tilde{\Psi}_{B'}(h')$ and (h, h', q) are invariant under the transformations $h \to q-h, h' \to q-h'$. This gives

$$\begin{aligned}
|S_3| &\leq 8\sqrt{2}q^{-3/2} \sum_{h,h'=1}^{[q/2]} \frac{1}{K}(\frac{\pi}{\pi h/q + (K+1)^{-1}})^2 \frac{1}{K'}(\frac{\pi}{\pi h/q + (K'+1)^{-1}})^2 (h, h', q)^{1/2} \\
&\leq 8\sqrt{2}q^{-3/2}\pi^4 (KK')^{-1} \sum_{k=0}^{n-1} p^{k/2} \sum_{h,h'=1, p^k|h, p^k|h'}^{q} (\frac{1}{\pi h/q + (K+1)^{-1}})^2 (\frac{1}{\pi h/q + (K'+1)^{-1}})^2 \\
&\leq 8\sqrt{2}q^{-3/2}\pi^4 (KK')^{-1} \sum_{k=0}^{n-1} p^{k/2} \sum_{h,h'=1}^{p^{n-k}} (\frac{1}{\pi h/p^{n-k} + (K+1)^{-1}})^2 (\frac{1}{\pi h/p^{n-k} + (K'+1)^{-1}})^2.
\end{aligned}$$

The function $f(x) = (1/(\pi x + (K+1)^{-1}))^2$ is concave up for $x \in [0,1]$. Hence

$$\sum_{h=1}^{p^{n-k}} f(h/p^{n-k}) = p^{n-k} \sum_{h=1}^{p^{n-k}} p^{k-n} f(h/p^{n-k}) \leq p^{n-k} \int_0^1 f(x)dx \leq p^{n-k}(K+1)/(\pi + (K+1)^{-1}).$$

The above implies

$$\begin{aligned}
|S_3| &\leq 8\sqrt{2}q^{-3/2}\pi^4 (KK')^{-1} \sum_{k=0}^{n-1} p^{k/2} [p^{n-k}(K+1)/(\pi + (K+1)^{-1})] \cdot [p^{n-k}(K'+1)/(\pi + (K'+1)^{-1})] \\
&\leq 8\sqrt{2}\pi^2 (1+1/K)(1+1/K') \sum_{k=0}^{\infty} p^{2n-3k/2} \leq 8\sqrt{2}\pi^2 (1+1/K)(1+1/K')\sqrt{q}/(1-p^{-3/2}).
\end{aligned}$$

By hypothesis, we have $K, K' \geq 5$, hence $1 + K^{-1}, 1 + K^{'-1} \leq \sqrt{2}$ and

$$|S_3| \leq \frac{64\pi^2}{2\sqrt{2}-1}\sqrt{q}.$$

Combining the estimations for S_1, S_2, S_2' and S_3, we get

$$\begin{aligned}
S &\geq \frac{1}{2q}(K+1)(K'+1) - \frac{3}{q}(K+K'+2) - \frac{64\pi^2}{2\sqrt{2}-1}\sqrt{q} \\
&\geq \frac{1}{2q}[(K-5)(K'-5) - 36] - \frac{64\pi^2}{2\sqrt{2}-1}\sqrt{q}.
\end{aligned}$$

Since

$$(K-5)(K'-5) \geq (|A|-11)(|B|-11)/4 > 36 + \frac{128\pi^2}{2\sqrt{2}-1}q^{3/2}.$$

We see that $S > 0$ and this completes the proof. □

References

[1] C. Hooley, Applications of sieve methods to number theory, Cambridge University Press, 1976.

[2] P. Parent, Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, arXiv:alg-geom/9604003, 1995, 17pp.

[3] P. Parent, Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, *J. Reine Angew. Math.*, **506** (1999), 85-116.