ASYMPTOTIC EQUIDISTRIBUTION OF QUADRATIC NONRESIDUES ON A SHORT INTERVAL

KIM, SUNGJIN

1. Introduction

Let $x \geq 2$ and p be a prime number. Let $\left(\frac{n}{p}\right)$ be the Legendre symbol. We investigate some character sums of the type

$$\sum_{p \leq x} \sum_{n < \log p} f(p) \left(\frac{n}{p}\right), \tag{1.1}$$

where f is a function satisfying $f(x) \to 0$ as $x \to \infty$. We expect nontrivial cancellations in these sums. Since, the length of the inner sum is short compared to p, we do not have enough techniques to detect the cancellations in the inner sums. Instead, we change the order of summation

$$\sum_{n < \log x} \sum_{e^n < p \leq x} f(p) \left(\frac{n}{p}\right). \tag{1.2}$$

Then we can apply Siegel-Walfisz theorem(See [2], page 124) and partial summation to the inner sums.

The first application of this technique is the following theorem.

Theorem 1.1. *Let N_p^* be the number of square-free quadratic nonresidues n modulo p such that $0 < n < \log p$, and S_p^* be the number of square-free integers in $0 < n < \log p$. Then we have*

$$\sum_{p \leq x} \left(\frac{N_p^*}{S_p^*} - \frac{1}{2}\right)^2 = \frac{\pi^2}{24} \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^{\frac{5}{2}}}\right). \tag{1.3}$$

This result can be interpreted as "The variance of $\frac{N_p^*}{S_p^*}$ over $p \leq x$ approaches to 0 as $x \to \infty$". The following corollary can be obtained directly by P. Erdos [1], however it can also be followed from Theorem 1.1.

Corollary 1.1. *Let n_p be the first quadratic nonresidue modulo p, and let N_x be the number of primes $p \leq x$ such that $n_p > \log p$. Then*

$$N_x = O\left(\frac{x}{(\log x)^2}\right). \tag{1.4}$$

Proof. If $n_p > \log p$ then $N_p^* = 0$. Hence,

$$\frac{1}{4} N_x \leq \sum_{p \leq x} \left(\frac{N_p^*}{S_p^*} - \frac{1}{2}\right)^2 = O\left(\frac{x}{(\log x)^2}\right). \tag{1.5}$$

□

Now, we drop the square-free conditions in Theorem 1.1. It contributes to a bigger error term.

Theorem 1.2. *Let N_p be the number of quadratic nonresidues n modulo p such that $0 < n < \log p$. Then we have*

$$\sum_{p\le x}\left(\frac{N_p}{\log p}-\frac{1}{2}\right)^2=\frac{3x\log\log x}{2\pi^2(\log x)^2}+O\left(\frac{x}{(\log x)^2}\right). \tag{1.6}$$

This result can also be interpreted as "The variance of $\frac{N_p}{\log p}$ over $p \le x$ approaches to 0 as $x \to \infty$". As a corollary, we have the following asymptotic equidistribution result.

Corollary 1.2. *Given any $0 < \epsilon < 1$, define E_x^ϵ by the set of primes $p \le x$ such that $\left|\frac{N_p}{\log p}-\frac{1}{2}\right| \ge (\log p)^{-1/2+\epsilon/2}$. Then*

$$|E_x^\epsilon| = O\left(\frac{x\log\log x}{(\log x)^{1+\epsilon}}\right). \tag{1.7}$$

Proof. We use Theorem 1.2 with $N = |E_x^\epsilon|$,

$$\frac{N}{(\log x)^{1-\epsilon}} \le \sum_{p\in E_x^\epsilon}\frac{1}{(\log p)^{1-\epsilon}} \le \sum_{p\in E_x^\epsilon}\left(\frac{N_p}{\log p}-\frac{1}{2}\right)^2 = O\left(\frac{x\log\log x}{(\log x)^2}\right). \tag{1.8}$$

□

2. Proof of the main theorem

Throughout this paper, $\sum^*$ is the sum over square-free integers, and $\sum'$ is the sum over non-square integers.

Note that $N_p^* - \frac{1}{2}S_p^* = -\frac{1}{2}\sum_{n<\log p}{}^*\left(\frac{n}{p}\right)$. The left-hand side of the equation (1.1) is then

$$\begin{aligned}\sum_{p\le x}\left(\frac{N_p^*}{S_p^*}-\frac{1}{2}\right)^2 &= \sum_{p\le x}\frac{1}{(S_p^*)^2}\left(-\frac{1}{2}\sum_{n<\log p}{}^*\left(\frac{n}{p}\right)\right)^2\\ &= \sum_{p\le x}\frac{1}{4(S_p^*)^2}\sum_{n_1,n_2<\log p}{}^*\left(\frac{n_1n_2}{p}\right).\end{aligned}$$

We divide into two cases, first we consider the case n_1n_2 is not a square. In fact, n_1n_2 is square if and only if $n_1 = n_2$ since they are square-free. By changing the order of summation

$$\sum_{p\le x}\frac{1}{(S_p^*)^2}\sum_{n_1,n_2<\log p}{}^*\left(\frac{n_1n_2}{p}\right) = \sum_{n_1,n_2<\log x}{}^*\sum_{\max(e^{n_1},e^{n_2})<p\le x}\frac{1}{(S_p^*)^2}\left(\frac{n_1n_2}{p}\right)$$

If n_1n_2 is not a square, $\left(\frac{n_1n_2}{\cdot}\right)$ is a nontrivial real character modulo n_1n_2. We can find a primitive real character $\left(\frac{n}{\cdot}\right)$ such that $\left(\frac{n}{p}\right) = \left(\frac{n_1n_2}{p}\right)$ for all p in

$\max(e^{n_1}, e^{n_2}) < p \le x$. Define $A(t) = \sum_{p\le t} \left(\frac{n}{p}\right)$, then by Siegel-Walfisz theorem, we have the estimate $A(t) = O\left(n\frac{t}{(\log t)^A}\right)$ for any $A > 0$.

$$\begin{aligned}\sum_{p\le x} \frac{1}{(S_p^*)^2}\left(\frac{n}{p}\right) &= \sum_{3\le t\le x} \frac{1}{(S_t^*)^2}(A(t) - A(t-1)) \\ &= \frac{A(x)}{(S_x^*)^2} - \frac{A(2)}{(S_3^*)^2} + \sum_{3\le t\le x-1} A(t)\left(\frac{1}{(S_t^*)^2} - \frac{1}{(S_{t+1}^*)^2}\right).\end{aligned}$$

It is clear that $\frac{A(x)}{(S_x^*)^2} - \frac{A(2)}{(S_3^*)^2} = O\left(n\frac{x}{(\log x)^{A+2}}\right)$, and note that $\frac{1}{(S_t^*)^2} - \frac{1}{(S_{t+1}^*)^2} = \frac{(S_{t+1}^*-S_t^*)(S_{t+1}^*+S_t^*)}{(S_t^* S_{t+1}^*)^2}$. Recall that $S_{t+1}^* - S_t^*$ is the number of square-free integers in the interval $\log t \le n < \log(t+1)$. Since there are only $\sim \frac{6}{\pi^2}\log x$ square free integers in $0 < n < \log x$, it follows that $S_{t+1}^* - S_t^* = 1$ for only $\sim \frac{6}{\pi^2}\log x$ times, and $= 0$ otherwise. Thus,

$$\begin{aligned}\sum_{3\le t\le x-1} A(t)\left(\frac{1}{(S_t^*)^2} - \frac{1}{(S_{t+1}^*)^2}\right) &= O\left(n\sum_{x-\log x\le t\le x-1} \frac{t}{(\log t)^{A+3}}\right) \\ &= O\left(n\frac{x}{(\log x)^{A+2}}\right).\end{aligned}$$

Hence, we have

$$\sum_{p\le x} \frac{1}{(S_p^*)^2}\left(\frac{n}{p}\right) = O\left(n\frac{x}{(\log x)^{A+2}}\right). \tag{2.1}$$

Also, changing A if necessary, it follows that

$$\sum_{p\le x} \frac{1}{(S_p^*)^2} \sum_{\substack{n_1,n_2<\log p \\ n_1\ne n_2}}^{*} \left(\frac{n_1n_2}{p}\right) = O\left(\frac{x}{(\log x)^A}\right). \tag{2.2}$$

When $n_1 = n_2$, we see that the character gives 1 always. The sum is in fact,

$$\sum_{p\le x}\sum_{n<\log p}^{*} \frac{1}{4(S_p^*)^2} = \sum_{p\le x} \frac{1}{4S_p^*} = \frac{\pi^2}{24}\frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^{\frac{5}{2}}}\right). \tag{2.3}$$

Combining (2.2), and (2.3), we obtain Theorem 1.1.

3. Removal of square-free conditions

We now prove Theorem 1.2. Notice that N_p can be obtained by $N_p = \sum_{n<\log p}{}' \frac{1}{2}\left(1 - \left(\frac{n}{p}\right)\right)$. The proof starts with the same line as in Theorem 1.1.

$$\begin{aligned}\sum_{p\le x}\left(\frac{-\frac{1}{2}\sum_{n<\log p}{}'\left(\frac{n}{p}\right) + O(1)}{\log p}\right)^2 &= \sum_{p\le x}\left(\frac{-\frac{1}{2}\sum_{n<\log p}{}'\left(\frac{n}{p}\right)}{\log p}\right)^2 + O\left(\frac{x}{(\log x)^2}\right) \\ &= \sum_{p\le x}\frac{1}{4(\log p)^2}\sum_{n_1,n_2<\log p}{}'\left(\frac{n_1n_2}{p}\right) + O\left(\frac{x}{(\log x)^2}\right).\end{aligned}$$

Similarly as before, we have

$$\sum_{p\leq x}\frac{1}{(\log p)^2}\sum_{\substack{n_1,n_2<\log p\\ n_1n_2\text{ is not a square}}}{}^{\prime}\left(\frac{n_1n_2}{p}\right)=O\left(\frac{x}{(\log x)^A}\right). \tag{3.1}$$

However, we need a slight modification of the argument. Change the order of summation, and find a primitive character $\left(\frac{n}{\cdot}\right)$ such that $\left(\frac{n}{p}\right)=\left(\frac{n_1n_2}{p}\right)$ for primes in $\max(e^{n_1},e^{n_2})<p\leq x$. Then we apply Siegel-Walfisz theorem with integration by part for inner sums.

Now, we take care of the remaining sum in which n_1n_2 is a square. In this case, $\left(\frac{n_1n_2}{p}\right)$ is always 1. For, we need the following estimate of the sum

$$\sum_{\substack{n_1,n_2<x\\ n_1n_2\text{ is a square}}}{}^{\prime}1=\frac{6}{\pi^2}x\log x+O(x). \tag{3.2}$$

We introduce a new variable n_0 which is the least number that makes n_1n_0 a square.

$$\begin{aligned}\sum_{\substack{n_1,n_2<x\\ n_1n_2\text{ is a square}}}{}^{\prime}1&=\sum_{n_1<x}{}^{\prime}\sum_{n_0t^2<x}1\\ &=\sum_{n_1<x}{}^{\prime}\sqrt{\frac{x}{n_0}}+O(x)\\ &=\sum_{n_0<x}{}^{*}\left(\sqrt{\frac{x}{n_0}}\right)^2+O(x)\\ &=\frac{6}{\pi^2}x\log x+O(x).\end{aligned}$$

Then we have,

$$\sum_{p\leq x}\sum_{\substack{n_1,n_2<\log p\\ n_1n_2\text{ is a square}}}{}^{\prime}\frac{1}{(\log p)^2}=\sum_{p\leq x}\frac{6\log\log p}{\pi^2\log p}+O\left(\sum_{p\leq x}\frac{1}{\log p}\right)=\frac{6x\log\log x}{\pi^2(\log x)^2}+O\left(\frac{x}{(\log x)^2}\right). \tag{3.3}$$

Combining (3.1), and (3.3), we obtain Theorem 1.2.

References

[1] P. Erdos, Remarks on number theory. I, Mat. Lapok 12 1961, 10.17.
[2] H. Iwaniec, I. Kowalski, *Analytic Number Theory*, volume 53, AMS Colloquium Publications.