MATHEMATICS OF COMPUTATION
Volume 86, Number 307, September 2017, Pages 2551–2554
http://dx.doi.org/10.1090/mcom/3261
Article electronically published on March 8, 2017

CORRIGENDUM TO "CONDITIONAL BOUNDS FOR THE LEAST QUADRATIC NON-RESIDUE AND RELATED PROBLEMS"

YOUNESS LAMZOURI, XIANNAN LI, AND KANNAN SOUNDARARAJAN

Abstract. We correct an error in one of the lemmas of "Conditional bounds for the least quadratic non-residue and related problems", Math. Comp. **84** (2015), no. 295.

1. Introduction

Emanuel Carneiro and Micah Milinovich have kindly drawn our attention to an error in Lemma 6.1 of our paper [1], which affects the asymptotic bounds in Theorems 1.2 and 1.3 there. These results must be replaced with the following corrected versions. All the other results in the paper, including all explicit bounds, remain unaltered.

Theorem 1.2. *Assume GRH. Let q be a large integer and let H be a subgroup of $G = (\mathbb{Z}/q\mathbb{Z})^*$ with index $h = [G : H] > 1$. Then the least prime p not in H satisfies*

$$p < (\alpha(h) + o(1))(\log q)^2,$$

where $\alpha(2) = 0.8$, $\alpha(3) = 0.7$ and in general $\alpha(h) = 0.66$ for all $h > 3$.

Theorem 1.3. *Assume GRH. Let q be a large integer and let H be a subgroup of $G = (\mathbb{Z}/q\mathbb{Z})^*$ with index $h = [G : H] \geq 4$. Then the least prime p not in H satisfies*

$$p < \Big(\frac{1}{4} + o(1)\Big)\Big(1 - \frac{1}{h}\Big)^2\Big(\frac{\log(2h)}{\log(2h) - 4}\Big)^2(\log q)^2.$$

The error is in the first displayed equation of Lemma 6.1, where the right side should have $K(1/2)\sqrt{x}$ instead of $K(1/2)\sqrt{x}/2$. In what follows, we shall outline the necessary modifications that should be made to Section 6 of [1]. All the other sections of the paper remain unchanged. The arXiv version of [1] has been updated to give complete details of the corrected versions of the theorems stated above; see `arXiv.org:1309.3595`. We are grateful to Professors Carneiro and Milinovich for informing us of this error.

2. Corrections in Section 6

Let δ be a fixed positive real number, and let $K(s)$ denote a function holomorphic in a region containing $-1/2 - \delta < \mathrm{Re}(s) \leq \frac{1}{2} + \delta$, save for possibly a simple pole

Received by the editor November 1, 2016 and, in revised form, January 12, 2017.
2010 *Mathematics Subject Classification.* Primary 11N60; Secondary 11R42.
The first author was supported in part by an NSERC Discovery grant. The third author was supported in part by NSF grant DMS-1001068, and a Simons Investigator grant from the Simons Foundation.

at $s = -1/2$ with residue r. Further suppose that for all s in this region bounded away from $-1/2$ we have $|K(s)| \ll 1/(1+|s|^2)$. In Section 6 of [1], we required K to be even and holomorphic in this region, however these assumptions are no longer necessary since most of the proofs hold (with very minor changes) in the above general setting.

For $\xi > 0$ define the inverse Mellin transform

$$\widetilde{K}(\xi) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} K(s)\xi^{-s}ds,$$

where the integral is over any vertical line with $-\frac{1}{2} < c \le \frac{1}{2}+\delta$. If $\xi \ge 1$, then by taking the $c = 1/2$ in the integral above, we find that $\widetilde{K}(\xi) \ll 1/\sqrt{\xi}$. If $\xi \le 1$, then moving the line of integration to $c = -1/2 - \delta/2$ (encountering potentially a pole at $-1/2$) we find that $\widetilde{K}(\xi) \ll \sqrt{\xi}$. Thus

$$|\widetilde{K}(\xi)| \ll \min(\xi, 1/\xi)^{\frac{1}{2}}. \tag{1}$$

Finally we assume that K is such that $\widetilde{K}(\xi) > 0$ for all $\xi > 0$.

Modifications to Lemma 6.1. In the statement of Lemma 6.1 of [1], we should replace $K(1/2)/2$ by $K(1/2)$ in the first displayed equation, and $\tilde{K}(x/n)$ by $\tilde{K}(n/x)$ in the sums of both displayed equations.

Proof of Lemma 6.1. Consider first the case when χ is non-principal. Let $\tilde{\chi}$ (mod $\tilde{q}$) denote the primitive character that induces χ and let $\xi(s,\tilde{\chi})$ denote the corresponding completed L-function. We consider the following integral:

$$I = \frac{1}{2\pi i}\int_{(1/2+\delta)} -\frac{\xi'}{\xi}(s+\tfrac{1}{2},\tilde{\chi})K(s)x^s ds. \tag{2}$$

Then, the exact same argument leading to equation (6.3) of [1] shows that

$$I = \sum_n \frac{\Lambda(n)\chi(n)}{\sqrt{n}}\tilde{K}(n/x) + O\Big(1 + \log q\frac{\log x}{\sqrt{x}}\Big). \tag{3}$$

We now evaluate the integral in (2) by shifting the line of integration to $\mathrm{Re}(s) = -1/2 - \delta/2$. Thus, with γ running over the ordinates of zeros of $\xi(s,\tilde{\chi})$,

$$I = -\sum_\gamma K(i\gamma)x^{i\gamma} - r\frac{\xi'}{\xi}(0,\tilde{\chi})x^{-1/2} + \frac{1}{2\pi i}\int_{(-1/2-\delta/2)} -\frac{\xi'}{\xi}(\tfrac{1}{2}+s,\tilde{\chi})K(s)x^s ds.$$

Using now the functional equation for ξ, we find that the integral on the right-hand side is bounded by $\ll x^{-1/2-\delta/2}$.

Recall that $\mathrm{Re}\frac{\xi'}{\xi}(0,\tilde{\chi}) \ll \log q$, so that

$$\mathrm{Re}(I) = \theta\sum_\gamma |K(i\gamma)| + O\left(\frac{\log q}{\sqrt{x}}\right) = \theta(1+o(1))\frac{\log\tilde{q}}{2\pi}\int_{-\infty}^{\infty}|K(it)|dt + O\left(\frac{\log q}{\sqrt{x}}\right),$$

where the final estimate follows from an application of the explicit formula. This establishes our lemma for non-principal characters. For principal characters, we have

$$\begin{aligned}\sum_n \frac{\Lambda(n)}{\sqrt{n}}\tilde{K}(n/x) &= \frac{1}{2\pi i}\int_{(1/2+\delta/2)} -\frac{\zeta'}{\zeta}(\tfrac{1}{2}+s)K(s)x^s ds \\ &= K(1/2)\sqrt{x} - \frac{1}{2\pi i}\int_{(-1/2-\delta/2)} \frac{\zeta'}{\zeta}(\tfrac{1}{2}+s)K(s)x^s ds - \sum_\gamma K(i\gamma)x^{i\gamma} \\ &= K(1/2)\sqrt{x} + O(1).\end{aligned}$$

Using the same argument leading to (6.3) of [1], we deduce in this case that

$$I = \sum_n \frac{\Lambda(n)\chi(n)}{\sqrt{n}}\tilde{K}(n/x) + O\Big(1 + \log q \frac{\log x}{\sqrt{x}}\Big). \qquad \square$$

Modifications to Proposition 6.1. In the statement of Proposition 6.1 of [1], we only need to replace $K(1/2)/2$ by $K(1/2)$. We now outline the necessary modifications to its proof.

Proof of Proposition 6.1. In view of the corrected Lemma 6.1, the first displayed equation in the proof of Proposition 6.1 of [1] now becomes

$$\sum_{\chi\in\tilde{H}} \mathrm{Re}\sum_n \frac{\Lambda(n)\chi(n)}{\sqrt{n}}\tilde{K}(n/x) \le K(1/2)\sqrt{x} + (1+o(1))(h-1)\log q\Big(\frac{1}{2\pi}\int_{-\infty}^{\infty}|K(it)|dt\Big).$$

The argument leading to the second displayed equation in the proof of Proposition 6.1 of [1] shows that the left-hand side above is

$$\ge h\int_1^X \tilde{K}(t/x)\frac{dt}{\sqrt{t}} + o(h\log q) = h\sqrt{x}\int_0^\lambda \tilde{K}(u)\frac{du}{\sqrt{u}} + o(h\log q),$$

by a change of variables $u = t/x$, completing the proof. $\square$

Modifications to Subsection 6.1. Here, we only need to change the main displayed equation. In view of the corrected Proposition 6.1 this becomes

$$h\int_0^\lambda \tilde{K}(u)\frac{du}{\sqrt{u}} - K(1/2) \le (h-1)\int_0^\lambda \tilde{K}(u)\frac{du}{\sqrt{u}} \le (2h-2)\sqrt{\lambda}\frac{1}{2\pi}\int_{-\infty}^{\infty}|K(it)|dt.$$

Hence Proposition 6.1 cannot lead to a bound for X that is better than $(\frac{1}{4}+o(1))(\log q)^2$.

Modifications to Subsection 6.2. There are no changes to this subsection. Indeed, by taking the same kernel $K(s)$ and the same choice of α, we obtain (in view of the corrected Proposition 6.1)

$$X \le \Big(\frac{1}{4}+o(1)\Big)\Big(1-\frac{1}{h}\Big)^2\Big(\frac{\log(2h)}{\log(2h)-4}\Big)^2(\log q)^2.$$

Modifications to Subsection 6.3. Here, we choose a different kernel that gives better bounds in view of the corrections made in Lemma 6.1 and Proposition 6.1. We take $K(s) = \Gamma(s+1/2)$. Note that $K(s)$ satisfies the conditions stated at the beginning of this section and that $\tilde{K}(u) = \sqrt{u}e^{-u} \ge 0$ for all u. Noting that $K(1/2) = \Gamma(1) = 1$, we apply the corrected Proposition 6.1 to see that

$$\left(h\int_0^\lambda e^{-u}du - 1\right)\sqrt{X} \le \sqrt{\lambda}(h-1)\frac{\log q}{2\pi}\int_{-\infty}^{\infty}|\Gamma(1/2+it)|\,dt,$$

so that

$$\sqrt{X} \leq \frac{\sqrt{\lambda}(h-1)\log q}{2\pi(h-1-he^{-\lambda})} \int_{-\infty}^{\infty} |\Gamma(1/2+it)|\, dt.$$

When $h = 2$, we choose $\lambda = 2.452$, which is more or less optimal, and find that $X < (0.794 + o(1))(\log q)^2$. For $h = 3$, we choose $\lambda = 2.025$, and find that $X < (0.7 + o(1))(\log q)^2$. For $h = 4$, we choose $\lambda = 1.825$ and get that $X < (0.66 + o(1))(\log q)^2$. We may apply this for other smaller values of h and get progressively better bounds as h increases, with $0.545(\log q)^2$ being the limit for this test function.

References

[1] Y. Lamzouri, X. Li, and K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Math. Comp. **84** (2015), no. 295, 2391–2412, DOI 10.1090/S0025-5718-2015-02925-1. MR3356031

Department of Mathematics and Statistics, York University, 4700 Keele Street, Toronto, Ontario M3J1P3, Canada

E-mail address: lamzouri@mathstat.yorku.ca

Department of Mathematics, Kansas State University, 138 Cardwell Hall, Manhattan, Kansas 66506

E-mail address: xiannan@ksu.edu

Department of Mathematics, Stanford University, Stanford, California 94305

E-mail address: ksound@math.stanford.edu