

SMALL PRIME SOLUTIONS OF QUADRATIC EQUATIONS II

KWOK-KWONG STEPHEN CHOI AND JIANYA LIU

(Communicated by David E. Rohrlich)

ABSTRACT. Let b_1, \dots, b_5 be non-zero integers and n any integer. Suppose that $b_1 + \dots + b_5 \equiv n \pmod{24}$ and $(b_i, b_j) = 1$ for $1 \leq i < j \leq 5$. In this paper we prove that (i) if the b_j are not all of the same sign, then the above quadratic equation has prime solutions satisfying $p_j \ll \sqrt{|n|} + \max\{|b_j|\}^{25/2+\varepsilon}$; and (ii) if all the b_j are positive and $n \gg \max\{|b_j|\}^{26+\varepsilon}$, then the quadratic equation $b_1 p_1^2 + \dots + b_5 p_5^2 = n$ is soluble in primes p_j . Our previous results are $\max\{|b_j|\}^{20+\varepsilon}$ and $\max\{|b_j|\}^{41+\varepsilon}$ in place of $\max\{|b_j|\}^{25/2+\varepsilon}$ and $\max\{|b_j|\}^{26+\varepsilon}$ above, respectively.

For any integer n , we consider the quadratic equations in the form

$$(1) \quad b_1 p_1^2 + \dots + b_5 p_5^2 = n,$$

where the p_j are prime variables and the coefficients b_j are non-zero integers. A necessary condition for the solubility of (1) is

$$(2) \quad b_1 + \dots + b_5 \equiv n \pmod{24}.$$

We also suppose

$$(3) \quad (b_i, b_j) = 1, \quad 1 \leq i < j \leq 5,$$

and write $B = \max\{2, |b_1|, \dots, |b_5|\}$. The main results in this note are the following two theorems.

Theorem 1. *Suppose (2) and (3). If b_1, \dots, b_5 are not all of the same sign, then (1) has solutions in the primes p_j satisfying*

$$p_j \ll \sqrt{|n|} + B^{25/2+\varepsilon},$$

where the implied constant depends only on ε .

Theorem 2. *Suppose (2) and (3). If b_1, \dots, b_5 are all positive, then (1) is soluble whenever*

$$n \gg B^{26+\varepsilon},$$

where the implied constant depends only on ε .

Theorem 2 with $b_1 = \dots = b_5 = 1$ is a classical result of Hua [3] in 1938. Theorems 1 and 2 improve our previous results in [1] with the bounds $B^{20+\varepsilon}$ and $B^{41+\varepsilon}$ in the place of $B^{25/2+\varepsilon}$ and $B^{26+\varepsilon}$, respectively.

Received by the editors February 3, 2003.

2000 *Mathematics Subject Classification.* Primary 11P32, 11P05, 11P55.

The first and second authors were supported by the NSERC and the NSF of China (Grant #10125101), respectively.

©2004 American Mathematical Society
Reverts to public domain 28 years from publication

Recently, the second author introduced in [4] an iterative procedure to deal with the enlarged major arcs in the Waring-Goldbach problem which can be used to improve the previous results substantially. In this note, we will demonstrate how to use this iterative procedure to improve our previous results in [1]. Most of the arguments are similar to those in [1] and we therefore only sketch the proof here. We refer the reader to [1] for all the details and only emphasize the main difference between the arguments.

Denote by $r(n)$ the weighted number of solutions of (1), i.e.,

$$r(n) = \sum_{\substack{n=b_1p_1^2+\dots+b_5p_5^2 \\ M < |b_j|p_j^2 \leq N}} (\log p_1) \cdots (\log p_5),$$

where $M = N/200$. We will investigate $r(n)$ by the circle method. To this end, we set

$$(4) \quad P = (N/B)^{1/5-\varepsilon}, \quad Q = N/(PL^{9000}), \quad \text{and} \quad L = \log N.$$

We should remark that the previous choice of P in [1] is $P = (N/B)^{1/8-\varepsilon}$. The improvement in our theorems is due to the choice of larger P in (4).

By Dirichlet’s lemma on rational approximation, each $\alpha \in [1/Q, 1 + 1/Q]$ may be written in the form

$$(5) \quad \alpha = a/q + \lambda, \quad |\lambda| \leq 1/(qQ),$$

for some integers a, q with $1 \leq a \leq q \leq Q$ and $(a, q) = 1$. We denote by $\mathfrak{M}(a, q)$ the set of α satisfying (5), and define the major arcs \mathfrak{M} and the minor arcs \mathfrak{m} as follows:

$$(6) \quad \mathfrak{M} = \bigcup_{q \leq P} \bigcup_{\substack{a=1 \\ (a,q)=1}}^q \mathfrak{M}(a, q), \quad \mathfrak{m} = \left[\frac{1}{Q}, 1 + \frac{1}{Q} \right] \setminus \mathfrak{M}.$$

It follows from $2P \leq Q$ that the major arcs $\mathfrak{M}(a, q)$ are mutually disjoint. Let

$$S_j(\alpha) = \sum_{M < |b_j|p_j^2 \leq N} (\log p) e(b_j p^2 \alpha),$$

where $e(x) := e^{2\pi i x}$. Then we have

$$(7) \quad r(n) = \int_0^1 S_1(\alpha) \cdots S_5(\alpha) e(-n\alpha) d\alpha = \int_{\mathfrak{M}} + \int_{\mathfrak{m}}.$$

For $\chi \bmod q$, we define

$$C(\chi, a) = \sum_{h=1}^q \bar{\chi}(h) e\left(\frac{ah^2}{q}\right), \quad C(q, a) = C(\chi^0, a).$$

Here χ^0 is the principal character mod q . If χ_1, \dots, χ_5 are characters mod q , then we write

$$B(n, q, \chi_1, \dots, \chi_5) = \sum_{\substack{a=1 \\ (a,q)=1}}^q e\left(-\frac{an}{q}\right) C(\chi_1, b_1 a) \cdots C(\chi_5, b_5 a),$$

and

$$(8) \quad \mathfrak{S}(n, x) = \sum_{q \leq x} \frac{B(n, q, \chi^0, \dots, \chi^0)}{\varphi^5(q)},$$

where $\varphi(q)$ is the Euler totient function. The integral on the major arcs \mathfrak{M} causes the main difficulty, which is solved by the following.

Theorem 3. *Assume (3). Let \mathfrak{M} be as in (6) with P and Q determined by (4). If $N \geq P^{5+\varepsilon}B$, then we have*

$$\int_{\mathfrak{M}} S_1(\alpha) \cdots S_5(\alpha) e(-n\alpha) d\alpha = \frac{1}{32} \mathfrak{S}(n, P) \mathfrak{J}(n) + O\left(\frac{N^{3/2}}{|b_1 \cdots b_5|^{1/2} L}\right),$$

where $\mathfrak{S}(n, P)$ is defined in (8) and

$$\mathfrak{J}(n) := \sum_{\substack{b_1 m_1 + \cdots + b_5 m_5 = n \\ M < |b_j| m_j \leq N}} (m_1 \cdots m_5)^{-1/2}.$$

As shown in [1], the integral on \mathfrak{m} satisfies

$$(9) \quad \left| \int_{\mathfrak{m}} \right| \ll \frac{N^{3/2+\varepsilon}}{|b_1 \cdots b_5|^{1/4} P^{1/4}}.$$

The contribution from the major arcs can be handled by Theorem 3, which together with (7) and (9) gives

$$r(n) = \frac{1}{32} \mathfrak{S}(n, P) \mathfrak{J}(n) + O\left(\frac{N^{3/2}}{|b_1 \cdots b_5|^{1/2} L} + \frac{N^{3/2+\varepsilon}}{|b_1 \cdots b_5|^{1/4} P^{1/4}}\right).$$

The lower bounds for $\mathfrak{S}(n, P)$ and $\mathfrak{J}(n)$ were estimated in [1]. The following are Lemmas 2.1 and 2.2 in [1].

Lemma 4. *Assuming (2), we have $\mathfrak{S}(n, P) \gg (\log \log B)^{-c_1}$ for some constant $c_1 > 0$.*

Lemma 5. *Suppose (3) and either (i) the b_j 's are not all of the same sign and $N \geq 10|n|$; or (ii) all the b_j 's are positive and $n = N$. Then we have*

$$\mathfrak{J}(n) \asymp \frac{N^{3/2}}{|b_1 \cdots b_5|^{1/2}}.$$

Now assume either condition (i) or (ii) in Lemma 5. Applying Lemmas 4 and 5 to the above formula, we conclude that

$$r(n) \gg |b_1 \cdots b_5|^{-1/2} N^{3/2} (\log \log B)^{-c_1}$$

provided that $P \gg N^\varepsilon |b_1 \cdots b_5|$, or equivalently $N \gg B^{1+\varepsilon} |b_1 \cdots b_5|^5$. This proves Theorems 1 and 2.

Therefore, it remains to prove Theorem 3.

For $j = 1, \dots, 5$, set

$$V_j(\lambda) = \sum_{M < |b_j| m^2 \leq N} e(b_j m^2 \lambda),$$

and

$$(10) \quad W_j(\chi, \lambda) = \sum_{M < |b_j| p^2 \leq N} (\log p) \chi(p) e(b_j p^2 \lambda) - \delta_\chi \sum_{M < |b_j| m^2 \leq N} e(b_j m^2 \lambda),$$

where $\delta_\chi = 1$ or 0 according to whether χ is principal or not. We can rewrite the exponential sum $S_j(\alpha)$ as (see for example [2], §26, (2))

$$S_j\left(\frac{h}{q} + \lambda\right) = \frac{C(q, b_j h)}{\varphi(q)} V_j(\lambda) + \frac{1}{\varphi(q)} \sum_{\chi \pmod q} C(\chi, b_j h) W_j(\chi, \lambda) =: T_j + U_j,$$

say. Thus,

$$\int_{\mathfrak{M}} S_1(\alpha) \cdots S_5(\alpha) e(-n\alpha) d\alpha = I_0 + \cdots + I_5,$$

where I_ν denotes the contribution from those products with ν pieces of U_j and $5 - \nu$ pieces of T_j , i.e.,

$$I_\nu = \sum_{q \leq P} \sum_{\substack{a=1 \\ (a,q)=1}}^q e\left(-\frac{an}{q}\right) \int_{-1/(qQ)}^{1/(qQ)} (U_1 \cdots U_\nu T_{\nu+1} \cdots T_5 + \text{s.t.}) e(-n\lambda) d\lambda,$$

where ‘‘s.t.’’ means similar terms. For example, ‘‘ $A_1 B_2 C_3 D_4 E_5 + \text{s.t.}$ ’’ means the sum of all possible terms $A_\alpha B_\beta C_\gamma D_\delta E_\iota$ with (α, \dots, ι) being any permutation of $(1, \dots, 5)$.

We will prove that I_0 gives the main term and I_1, \dots, I_5 the error term. The estimation of I_0 is the same as that in [1] and we have

$$I_0 = \frac{1}{32} \mathfrak{S}(n, P) \mathfrak{J}(n) + O\left(\frac{N^{3/2}}{|b_1 \cdots b_5|^{1/2} L}\right).$$

It remains to show that $|I_i| \ll N^{3/2} |b_1 \cdots b_5|^{-1/2} L^{-1}$ for $1 \leq i \leq 5$. To this end, we define, for any $g \geq 1$

$$J_j(g) = \sum_{r \leq P} [g, r]^{-1+\varepsilon} \sum_{\chi \bmod r}^* \max_{|\lambda| \leq 1/(rQ)} |W_j(\chi, \lambda)|$$

and

$$K_j(g) = \sum_{r \leq P} [g, r]^{-1+\varepsilon} \sum_{\chi \bmod r}^* \left(\int_{-1/(rQ)}^{1/(rQ)} |W_j(\chi, \lambda)|^2 d\lambda \right)^{1/2},$$

where $\sum_{\chi \bmod r}^*$ is over all the primitive characters modulo r and $[g, r]$ is the least common multiple of g and r .

Our Theorem 3 depends on the following three main lemmas.

Lemma 6. *For P, Q satisfying (4), we have*

$$J_j(g) \ll g^{-1+2\varepsilon} N^{1/2} |b_j|^{-1/2} L^c$$

for some constant $c > 0$.

Lemma 7. *Let P, Q satisfy (4). For $g = 1$, Lemma 6 can be improved to*

$$J_j(1) \ll N^{1/2} |b_j|^{-1/2} L^{-A},$$

where $A > 0$ is arbitrary.

Lemma 8. *For P, Q satisfying (4), we have*

$$K_j(g) \ll g^{-1+2\varepsilon} |b_j|^{-1/2} L^c$$

for some constant $c > 0$.

We omit the proof of Lemmas 6–8, since they can be proved by combining the corresponding arguments in [4] and [1]. In fact, Lemmas 6–8 with $b_j = 1$ can be established in exactly the same way as Lemmas 3.1–3.3 of [4], which depend on Lemma 2.1 of [4], a hybrid estimate for Dirichlet polynomials. Lemmas 6–8 are essential in our iterative argument below; another application of the iterative method appears in [5].

For example, following the same proof of Lemma 3.1 of [4], one can show that our Lemma 6 is a consequence of the following two estimates: For $R \leq P$ and $0 < T_1 \leq T_0$, we have

$$(11) \quad \sum_{r \sim R} [g, r]^{-1+\varepsilon} \sum_{\chi \bmod r}^* \int_{T_1}^{2T_1} \left| F\left(\frac{1}{2} + it, \chi\right) \right| dt \ll g^{-1+2\varepsilon} N_j^{1/4} (T_1 + 1)^{1/2} L^c,$$

while for $R \leq P$ and $T_0 < T_2 \leq T$, we have

$$(12) \quad \sum_{r \sim R} [g, r]^{-1+\varepsilon} \sum_{\chi \bmod r}^* \int_{T_2}^{2T_2} \left| F\left(\frac{1}{2} + it, \chi\right) \right| dt \ll g^{-1+2\varepsilon} N_j^{1/4} T_2 L^c.$$

Here $T_0 = 8\pi N/(RQ)$, $N_j = N/|b_j|$, and $F(s, \chi)$ is as in §2 of [4] with $X = N_j^{1/2}$ and $Y = (N_j/200)^{1/2}$. To show (11), we note that $g, r = gr$. Then the left-hand side of (11) is

$$\ll g^{-1+\varepsilon} \sum_{\substack{d|g \\ d \leq R}} \left(\frac{R}{d}\right)^{-1+\varepsilon} \sum_{r \sim R} \sum_{\chi \bmod r}^* \int_{T_1}^{2T_1} \left| F\left(\frac{1}{2} + it, \chi\right) \right| dt.$$

Let $\tau(g)$ be the divisor function. By Lemma 2.1 in [4], the above quantity can be estimated as

$$\begin{aligned} &\ll g^{-1+\varepsilon} \sum_{\substack{d|g \\ d \leq R}} \left(\frac{R}{d}\right)^{-1+\varepsilon} \left(\frac{R^2}{d} T_1 + \frac{R}{d^{1/2}} T_1^{1/2} N_j^{3/20} + N_j^{1/4}\right) L^c \\ &\ll g^{-1+\varepsilon} \tau(g) (R^{1+\varepsilon} T_1 + R^{1/2+\varepsilon} T_1^{1/2} N_j^{3/20} + N_j^{1/4}) L^c \\ &\ll g^{-1+2\varepsilon} N_j^{1/4} (T_1 + 1)^{1/2} L^c, \end{aligned}$$

provided that $R \leq N_j^{1/5-\varepsilon}$. This requirement is necessary, since otherwise $R^{1/2+\varepsilon} T_1^{1/2} N_j^{3/20}$ cannot be bounded from above by $N_j^{1/4} (T_1 + 1)^{1/2}$. This establishes (11). Similarly we can prove (12). Therefore $P = (N/B)^{1/5-\varepsilon}$ in (4) is the optimal choice. The general assertions in Lemmas 6–8 can be obtained as in Lemmas 4.1, 4.2, and 5.1 of [1].

We demonstrate by estimating I_5 here, and the treatment of the other I_i are similar. We first reduce the characters in I_5 into primitive characters, to get

$$\begin{aligned} |I_5| &= \left| \sum_{q \leq P} \sum_{\chi_1 \bmod q} \cdots \sum_{\chi_5 \bmod q} \frac{B(n, q, \chi_1, \dots, \chi_5)}{\varphi^5(q)} \right. \\ &\quad \left. \times \int_{-1/(qQ)}^{1/(qQ)} W_1(\chi_1, \lambda) \cdots W_5(\chi_5, \lambda) e(-n\lambda) d\lambda \right| \\ &\leq \sum_{r_1 \leq P} \cdots \sum_{r_5 \leq P} \sum_{\chi_1 \bmod r_1}^* \cdots \sum_{\chi_5 \bmod r_5}^* \sum_{\substack{q \leq P \\ r_0|q}} \frac{|B(n, q, \chi_1 \chi^0, \dots, \chi_5 \chi^0)|}{\varphi^5(q)} \\ &\quad \times \int_{-1/(qQ)}^{1/(qQ)} |W_1(\chi_1 \chi^0, \lambda)| \cdots |W_5(\chi_5 \chi^0, \lambda)| d\lambda, \end{aligned}$$

where $r_0 = [r_1, \dots, r_5]$. For $q \leq P$ and $M < |b_j| p^2 \leq N$, we have $(q, p) = 1$. Using this and (10), we have $W_j(\chi_j \chi^0, \lambda) = W_j(\chi_j, \lambda)$ for the primitive characters χ_j

above. Consequently by Lemma 3.1 in [1], we obtain

$$\begin{aligned}
 |I_5| &\leq \sum_{r_1 \leq P} \cdots \sum_{r_5 \leq P} \sum_{\chi_1 \bmod r_1}^* \cdots \sum_{\chi_5 \bmod r_5}^* \int_{-1/(r_0Q)}^{1/(r_0Q)} |W_1(\chi_1, \lambda)| \cdots |W_5(\chi_5, \lambda)| d\lambda \\
 &\quad \times \sum_{\substack{q \leq P \\ r_0|q}} \frac{|B(n, q, \chi_1 \chi^0, \dots, \chi_5 \chi^0)|}{\varphi^5(q)} \\
 &\ll L^{c_2} \sum_{r_1 \leq P} \cdots \sum_{r_5 \leq P} r_0^{-1+\varepsilon} \sum_{\chi_1 \bmod r_1}^* \cdots \sum_{\chi_5 \bmod r_5}^* \int_{-1/(r_0Q)}^{1/(r_0Q)} |W_1(\chi_1, \lambda)| \cdots |W_5(\chi_5, \lambda)| d\lambda.
 \end{aligned}$$

The previous estimate of I_5 used the trivial inequality $r_0^{-1+\varepsilon} \leq r_1^{-1/5+\varepsilon} \cdots r_5^{-1/5+\varepsilon}$. Instead of using this inequality which is responsible for a weaker result, we employ an iterative argument introduced in [4] to bound the above sums over r_1, r_2, r_3, r_4, r_5 consecutively. By Cauchy's inequality, we get

$$\begin{aligned}
 |I_5| &\ll L^{c_2} \sum_{r_1 \leq P} \sum_{\chi_1 \bmod r_1}^* \max_{|\lambda| \leq 1/(r_1Q)} |W_1(\chi_1, \lambda)| \\
 &\quad \times \cdots \times \sum_{r_3 \leq P} \sum_{\chi_3 \bmod r_3}^* \max_{|\lambda| \leq 1/(r_3Q)} |W_3(\chi_3, \lambda)| \\
 &\quad \times \sum_{r_4 \leq P} \sum_{\chi_4 \bmod r_4}^* \left(\int_{-1/(r_4Q)}^{1/(r_4Q)} |W_4(\chi_4, \lambda)|^2 d\lambda \right)^{1/2} \\
 (13) \quad &\quad \times \sum_{r_5 \leq P} r_0^{-1+\varepsilon} \sum_{\chi_5 \bmod r_5}^* \left(\int_{-1/(r_5Q)}^{1/(r_5Q)} |W_5(\chi_5, \lambda)|^2 d\lambda \right)^{1/2}.
 \end{aligned}$$

The summation over r_5 on the last line is $K_5([r_1, r_2, r_3, r_4])$. Therefore, by Lemma 8,

$$K_5([r_1, r_2, r_3, r_4]) \ll [r_1, r_2, r_3, r_4]^{-1+2\varepsilon} |b_5|^{-1/2} L^{c_3}.$$

The contribution of the above quantity to the summation over r_4 in (13) is, by Lemma 8 again,

$$\begin{aligned}
 &\ll |b_5|^{-1/2} L^{c_3} \sum_{r_4 \leq P} [r_1, r_2, r_3, r_4]^{-1+2\varepsilon} \sum_{\chi_4 \bmod r_4}^* \left(\int_{-1/(r_4Q)}^{1/(r_4Q)} |W_4(\chi_4, \lambda)|^2 d\lambda \right)^{1/2} \\
 &= |b_5|^{-1/2} L^{c_3} K_4([r_1, r_2, r_3]) \\
 &\ll [r_1, r_2, r_3]^{-1+4\varepsilon} |b_4 b_5|^{-1/2} L^{c_4}.
 \end{aligned}$$

Using Lemma 6, we can compute the contribution of the above quantity to the sum over r_3 in (13) as follows:

$$\begin{aligned}
 &\ll |b_4 b_5|^{-1/2} L^{c_4} \sum_{r_3 \leq P} [r_1, r_2, r_3]^{-1+4\varepsilon} \sum_{\chi_3 \bmod r_3}^* \max_{|\lambda| \leq 1/(r_3Q)} |W_3(\chi_3, \lambda)| \\
 &= |b_4 b_5|^{-1/2} L^{c_4} J_3([r_1, r_2]) \\
 &\ll |b_3 b_4 b_5|^{-1/2} [r_1, r_2]^{-1+8\varepsilon} N^{1/2} L^{c_5}.
 \end{aligned}$$

Inserting this into (13) and applying Lemma 7, we have

$$\begin{aligned} I_5 &\ll N^{1/2} |b_3 b_4 b_5|^{-1/2} L^{c_5} \sum_{r_1 \leq P} \sum_{\chi_1 \bmod r_1}^* \max_{|\lambda| \leq 1/(r_1 Q)} |W_1(\chi_1, \lambda)| J_2(r_1) \\ &\ll N |b_2 b_3 b_4 b_5|^{-1/2} L^{c_6} J_1(1) \\ &\ll N^{3/2} |b_1 b_2 b_3 b_4 b_5|^{-1/2} L^{-A} \end{aligned}$$

for arbitrary $A > 0$ by applying Lemma 6 to J_2 and Lemma 7 to J_1 . Similarly we have $|I_4|, \dots, |I_1| \ll N^{3/2} |b_1 b_2 b_3 b_4 b_5|^{-1/2} L^{-A}$. This completes our proof.

REFERENCES

- [1] K. K. Choi and J. Y. Liu, Small prime solutions of quadratic equations, *Canad. J. Math.* 54(2002), 71-91. MR1880960 (2002k:11175)
- [2] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, Berlin, 1980. MR0606931 (82m:10001)
- [3] L. K. Hua, Some results in the additive prime number theory, *Quart. J. Math. (Oxford)* 9(1938), 68-80.
- [4] J. Y. Liu, On Lagrange's theorem with prime variables, *Quart. J. Math. (Oxford)* 54(2003), 453-462. MR2031178
- [5] J. Y. Liu and T. Zhan, An iterative method in the Waring-Goldbach problem, to appear.

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, BURNABY, BRITISH COLUMBIA, CANADA V5A 1S6

E-mail address: kkchoi@cecm.sfu.ca

DEPARTMENT OF MATHEMATICS, SHANDONG UNIVERSITY, JINAN, SHANDONG 250100, PEOPLE'S REPUBLIC OF CHINA

E-mail address: jyliu@sdu.edu.cn