Michigan Math. J. 59 (2010), 231–240

Iterates of Vinogradov's Quadric and Prime Paucity

VALENTIN BLOMER & JÖRG BRÜDERN

1. Introduction

Vinogradov's quadric is the variety defined by the pair of equations

$$x_1^2 + x_2^2 + x_3^2 = y_1^2 + y_2^2 + y_3^2, \qquad x_1 + x_2 + x_3 = y_1 + y_2 + y_3,$$

which is the special case $k = 2$ of the more general system

$$\begin{aligned} x_{1,1} + x_{2,1} + x_{3,1} &= x_{1,j} + x_{2,j} + x_{3,j} \quad (2 \le j \le k), \\ x_{1,1}^2 + x_{2,1}^2 + x_{3,1}^2 &= x_{1,j}^2 + x_{2,j}^2 + x_{3,j}^2 \quad (2 \le j \le k). \end{aligned} \tag{1}$$

In this paper, we study the distribution of integral solutions to (1). Our first result concerns the number $V_k(N)$ of such solutions inside the sphere

$$x_{1,j}^2 + x_{2,j}^2 + x_{3,j}^2 \le 3N^2, \quad 1 \le j \le k. \tag{2}$$

THEOREM 1. *Let $k \ge 2$ be a natural number. Then, for any real number δ with $0 < \delta < 3/2^k$,*

$$V_k(N) = N^3 P_k(\log N) + O(N^{3-\delta}), \tag{3}$$

where P_k is a polynomial of degree $2^{k-1} - 1$. In particular, $P_2(x) = 48(x + c)$, where

$$c = \gamma + \frac{1}{2}\log 2 + \log 3 - \frac{4}{3} + \frac{L'(1,\chi)}{L(1,\chi)} - \frac{\zeta'(2)}{\zeta(2)}$$

and where χ is the nontrivial character modulo 3. Moreover,

$$V_2(N) = N^3 P_2(\log N) + O(N^2 \log N). \tag{4}$$

The error term in (3) stems from the use of Weyl's bound for $\zeta(s)$ and $L(s,\chi)$ in the critical strip, and it can be improved by working with a truncated version of the Mellin integral (see equation (21) in Section 3) and with better bounds for $\zeta(s)$ and $L(s,\chi)$. When $k = 2$, one can use fourth moments of these functions over the critical line to obtain (4). If the Lindelöf hypothesis were true for $\zeta(s)$ and $L(s,\chi)$, then for any $k \ge 3$ the formula (3) would hold for any $\delta < 1$.

From the point of view of arithmetic geometry it is perhaps more natural to count solutions of (1) inside the box $|x_{i,j}| \le N$. Let $\tilde{V}_k(N)$ denote the number

Received November 25, 2008. Revision received March 23, 2009.
The first author was supported by an NSERC grant and a Sloan Research Fellowship.

of such solutions. Then, by (2), one has $V_k\big(N/\sqrt{3}\big) \le \tilde{V}_k(N) \le V_k(N)$, whence Theorem 1 implies the bounds

$$\tilde{V}_k(N) \asymp N^3(\log N)^{2^{k-1}-1}. \tag{5}$$

This suffices for the applications that follow, but an asymptotic formula for $\tilde{V}_k(N)$ should be within reach of elementary methods. In fact, when $k = 2$, we applied a technique that is Dirichlet's hyperbola method in disguise and obtained the estimate

$$\tilde{V}_2(N) = \left(\frac{12}{\pi}\right)^2 N^3 \log N + \tilde{c}N^3 + O(N^{5/2}\log N),$$

where

$$\tilde{c} = \left(\frac{12}{\pi}\right)^2 \left(\log 2 + 2\gamma - \frac{\zeta'(2)}{\zeta(2)} - \frac{5}{6}\right)$$

(see [3], the theorem and the following comment). Apparently, the reason for the much superior error term in (4) is the smoother kernel in (21), which in turn results from the spherical summation conditions (2).

A solution of the system (1) may be regarded as *trivial* if for some pair $1 \le j < j' \le k$ the triple $x_{1,j}, x_{2,j}, x_{3,j}$ is a permutation of $x_{1,j'}, x_{2,j'}, x_{3,j'}$, because such solutions may be viewed as arising from the smaller system with $k-1$ in place of k. Note that this remark, coupled with Theorem 1 or (5), shows that the number of trivial solutions is of smaller order of magnitude than $V_k(N)$ or $\tilde{V}_k(N)$. However, one may try to force the trivial solutions to dominate by restricting the variables to a suitably thin set. If this is successful for prime variables, then we described the effect as *prime paucity* in [1]. Here we follow an inquiry from Professor Wooley and determine those systems (1) with prime paucity. Let $\Pi_k(N)$ denote the number of primes $x_{i,j}$ in the box $1 \le x_{i,j} \le N$ $(1 \le i \le 3, 1 \le j \le k)$ that satisfy (1), and let $U_k(N)$ denote the number of such solutions that in addition satisfy

$$\{x_{1,j}, x_{2,j}, x_{3,j}\} \ne \{x_{1,j'}, x_{2,j'}, x_{3,j'}\} \quad \text{for all } 1 \le j < j' \le k. \tag{6}$$

THEOREM 2. *For any $k \ge 2$,*

$$U_k(N) \ll N^3(\log N)^{2^{k-1}-1-3k}(\log\log N)^{3k}.$$

In particular, we see that for $2 \le k \le 4$ one has

$$U_k(N) \ll N^3(\log N)^{-5}(\log\log N)^{12}.$$

It is now straightforward to evaluate $\Pi_k(N)$. One chooses a triple of primes $x_{1,1}, x_{1,2}, x_{1,3}$ and permutes it $k-1$ times to find $6^{k-1}\pi(N)^3 + O(N^2)$ "diagonal" solutions. By the argument preceding Theorem 2, the remaining solutions are at most $O(U_2(N) + \cdots + U_k(N))$ in number. For $2 \le k \le 4$, it follows that

$$\Pi_k(N) = 6^{k-1}\pi(N)^3 + O(N^3(\log N)^{-5}(\log\log N)^{12}), \tag{7}$$

which confirms prime paucity in these cases. For $k = 2$, a more general form of (7) was obtained in [2].

We shall deduce Theorem 2 from a simple version of Selberg's sieve. With extra work along the lines of Rieger [10, pp. 94–96], the factor $(\log\log N)^{3k}$ could be removed from the upper bound estimate. In an effort to keep the underlying Diophantine considerations transparent, rather than disguised by elementary but tedious technicalities, we have preferred to confine ourselves to this marginally weaker result that still features the prime paucity effect for $k \le 4$. Probabilistic heuristics and the approach of computing the major arc contribution in a circle both suggest that the order of magnitude of $U_k(N)$ should be $N^3(\log N)^{2^{k-1}-1-3k}$. In particular, one would predict that $U_5(N) \gg N^3$, so it is likely that the variety (1) exhibits prime paucity if and only if $2 \le k \le 4$.

One may compare our results with similar ones for sums of two squares. If one counts the integral solutions of a system

$$x_1^2 + x_2^2 = x_3^2 + x_4^2 = \cdots = x_{2k-1}^2 + x_{2k}^2$$

inside a sphere $x_1^2 + x_2^2 \le N$, then one must evaluate the moment

$$\sum_{n \le N} r_4(n)^k, \tag{8}$$

where $r_4(n)$ is the number of representations $n = x_1^2 + x_2^2$ with $x_1, x_2 \in \mathbb{Z}$, and one finds an asymptotic formula by Dirichlet series techniques (see, most recently, [4]). Also, one experiences prime paucity for $k = 2$ (Erdős [5]) and $k = 3$ (Brüdern and Blomer [2]) but would not predict this effect for larger values of k. Rather than working with the quadratic form $x^2 + y^2$ of discriminant -4, we relate $V_k(N)$ to moments similar to (8) but with $q(x, y) = x^2 + xy + y^2$ of discriminant -3 in the role of sums of two squares.

For fixed $a \in \mathbb{Z}$ and $b \in \mathbb{N}_0$, consider the pair of equations

$$x_1 + x_2 + x_3 = a, \qquad x_1^2 + x_2^2 + x_3^2 = b, \tag{9}$$

and let $R(a, b)$ denote the number of its solutions in $x_1, x_2, x_3 \in \mathbb{Z}$. Then

$$V_k(N) = \sum_{a \in \mathbb{Z}} \sum_{0 \le b \le 3N^2} R(a, b)^k. \tag{10}$$

Note that (9) implies $a \equiv b \bmod 2$, so it suffices to sum over such pairs in (10). Now substitute the linear equation in (9) into the quadratic one to see that (9) is equivalent to

$$q(3x_1 - a, 3x_2 - a) = \tfrac{1}{2}(9b - 3a^2), \qquad x_1 + x_2 + x_3 = a. \tag{11}$$

In particular, it follows that

$$\begin{aligned} &R(a, b) \\ &\quad = \#\big\{(y_1, y_2) \in \mathbb{Z}^2 : q(y_1, y_2) = \tfrac{1}{2}(9b - 3a^2),\ y_1 \equiv y_2 \equiv a \bmod 3\big\}, \end{aligned} \tag{12}$$

and by substituting this into (10) we obtain a formula for $V_k(N)$ that is not dissimilar to (8). One may exploit this idea further and express $V_k(N)$ in terms of certain weighted moments of the number of representations of integers by the

form $q(x,y)$. We present this in Section 2 and then, in Section 3, discuss the relevant moments by classical Dirichlet series techniques; this will complete the proof of Theorem 1. In Section 4 we review some arithmetical facts about the ring $\mathbb{Z}\big[\frac{1}{2}\big(1+\sqrt{-3}\big)\big]$. The factorization described in Lemma 4 is an abstracted form of the main idea in the sieve preparation work in our related recent paper [2], and it is also fundamental for the proof of Theorem 2 in Section 5.

2. Reduction to Binary Quadratic Forms

Let $\omega = \frac{1}{2}\big(1+\sqrt{-3}\big)$. The integers in the number field $\mathbb{Q}(\omega)$ form the ring $\mathbb{Z}[\omega]$ with unique factorization and six units $\pm 1, \pm\omega, \pm\omega^2$. We will typically denote elements in $\mathbb{Z}[\omega]$ with Greek letters and use lowercase Latin for rational integers. For $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, define the *conjugate* by $\bar{\alpha} = (a+b) - b\omega = a + b\bar{\omega}$ and the *norm* by $\mathcal{N}\alpha := \alpha\bar{\alpha} = q(a,b)$.

Let χ denote the nontrivial Dirichlet character modulo 3, and define the arithmetical function $r(n) = \sum_{d|n} \chi(d)$. Then $6r(n)$ equals the number of solutions of $q(x,y) = n$ in integers x, y; also, $r(n)$ equals the number of ideals $\mathfrak{a} \subset \mathbb{Z}[\omega]$ of norm n. This much of the theory of $\mathbb{Z}[\omega]$ is found in Hua [7], for example.

We are ready to rewrite $V_k(N)$ in terms of moments of $r(n)$. Note that integers y_1, y_2 satisfy $y_1 \equiv y_2 \equiv a \bmod 3$ if and only if $y_1 + y_2\omega \equiv a(1+\omega) \bmod 3$ in $\mathbb{Z}[\omega]$. By (12),

$$R(a,b) = \#\big\{\delta \in \mathbb{Z}[\omega] : \mathcal{N}\delta = \tfrac{1}{2}(9b - 3a^2),\ \delta \equiv a + a\omega \bmod 3\big\}. \tag{13}$$

However, if $\delta = r + s\omega$ then $3 \mid \mathcal{N}\delta$ is equivalent to $3 \mid q(r,s)$, which in turn holds if and only if $r \equiv s \bmod 3$. Hence, if $3 \nmid a$, then $\mathcal{N}\delta = \frac{1}{2}(9b - 3a^2)$ implies that δ is either in the class $1 + \omega \bmod 3$ or in $2(1+\omega) \bmod 3$. Yet exactly three of the units $\eta \in \mathbb{Z}[\omega]$ satisfy $\eta(1+\omega) \equiv 1 + \omega \bmod 3$, and the other three yield $\eta(1+\omega) \equiv 2(1+\omega) \bmod 3$. Consequently, when $3 \nmid a$, we find that

$$R(a,b) = \tfrac{1}{2}\#\big\{\mathfrak{a} \subset \mathbb{Z}[\omega] : \mathcal{N}\mathfrak{a} = \tfrac{1}{2}(9b - 3a^2)\big\} = 3r\big(\tfrac{1}{2}(9b - 3a^2)\big).$$

If $3 \mid a$ but $a^2 \neq 3b$, then the same argument shows that $3 \mid \delta$ whenever $\mathcal{N}\delta = \frac{1}{2}(9b - 3a^2)$, and we may cancel a factor 9 in (13) to deduce that, whenever $a = 3\tilde{a}$ and $a^2 \neq 3b$, one has

$$R(3\tilde{a}, b) = \#\big\{\mathfrak{a} \subset \mathbb{Z}[\omega] : \mathcal{N}\mathfrak{a} = \tfrac{1}{2}(b - 3\tilde{a}^2)\big\} = 6r\big(\tfrac{1}{2}(b - 3\tilde{a}^2)\big).$$

We next insert these formulas into (10). In the exceptional case where $a^2 = 3b$ one trivially has $R(a,b) = 1$, so these terms contribute at most $O(N)$ to (10). For notational convenience, put $r(n) = 0$ when $n \leq 0$. It then follows that

$$V_k(N) = 6^k V_k'(N) + 3^k V_k''(N) + O(N), \tag{14}$$

where

$$V_k'(N) = \sum_{a \in \mathbb{Z}} \sum_{\substack{0 \leq b \leq 3N^2 \\ b \equiv a \bmod 2}} r\big(\tfrac{1}{2}(b - 3a^2)\big)^k$$

and

$$V_k''(N) = \sum_{\substack{a\in\mathbb{Z}\\ 3\nmid a}} \sum_{\substack{0\le b\le 3N^2\\ b\equiv a \bmod 2}} r\big(\tfrac{1}{2}(9b-3a^2)\big)^k.$$

In the sum defining $V_k'(N)$ we fix a and substitute $n = \frac{1}{2}(b-3a^2)$ for b to deduce that

$$\begin{aligned} V_k'(N) &= \sum_{a\in\mathbb{Z}} \sum_{n\le (3/2)(N^2-a^2)} r(n)^k \\ &= \sum_{n\le (3/2)N^2} r(n)^k \big(2\big(N^2-\tfrac{2}{3}n\big)^{1/2} + O(1)\big). \end{aligned} \tag{15}$$

Similarly, when $3\nmid a$ and $a \equiv b \bmod 2$, one may write $\frac{1}{2}(9b-3a^2) = 3n$ with $3\nmid n$. Substitute n for b in the sum defining $V_k''(N)$ and then use multiplicativity for r. Since $r(3) = 1$, we find that

$$\begin{aligned} V_k''(N) &= \sum_{\substack{a\in\mathbb{Z}\\ 3\nmid a}} \sum_{\substack{n\le (1/2)(9N^2-a^2)\\ 3\nmid n}} r(n)^k \\ &= \sum_{\substack{n\le (9/2)N^2\\ 3\nmid a}} r(n)^k \big(\tfrac{4}{3}(9N^2-2n)^{1/2} + O(1)\big). \end{aligned} \tag{16}$$

It remains to evaluate the weighted moments that occur in (15) and (16). We summarize the relevant asymptotics in the next lemma. The results feature the Riemann zeta function $\zeta(s)$, the Dirichlet L-function $L(s,\chi)$, the logarithmic derivative $\psi(s)$ of the Gamma function, and the Euler–Mascheroni constant γ.

LEMMA 1. *Let $k \ge 2$ and $K = 2^{k-1}$. Then*

$$\sum_{m\le M} r(m)^k \ll M(\log M)^{K-1}, \tag{17}$$

and there exist real polynomials $Q_k, \tilde{Q}_k$ of degree $K-1$ such that

$$\sum_{m\le M} (M-m)^{1/2} r(m)^k = M^{3/2} Q_k(\log M) + O(M^{3/2-\eta}) \tag{18}$$

and

$$\sum_{\substack{m\le M\\ 3\nmid m}} (M-m)^{1/2} r(m)^k = M^{3/2} \tilde{Q}_k(\log M) + O(M^{3/2-\eta}) \tag{19}$$

hold for any $\eta < \frac{3}{4K}$. If $k = 2$, then (18) *and* (19) *hold with $\eta = \frac{1}{2}$ and one has*

$$\begin{aligned} Q_2(x) &= \frac{1}{9}\left(x + \gamma + \frac{1}{4}\log 3 - \psi\left(\frac{5}{2}\right) + 2\frac{L'(1,\chi)}{L(1,\chi)} - 2\frac{\zeta'(2)}{\zeta(2)}\right), \\ \tilde{Q}_2(x) &= \frac{2}{27}\left(x + \gamma + \frac{3}{4}\log 3 - \psi\left(\frac{5}{2}\right) + 2\frac{L'(1,\chi)}{L(1,\chi)} - 2\frac{\zeta'(2)}{\zeta(2)}\right). \end{aligned}$$

With this lemma in hand, choose $M = \frac{3}{2}N^2$ in (18) and $M = \frac{9}{2}N^2$ in (19) to determine asymptotic formulas for $V_k'(N)$ and $V_k''(N)$. When substituted into (14), Theorem 1 follows with

$$P_2(x) = 108Q_2\big(2x + \log\tfrac{3}{2}\big) + 162\tilde{Q}_2\big(2x + \log\tfrac{9}{2}\big).$$

The explicit form of $P_2(x)$ in Theorem 1 is then found using the formula $\psi\big(\frac{5}{2}\big) = \frac{8}{3} - 2\log 2 - \gamma$, which is derived from the standard formula for $\psi\big(\frac{1}{2}\big)$ and the functional equation.

3. Moments of Representation Numbers

In this section we prove Lemma 1. Let $k \geq 2$. Since $r(n)^k$ is multiplicative, we may compare Euler products to find that

$$\sum_{n=1}^{\infty} \frac{r(n)^k}{n^s} = G_k(s)(\zeta(s)L(s,\chi))^K, \tag{20}$$

where $K = 2^{k-1}$ as before and where

$$G_k(s) = \Big(1 - \frac{1}{3^s}\Big)^{K-1} \prod_{p\equiv 1\,(3)} \Big(\sum_{m=0}^{\infty} \frac{(m+1)^k}{p^{ms}}\Big)\Big(1 - \frac{1}{p^s}\Big)^{2K} \prod_{p\equiv 2\,(3)} \Big(1 - \frac{1}{p^{2s}}\Big)^{K-1}.$$

The function G_k is holomorphic, nonzero, and bounded uniformly in $\Re s \geq \frac{1}{2} + \delta$ for any fixed $\delta > 0$; this follows, for example, from [9, Lemma 2] (with $2c = 2^k$ and $\cos\phi = 0$). The identity (20) now implies (17) (cf. [4, Thm. 1]).

For the asymptotic formula (18), we note that whenever $M > 0$ one has

$$\int_0^M (M-x)^{1/2} x^{s-1}\, dx = \frac{\sqrt{\pi}\,\Gamma(s)}{2\Gamma\big(s+\frac{3}{2}\big)} M^{s+1/2}$$

in the right half-plane $\Re s > 0$ (see [6, (3.191.1)]). By Mellin inversion,

$$\sum_{n\leq M} (M-n)^{1/2} r^k(n) = \frac{1}{2\pi i} \int_{(2)} \frac{\sqrt{\pi}\,\Gamma(s)}{2\Gamma\big(s+\frac{3}{2}\big)} G_k(s)(\zeta(s)L(s,\chi))^K M^{s+1/2}\, ds. \tag{21}$$

Note that the integrand has a pole at $s = 1$ of order K and residue $M^{3/2}Q_k(\log M)$ for some polynomial Q_k of degree $K-1$. We wish to move the line of integration in (21) to $\Re(s) = \sigma$ with $\sigma < 1$ as small as possible. The familiar Weyl bound coupled with the Phragmén–Lindelöf convexity principle gives

$$\zeta(\sigma+it)L(\sigma+it,\chi) \ll_\varepsilon (1+|t|)^{(2/3)(1-\sigma)+\varepsilon}, \quad \tfrac{1}{2} \leq \sigma \leq 1,\ t \in \mathbb{R},$$

and Stirling's formula yields $\Gamma(s)/\Gamma\big(s+\frac{3}{2}\big) \ll |s|^{-3/2}$. Thus we may move the line of integration to $\Re(s) = \sigma$ whenever $\sigma > 1 - \frac{3}{4K}$. The new integral is still absolutely convergent, and it follows that

$$\sum_{m\leq M} (M-m)^{1/2} r(m)^k = M^{3/2}Q_k(\log M) + O(M^{3/2-(3/4K)+\varepsilon}).$$

This establishes (18). For (19), we need only note that the condition $3 \nmid n$ removes the Euler factor for $p = 3$ from the generating function (20). Thus, no substanstial changes are needed in the preceding argument to confirm (19) as well.

Now suppose that $k = 2$. In this special case, the function $G_2(s)$ and its companion can be made very explicit. In fact, one has

$$\sum_{n=1}^{\infty} \frac{r(n)^2}{n^s} = \frac{(\zeta(s)L(s,\chi))^2}{(1+3^{-s})\zeta(2s)}, \qquad \sum_{\substack{n=1 \\ 3\nmid n}}^{\infty} \frac{r(n)^2}{n^s} = \frac{(\zeta(s)L(s,\chi))^2(1-3^{-s})}{(1+3^{-s})\zeta(2s)}.$$

One proceeds as before except now shifting the line of integration to $\Re s = \frac{1}{2}$. Again, the integral remains in the range of absolute convergence owing to the classical upper bound

$$\int_1^T |\zeta(1/2+it)|^2 |L(1/2+it,\chi)|^2\, dt \ll T \log T.$$

By the class number formula we have $L(1,\chi) = \pi/3\sqrt{3}$, so the residue at $s = 1$ can be written explicitly. This yields the formulas for Q_2 and $\tilde{Q}_2$, proving Lemma 1.

4. Preparation for the Sieve

We begin with some simple comments on the ring $\mathbb{Z}[\omega]$. For $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, define the integers

$$\mathcal{R}\alpha = a, \quad \mathcal{I}\alpha = b, \quad \mathcal{S}\alpha = -a - b.$$

LEMMA 2. *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ and assume that*

$$\{\mathcal{R}(\alpha\beta), \mathcal{I}(\alpha\beta), \mathcal{S}(\alpha\beta)\} \neq \{\mathcal{R}(\alpha\bar{\beta}), \mathcal{I}(\alpha\bar{\beta}), \mathcal{S}(\alpha\bar{\beta})\}.$$

Then all six integers

$$\mathcal{R}\beta,\ \mathcal{I}\beta,\ \mathcal{S}\beta,\ \mathcal{R}\alpha - \mathcal{I}\alpha,\ 2\mathcal{R}\alpha + \mathcal{I}\alpha,\ \mathcal{R}\alpha + 2\mathcal{I}\alpha \tag{22}$$

are nonzero.

Proof. This is straightforward to check using the formulas

$$\begin{aligned} (a+b\omega)(c+d\omega) &= (ac-bd) + (bc+ad+bd)\omega, \\ (a+b\omega)(c+d\bar{\omega}) &= (ac+bd+ad) + (bc-ad)\omega. \end{aligned} \tag{23}$$

For example, $\mathcal{R}\beta = 0$ implies $\mathcal{R}(\alpha\beta) = \mathcal{S}(\alpha\bar{\beta})$, $\mathcal{I}(\alpha\beta) = \mathcal{R}(\alpha\bar{\beta})$, and $\mathcal{S}(\alpha\beta) = \mathcal{I}(\alpha\bar{\beta})$. The other five cases are similar. □

LEMMA 3. *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ and assume that the six integers in* (22) *are nonzero. Then the integers*

$$\mathcal{R}(\alpha\beta),\ \mathcal{I}(\alpha\beta),\ \mathcal{S}(\alpha\beta),\ \mathcal{R}(\alpha\bar{\beta}),\ \mathcal{I}(\alpha\bar{\beta}),\ \mathcal{S}(\alpha\bar{\beta})$$

are pairwise different.

Proof. This is again straightforward to check using the formulas (23). For example, $\mathcal{R}(\alpha\beta) = \mathcal{S}(\alpha\bar{\beta})$ implies $\mathcal{R}\beta \cdot (2\mathcal{R}\alpha + \mathcal{I}\beta) = 0$, contradicting the hypothesis. The other cases are similar. □

For $k \in \mathbb{N}$, let $K = 2^{k-1}$ and $A_k := \{0, 1, \dots, K-1\}$. We represent a typical member $n \in A_k$ in 2-adic representation: $n = \sum a_\nu 2^\nu$ with $a_\nu \in \{0, 1\}$. For $1 \le j \le k$ we define $B_{k,j}, C_{k,j}$ as follows:

$$B_{k,1} := A_k, \qquad B_{k,j} := \Big\{ n = \sum_{\nu=0}^{k-2} a_\nu 2^\nu \;\Big|\; a_{k-j} = 0 \Big\} \quad \text{if } 2 \le j \le k;$$

$$C_{k,1} := \emptyset, \qquad C_{k,j} := \Big\{ n = \sum_{\nu=0}^{k-2} a_\nu 2^\nu \;\Big|\; a_{k-j} = 1 \Big\} \quad \text{if } 2 \le j \le k.$$

Then, for any $j \in \{1, \dots, k\}$, the set A_k is the disjoint union of $B_{k,j}$ and $C_{k,j}$.

LEMMA 4. *Let $M \in \mathbb{N}$, and let $\alpha_1, \dots, \alpha_k \subseteq \mathbb{Z}[\omega]$ such that $\mathcal{N}\alpha_1 = \dots = \mathcal{N}\alpha_k = M$. Then there are $\delta_0, \dots, \delta_{K-1} \in \mathbb{Z}[\omega]$ such that*

$$\alpha_j = \prod_{n \in B_{k,j}} \delta_n \prod_{m \in C_{k,j}} \bar{\delta}_m, \quad 1 \le j \le k;$$

in particular, $\mathcal{N}(\delta_0 \cdots \delta_{K-1}) = M$.

Note that we do not claim that the numbers δ_n are unique, and in general they are not, not even up to units. But they are not "too far" from being unique. However, we need not investigate this any further. For the sieve argument in the next section, the existence alone has an enveloping effect that suffices.

Proof of Lemma 4. We proceed by induction on k. There is nothing to show for $k = 1$. Assume we have found suitable $\delta_0, \dots, \delta_{K-1}$ for given numbers $\alpha_1, \dots, \alpha_k$, and assume we add another $\alpha_{k+1} \in \mathbb{Z}[\omega]$ with $\mathcal{N}\alpha_{k+1} = M$. By unique factorization, α_{k+1} contains the same prime factors, with the same multiplicities as the product of the δ_n, except that some of the prime factors may be conjugated. Hence, for $0 \le n \le K-1$ we can decompose δ_n in the form $\delta_n = \delta'_{2n}\delta'_{2n+1}$, where δ'_{2n} is the product of all prime factors of δ_n that also divide α_{k+1}. Now

$$\alpha_{k+1} = \delta'_0\bar{\delta}'_1 \cdot \delta_2\bar{\delta}'_3 \cdots \delta'_{2K-2}\bar{\delta}'_{2K-1},$$

and the collection $\delta'_0, \dots, \delta'_{2K-1}$ gives the desired elements. □

Before we move on to the sieve, we also recall the well-known bound $\#\{\delta \in \mathbb{Z}[\omega] : \mathcal{N}\delta \le X\} \ll X$. By a standard divisor estimate, this yields

$$\sum_{\substack{\delta_0, \dots, \delta_{m-1} \in \mathbb{Z}[\omega] \\ \mathcal{N}(\delta_0 \cdots \delta_{m-1}) \le X}} 1 \ll_m X(\log X)^{m-1} \tag{24}$$

for any fixed value of $m \in \mathbb{N}$.

5. An Upper Bound Sieve Estimate

We derive Theorem 2 from the following consequence of Selberg's sieve.

LEMMA 5. *Let $m \in \mathbb{N}$, and let $r_1, \dots, r_s \in \mathbb{Z}$ be pairwise distinct. Then the number of positive integers $n \le X$ such that $\frac{1}{m}(n + r_j)$ is simultaneously a prime number for $1 \le j \le s$ does not exceed*

$$O\Big(X(\log X)^{-s}\Big(\log\log\Big(3 + \max_{1\le j\le s}|r_j|\Big)\Big)^s\Big).$$

The implicit constant depends only on s.

Proof. For $m = 1$, this is a special case of [8, Satz 2.4.2]. The case $m > 1$ is easily reduced to the case $m = 1$: we observe that the lemma is trivial unless $r_1 \equiv \cdots \equiv r_s \equiv r \pmod m$ for some $r \in \{0, \dots, m-1\}$, in which case we write n as $mn' - r$. □

We are ready to estimate $U_k(n)$. Eliminate x_3 from (11), where x_1, x_2, x_3 are rational primes in the current context. This shows that

$$U_k(N) = \sum_{a\in\mathbb{Z}} \sum_{\substack{0\le b\le 3N^2\\ b\equiv a \bmod 2}} U_k(N; a, b),$$

where $U_k(N; a, b)$ is the number of $2k$-tuples $p_{1,1}, p_{2,1}, \dots, p_{1,k}, p_{2,k}$ of primes such that $a - p_{1,j} - p_{2,j}$ is also prime for $1 \le j \le k$, such that

$$\mathcal{N}(3p_{1,j} - a + (3p_{2,j} - a)\omega) = \tfrac{1}{2}(9b - 3a^2)$$

holds for all j, and that satisfy the nontriviality conditions (6). The latter now read

$$\{p_{1,j}, p_{2,j}, a - p_{1,j} - p_{2,j}\} \ne \{p_{1,j'}, p_{2,j'}, a - p_{1,j'} - p_{2,j'}\} \tag{25}$$

for all $1 \le j < j' \le k$. By Lemma 4 and the notation in the paragraph preceding it, an upper bound for this quantity is given by

$$U_k(N; a, b) \le \sum_{\delta_0, \dots, \delta_{K-1}} 1, \tag{26}$$

where the $\delta_0, \dots, \delta_{K-1}$ run over elements of $\mathbb{Z}[\omega]$ subject to $\mathcal{N}(\delta_0 \cdots \delta_{K-1}) = \frac{1}{2}(9b - 3a^2)$ and the condition that the rational numbers

$$p_{1,j} = \frac{1}{3}\Big(\mathcal{R}\Big(\prod_{n\in B_{k,j}} \delta_n \prod_{m\in C_{k,j}} \bar{\delta}_m\Big) + a\Big), \tag{27a}$$

$$p_{2,j} = \frac{1}{3}\Big(\mathcal{I}\Big(\prod_{n\in B_{k,j}} \delta_n \prod_{m\in C_{k,j}} \bar{\delta}_m\Big) + a\Big), \quad \text{and} \tag{27b}$$

$$p_{3,j} = a - p_{1,j} - p_{2,j} = \frac{1}{3}\Big(\mathcal{S}\Big(\prod_{n\in B_{k,j}} \delta_n \prod_{m\in C_{k,j}} \bar{\delta}_m\Big) + a\Big) \tag{27c}$$

are prime for $1 \le j \le k$ and satisfy (25). Now sum (26) over a and b, and interchange the order of summation. Then

$$U_k(N) \le \sum_{\delta_0,\dots,\delta_{K-1}} \sum_{a \le \sqrt{9N^2-(2/3)\mathcal{N}(\delta_0\cdots\delta_{K-1})}} 1 \le \sum_{\mathcal{N}(\delta_0\cdots\delta_{K-1})\le(27/2)N^2} \sum_{a\le 3N} 1,$$

where the sums over a are subject to the conditions (27) and (25). We are now in a position to apply Lemma 5 to the inner sum with $m = 3$ and $s = 3k$. We observe that (25) when combined with Lemmas 2 and 3 guarantees the applicability of Lemma 5. Thus we obtain

$$U_k(N) \ll_k \frac{N(\log\log N)^{3k}}{(\log N)^{3k}} \sum_{\mathcal{N}(\delta_0\cdots\delta_{K-1})\le(27/2)N^2} 1,$$

and Theorem 2 now follows from (24).

References

[1] V. Blomer and J. Brüdern, *Prime paucity for sums of two squares,* Bull. London Math. Soc. 40 (2008), 457–462.

[2] ———, *A quadric with arithmetic paucity,* Quart. J. Math. 60 (2009), 283–290.

[3] ———, *The number of integer points on Vinogradov's quadric,* Monatsh. Math. (to appear).

[4] V. Blomer and A. Granville, *Estimates for representation numbers of quadratic forms,* Duke Math. J. 135 (2006), 261–302.

[5] P. Erdős, *On additive properties of squares of primes, I,* Proc. Acad. Wet. Amsterdam 41 (1938), 37–41.

[6] I. S. Gradshteyn and I. M. Ryzhik, *Tables of integrals, series, and products,* 5th ed., Academic Press, Boston, 1994.

[7] L. K. Hua, *Introduction to number theory,* Springer-Verlag, Berlin, 1982.

[8] K. Prachar, *Primzahlverteilung,* Springer-Verlag, Berlin, 1957.

[9] R. A. Rankin, *Sums of powers of cusp form coefficients,* Math. Ann. 263 (1983), 227–236.

[10] G. J. Rieger, *Über die Summe aus einem Quadrat und einem Primzahlquadrat,* J. Reine Angew. Math. 231 (1968), 89–100.

V. Blomer
Mathematisches Institut
Bunsenstraße 3-5
37073 Göttingen
Germany

blomer@uni-math.gwdg.de

J. Brüdern
Institut für Algebra und Zahlentheorie
Universität Stuttgart
70511 Stuttgart
Germany

bruedern@mathematik.uni-stuttgart.de