ACTA ARITHMETICA
138.2 (2009)

Cyclic polygons of integer points

by

M. N. Huxley (Cardiff) and S. V. Konyagin (Moscow)

1. Introduction. Among the circles drawn through three distinct integer points in the plane, are circles which pass through four or more integer points rare? This question is a simplification of one asked by Huxley and Žunić in their investigation of configurations of integer points in convex plane sets [6, 7]. For a convex plane set S, the discrete version of S is the set $J(S)$ of integer points in S. The (discrete) weight of S is the size $N(S)$ of $J(S)$, the number of integer points in S. There is a natural equivalence relation on sets of integer points, that J is equivalent to J' when J' is the translation of J by an integer vector. We extend this equivalence to the convex sets S and S' themselves, which we call equivalent when the configurations $J(S)$ and $J'(S)$ are equivalent. The question which arose in [7] is: among the equivalence classes of circles of fixed weight drawn through three distinct points in the plane, are circles which pass through four or more integer points rare? More generally, Huxley and Žunić define the family of S-ovals to be all sets S' obtained from a given convex plane set S (the "oval") by enlargement and translation, and they ask the same question with the family of circles replaced by the family of S-ovals. In this generality the answer can be No, as when S is a square.

Let $P_k(R)$ denote the number of equivalence classes of sets of k distinct integer points such that the k points lie on some circle radius $r \le R$.

Theorem 1. *For R sufficiently large*

$$P_3(R) = \pi^2 R^4 + O(R^{2+\kappa}(\log R)^\lambda),$$

where $\kappa = 131/208$ and $\lambda = 18627/8320$.

Theorem 2. *Let $\varepsilon > 0$. For R sufficiently large*

$$P_4(R) = \frac{32(3+\sqrt{2})}{21\zeta(3)}\,\zeta\left(\frac{3}{2}\right)L\left(\frac{3}{2},\chi\right)R^3 + O(R^{76/29+\varepsilon}),$$

2000 *Mathematics Subject Classification*: Primary 11E25; Secondary 11P21.
Key words and phrases: lattice points (integer points), cyclic quadrilaterals.

DOI: 10.4064/aa138-2-2 © Instytut Matematyczny PAN, 2009

where $L(s,\chi)$ is the Dirichlet L-function formed with the non-trivial character mod 4. The constant implied in the O-sign depends on ε.

THEOREM 3. *There is a constant c such that for each $k \geq 5$ and R sufficiently large (depending on k)*

$$P_k(R) \geq cR^2 \log R.$$

Let $\varepsilon > 0$. For each $k \geq 5$ there is a constant $C(k,\varepsilon)$ such that for R sufficiently large

$$P_k(R) \leq C(k,\varepsilon) R^{76/29+\varepsilon}.$$

The proof of Theorem 1 follows a suggestion of Kolountzakis developed for general ovals in [8].

With more work we can replace the factor $c \log R$ in Theorem 3 by a polynomial in $\log R$ of degree $2^{k-1} - 1$, so for large enough R the lower estimate increases with k for small $k \geq 5$. This is because we consider a small number of circles (decreasing with k), which however contain many integer points.

Let $P'_k(R)$ be the number of equivalence classes of sets of k distinct integer points which form the complete set of integer points on some circle radius $r \leq R$. Schinzel [9] showed that $P'_k(R)$ is non-zero for large R. Then we have

$$P_4(R) = \sum_{k=4}^{K(R)} {}_kC_4 P'_k(R).$$

In [7] Huxley and Žunić consider $M(N)$, the number of equivalence classes of S-ovals with weight at most N. They impose the Line Condition, that S is a convex bounded plane set with no straight line segment of rational gradient in the boundary. The unit circle satisfies the Line Condition, but the unit square does not. In particular, when S is the circle, the argument of [7] shows that

$$N^2 \geq M(N) \geq N^2 - O\Big(\sum_{k=4}^{K(R)} k^2 P'_k(R)\Big)$$

for some value of R of the form $O(\sqrt{N})$. Since $k^2 \leq 16\,{}_kC_4$ for $k \geq 4$, we deduce that

$$M(N) = N^2 + O(C(\varepsilon) N^{3/2+\varepsilon})$$

for any $\varepsilon > 0$, with $C(\varepsilon)$ some constant depending on ε.

2. Proof of Theorem 1 and Theorem 3 (lower bound)

Proof of Theorem 1. Each equivalence class contains three triangles with one vertex at the origin. The next vertex M_1 lies in the closed circular disc

centre the origin, radius $2R$. The third vertex lies on some circle of the coaxial system through O and M_1 with radius at most R. Two circles of the system, C_1 and C_2, have radius R. If M_2 lies on or inside C_1, and on or outside C_2, but not at O or M_1, then the circle OM_1M_2 has some radius $r \le R$, and O, M_1, M_2 are numbered anticlockwise; if M_2 lies on or inside C_2, and on or outside C_1, but not at O or M_1, then the circle OM_1M_2 has some radius $r \le R$, but O, M_1, M_2 are numbered clockwise. The search region for M_2 consists of the points of the circular disc bounded by C_1 which do not lie in the circular disc bounded by C_2, and also the shorter arc of C_2 strictly between M_1 and O. Let $OM_1 = 2d$, and let the chord OM_1 subtend an angle 2θ at the centre of C_1. Then

$$d = R\sin\theta, \tag{2.1}$$

and the area of the search region for M_2 is

$$\pi R^2 - 2(\theta R^2 - R^2\sin\theta\cos\theta).$$

We regard the search region as a disc radius R minus a "vesica", a region bounded by arcs of two equal circles. Theorem 5 of [5] applies to the disc and the vesica, so the number of integer points in this region is

$$(\pi - 2\theta + \sin 2\theta)R^2 + O(R^\kappa(\log R)^\lambda)$$

for R sufficiently large, where $\kappa = 131/208$ and $\lambda = 18627/8320$.

In order to sum over M_1, we take a continuous variable t corresponding to $2d$ in (2.1), and we put

$$F(t) = \pi - 2\theta + \sin 2\theta,$$

where θ in $0 < \theta < \pi/2$ is defined by $\sin\theta = t/2R$. Then

$$3P_3(R) = \sum_{M_1}(R^2F(\sqrt{m_1^2+n_1^2}) + O(R^\kappa(\log R)^\lambda)),$$

where the sum is over integer points $M_1 = (m_1, n_1)$ in the circle centre O, radius $2R$. We use Theorem 5 of [5] again to pass from the discrete sum to the integral. For $t \le 2R$, let $I(t)$ be the number of integer points in the circle centre O, radius t. Then

$$I(t) = \pi t^2 + O(t^\kappa(\log(t+2))^\lambda) + O(1) \tag{2.2}$$

uniformly in $0 \le t \le 2R$. We can write

$$\begin{aligned} 3P_3(R) &= R^2\int_0^{2R} F(t)\,dI(t) + O(R^{2+\kappa}(\log R)^\lambda) \\ &= 2\pi R^2\int_0^{2R} F(t)t\,dt + O(R^{2+\kappa}(\log R)^\lambda). \end{aligned} \tag{2.3}$$

We evaluate the integral by the substitution $t = 2R\sin\theta$, so

$$\int_0^{2R} F(t)t\,dt = 4R^2 \int_0^{\pi/2} (\pi - 2\theta + \sin 2\theta)\sin\theta\cos\theta\,d\theta = \frac{3\pi R^2}{2}$$

by an elementary calculation. We substitute into (2.3) to obtain the result of Theorem 1.

Proof of Theorem 3 (lower bound). We consider cyclic polygons with centre at the origin; we expect these to provide the majority of equivalence classes when $k \geq 5$. For $n \geq 1$, let $r(n)$ be the number of solutions in integers (not necessarily positive) of $n = x^2 + y^2$. Let $Q_\ell(N)$ be the number of integers n in $1 \leq n < N$ with $r(n) = \ell$; we know that $Q_\ell(N) = 0$ unless $4 \mid \ell$. Using the notation $I(t)$ as in (2.2), we have for N sufficiently large

$$\sum_\ell \ell Q_\ell(N) = \sum_{n=1}^{N} r(n) = I(\sqrt{N}) - 1 = \pi N + O(N^{\kappa/2}(\log N)^\lambda). \tag{2.4}$$

We compare (2.4) with a result stated by Ramanujan and proved by Wilson [10]:

$$\sum_\ell \ell^2 Q_\ell(N) = \sum_{n=1}^{N} r(n)^2 = \left(\frac{1}{4} + o(1)\right) N\log N.$$

If $r(n) = \ell \geq k$, then the number of ways of selecting k vertices of a cyclic polygon centre O is the binomial coefficient

$${}_\ell C_k = \frac{\ell(\ell-1)\cdots(\ell-k+1)}{k!} \geq \frac{\ell(\ell-1)}{k(k-1)}.$$

Hence

$$\begin{aligned} P_k(\sqrt{N}) &\geq \sum_{\ell\geq k} \frac{\ell(\ell-1)}{k(k-1)} Q_\ell(N) \\ &\geq \frac{1}{k(k-1)}\Big(\sum_\ell \ell^2 Q_\ell(N) - \sum_\ell \ell Q_\ell(N) - \sum_{\ell<k} \ell^2 Q_\ell(N)\Big) \\ &\geq \left(\frac{1}{4k(k-1)} + o(1)\right) N\log N, \end{aligned}$$

which establishes Theorem 3.

Wilson's closing remarks in [10] imply further moments:

$$\sum_\ell \ell^m Q_\ell(N) = \sum_{n=1}^{N} r(n)^m = (c_m + o(1))N(\log N)^{b_m}$$

with $b_m = 2^{m-1} - 1$. A careful residue calculation will show that

$$P_k(\sqrt{N}) \geq \sum_{\ell \geq k} \ell C_k Q_\ell(N) = (1 + o(1))NF_k(\log N)$$

for fixed k and large N, where $F_k(x)$ is a polynomial in x of degree b_k, with leading coefficient $c_k/k!$, whose terms correspond to the Laurent expansion of a certain Dirichlet series at the pole $s = 1$ of order $b_k + 1$.

3. Symmetric cyclic quadrilaterals. We need ten lemmas to prove Theorem 2. We set up some notation. The integer points M_i are (m_i, n_i). By equivalence we can suppose that one vertex of the polygon is the origin O. The centre of the circle OM_1M_2 is the point $(A/2Q, B/2Q)$ with

$$A = (m_1^2 + n_1^2)n_2 - (m_2^2 + n_2^2)n_1, \tag{3.1}$$

$$B = m_1(m_2^2 + n_2^2) - m_2(m_1^2 + n_1^2), \tag{3.2}$$

$$Q = m_1 n_2 - m_2 n_1. \tag{3.3}$$

Let d be the highest common factor $d = (A, B, Q)$, with $A = ad$, $B = bd$, $Q = dq$.

We adopt the convention that ε denotes any exponent which can be taken arbitrarily small, not always the same at each occurrence, and the order-of-magnitude constants implied in the $O()$ and $\ll$ notations depend on the choice of any exponent ε in the same formula.

LEMMA 1. *The size of $K(R)$, the maximum number of integer points on a circle with radius $r \leq R$, is*

$$K(R) = O(R^\varepsilon).$$

Proof. By (3.3) the denominator has $q \leq 8R^2$, so that

$$(2qm_j - a)^2 + (2qn_j - b)^2 = 4q^2r^2. \tag{3.4}$$

The left hand side of (3.4) is an integer, so the right hand side of (3.4) is an integer $T \leq 256R^6$ which does not depend on the integer point M_j. The number of integer points on the circle $x^2 + y^2 = T$ is $O(T^\varepsilon)$ (Hardy and Wright [3, Chapter 18]), and the result follows, using our convention on exponents ε.

LEMMA 2. *The number of equivalence classes of triangles of integer points with circumradius $r \leq R$ and with common factor $d > D$ is*

$$O\left(\frac{R^4 \log^7 R}{D}\right).$$

Proof. We represent the vertices of the triangle OM_1M_2 as Gaussian integers 0, $m_1 + in_1$, and $m_2 + in_2$. By (3.1)–(3.3) the centre of the circle

OM_1M_2 in the complex plane is

$$\frac{a+ib}{2q} = \frac{(m_1^2+n_1^2)(n_2-im_2)-(m_2^2+n_2^2)(n_1-im_1)}{2(m_1n_2-m_2n_1)}$$
$$= \frac{(m_1+in_1)(m_1-in_1)(m_2+in_2)-(m_2+in_2)(m_2-in_2)(m_1+in_1)}{(m_1-in_1)(m_2+in_2)-(m_1+in_1)(m_2-in_2)}$$
$$= \frac{(m_1+in_1)(m_2+in_2)(m_1-m_2-i(n_1-n_2))}{(m_1-in_1)(m_2+in_2)-(m_1+in_1)(m_2-in_2)}.$$

Let δ be a generator of the ideal

$$\langle\delta\rangle = \langle m_1+in_1, m_2+in_2\rangle.$$

Then there are Gaussian integers α_1, α_2, and α_3 with

$$m_1+in_1=\alpha_1\delta, \quad m_2+in_2=\alpha_2\delta, \quad m_2-m_1+i(n_2-n_1)=\alpha_3\delta$$

and with

$$\alpha_2 = \alpha_1+\alpha_3. \tag{3.5}$$

Since $\langle a_1,\alpha_2\rangle = \langle 1\rangle$ by construction, the ideals $\langle\alpha_1\rangle$, $\langle\alpha_2\rangle$ and $\langle\alpha_3\rangle$ are pairwise coprime. In this notation, the centre of the circle OM_1M_2 is

$$\frac{a+ib}{2q} = -\frac{\alpha_1\alpha_2\overline{\alpha}_3\delta}{\overline{\alpha}_1\alpha_2-\alpha_1\overline{\alpha}_2}, \tag{3.6}$$

where we have cancelled a factor $\operatorname{Norm}\delta$.

There may be further cancellation by positive integer factors on the right of (3.6). If so, then there is cancellation by Gaussian ideal factors. We have

$$\langle\alpha_1,\overline{\alpha}_1\alpha_2-\alpha_1\overline{\alpha}_2\rangle = \langle\alpha_1,\overline{\alpha}_1\alpha_2\rangle = \langle\alpha_1,\overline{\alpha}_1\rangle,$$

and similarly

$$\langle\alpha_2,\overline{\alpha}_1\alpha_2-\alpha_1\overline{\alpha}_2\rangle = \langle\alpha_2,\overline{\alpha}_2\rangle.$$

By (3.5),

$$\overline{\alpha}_1\alpha_2-\alpha_1\overline{\alpha}_2 = \overline{\alpha}_1\alpha_3-\alpha_1\overline{\alpha}_3$$

and we obtain similarly

$$\langle\overline{\alpha}_3,\overline{\alpha}_1\alpha_2-\alpha_1\overline{\alpha}_2\rangle = \langle\alpha_3,\overline{\alpha}_3\rangle.$$

We call a Gaussian integer α *primitive* if we cannot write $\alpha=c\beta$, where c is a positive integer and β is another Gaussian integer. If β is primitive, then

$$\langle\beta,\overline{\beta}\rangle = \begin{cases} \langle 1\rangle & \text{if } \beta \text{ is odd,} \\ \langle 1+i\rangle & \text{if } \beta \text{ is even.} \end{cases}$$

We write $\alpha_j = c_j\beta_j$, where c_j is a positive integer, and β_j is a primitive Gaussian integer. Then

$$\langle\alpha_j,\overline{\alpha}_j\rangle = \langle c_j\rangle \text{ or } \langle 1+i\rangle\langle c_j\rangle. \tag{3.7}$$

Since the ideals $\langle\alpha_1\rangle$, $\langle\alpha_2\rangle$, $\langle\alpha_3\rangle$ are pairwise coprime, at most one of $\langle\beta_1\rangle$, $\langle\beta_2\rangle$, $\langle\beta_3\rangle$ is even, and the extra factor $\langle 1+i\rangle$ in (3.7) occurs for at most one value of j. The positive integers c_1, c_2, c_3 are pairwise coprime, so the factor $c_1c_2c_3$ cancels in (3.6).

Finally, let e be the largest integer with

$$\langle e\rangle \mid \langle\delta\rangle, \qquad \langle c_1c_2c_3e\rangle \mid \langle\overline{\alpha}_1\alpha_2 - \alpha_1\overline{\alpha}_2\rangle.$$

The largest positive integer factor which cancels in (3.6) is either $c_1c_2c_3e$ or $2c_1c_2c_3e$. Hence

$$(m_1 - in_1)(m_2 + in_2) - (m_1 + in_1)(m_2 - in_2) = 2dqi,$$

where

$$d = c_1c_2c_3e \operatorname{Norm}\delta \text{ or } \frac{1}{2}c_1c_2c_3e \operatorname{Norm}\delta,$$

and the positive integer e satisfies

$$e^2 \mid \operatorname{Norm}\delta, \qquad e^3 \mid d.$$

Suppose that the common factor d and the factors c_1, c_2, c_3, and e and the ideal $\langle\delta\rangle$ have been fixed. We choose β_1 and β_3 so that the triangle OM_1M_2 has circumradius at most R, with

$$\operatorname{Norm}\beta_1 \le \frac{4R^2}{c_1^2 \operatorname{Norm}\delta}, \qquad \operatorname{Norm}\beta_3 \le \frac{4R^2}{c_3^2 \operatorname{Norm}\delta}. \tag{3.8}$$

From (3.5) we have

$$c_2\beta_2 = c_1\beta_1 + c_3\beta_3,$$

and β_2 is determined by the values of β_1 and β_3, which must satisfy the congruence

$$c_1\beta_1 + c_3\beta_3 \equiv 0 \pmod{\langle c_2\rangle}. \tag{3.9}$$

The solutions of (3.9) form a complex lattice Γ of Gaussian vectors (β_1, β_3) in $\mathbb{C}^2$, and a lattice Λ of real vectors in $\mathbb{R}^4$ of determinant $\det\Lambda = c_2^2$. As a real set in $\mathbb{R}^4$, the search region in (3.8) is a polydisc D, the product of two two-dimensional discs.

We distinguish two cases.

Major arc case. All points of the lattice Γ in D are multiples of a single basis vector (η_1, η_3). At most four of these multiples can have $\langle\beta_1, \beta_3\rangle = \langle\eta_1, \eta_3\rangle = \langle 1\rangle$.

Minor arc case. There are two vectors (η_1, η_3) and (ζ_1, ζ_3) of Γ in D that are linearly independent over $\mathbb{C}$. We also consider the vectors $(i\eta_1, i\eta_3)$ and $(i\zeta_1, i\zeta_3)$ to form a set of four vectors linearly independent over $\mathbb{R}$. Let N be the number of vectors of Γ in D. In $\mathbb{R}^4$ we have N vectors in a convex

region of volume

$$\frac{16\pi^2R^4}{c_1^2c_3^2(\operatorname{Norm}\delta)^2}.$$

These include a linearly independent set of four vectors, their negatives, and the zero vector, so $N \geq 9$. By triangulating the convex hull of the N points, we form $N-4$ disjoint simplices. The volume of each simplex is an integral multiple of $\det \Lambda/24$. Hence the number of non-zero vectors of Λ in D is

$$N-1 \leq 2(N-4) \leq \frac{768\pi^2R^4}{c_1^2c_3^2(\operatorname{Norm}\delta)^2\det\Lambda} = \frac{768\pi^2R^4}{c_1^2c_2^2c_3^2(\operatorname{Norm}\delta)^2}.$$

The total number of choices for the Gaussian integers β_1, β_2, β_3 is

$$O\left(\frac{R^4}{c_1^2c_2^2c_3^2(\operatorname{Norm}\delta)^2}+1\right) = O\left(\frac{e^2R^4}{d^2}\right) \tag{3.10}$$

in both cases. We write $8d = e^3f$, so the bound (3.10) is $O(R^4/e^4f^2)$.

Let $h = \operatorname{Norm}\delta$. Then $h = e^2g$ for some integer $g \mid f$. Let $d(n)$ denote the usual divisor function (Hardy and Wright [3, Chapters 16–18]), and let $d_5(n)$ denote the number of representations of n as a product of five positive integers, with analogous properties. The number of primitive Gaussian integers whose Norm is h is at most $d(e)d(g)$. If e and f are given, then there are at most $d(e)d_5(f)$ choices for c_1, c_2, c_3, and the ideal $\langle\delta\rangle$. Hence the number of triangles OM_1M_2 with circumradius at most R, and common factor d in a range

$$8D < 8d = e^3f \leq 256R^2,$$

is

$$\begin{aligned} &O\left(R^4 \sum_{\substack{e\\ 8D<e^3f\leq 256R^2}}\sum_{f} \frac{d(e)d_5(f)}{e^4f^2}\right)\\ &\qquad = O\left(R^4 \sum_{f\leq 256R^2}\frac{d_5(f)}{f^2}\sum_{e>2(D/f)^{1/3}}\frac{d(e)}{e^4}\right)\\ &\qquad = O\left(R^4\sum_{f\leq 256R^2}\frac{d_5(f)}{f^2}\cdot\frac{f\log R}{D}\right) = O\left(\frac{R^4\log^7 R}{D}\right), \end{aligned}$$

as asserted in the lemma.

When we consider cyclic quadrilaterals, there are four triangles with the same circumcentre $(a/2q, b/2q)$. We put

$$m_1n_2-m_2n_1 = d_3q, \quad m_1n_3-m_3n_1 = d_2q, \quad m_2n_3-m_3n_2 = d_1q, \tag{3.11}$$
$$d_0 = d_1+d_3-d_2,$$

so that the areas of the triangles OM_1M_2, OM_1M_3, OM_2M_3 and $M_1M_2M_3$ are $d_3q/2$, $d_2q/2$, $d_1q/2$ and $d_0q/2$ respectively. If we shift the vertex M_1 to the origin, then $OM_1M_2M_3$ becomes a quadrilateral $N_3ON_1N_2$. The centre of the circle moves by an integer vector, so the denominator q is unchanged. The vertices are renumbered, so the new common factors d_0', d_1', d_2', and d_3' are related to the old d_0, d_1, d_2, and d_3 by

$$\begin{aligned} d_0'q &= 2\operatorname{area} N_1N_2N_3 = 2\operatorname{area} M_2M_3O = d_1q,\\ d_1'q &= 2\operatorname{area} ON_2N_3 = 2\operatorname{area} M_1M_3O = d_2q,\\ d_2'q &= 2\operatorname{area} ON_1N_3 = 2\operatorname{area} M_1M_2O = d_3q,\\ d_3'q &= 2\operatorname{area} ON_1N_2 = 2\operatorname{area} M_1M_2M_3 = d_0q, \end{aligned}$$

so the suffixes are renumbered cyclically.

It is often convenient to remove the highest common factor $e = (d_1, d_2, d_3)$, which is also a factor of d_0, and to write $d_j = ef_j$ for $j = 0, 1, 2, 3$, with

$$f_0 + f_2 = f_1 + f_3. \tag{3.12}$$

There are interesting special cases when $d_1 = d_2$ or $d_2 = d_3$. If $d_1 = d_2$, then the triangles OM_2M_3, OM_1M_3 have equal area, so the line M_1M_2 is parallel to OM_3, and there is a symmetry axis through the centre of the circle, bisecting M_1M_2 and OM_3 at right angles. Similarly, if $d_2 = d_3$, there is a symmetry axis through the centre of the circle bisecting OM_1 and M_2M_3 at right angles. We call these cases *symmetrical cyclic quadrilaterals* or *cyclic trapezia*. They provide the main term in Theorem 2.

LEMMA 3. *The number of equivalence classes of symmetrical cyclic quadrilaterals with vertices at integer points and circumradius $r \le R$ is*

$$\frac{32(3+\sqrt{2})}{21\zeta(3)}\,\zeta\left(\frac{3}{2}\right)L\left(\frac{3}{2},\chi\right)R^3 + O(R^2\log R),$$

where $L(s,\chi)$ is the Dirichlet L-function formed with the non-trivial character mod 4.

Proof. Each equivalence class of symmetric cyclic quadrilaterals contains two representatives (four if it is a rectangle) in which one vertex is the origin O, and M_1M_2 is parallel to M_3O with the vertices numbered anticlockwise round the circle. As in Lemma 2 we represent the vertices O, M_1, M_2, and M_3 by Gaussian integers 0, μ_1, μ_2, μ_3. Let δ be a generator of the ideal $\langle\mu_1, \mu_2, \mu_3\rangle$. Then there are Gaussian integers α_1, α_2, α_3 with $\mu_j = \alpha_j\delta$, and highest common factor $\langle\alpha_1, \alpha_2, \alpha_3\rangle = \langle 1\rangle$. As in (3.5) and (3.6) of Lemma 2, the centre of the circle OM_1M_2 is

$$\frac{a+ib}{2q} = \frac{\alpha_1\alpha_2(\overline{\alpha}_1 - \overline{\alpha}_2)\delta}{\overline{\alpha}_1\alpha_2 - \alpha_1\overline{\alpha}_2},$$

where the denominator is pure imaginary. Considering the two triangles OM_2M_3 and OM_1M_3, we also have

$$\frac{a+ib}{2q} = \frac{\alpha_2\alpha_3(\overline{\alpha}_2-\overline{\alpha}_3)\delta}{\overline{\alpha}_2\alpha_3-\alpha_2\overline{\alpha}_3} = \frac{\alpha_1\alpha_3(\overline{\alpha}_1-\overline{\alpha}_3)\delta}{\overline{\alpha}_1\alpha_3-\alpha_1\overline{\alpha}_3}.$$

Again, the denominators are pure imaginary.

We introduce an equivalence relation $\beta \sim \gamma$ on Gaussian integers, meaning that there are non-zero integers s and t with $s\beta = t\gamma$. Then

$$i(a+ib) \sim \alpha_2\alpha_3(\overline{\alpha}_2-\overline{\alpha}_3)\delta \sim \alpha_1\alpha_3(\overline{\alpha}_1-\overline{\alpha}_3)\delta \sim \alpha_1\alpha_2(\overline{\alpha}_1-\overline{\alpha}_2)\delta,$$

and since M_1M_2 is parallel to M_3O,

$$\mu_1-\mu_2 \sim \mu_3.$$

For any non-zero Gaussian integer η we have

$$\beta \sim \gamma \;\Leftrightarrow\; \beta\eta \sim \gamma\eta.$$

Hence

$$\alpha_1-\alpha_2 \sim \alpha_3, \quad \overline{\alpha}_1-\overline{\alpha}_2 \sim \overline{\alpha}_3, \quad \alpha_3(\overline{\alpha}_2-\overline{\alpha}_3) \sim \alpha_1(\overline{\alpha}_1-\overline{\alpha}_2) \sim \alpha_1\overline{\alpha}_3. \tag{3.13}$$

We call the Gaussian prime ideal $\langle\phi\rangle$ a *balanced factor* of the ideal $\langle\beta\rangle$ if $\langle\phi\rangle$ and $\langle\overline{\phi}\rangle$ occur to the same power in the factorisation of $\langle\beta\rangle$, and a *heavy factor*, written $\langle\phi\rangle \,|!\, \langle\beta\rangle$, if $\langle\phi\rangle$ occurs to a greater power than $\langle\overline{\phi}\rangle$. We note two basic properties:

$$\langle\phi\rangle \,|!\, \langle\beta\rangle \;\Leftrightarrow\; \langle\overline{\phi}\rangle \,|!\, \langle\overline{\beta}\rangle,$$

and when $\beta \sim \gamma$ then

$$\langle\phi\rangle \,|!\, \langle\beta\rangle \;\Leftrightarrow\; \langle\phi\rangle \,|!\, \langle\gamma\rangle.$$

We use (3.13) to show that all prime ideal factors of $\langle\alpha_3\rangle$ are balanced. Suppose that $\langle\phi\rangle$ is a heavy prime ideal factor of $\langle\alpha_3\rangle$. Since $\langle\phi\rangle$ occurs to a greater power in $\langle\alpha_3\rangle$ than in $\langle\alpha_3\rangle$, we have $\langle\phi\rangle \,|\, \langle\alpha_1\rangle$. As $\langle\overline{\phi}\rangle$ occurs to a greater power in $\langle\overline{\alpha}_3\rangle$ than in $\langle\overline{\alpha}_3\rangle$, we have $\langle\overline{\phi}\rangle \,|\, \langle\overline{\alpha}_2\rangle$, and so $\langle\phi\rangle \,|\, \langle\alpha_2\rangle$. But this is impossible, since $\langle\alpha_1,\alpha_2,\alpha_3\rangle = \langle 1\rangle$.

We deduce that all Gaussian integer prime ideal factors of $\langle\alpha_3\rangle$ are balanced, so for some positive integer c,

$$\langle\alpha_3\rangle = \langle c\rangle \text{ or } \langle 1+i\rangle\langle c\rangle.$$

We can choose the generator δ of the ideal $\langle\delta\rangle$ so that $\mu_3 = \delta\alpha_3$,

$$\alpha_3 = c \text{ or } (1+i)c.$$

In the case $\alpha_3 = c$, the symmetry axis is $x = c/2$ with

$$1 \le c \le R' = \frac{R}{\operatorname{Norm}\delta},$$

and the symmetry acts by $(u,v) \mapsto (c-u,v)$. In the case $\alpha_3 = (1+i)c$, the symmetry axis is $x+y=c$ with

$$1 \le c \le \frac{R'\sqrt{2}}{2} = \frac{R\sqrt{2}}{2\,\mathrm{Norm}\,\delta},$$

and the symmetry acts by $(u, v) \mapsto (c - v, c - u)$.

Not all choices of $\alpha_1 = u+iv$ give primitive quadrilaterals with $\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \langle 1 \rangle$. For a general choice of $\alpha_3 = c$, $\alpha_1 = u + iv$ we have

$$\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \langle u + iv, c - u + iv, c \rangle = \langle u + iv, u - iv, c \rangle.$$

The highest common factor is of the form $\langle e \rangle$ or $\langle 1 + i \rangle \langle e \rangle$ for some positive integer e with $e \,|\, c/(2, c)$. Similarly, for a general choice of $\alpha_3 = c$, $\alpha_1 = u+iv$ we have

$$\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \langle u + iv, c - v + ic - iu, c + ic \rangle = \langle u + iv, u - iv, c + ic \rangle.$$

The highest common factor is of the form $\langle e \rangle$ or $\langle 1 + i \rangle \langle e \rangle$ with $e \,|\, c$. When counting the Gaussian integers α_1, we must sieve out multiples of odd primes which divide α_3, and multiples of $\langle 1 + i \rangle$ if α_3 is even.

We choose α_3 first, and perform a simple asymptotic sieve ([4], [1]) to enforce the condition $\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \langle 1 \rangle$. For fixed α_3, we must count Gaussian integers α_1 which lie in ideals $\langle \eta \rangle$ of the form $\langle e \rangle$ or $\langle 1 + i \rangle \langle e \rangle$ with $\langle \eta \rangle \,|\, \langle \alpha_3 \rangle$.

Let A_1, A_2 and A_3 be the integer points α_1, α_2 and α_3. If A_3 is fixed, then O, A_1, A_2, A_3 lie in anti-clockwise order on some circle of the coaxial system through O and A_3. The search region for A_1 and A_2 lies on one side of OA_3, and between the two circles of the coaxial system which have radius $R' = R/\mathrm{Norm}\,\delta$, as in Theorem 1. The point A_1 lies on the same side of the symmetry axis as O, and the point A_2 lies on the same side as A_3. Let

$$|\alpha_3| = 2R' \sin\theta.$$

By the calculation in the proof of Theorem 1, the area of the search region for A_1 is

$$\frac{1}{2}\,\pi R'^2 - (\theta R'^2 - R'^2 \sin\theta\cos\theta) = \frac{1}{2}\,R'^2 f(\theta),$$

say.

We want to count Gaussian integers α_1 in the ideal $\langle \eta \rangle$ lying in this region. Part of the boundary of the search region is a straight line segment containing integer points, so the best estimate for the number of integer points A_1 with α_1 in $\langle \eta \rangle$ is

$$A(R', \eta, \theta) = \frac{f(\theta)}{2} \cdot \frac{R'^2}{\mathrm{Norm}\,\eta} + O\left(\frac{R'}{|\eta|}\right). \tag{3.14}$$

Let $t = 2R' \sin\theta$ be a continuous variable corresponding to $|\alpha_3|$. The angle $\theta = \theta(t)$ runs from 0 to $\pi/2$. We approximate the sum of $A(R', \eta, \theta(|\alpha_3|))$ by an integral over t.

Case $(1,1)$. When $\alpha_3 = c$, $\eta = e$, then $\operatorname{Norm}\eta = e^2$, and the steps in t have length e. Then

$$\sum_{c\le R'} A(R', e, \theta(c)) = \frac{R'^2}{2e^2} \int_0^{2R'} f(\theta)\,\frac{dt}{e} + O\Big(\frac{R'^2}{e^2}\Big).$$

We have

$$\int_0^{2R'} f(\theta)\,dt = 2R' \int_0^{\pi/2} f(\theta)\,d(\sin\theta),$$

and by an elementary calculation

$$\int_0^{\pi/2} f(\theta)\,d(\sin\theta) = -\int_0^{\pi/2} f'(\theta)\sin\theta\,d\theta = \int_{\cos\theta=0}^{\cos\theta=1} (4-4\cos^2\theta)\,d(\cos\theta) = \frac{8}{3},$$

and

$$\sum_{c\le R'} A(R', e, \theta(c)) = \frac{8R'^3}{3e^3} + O\Big(\frac{R'^2}{e^2}\Big). \tag{3.15}$$

Case $(1,2)$. When $\alpha_3 = c$, $\eta = (1+i)e$, then $\operatorname{Norm}\eta = 2e^2$, and the steps in t have length $2e$. The sum of $A(R', (1+i)e, \theta(c))$ is given by (3.15) with the factor $8/3$ replaced by $2/3$.

Case $(2,1)$. When $\alpha_3 = (1+i)c$, $\eta = e$, then $\operatorname{Norm}\eta = e^2$, and the steps in t have length $e\sqrt{2}$. The sum of $A(R', e, \theta(c\sqrt{2}))$ is given by (3.15) with the factor $8/3$ replaced by $4\sqrt{2}/3$.

Case $(2,2)$. When $\alpha_3 = (1+i)c$, $\eta = (1+i)e$, then $\operatorname{Norm}\eta = 2e^2$, and the steps in t have length $e\sqrt{2}$. The sum of $A(R', (1+i)e, \theta(c\sqrt{2}))$ is given by (3.15) with the factor $8/3$ replaced by $2\sqrt{2}/3$.

The four sums of type (3.15) count numberings of vertices of equivalence classes of cyclic trapezia. A rectangle can be labelled $OM_1M_2M_3$ in four ways; this does not affect the ideals $\langle\delta\rangle$ and $\langle\eta\rangle$, and the four numberings will belong to the same case, either Case $(1,1)$ or Case $(1,2)$. Other cyclic trapezia can be labelled $OM_1M_2M_3$ in two ways; this does not affect the ideals $\langle\delta\rangle$ and $\langle\eta\rangle$, and the two numberings will belong to the same case. If the trapezium $OM_1M_2M_3$ is a rectangle, then A_1 lies on a straight line perpendicular to OM_3. The number of rectangles in any case is $O(R'^2/e^2)$, within the error allowed in (3.15). Hence the number of equivalence classes of cyclic trapezia in Case $(1,1)$ with $\langle\eta\rangle$ fixed is given by (3.15) with the factor $8/3$ halved to $4/3$, and similarly in the other cases.

In the simple asymptotic sieve, the possible common factors to remove are built up from odd primes and the Gaussian prime ideal $\langle 1+i\rangle$. The number of equivalence classes of primitive cyclic trapezia with α_3 of the

form c is

$$\frac{4}{3}R'^3\Big(1-\frac{1}{4}\Big)\prod_{p\,\text{odd}}\Big(1-\frac{1}{p^3}\Big)+O\Big(R'^3\sum_{e>R'/2}\frac{1}{e^3}\Big)+O\Big(R'^2\sum_{e\le R'}\frac{1}{e^2}\Big)$$
$$=\frac{8R'^3}{7\zeta(3)}+O(R'^2).$$

In the case with α_3 of the form $(1+i)c$, the numerical factor $(4/3)(1-1/4)$ is replaced by

$$\frac{2\sqrt{2}}{3}\Big(1-\frac{1}{2}\Big)=\frac{\sqrt{2}}{3},$$

so the total number of equivalence classes of primitive cyclic trapezia is

$$\frac{8(3+\sqrt{2})}{21\zeta(3)}R'^3+O(R'^2)=\frac{8(3+\sqrt{2})}{21\zeta(3)}\cdot\frac{R^3}{(\operatorname{Norm}\delta)^{3/2}}+O\Big(\frac{R^2}{\operatorname{Norm}\delta}\Big).$$

The final step is to replace the common factor $\langle\delta\rangle$. We chose a particular generator δ of the ideal $\langle\delta\rangle$, so we sum over non-zero Gaussian integers δ with $\operatorname{Norm}\delta\le R^2$. This introduces an extra factor in the main term, 4 times the Dedekind zeta function of the Gaussian field at 3/2. We deduce the result of the lemma.

4. Factorisation. We extend the notation of (3.11) and (3.12), putting $d_4=d_1+d_3=d_0+d_2$ to correspond to the area of the whole quadrilateral, and $d_j=ef_j$.

LEMMA 4. *Let d_0, d_1, d_2, d_3 and d_4 be positive integers. Then there are* 31 *positive integers e_α, the total decomposition set of $d_0,\dots,d_4$, indexed by the non-empty subsequences of* 01234, *such that*

$$d_j=\prod_{j\in\alpha}e_\alpha, \tag{4.1}$$

with the highest common factor property

$$(e_\alpha,e_\beta)>1\ \Rightarrow\ \alpha\subset\beta\text{ or }\beta\subset\alpha. \tag{4.2}$$

If

$$d_0+d_2=d_1+d_3=d_4, \tag{4.3}$$

then all the e_α are 1 *except possibly for the uncommon factors e_0, e_1, e_2, e_3 and e_4, the side factors e_{01}, e_{03}, e_{12}, e_{23}, e_{024} and e_{134}, and the common factor $e=e_{01234}$, so that*

$$d_0=e_0e_{01}e_{03}e_{024}e,\quad d_1=e_1e_{01}e_{12}e_{134}e, \tag{4.4}$$

$$d_2=e_2e_{12}e_{23}e_{024}e,\quad d_3=e_3e_{03}e_{23}e_{134}e, \tag{4.5}$$

$$d_4=e_4e_{024}e_{134}e, \tag{4.6}$$

and (4.3) *gives the relations*

$$e_0e_{01}e_{03} + e_2e_{12}e_{23} = e_4e_{134}, \tag{4.7}$$

$$e_1e_{01}e_{12} + e_3e_{03}e_{23} = e_4e_{024}. \tag{4.8}$$

Proof. The total decomposition set was introduced by Hall in [2]. The basic property (4.2) allows us to read off highest common factors, such as

$$(d_1, d_2, d_3, d_4) = e_{1234}e, \quad (d_1, d_3, d_4) = e_{134}e_{0134}e_{1234}e,$$
$$(d_1, d_3) = e_{13}e_{013}e_{123}e_{134}e_{0123}e_{0134}e_{1234}e.$$

Since $d_4 = d_1 + d_3$, we have $(d_1, d_3) = (d_1, d_3, d_4)$ and so $e_\alpha = 1$ if α contains 1 and 3 but not 4. Similarly, $e_\alpha = 1$ if α contains 1 and 4 but not 3, or 3 and 4 but not 1, or 0 and 2 but not 4, or 0 and 4 but not 2, or 2 and 4 but not 0. With these restrictions we can write out (4.1) explicitly in the five cases as in (4.4) to (4.6). Substituting in (4.3) and cancelling common factors gives (4.7) and (4.8).

LEMMA 5. *Let $OM_1M_2M_3$ be a cyclic quadrilateral, with vertices at the Gaussian integers* 0, μ_1, μ_2, μ_3. *Let the circum-centre be $(a + ib)/2q$, where $(a, b, q) = 1$. Let the areas of the triangles $M_1M_2M_3$, OM_2M_3, OM_1M_3, OM_1M_2 and of the quadrilateral $OM_1M_2M_3$ be $d_0q/2$, $d_1q/2$, $d_2q/2$, $d_3q/2$ and $d_4q/2$ respectively. Let $\{e_\alpha\}$ be the total decomposition set of $d_0, \dots, d_4$. Then we have the Gaussian factorisations*

$$\mu_1 = e_{23}\delta\sigma_2\sigma_3\tau_1, \quad \mu_2 = e_{134}\delta\sigma_1\sigma_3\tau_2, \quad \mu_3 = e_{12}\delta\sigma_1\sigma_2\tau_3, \tag{4.9}$$

$$\mu_2 - \mu_3 = e_{01}\delta\overline{\sigma}_0\sigma_1\overline{\tau}_1, \tag{4.10}$$

$$\mu_1 - \mu_3 = e_{024}\delta\overline{\sigma}_0\sigma_2\overline{\tau}_2, \tag{4.11}$$

$$\mu_1 - \mu_2 = e_{03}\delta\overline{\sigma}_0\sigma_3\overline{\tau}_3, \tag{4.12}$$

where $\langle\delta\rangle = \langle\mu_1, \mu_2, \mu_3\rangle$, and $\operatorname{Norm}\sigma_j = e_j$, *and*

$$a + ib = \frac{\sigma_1\sigma_2\sigma_3\tau_1\tau_2\tau_3\delta \operatorname{Norm}\delta}{ie}. \tag{4.13}$$

There are the relations

$$e_{134}\sigma_3\tau_2 - e_{12}\sigma_2\tau_3 = e_{01}\overline{\sigma}_0\overline{\tau}_1, \tag{4.14}$$

$$e_{23}\sigma_3\tau_1 - e_{12}\sigma_1\tau_3 = e_{024}\overline{\sigma}_0\overline{\tau}_2, \tag{4.15}$$

$$e_{23}\sigma_2\tau_1 - e_{134}\sigma_1\tau_2 = e_{03}\overline{\sigma}_0\overline{\tau}_3, \tag{4.16}$$

$$e_{01}\overline{\sigma}_1\tau_1 + e_{03}\overline{\sigma}_3\tau_3 = e_{024}\overline{\sigma}_2\tau_2, \tag{4.17}$$

and

$$e_{01}e_{23}\operatorname{Norm}\tau_1 + e_{03}e_{12}\operatorname{Norm}\tau_3 = e_{024}e_{134}\operatorname{Norm}\tau_2. \tag{4.18}$$

Proof. The perpendicular bisector of OM_1 is

$$m_1x + n_1y = \frac{1}{2}(m_1^2 + n_1^2).$$

This line passes through the centre of the circle, $(a/2q, b/2q)$, so

$$am_1 + bn_1 = (m_1^2 + n_1^2)q,$$

and similarly we have

$$am_j + bn_j = (m_j^2 + n_j^2)q$$

for $j = 2, 3$. Hence

$$\begin{aligned}(4.19)\qquad & d_1(m_1^2 + n_1^2) - d_2(m_2^2 + n_2^2) + d_3(m_3^2 + n_3^2) \\ &= \frac{d_1}{q}(am_1 + bn_1) - \frac{d_2}{q}(am_2 + bn_2) + \frac{d_3}{q}(am_3 + bn_3) \\ &= \frac{1}{q^2}\begin{vmatrix} am_1 + bn_1 & am_2 + bn_2 & am_3 + bn_3 \\ m_1 & m_2 & m_3 \\ n_1 & n_2 & n_3 \end{vmatrix} = 0.\end{aligned}$$

Next we write $\mu_j = m_j + in_j$ for $j = 1, 2, 3$. Then

$$(4.20)\qquad d_1\mu_1 - d_2\mu_2 + d_3\mu_3 = \frac{1}{q}\begin{vmatrix} m_1 + in_1 & m_2 + in_2 & m_3 + in_3 \\ m_1 & m_2 & m_3 \\ n_1 & n_2 & n_3 \end{vmatrix} = 0.$$

Eliminating μ_3 from (4.19) using (4.20), we have

$$\begin{aligned} d_1d_2\mu_1\overline{\mu}_1 + d_2d_3\mu_3\overline{\mu}_3 &= (d_1\mu_1 + d_3\mu_3)(d_1\overline{\mu}_1 + d_3\overline{\mu}_3), \\ d_1(d_2 - d_1)\mu_1\overline{\mu}_1 + d_3(d_2 - d_3)\mu_3\overline{\mu}_3 &= -d_1d_3(\mu_1\overline{\mu}_3 + \overline{\mu}_1\mu_3).\end{aligned}$$

Completing the square on the right, we have

$$\begin{aligned}(4.21)\qquad d_1d_3\,\mathrm{Norm}(\mu_1 - \mu_3) &= d_1d_3(\mu_1 - \mu_3)(\overline{\mu}_1 - \overline{\mu}_3) \\ &= d_1(d_1 - d_2 + d_3)\mu_1\overline{\mu}_1 + d_3(d_1 - d_2 + d_3)\mu_3\overline{\mu}_3 \\ &= d_0d_2\mu_2\overline{\mu}_2 = d_0d_2\,\mathrm{Norm}\,\mu_2,\end{aligned}$$

where we have used (4.19).

To remove common factors from (4.21), we pick a generator δ of the ideal $\langle\mu_1, \mu_2, \mu_3\rangle$, and we write $\mu_j = \alpha_j\delta$. Then

$$d_1d_3\,\mathrm{Norm}(\alpha_1 - \alpha_3) = d_0d_2\,\mathrm{Norm}\,\alpha_2.$$

We express $d_0, \ldots, d_3$ in terms of the total decomposition set of Lemma 4 and cancel common factors to obtain

$$(4.22)\qquad e_1e_3e_{134}^2\,\mathrm{Norm}(\alpha_1 - \alpha_3) = e_0e_2e_{024}^2\,\mathrm{Norm}\,\alpha_2.$$

Now we remove highest common factors from (4.20). First we have

$$d_1\alpha_1 + d_3\alpha_3 = d_2\alpha_2,$$

then in terms of the total decomposition set

$$(4.23)\qquad e_1e_{01}e_{12}e_{134}\alpha_1 + e_3e_{03}e_{23}e_{134}\alpha_3 = e_2e_{12}e_{23}e_{024}\alpha_2.$$

By the highest common factor property (4.2) we see that $\langle e_{134}\rangle \mid \langle \alpha_2\rangle$, so $\alpha_2 = e_{134}\beta_2$ for some Gaussian integer β_2. Similarly we can write

$$\alpha_1 = e_{23}\beta_1, \quad \alpha_2 = e_{134}\beta_2, \quad \alpha_3 = e_{12}\beta_3. \tag{4.24}$$

Eliminating d_2 from (4.20) leads to

$$d_1(\alpha_1 - \alpha_2) + d_0\alpha_2 = d_3(\alpha_2 - \alpha_3),$$

so $\langle e_{03}\rangle \mid \langle \alpha_1 - \alpha_2\rangle$, and similarly we can write

$$\alpha_2 - \alpha_3 = e_{01}\beta_{01}, \quad \alpha_1 - \alpha_3 = e_{024}\beta_{02}, \quad \alpha_1 - \alpha_2 = e_{03}\beta_{03}, \tag{4.25}$$

and (4.23) reduces to

$$e_1e_{01}\beta_1 + e_3e_{03}\beta_3 = e_2e_{024}\beta_2. \tag{4.26}$$

The centre of the circle OM_1M_2 was calculated in Lemma 2 as

$$\frac{a+ib}{2q} = \frac{\mu_1\mu_2(\overline{\mu}_1 - \overline{\mu}_2)}{2id_3q} = \frac{\alpha_1\alpha_2(\overline{\alpha}_1 - \overline{\alpha}_2)\delta \operatorname{Norm}\delta}{2id_3q} = \frac{\beta_1\beta_2\overline{\beta}_{03}\delta \operatorname{Norm}\delta}{2ie_3eq}. \tag{4.27}$$

This point is also the centre of the circles OM_1M_3 and OM_2M_3, so

$$\frac{a+ib}{2q} = \frac{\beta_1\beta_3\overline{\beta}_{02}\delta \operatorname{Norm}\delta}{2ie_2eq} = \frac{\beta_2\beta_3\overline{\beta}_{01}\delta \operatorname{Norm}\delta}{2ie_1eq}.$$

We deduce that

$$\frac{\overline{\beta}_{01}}{e_1\beta_1} = \frac{\overline{\beta}_{02}}{e_2\beta_2} = \frac{\overline{\beta}_{03}}{e_3\beta_3}. \tag{4.28}$$

We can write (4.22) using (4.24) and (4.25) as

$$e_1e_3 \operatorname{Norm}\beta_{02} = e_0e_2 \operatorname{Norm}\beta_2.$$

Hence the expression in (4.28) is a Gaussian fraction whose Norm equals $e_0/e_1e_2e_3$. The positive integers e_0, e_1, e_2 and e_3 are pairwise coprime by (4.2) of Lemma 4, so the expression in (4.28) must be of the form $\sigma_0/\sigma_1\sigma_2\sigma_3$, where σ_j is a Gaussian integer with $\operatorname{Norm}\sigma_j = e_j$, and

$$\sigma_1\sigma_3\overline{\beta}_{02} = \sigma_0\overline{\sigma}_2\beta_2.$$

The ideals $\langle\sigma_0\rangle$, $\langle\sigma_1\rangle$, $\langle\sigma_2\rangle$ and $\langle\sigma_3\rangle$ are pairwise coprime, so for some Gaussian integer τ_2 we have

$$\beta_2 = \sigma_1\sigma_3\tau_2, \quad \overline{\beta}_{02} = \sigma_0\overline{\sigma}_2\tau_2.$$

Similarly, there are Gaussian integers τ_1 and τ_3 with

$$\beta_1 = \sigma_2\sigma_3\tau_1, \quad \overline{\beta}_{01} = \sigma_0\overline{\sigma}_1\tau_1, \quad \beta_3 = \sigma_1\sigma_2\tau_3, \quad \overline{\beta}_{03} = \sigma_0\overline{\sigma}_3\tau_3,$$

and we substitute in (4.24) and (4.25) to obtain (4.9) to (4.12), in (4.27) to get (4.13), and in (4.26) to get (4.17). The relations (4.14), (4.15) and (4.16)

are found by substituting (4.9) into (4.10), (4.11) and (4.12). Finally, we substitute (4.9) into (4.19) to obtain the Norm relation (4.18).

5. Non-symmetric cyclic quadrilaterals. We aim for an upper estimate, which allows certain simplifications. Each equivalence class contains four quadrilaterals with a vertex at the origin. The vertices are numbered anti-clockwise from the origin. We pick a representative with

$$e_0 e_2 e_{024}^2 \geq e_1 e_3 e_{134}^2. \tag{5.1}$$

As in the proof of Lemma 2, we first count primitive cyclic quadrilaterals for which the ideal $\langle \delta \rangle$ in Lemma 5 is $\langle 1 \rangle$. We replace the common factors at the end of the argument. The common factor $e = e_{01234}$ in Lemma 4 may still be non-trivial. We put $d_j = ef_j$, and we consider size ranges

$$D \leq f_4 = f_1 + f_3 \leq 2D. \tag{5.2}$$

Our main strategy is to fix components of the total decomposition set of $d_0, \ldots, d_4$, and to count the number of possible Gaussian integers τ_1, τ_2 and τ_3 in Lemma 5. Cyclic quadrilaterals for which τ_1, τ_2 and τ_3 are small are treated by fixing τ_1, τ_2 and τ_3, and counting the possible Gaussian integers σ_0, σ_1, σ_2 and σ_3 in Lemma 5. The Dirichlet interchange principle "sum the largest range first and the shortest range last" leads to further case-splitting.

LEMMA 6. *Let all the total decomposition set except $e = e_{01234}$ be fixed, and let the Gaussian integers σ_0, σ_1, σ_2 and σ_3 be fixed. Then the number of different cyclic quadrilaterals $OM_1M_2M_3$ with circumradius $r \leq R$ is at most*

$$O\left(\frac{R^2}{e_1 e_3 e_4 e_{134}^2 \operatorname{Norm} \delta} + 1 \right). \tag{5.3}$$

Proof. The choice of τ_2 determines τ_1 and τ_3 by the simultaneous equations (4.15) and (4.17), which give

$$(e_1 e_{01} e_{12} + e_3 e_{03} e_{23})\tau_1 = e_{12} e_{024} \sigma_1 \overline{\sigma}_2 \tau_2 + e_{03} e_{024} \overline{\sigma}_0 \overline{\sigma}_3 \overline{\tau}_2,$$
$$(e_1 e_{01} e_{12} + e_3 e_{03} e_{23})\tau_3 = e_{23} e_{024} \overline{\sigma}_2 \sigma_3 \tau_2 - e_{01} e_{024} \overline{\sigma}_0 \overline{\sigma}_1 \overline{\tau}_2.$$

We can simplify again using (4.8) to

$$e_4 \tau_1 = e_{12} \sigma_1 \overline{\sigma}_2 \tau_2 + e_{03} \overline{\sigma}_0 \overline{\sigma}_3 \overline{\tau}_2, \tag{5.4}$$

$$e_4 \tau_3 = e_{23} \overline{\sigma}_2 \sigma_3 \tau_2 - e_{01} \overline{\sigma}_0 \overline{\sigma}_1 \overline{\tau}_2. \tag{5.5}$$

Let $\tau_2 = x + iy$. Then (5.4) and (5.5) both imply congruences for x and y modulo e_4. These congruences are not independent because of (4.7). Since

$$\langle e_4, e_{12} \sigma_1 \overline{\sigma}_2 \rangle = \langle e_4, e_{03} \overline{\sigma}_0 \overline{\sigma}_3 \rangle = \langle 1 \rangle,$$

the only possible common factor is 2, and (5.4) gives a linear congruence of

the form

$$kx + \ell y \equiv 0 \pmod{e_4/(2, e_4)},$$

whose solutions form a lattice Λ of determinant $e_4/(2, e_4)$.

From (4.9) we have

$$\operatorname{Norm} \tau_2 \le \frac{4R^2}{e_1 e_3 e_{134}^2 \operatorname{Norm} \delta},$$

so τ_2 lies within a circle in the complex plane.

Major arc case. All points of the lattice Λ within the circle lie on a straight line through the origin, so the values of τ_2 are positive and negative multiples of the smallest non-zero point λ of Λ on this straight line. By homogeneity, only two multiples $\pm n\lambda$ will give $\langle \mu_1, \mu_2, \mu_3 \rangle = \langle \delta \rangle$. Hence there are only two possible values of τ_2.

Minor arc case. The points of Λ within the circle do not all lie on a straight line. By triangulating the convex hull, we see that the number of non-zero lattice points in the circle is

$$O\left(\frac{R^2}{e_1 e_3 e_{134}^2 \operatorname{Norm} \delta \cdot \det \Lambda}\right) = O\left(\frac{R^2}{e_1 e_3 e_4 e_{134}^2 \operatorname{Norm} \delta}\right).$$

These two cases give the two terms in (5.3) of the lemma.

In the symmetric case some of the side factors in Lemma 4 are large, and the uncommon factors are small. Our next lemma discusses non-symmetric quadrilaterals of this type.

LEMMA 7. *Let $\varepsilon > 0$ and let θ in $0 \le \theta \le 1$ be given. Let D be a large positive integer. We consider a sum over quintuples of positive integers $d_0, \dots, d_4$ related by* (4.3) *and satisfying conditions involving the total decomposition set of Lemma* 4:

$$e_{01234} = (d_0, d_1, d_2, d_3, d_4) = 1, \tag{5.6}$$

$$D \le d_4 \le 2D, \tag{5.7}$$

$$e_0 e_2 e_{024}^2 \le D^{1+\theta}. \tag{5.8}$$

Let $\sum^{(1)}$ denote a sum over sets of integers satisfying (5.6)–(5.8). *Then*

$$\sum_{d_2 \ne d_1, d_3}^{(1)} \frac{1}{e_1 e_3 e_4 e_{134}^2} = O(D^{\theta+\varepsilon}), \tag{5.9}$$

with the implied constant depending on ε.

Proof. We fix e_0, e_1, e_2, e_3, e_{024} and e_{134} in the total decomposition set, and we consider the possible values of the side factors e_{01}, e_{03}, e_{12} and e_{23}. Combining (4.7) and (4.8), we have

$$e_{01}(e_0 e_{03} e_{024} - e_1 e_{12} e_{134}) = e_{23}(e_3 e_{03} e_{134} - e_2 e_{12} e_{024}),$$

and since $(e_{01}, e_{23}) = 1$ by (4.2), we have, for some integer a,

$$e_0 e_{03} e_{024} - e_1 e_{12} e_{134} = a e_{23}, \tag{5.10}$$

$$e_3 e_{03} e_{134} - e_2 e_{12} e_{024} = a e_{01}. \tag{5.11}$$

The pairs of terms on the left of (5.10) and (5.11) are coprime. Hence if $a = 0$, then we have

$$e_0 = e_1 = e_2 = e_3 = e_{03} = e_{12} = e_{024} = e_{134} = 1.$$

The factors e_{01} and e_{23} are unconstrained, and

$$d_0 = d_1 = e_{01}, \quad d_2 = d_3 = e_{23}.$$

This case is explicitly excluded in the sum on the left of (5.9).

Suppose that $a \neq 0$. The equations (5.10) and (5.11) give congruences modulo the absolute value of a. We deduce that

$$e_0 e_2 e_{03} e_{024}^2 \equiv e_1 e_2 e_{12} e_{024} e_{134} \equiv e_1 e_3 e_{03} e_{134}^2 \pmod{|a|},$$

$$e_1 e_3 e_{12} e_{134}^2 \equiv e_0 e_3 e_{03} e_{024} e_{134} \equiv e_0 e_2 e_{12} e_{024}^2 \pmod{|a|}.$$

Let

$$h = e_0 e_2 e_{024}^2 - e_1 e_3 e_{134}^2. \tag{5.12}$$

Then we have

$$|a| \,|\, e_{03} h, \quad |a| \,|\, e_{12} h.$$

The highest common factor (e_{03}, e_{12}) is 1 by (4.2), so $|a| \,|\, h$.

The integer h in (5.12) is a difference of two coprime integers, so if $h = 0$, then

$$e_0 = e_1 = e_2 = e_3 = e_{024} = e_{134} = 1.$$

The left-hand sides of (5.10) and (5.11) are now both $e_{03} - e_{12}$. Since $a \neq 0$, we have $e_{01} = e_{23}$, and since $(e_{01}, e_{23}) = 1$ by (4.2), the common value must be 1. Thus

$$d_0 = d_3 = e_{03}, \quad d_1 = d_2 = e_{12}.$$

This case also is explicitly excluded in the sum on the left of (5.9).

Suppose that e_0, e_1, e_2, e_3, e_{024}, and e_{134} have been fixed, with $h \neq 0$ in (5.12). The absolute value $|a|$ is one of the $O(D^\varepsilon)$ divisors of h, so there are $O(D^\varepsilon)$ possibilities for a. When a has also been fixed, then the integer vector $(e_{01}, e_{03}, e_{12}, e_{23})$ lies in a two-dimensional lattice by (5.10) and (5.11). There is a necessary condition from (5.11):

$$a e_{01} \equiv e_3 e_{03} e_{134} \pmod{e_2 e_{024}}. \tag{5.13}$$

When (5.13) is satisfied, then the values of e_{01} and e_{03} determine e_{12} by (5.11) and e_{23} by (5.10). The value of e_{23} given by (5.10) will be an integer; this follows from (5.12) and the congruence (5.13).

We count the two-dimensional projections (e_{01}, e_{03}) of the vectors $(e_{01}, e_{03}, e_{12}, e_{23})$, which lie in a lattice of determinant $e_2 e_{024}$ defined by the congruence (5.13). By (5.7) we have

$$e_0 e_{01} e_{03} e_{024} = d_0 < d_4 \le 2D.$$

Hence the integer vector (e_{01}, e_{03}) lies in one of $O(\log D)$ boxes of the form

$$1 \le e_{01} \le E_1, \quad 1 \le e_{03} \le E_3, \tag{5.14}$$

with

$$E_1 E_3 = O\Big(\frac{D}{e_0 e_{024}}\Big).$$

For each box (5.14), either all the lattice points in the box lie on a straight line (the major arc case), or the convex hull has non-zero area (the minor arc case). In the minor arc case, we can estimate the number of lattice points in the box by triangulating the convex hull as

$$O\Big(\frac{E_1 E_3}{e_2 e_{024}}\Big) = O\Big(\frac{D}{e_0 e_2 e_{024}^2}\Big).$$

In the major arc case, since the highest common factor of e_{01} and e_{03} is 1, only one point on the straight line gives a valid solution. By (5.8) the estimate

$$O\Big(\frac{D^{1+\theta}}{e_0 e_2 e_{024}^2}\Big)$$

is valid in both cases.

Hence we can write the sum in the lemma as

$$\begin{aligned} &O\Bigg(\sum_{e_0}\sum_{\substack{e_1\\ D\le e_4 e_{024} e_{134}\le 2D}}\sum_{e_2}\sum_{e_3}\sum_{e_{024}}\sum_{e_{134}}\sum_{a}\sum_{h}\frac{1}{e_1 e_3 e_4 e_{134}^2}\cdot\frac{D^{1+\theta}\log D}{e_0 e_2 e_{024}^2}\Bigg) \\ &\quad = O\Bigg(D^{\theta+2\varepsilon}\log D\sum_{e_0}\sum_{e_1}\sum_{e_2}\sum_{e_3}\sum_{e_{024}}\sum_{e_{134}}\frac{1}{e_0 e_1 e_2 e_3 e_{024} e_{134}}\Bigg) \\ &\quad = O(D^{\theta+2\varepsilon}\log^7 D), \end{aligned} \tag{5.15}$$

since the number of choices of a and h is of the order of a divisor function, at most $O(D^{\varepsilon})$. By our convention on exponents ε, we can write the expression in (5.15) as $O(D^{\theta+\varepsilon})$, which completes the proof of the lemma.

LEMMA 8. *Let $\varepsilon > 0$ and let θ in $0 \le \theta \le 1$ be given. Let D be a large positive integer. We consider a sum over quintuples of positive integers $d_0, \dots, d_4$ related by* (4.3) *and satisfying conditions involving the total*

decomposition set of Lemma 4:

$$e_{01234} = (d_0, d_1, d_2, d_3, d_4) = 1, \tag{5.16}$$

$$D \le d_4 \le 2D, \tag{5.17}$$

$$e_{01}e_{03}e_{12}e_{23} \le 4D^{1-\theta}. \tag{5.18}$$

Let $\sum^{(2)}$ *denote a sum over sets satisfying* (5.16)–(5.18). *Then*

$$\sum_{d_2 \ne d_1, d_3}^{(2)} \frac{1}{e_1 e_3 e_4 e_{134}^2} = O(D^{2(1-\theta)/3+\varepsilon}), \tag{5.19}$$

with the implied constant depending on ε.

Proof. We fix all the total decomposition set except e_0, e_2, e_4 and e_{024}. The product $e_4 e_{024}$ is fixed by (4.8) of Lemma 4, so there are $O(D^\varepsilon)$ possibilities for e_4 and e_{024}. When e_4 has been chosen, then by (4.7),

$$e_0 e_{01} e_{03} + e_2 e_{12} e_{23} = e_4 e_{134},$$

which is a linear relation between e_0 and e_2 with highest common factor $(e_{01}e_{03}, e_{12}e_{23}) = 1$ by (4.2) of Lemma 4. The integer values of e_0 which give integer values of e_2 are spaced $e_{12}e_{23}$ apart. Since $d_0 \le 2D$, the integer values of e_0 lie in an interval of length

$$O\bigg(\frac{D}{e_{01}e_{03}e_{024}}\bigg).$$

The number of positive solutions for e_0 and e_2 is

$$O\bigg(\frac{D}{e_{01}e_{03}e_{12}e_{23}e_{024}} + 1\bigg).$$

We want to estimate the sum

$$\sum_{e_{01}}\sum_{e_{03}}\sum_{e_{12}}\sum_{e_{23}}\sum_{e_1 \le D}\sum_{e_3 \le D}\sum_{e_{134} \le D}\sum_{e_{024}}^{(2)} \frac{1}{e_1 e_3 e_4 e_{134}^2} \times \bigg(\frac{D}{e_{01}e_{03}e_{12}e_{23}e_{024}} + 1\bigg). \tag{5.20}$$

There are $O(D^\varepsilon)$ values of e_4 and e_{024}, and by (5.17) the main term is

$$O\bigg(\sum_{e_{01}}\sum_{e_{03}}\sum_{e_{12}}\sum_{e_{23}}\sum_{e_1}\sum_{e_3}\sum_{e_{134}}^{(2)} \frac{D^\varepsilon}{e_1 e_3 e_{01} e_{03} e_{12} e_{23} e_{134}}\bigg) = O(D^\varepsilon \log^7 D). \tag{5.21}$$

We can write this bound as $O(D^\varepsilon)$ with our convention on exponents ε.

Next we consider the remainder term $+1$ in (5.20). We pick a parameter E in $1 \le E \le D$. If $e_{024} \le E$ then by (5.17), $e_4 e_{134} \le D/E$, so the remainder

terms when $e_{024} \le E$ in (5.20) contribute

$$O\Big(\sum_{e_{01}}\sum_{e_{03}}\sum_{e_{12}}\sum_{e_{23}}\sum_{e_1}\sum_{e_3}\sum_{e_{134}}\sum_{e_{024}\le E}^{(2)} \frac{E}{e_1e_3e_{134}D}\Big)$$
$$= O\Big(\sum_{e_{01}}\sum_{e_{03}}\sum_{e_{12}}\sum_{e_{23}}^{(2)} \frac{ED^\varepsilon \log^3 D}{D}\Big) = O(D^{-\theta+\varepsilon}E\log^7 D),$$

which we can write as

$$O(D^{-\theta+\varepsilon}E) \tag{5.22}$$

with our convention on exponents ε.

From (5.17),

$$e_0e_2e_{01}e_{03}e_{12}e_{23}e_{024}^2 = d_0d_2 < d_4^2 \le 4D^2,$$

so if $e_{024} > E$ then

$$e_{01}e_{03}e_{12}e_{23} < \frac{4D^2}{E^2}.$$

The remainder terms in (5.20) when $e_{024} > E$ contribute

$$O\Big(\sum_{\substack{e_{01}\,e_{03}\,e_{12}\,e_{23}\\ e_{01}e_{03}e_{12}e_{23}<4D^2/E^2}}\sum_{e_1}\sum_{e_3}\sum_{e_{134}}\sum_{e_{024}}^{(2)} \frac{1}{e_1e_3e_{134}^2}\Big)$$
$$= O\Big(D^\varepsilon\log^2 D \sum_{\substack{e_{01}\,e_{03}\,e_{12}\,e_{23}\\ e_{01}e_{03}e_{12}e_{23}<4D^2/E^2}} 1\Big) = O\Big(D^\varepsilon\log^2 D\cdot\frac{D^2\log^3 D}{E^2}\Big),$$

which we can write as

$$O\Big(\frac{D^{2+\varepsilon}}{E^2}\Big) \tag{5.23}$$

with our convention on exponents ε.

When we choose

$$E = D^{(2+\theta)/3},$$

then both bounds (5.22) and (5.23) become

$$O(D^{2(1-\theta)/3+\varepsilon}),$$

which establishes the lemma.

Lemma 6 has to be complemented by a counting argument that still works when the Gaussian factors τ_j in Lemma 5 are small. Lemma 9 is based on the identity (4.18), which corresponds to Ptolemy's theorem in the geometry of circles. We thank W. Zudilin for suggesting that Ptolemy's theorem was relevant.

LEMMA 9. *Let $\varepsilon > 0$ be given. Let E be a large positive integer. Let the Gaussian integer δ be fixed. Then the number of different cyclic quadrilaterals $OM_1M_2M_3$ with circumradius $r \le R$ and*

$$e_{024}e_{134}\operatorname{Norm}\tau_2 \le E \tag{5.24}$$

is

$$O\left(\frac{R^{2+\varepsilon}}{\operatorname{Norm}\delta} + E^2R^{\varepsilon}\right), \tag{5.25}$$

where the implied constant depends on ε.

Proof. We write (4.18) as

$$u_1 + u_3 = u_2, \tag{5.26}$$

where

$$u_1 = e_{01}e_{23}\operatorname{Norm}\tau_1, \quad u_2 = e_{024}e_{134}\operatorname{Norm}\tau_2, \quad u_3 = e_{03}e_{12}\operatorname{Norm}\tau_3.$$

When u_2 has been chosen to satisfy (5.24), then there are $O(R^{\varepsilon})$ choices for e_{024}, e_{134} and the Gaussian integer τ_2. There are $u_2 - 1$ choices for $u_1 < u_2$ by (5.26), and then $O(R^{\varepsilon})$ choices for e_{01}, e_{23} and the Gaussian integer τ_3. The integer u_3 is determined by (5.26), and there are $O(R^{\varepsilon})$ choices for e_{03}, e_{12} and the Gaussian integer τ_3.

When $e_{134} \ge e_{024}$, then we see from (4.9) that

$$\operatorname{Norm}\sigma_1\sigma_3 \le \frac{4R^2}{e_{134}^2\operatorname{Norm}\delta\operatorname{Norm}\tau_2}. \tag{5.27}$$

When the non-zero Gaussian integers σ_1 and σ_3 have been chosen, then (4.15) gives the value of σ_0 and (4.17) gives the value of σ_2, provided that σ_1 and σ_3 satisfy the necessary congruences

$$e_{23}\sigma_3\tau_1 \equiv e_{12}\sigma_1\tau_3 \pmod{\langle e_{024}\overline{\tau}_2\rangle}, \tag{5.28}$$

$$e_{03}\sigma_3\overline{\tau}_3 \equiv -e_{01}\sigma_1\overline{\tau}_1 \pmod{\langle e_{024}\overline{\tau}_2\rangle}. \tag{5.29}$$

Let $\langle\eta\rangle$ be the ideal

$$\langle\eta\rangle = \langle e_{23}\tau_1, e_{03}\overline{\tau}_3, e_{024}\overline{\tau}_2\rangle.$$

We see from (4.9), (4.10) and (4.11) that the Gaussian integers α_1, $\alpha_1 - \alpha_2$ and $\alpha_1 - \alpha_3$ in the proof of Lemma 5 are all in $\langle\eta\rangle$. But $\langle\alpha_1, \alpha_2, \alpha_3\rangle = \langle 1\rangle$, so $\langle\eta\rangle = \langle 1\rangle$. Hence (5.28) and (5.29) can be combined into one congruence of the form

$$\sigma_3 \equiv \gamma\sigma_1 \pmod{\langle e_{024}\overline{\tau}_2\rangle}. \tag{5.30}$$

As in the proof of Lemma 2, the solutions of (5.30) form a complex lattice Γ of Gaussian vectors (σ_1, σ_3) in $\mathbb{C}^2$, and a lattice Λ of real vectors in $\mathbb{R}^4$ of determinant $\det\Lambda = e_{024}^2\operatorname{Norm}\tau_2$. We cover the region of $\mathbb{C}^2$

satisfying (5.27) by $O(\log R)$ domains $D(U,V)$, defined by the inequalities

$$\operatorname{Norm}\sigma_1 \le U, \qquad \operatorname{Norm}\sigma_3 \le V,$$

with

$$UV \le \frac{16R^2}{e_{134}^2 \operatorname{Norm}\delta \operatorname{Norm}\tau_2}. \tag{5.31}$$

As a real set in $\mathbb{R}^4$, $D(U,V)$ is a polydisc, the product of two two-dimensional discs.

We distinguish two cases.

Major arc case. All points of the lattice Γ in $D(U,V)$ are multiples of a single basis vector (η_1,η_3). At most four of these multiples can have $\langle\sigma_1,\sigma_3\rangle = \langle\eta_1,\eta_3\rangle = \langle 1\rangle$.

Minor arc case. There are two vectors (η_1,η_3) and (ζ_1,ζ_3) of Γ in $D(U,V)$ that are linearly independent over $\mathbb{C}$. We also consider the vectors $(i\eta_1, i\eta_3)$ and $(i\zeta_1, i\zeta_3)$ to form a set of four vectors linearly independent over $\mathbb{R}$. Let N be the number of vectors of Γ in $D(U,V)$. In $\mathbb{R}^4$ we have N vectors in a convex region of volume π^2UV. These include a linearly independent set of four vectors, their negatives, and the zero vector, so $N \ge 9$. By triangulating the convex hull of the N points, we form $N-4$ disjoint simplices. The volume of each simplex is an integral multiple of $\det\Lambda/24$. Hence the number of non-zero vectors of Λ in $D(U,V)$ is

$$N-1 \le 2(N-4) \le \frac{48\pi^2UV}{\det\Lambda} \le \frac{768\pi^2R^2}{u_2^2\operatorname{Norm}\delta},$$

where we have substituted from (5.31).

We sum over $O(\log R)$ regions $D(U,V)$, so the number of choices for the Gaussian integers σ_1 and σ_3, which determine σ_0 and σ_2, is

$$O\left(\frac{R^2\log R}{u_2^2\operatorname{Norm}\delta} + \log R\right), \tag{5.32}$$

where the first term comes from the minor arc case and the second term from the major arc case.

When $e_{024} \ge e_{134}$, then we see from (4.11) that

$$\operatorname{Norm}\overline{\sigma}_0\sigma_2 \le \frac{4R^2}{e_{024}^2 \operatorname{Norm}\delta \operatorname{Norm}\tau_2}.$$

When the non-zero Gaussian integers $\overline{\sigma}_0$ and σ_2 have been chosen, then (4.16) gives the value of σ_1 and (4.14) gives the value of σ_3, provided that $\overline{\sigma}_0$ and σ_2 satisfy the necessary congruence conditions

$$e_{23}\sigma_2\tau_1 \equiv e_{03}\overline{\sigma}_0\overline{\tau}_3 \pmod{\langle e_{134}\tau_2\rangle}, \tag{5.33}$$

$$e_{12}\sigma_2\tau_3 \equiv -e_{01}\overline{\sigma}_0\overline{\tau}_1 \pmod{\langle e_{134}\tau_2\rangle}. \tag{5.34}$$

The ideal $\langle e_{23}\tau_1, e_{12}\tau_3, e_{134}\tau_2\rangle$ contains α_1, α_3 and α_2, so it is $\langle 1\rangle$, and we can combine (5.33) and (5.34) into one congruence of the form

$$\sigma_2 \equiv \gamma\overline{\sigma}_0 \pmod{\langle e_{134}\tau_2\rangle}.$$

We obtain the bound (5.32) for the number of choices of σ_0, σ_1, σ_2 and σ_3 again.

To estimate the number of cyclic quadrilaterals in the lemma, we sum the bound (5.32) over positive integers u_1, u_2 and u_3 satisfying (5.24) and (5.26). We obtain

$$O\bigg(R^{3\varepsilon}\sum_{u_2=2}^{E}\sum_{u_1=1}^{u_2-1}\bigg(\frac{R^2\log R}{u_2^2\operatorname{Norm}\delta}+\log R\bigg)\bigg) = O\bigg(\frac{R^{2+3\varepsilon}\log^2 R}{\operatorname{Norm}\delta}+E^2R^{3\varepsilon}\log R\bigg),$$

which gives the result of the lemma by our convention on exponents ε.

LEMMA 10. *Let $\varepsilon > 0$ be given. Then the number of different non-symmetric cyclic quadrilaterals $OM_1M_2M_3$ with circumradius $r \le R$ is*

$$O(R^{76/29+\varepsilon}), \tag{5.35}$$

where the implied constant depends on ε.

Proof. First we consider primitive quadrilaterals, for which the ideal $\langle\delta\rangle = \langle\mu_1,\mu_2,\mu_3\rangle$ is $\langle 1\rangle$. We count representatives of equivalence classes for which (5.1) holds. The denominator q and the highest common factor $e = e_{01234}$ do not enter the argument. We consider size ranges of the form (5.2).

We apply Lemmas 7 and 8 to the total decomposition set of $f_0,\dots,f_4$, which is the same as that of $d_0,\dots,d_4$, except that the highest common factor e_{01234} is replaced by 1. From (4.4), (4.5) and (5.2) we have

$$e_0e_1e_2e_3(e_{01}e_{03}e_{12}e_{23}e_{024}e_{134})^2 = f_0f_1f_2f_3 \le 16D^4.$$

Hence either the condition (5.8) of Lemma 7 or the condition (5.18) of Lemma 8 must hold. We take $\theta = 2/5$, and then the bounds in both Lemma 7 and Lemma 8 are

$$O(D^{2/5+\varepsilon}).$$

We pick a parameter $K \ge 1$. If

$$e_1e_3e_4e_{134}^2 \le KR^2, \tag{5.36}$$

then the upper bound in Lemma 6 is

$$O\bigg(\frac{KR^2}{e_1e_3e_4e_{134}^2}\bigg). \tag{5.37}$$

The number of primitive non-symmetric cyclic quadrilaterals with circumradius $r \le R$ satisfying (5.1), (5.2) and (5.36) is

$$O(D^{2/5}KR^{2+\varepsilon}). \tag{5.38}$$

In the contrary case to (5.36) we have

$$e_0e_2e_4e_{024}^2 \ge e_1e_3e_4e_{134}^2 > KR^2, \tag{5.39}$$

so that by (5.2),

$$K^2R^4 < e_0e_1e_2e_3e_4^2e_{024}^2e_{134}^2 < 4e_0e_1e_2e_3D^2.$$

Now by (4.9) and (4.11),

$$e_0e_1e_2e_3e_{024}^2e_{134}^2(\operatorname{Norm}\tau_2)^2 = \operatorname{Norm}(\mu_2(\mu_1-\mu_3)) \le 16R^4,$$

and in Lemma 9,

$$u_2 = e_{024}e_{134}\operatorname{Norm}\tau_2 \le \frac{4R^2}{\sqrt{e_0e_1e_2e_3}} < \frac{8D}{K}.$$

We take $E = [8D/K]$ in Lemma 9. Then the number of primitive cyclic quadrilaterals with circumradius $r \le R$ satisfying (5.1), (5.2) and (5.39) is

$$O\left(R^{2+\varepsilon} + \frac{D^2R^\varepsilon}{K^2}\right). \tag{5.40}$$

We choose

$$K = \frac{D^{8/15}}{R^{2/3}} + 1,$$

so that both bounds (5.38) and (5.40) are

$$O(D^{14/15}R^{4/3+\varepsilon} + R^{5/2+\varepsilon}). \tag{5.41}$$

We sum the bound (5.41) over all ranges (5.2) with $D \le R^{40/29}$ to get the bound

$$O(R^{76/29+\varepsilon}). \tag{5.42}$$

The remaining primitive cyclic quadrilaterals of integer points have

$$d_j \ge \frac{1}{2}\,d_4 \ge \frac{1}{2}\,R^{40/29}$$

for some $j = 1$, 2, or 3. By Lemma 2, the four points O, M_1, M_2, M_3 include the vertices of one of the

$$O(R^{76/29}\log^7 R)$$

equivalence classes of triangles with $2d > R^{40/29}$. By Lemma 1 each such triangle can be completed to a cyclic quadrilateral $OM_1M_2M_3$ of integer points in at most $K(R) = O(R^\varepsilon)$ ways. With our convention on exponents ε, the number of cyclic quadrilaterals of integer points with some common factor d_j large and with circumradius $r \le R$ is again estimated by (5.42).

To count imprimitive quadrilaterals, we replace R^2 by $R^2/\operatorname{Norm}\delta$ in (5.42). We sum over Gaussian integers δ with $\operatorname{Norm}\delta \le 4R^2$ to obtain

$$O\bigg(R^{\varepsilon} \sum_{\operatorname{Norm}\delta \le 4R^2} \bigg(\frac{R^2}{\operatorname{Norm}\delta}\bigg)^{38/29}\bigg) = O(R^{76/29+\varepsilon}),$$

which is the result of the lemma.

Theorem 2 follows at once from the asymptotic formula of Lemma 2 and the upper bound of Lemma 10.

6. Completion of the proof of Theorem 3. To prove the upper bound in Theorem 3 we need a combinatorial lemma.

LEMMA 11. *Let V be a set of five or more integer points lying on a circle. Then there is some subset of four points of V which does not form the vertices of a symmetric trapezium.*

Proof. Let A, B, C, D, E be five distinct points on a circle, in cyclic order, such that among any subset of four points, there is a pair of parallel joins. Line segments which share a vertex cannot be parallel. Line segments which cross within the circle cannot be parallel. Each of the five quadrilaterals $ABCD$, $ABCE$, $ABDE$, $ACDE$ and $BCDE$ contains a different pair of parallel line segments. The only configuration consistent with these constraints has $AD \parallel BC$, $AB \parallel CE$, $AE \parallel BD$, $AC \parallel DE$ and $BC \parallel CD$. In each case a side of the pentagon $ABCDE$ is parallel to the proper diagonal which does not meet that side.

The five trapezia $ABCD$, $ABCE$, $ABDE$, $ACDE$ and $BCDE$ are symmetric, so the angles of the pentagon $ABCDE$ are all equal. Since the pentagon is inscribed in a circle, it is regular. The complex numbers α, β and γ representing A, B and C have $\gamma - \beta = \zeta(\beta - \alpha)$, where ζ is some fifth root of unity. Since ζ does not lie in the Gaussian field $\mathbb{Q}(i)$, the complex numbers α, β and γ cannot all be Gaussian integers. The set V in the lemma cannot be the vertices of a regular pentagon, and some four-point subset of V does not form a symmetric trapezium.

We complete the proof of Theorem 3 using the following trivial upper bound for $k \ge 5$:

$$P_k(R) \le K(R)^{k-4} P_4^*(R),$$

where $P_4^*(R)$ is the number of equivalence classes of non-symmetric cyclic quadrilaterals with circumradius $r \le R$, and $K(R)$ is the maximum number of integer points on a circle of radius $r \le R$. The estimates for $K(R)$ in Lemma 2 and for $P_4^*(R)$ in Lemma 9 give the upper bound in Theorem 3.

Acknowledgements. This work forms part of INTAS research project number 03-51-5070, Analytical and Combinatorial Methods in Number Theory and Geometry.

We thank Shaunna Plunkett-Levin for reading the typescript carefully.

References

[1] G. R. H. Greaves, *Sieves in Number Theory*, Springer, Berlin, 2001.
[2] R. R. Hall, *The distribution of squarefree numbers*, J. Reine Angew. Math. 394 (1989), 107–117.
[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, 1960.
[4] C. Hooley, *Applications of Sieve Methods*, Cambridge Univ. Press, 1976.
[5] M. N. Huxley, *Exponential sums and lattice points III*, Proc. London Math. Soc. (3) 87 (2003), 591–609.
[6] M. N. Huxley and J. Žunić, *The number of configurations in lattice point counting I*, submitted.
[7] —, —, *The number of configurations in lattice point counting II*, submitted.
[8] M. N. Huxley, M. Kolountzakis and J. Žunić, *The number of configurations in lattice point counting III*, in preparation.
[9] A. Schinzel, *Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières*, Enseign. Math. 4 (1958), 71–72.
[10] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, J. London Math. Soc. (2) 21 (1922), 235–255.

School of Mathematics
University of Cardiff
23, Senghennydd Road
Cardiff, CF24 4AG, Wales, U.K.
E-mail: huxley@cf.ac.uk

Department of Mechanics and Mathematics
Moscow State University
Moscow, 119992, Russia
E-mail: konyagin@ok.ru

Received on 31.3.2008 (5677)