ACTA ARITHMETICA
158.2 (2013)

Circles passing through five or more integer points

by

Shaunna M. Plunkett-Levin (Cardiff)

1. Introduction. The work of Huxley and Konyagin [8] considers the question, “Among the circles drawn through three distinct integer points in the plane, are circles which pass through four or more points rare?” This question arose from the investigation by Huxley and Žunić [10, 11] of the configurations of integer points in convex plane sets. Huxley and Konyagin [8] study families of circles passing through three, four and five integer points, finding upper and lower bounds.

This paper gives an improvement to Huxley and Konyagin’s current lower bound for the number of circles passing through five integer points. We conjecture that the improved lower bound is the asymptotic formula for the number of circles passing through five integer points. We also generalise our result to circles passing through more than five integer points. The current lower bound has the form $c \log R$, and we improve this to a polynomial in $\log R$ of degree $2^{m-1} - 1$. For small $m \geq 5$, the estimate increases for sufficiently large R, since we consider a small number of circles (the number of which decreases with m) passing through many integer points.

Using the notation of [8], let $P_m(R)$ denote the number of sets of m distinct integer points lying on a circle of radius r, with $r \leq R$, where the centre of the circle is located in the unit square. Again, using the notation of [8], for sufficiently large R, $C(m, \epsilon)$ is a constant dependent on m and ϵ. For sufficiently large R, Huxley and Konyagin have bounded $P_m(R)$ for $m = 3, 4, 5$. They proved

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

where $\kappa = 131/208$ and $\lambda = 18627/8320$ (see [6]), and

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

2010 *Mathematics Subject Classification*: Primary 11P21; Secondary 11N37, 11M41.
Key words and phrases: integer points, cyclic polygons, circles.

DOI: 10.4064/aa158-2-3

where $\epsilon > 0$ and $L(s,\chi)$ is the Dirichlet L-function formed with the nontrivial character mod 4. We use this definition of $L(s,\chi)$ throughout the paper. For $P_5(R)$ with $\epsilon > 0$, the current bounds are

$$cR^2 \log R \le P_5(R) \le C(5,\epsilon)R^{76/29+\epsilon}.$$

To improve the lower bound on $P_5(R)$ we consider $r(n)$, the arithmetic function that counts the number of integer solutions of $x^2+y^2=n$ with $x>0$, $y\ge 0$. In a paper mainly concerned with moments of the divisor function, Wilson [17] predicted the existence of analogues for powers of $r(n)$:

Proposition A (Wilson). *For each integer $m \ge 1$, there are constants b_m, $b_m = 2^{m-1}-1$, and c_m such that as $N\to\infty$, we have*

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

Our first result is a more precise form of Wilson's proposition for $m\ge 3$.

Theorem 1.1. *Let $m\ge 3$ be a fixed integer, and $r(n)$ be the arithmetic function counting the number of integer solutions of $x^2+y^2=n$ with $x>0$ and $y\ge 0$. Then, as $N\to\infty$,*

$$\sum_{n\le N} r^m(n) = NP_m(\log N) + O(N^{\Phi+\epsilon}), \tag{1.1}$$

where $P_m(x)$ is a polynomial of degree $b=2^{m-1}-1$, and the Φ term in the exponent is less than 1. The leading coefficient c of $P_m(x)$ is

$$c = \left(\frac{\pi}{4}\right)^{b+1}\frac{E}{b!}, \tag{1.2}$$

where E is the Euler product

$$E = \left(\frac{1}{2}\right)^b \prod_{p\equiv 1 \bmod 4}\left(1-\frac{1}{p}\right)^{A(m,2)}\sum_{k=1}^{m}A(m,k)p^{(1-k)}\prod_{p\equiv 3 \bmod 4}\left(1-\frac{1}{p^2}\right)^b, \tag{1.3}$$

and $A(m,k)$ denotes the Eulerian number [1]

$$A(m,k) = \sum_{j=0}^{k}(-1)^j\,{}_{m+1}\mathrm{C}_j(k-j)^m,$$

with $A(m,2) = 2^m-m-1$.

The Φ term in the exponent of (1.1) *is related to the value of the ϕ term in the exponent for the size of the Riemann zeta function* [15]:

$$\zeta(1/2+it) = O(t^{\phi+\eta})$$

for all $\eta>0$ as $t\to\infty$. The relationship is

$$\Phi = \frac{(4b-4)\phi+1}{(4b-4)\phi+2}, \tag{1.4}$$

where b is the degree of $P_m(x)$. By Huxley's estimate [7], *we take $\phi = 32/205$. The constant ϵ and the constant implied in the O symbol follow the conventions given below.*

We then establish our conjectured asymptotic formula for the number of cyclic polygons with m integer vertices, that is, the number of circles passing through m integer points, for each $m \geq 3$, which have circumcentre at the origin and circumradius at most $\sqrt{N}$.

THEOREM 1.2. *Let $m \geq 3$ be a fixed integer. Let $X_m(N)$ denote the number of cyclic polygons with circumcentre at the origin, m integer vertices, and circumradius at most $\sqrt{N}$. Then*

$$X_m(N) = \frac{N}{m!}\Big(\sum_{j=1}^{m} 4^j s(m,j) P_j(\log N)\Big) + O(N^{\Phi+\epsilon}).$$

The polynomials $P_j(x)$ and the Φ term in the exponent are as in Theorem 1.1, *where b in* (1.4) *is the degree of $P_m(x)$, and $s(m,j)$ denotes the signed Stirling numbers of the first kind* [2].

Next, we restrict this result to $r^*(n,q)$, an arithmetic function related to the function $r(n)$.

THEOREM 1.3. *Let $m \geq 3$ and $q \geq 1$ be fixed integers. Let $r^*(n,q)$ be the arithmetic function which counts integer solutions of $x^2 + y^2 = n$ with $x > 0$, $y \geq 0$ and highest common factor $(x,y,q) = 1$. Then for $\sigma \geq 1/2$, as $N \to \infty$,*

$$\sum_{n \leq N} \frac{(r^*(n,q))^m}{n^s} = N P_{m,q}(\log N) + O(q^{\epsilon} N^{\Phi+\epsilon}), \tag{1.5}$$

where $P_{m,q}(x)$ is a polynomial of degree $b = 2^{m-1} - 1$ whose coefficients depend on q, and $\Phi < 1$ is the same as in (1.4) *of Theorem* 1.1. *The leading coefficient c_q of $P_{m,q}(x)$ can be expressed as*

$$c_q = \frac{1}{b!}\left(\frac{\pi}{4}\right)^{b+1} E(q,1) \tag{1.6}$$

where $E(q,1) = E\Psi(q,1)$, for E as in (1.3) *of Theorem* 1.1, *and $\Psi(q,1)$ a certain convergent Euler product.*

We establish a lower bound for the number of cyclic polygons with five or more integer point vertices.

LEMMA 1.4. *Let $m \geq 5$ and $q \geq 1$ be fixed integers. Let n be a positive integer with $q^2 < n$. Let $f(q)$ be the arithmetic function*

$$f(q) = q^2 \prod_{p|q}\left(1 - \frac{1}{p^2}\right) \tag{1.7}$$

which counts pairs of residue classes $a \bmod q$, $b \bmod q$, *with highest common factor* $(a,b,q)=1$.

Let $r^* = (m-1)r^*(n,q)$ *denote the number of integer points* (x,y) *on the circle* $x^2+y^2=n$ *with highest common factor* $(x,y,q)=1$. *Let* $V_m(n,q)$ *be the number of cyclic polygons with* m *integer point vertices, with radius* $r=\sqrt{n}/q$, *centred at the point* $(a/q,b/q)$ *in the unit square, where* $0 \le a < q$, $0 \le b < q$ *and the highest common factor* (a,b,q) *equals* 1. *Then*

$$V_m(n,q) \ge f(q)\,{}_l\mathrm{C}_m,$$

where $l=[r^*/f(q)]$, *the integer part of* $r^*/f(q)$, *and* ${}_l\mathrm{C}_m$ *is interpreted as* 0 *for* $l \le m-1$.

We restrict the size of the circumradius r in Lemma 1.4 to the range $r \le R$ and obtain a theorem giving a lower bound for the number of m-sided cyclic polygons with radius up to size R. This theorem is our conjectured asymptotic formula for the number of circles passing through five or more integer points.

Theorem 1.5. *Let* $m \ge 4$ *be a fixed integer. Let* $W_m(R)$ *be the number of cyclic polygons with* m *integer point vertices centred in the unit square with radius* $r \le R$. *There exists a polynomial* $w(x)$ *such that*

$$W_m(R) \ge \frac{4^m}{m!}R^2 w(\log R)(1+o(1)),$$

where $w(x)$ *is an explicit polynomial of degree* $b=2^{m-1}-1$.

We use the standard notation of $\zeta(s)$ for the Riemann zeta function, with $s=\sigma+it$ where $\sigma=\mathrm{Re}(s)$ and $t=\mathrm{Im}(s)$. We follow the convention that when we have the constant ϵ in the exponent of an error term, ϵ may be taken to be arbitrarily small and positive, but the constant implied in the O symbol will depend on it. The Vinogradov symbol $f(x) \ll g(x)$ as $x \to \infty$ means $f(x)=O(g(x))$ as $x \to \infty$, where $g(x)$ is positive for all large x. The symbol $\asymp$ means asymptotically equal to, that is, $A \ll B \ll A$, with some implied constants.

2. Proof of Theorem 1.1. We begin our proof by writing the Dirichlet series $F(s)$ for $r^m(n)$ as an Euler product,

$$F(s)=\sum_{n=1}^{\infty}\frac{r^m(n)}{n^s}=G\Big(\frac{1}{2^s}\Big)\prod_{p\equiv 1 \bmod 4}H\Big(\frac{1}{p^s}\Big)\prod_{p\equiv 3 \bmod 4}G\Big(\frac{1}{p^{2s}}\Big). \tag{2.1}$$

Here $G(x)$ and $H(x)$ are infinite series that can be expressed as rational functions,

$$G(x) = \frac{1}{1-x}, \tag{2.2}$$

$$H(x) = 1 + 2^m x + 3^m x^2 + \cdots = \frac{1}{(1-x)^{m+1}} \sum_{k=1}^{m} A(m,k) x^{k-1}, \tag{2.3}$$

with the defining property of the Eulerian numbers $A(m,k)$ given in [1].

The Dirichlet series for $r^m(n)$ can be written in terms of the Dedekind zeta function $Z(s) = \zeta(s)L(s,\chi)$, the product of the Riemann zeta function and the Dirichlet L-function for the Gaussian field, so that $F(s) = Z^{b+1}(s)E(s)$. From (2.1)–(2.3) we have

$$\begin{aligned} E(s) = {} & \left(1 - \frac{1}{2^s}\right)^b \prod_{p \equiv 3 \bmod 4} \left(1 - \frac{1}{p^{2s}}\right)^b \\ & \times \prod_{p \equiv 1 \bmod 4} \left(1 - \frac{1}{p^s}\right)^{A(m,2)} \sum_{k=1}^{m} A(m,k) p^{s(1-k)}. \end{aligned} \tag{2.4}$$

The product E in (1.3) is $E(1)$ in the notation (2.4).

We find the analytic continuation of $E(s)$ by comparing $E(s)$ to $\zeta(2s)$ and $L(2s,\chi)$ as infinite products of primes. We write

$$E(s) = \frac{J(s)}{\zeta^{j_1}(2s) L^{j_2}(2s,\chi)}, \tag{2.5}$$

where the exponents j_1 and j_2 are found from $b = 2^{m-1} - 1$ and

$$d = 2^{m-1}(2^m + 1) - 3^m, \tag{2.6}$$

by

$$\begin{aligned} j_1 &= \frac{d+b}{2} = 2^{m-1}(2^{m-1}+1) - \frac{1}{2}(3^m + 1), \\ j_2 &= \frac{d-b}{2} = 2^{2(m-1)} + \frac{1}{2}(1 - 3^m). \end{aligned}$$

The residual factor $J(s)$ of the expression $E(s)$ given in (2.5) is

$$J(s) = A(2) \prod_{p \equiv 1 \bmod 4} B(p) \prod_{p \equiv 3 \bmod 4} C(p),$$

where

$$A(2) = \left(1 + \frac{1}{2^s}\right)^{-j_1} \left(1 - \frac{1}{2^s}\right)^{-j_2},$$

so $A(2)$ is a rational function in $1/2^s$, with poles on $\sigma = 0$. For calculable constants β and γ, dependent only on m, we have

$$B(p) = 1 + \frac{\beta}{p^{3s}} + \frac{\gamma}{p^{4s}} + \cdots,$$

and

$$C(p) = \left(1 - \frac{1}{p^{4s}}\right)^{-j_2} = 1 + \frac{j_2}{p^{4s}} + \frac{j_2(j_2+1)}{2}\frac{1}{p^{8s}} + \cdots .$$

The Dirichlet series for $\log J(s)$ converges absolutely for $\sigma > 1/3$ by comparison with the series $\zeta(3\sigma)$. However, at $s = 1/2$, $\zeta(2s)$ has a pole, whilst the series for $L(2s,\chi)$ converges for $\sigma > 0$. Hence $E(s)$ can be continued analytically to $\sigma > 1/2$.

We now consider the size of $E(s)$,

$$|E(s)| = \frac{|J(s)|}{|\zeta(2s)|^{j_1}|L(2s,\chi)|^{j_2}}.$$

The series $\log J(s)$, and hence $|J(s)|$, are uniformly bounded for $\sigma \geq 1/2$, with $|J(s)| < \tilde{J}$ for some constant $\tilde{J}$. For $\sigma > 1/2$, we have the inequalities

$$\frac{1}{|\zeta(2s)|} \leq \zeta(2\sigma), \qquad \frac{1}{|L(2s,\chi)|} \leq \zeta(2\sigma),$$

and

$$|E(s)| = \frac{|J(s)|}{|\zeta(2s)|^{j_1}\,|L(2s,\chi)|^{j_2}} \leq \tilde{J}(\zeta(2\sigma))^{j_1+j_2} = \tilde{J}\zeta^d(2\sigma).$$

We need several lemmas to continue the proof of Theorem 1.1.

Lemma 2.1. *Let $\eta > 0$. Then*

$$\frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT}\left(\frac{x}{n}\right)^s\frac{ds}{s} = \begin{cases} 1 + O\left(\left(\frac{x}{n}\right)^{1+\eta}\frac{1}{T\log(x/n)}\right) & \textit{if } n < x, \\ O\left(\left(\frac{x}{n}\right)^{1+\eta}\frac{1}{T\log(n/x)}\right) & \textit{if } n > x. \end{cases}$$

Proof. This is a standard result; see Montgomery and Vaughan ([13, Chapter 5]). ■

Lemma 2.2. *Let*

$$F(s) = \sum_{n=1}^{\infty}\frac{r^m(n)}{n^s}.$$

Let N be a positive integer. Set $x = N + 1/2$ and $\eta = 2/\log x$. Then

$$\sum_{n\leq N} r^m(n) = \frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} F(s)\frac{x^s}{s}\,ds + O\left(\frac{x^{1+\epsilon}\log x}{T}\right).$$

Proof. This is deduced by the standard method from the inequality $r(n) \leq A(\delta)n^{\delta}$, given by Hardy and Wright ([4, Chapter 18]). ■

Lemma 2.3. *In Lemma 2.2, we can choose $T \geq 10$ so that, for large x,*

$$\frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} F(s)\frac{x^s}{s}\,ds = \operatorname*{Res}_{s=1}\left[F(s)\frac{x^s}{s}\right] + O(x^{\varPhi+\epsilon}),$$

where $T = x^{1-\varPhi}$, and $\varPhi$ was defined in (1.4).

Proof. We take a bounded closed contour D around the pole of the integrand at $s=1$. Let $\alpha = 1/2+1/\log x$. Let $T \geq 10$ be a parameter, chosen so that T is a fractional power of x. The contour $D = C_1 + D_1 + D_2 + D_3$ is constructed once a second parameter U has been chosen, $T/2 \leq U \leq T$. Then C_1 is the line segment from $1+\eta+iU$ to $1+\eta-iU$, D_1 is the line segment from $1+\eta+iU$ to $\alpha+iU$, D_2 is the line segment from $\alpha+iU$ to $\alpha-iU$, and D_3 is the line segment from $\alpha-iU$ to $1+\eta-iU$.

By the calculus of residues, the integral along C_1 is

$$\frac{1}{2\pi i}\int_{C_1} F(s)\frac{x^s}{s}\,ds = \operatorname*{Res}_{s=1}\left[F(s)\frac{x^s}{s}\right] - \frac{1}{2\pi i}\int_{D_1} F(s)\frac{x^s}{s}\,ds - \frac{1}{2\pi i}\int_{D_2} F(s)\frac{x^s}{s}\,ds - \frac{1}{2\pi i}\int_{D_3} F(s)\frac{x^s}{s}\,ds.$$

Firstly we consider the integral along D_2. Here we have $\sigma = \alpha$, so that $E(s) \leq \tilde{J}\zeta^d(2\alpha)$, and $|E(s)| \ll \log^d x$.

For $1 \leq \tau \leq T$ and $1/2 \leq \alpha \leq 3/4$,

$$\int_1^\tau |\zeta(\alpha+it)|^4\,dt \ll \tau\log^4\tau \ll T\log^4 T \tag{2.7}$$

(Titchmarsh [15, Chapter 7]), so that

$$\int_{-T}^{T} \frac{|\zeta(\alpha+it)|^4}{|\alpha+it|}\,dt \ll \log^5 T.$$

The proof in [7] of Huxley's estimate

$$\zeta(1/2+it) \ll t^\phi(\log t)^\gamma,$$

with $\phi = 32/205$ and $\gamma = 4157/2050$ and $10 \leq |t| \leq T$, can be adapted (Huxley [5], Huxley and Watt [9]) to show that for $\sigma \geq 1/2$ and $10 \leq |t| \leq T$,

$$\zeta(\sigma+it) \ll |t|^{2\phi(1-\sigma)}(\log|t|)^\gamma \ll T^{2\phi(1-\sigma)}(\log T)^\gamma \ll T^\phi(\log T)^\gamma, \tag{2.8}$$

$$L(\sigma+it,\chi) \ll |t|^{2\phi(1-\sigma)}(\log|t|)^\gamma \ll T^{2\phi(1-\sigma)}(\log T)^\gamma \ll T^\phi(\log T)^\gamma. \tag{2.9}$$

We use (2.8) and (2.9) to obtain

$$\int_{-T}^{T} \frac{|\zeta(\alpha+it)|^{b+1}|L(\alpha+it,\chi)|^{b+1}}{|\alpha+it|}\,dt \ll \log^5 T(T^\phi\log^\gamma T)^{2(b-1)}.$$

Hence

$$\begin{aligned}(2.10)\qquad &\int\limits_{D_2} \frac{|F(s)|\,|x|^s}{|s|}\,|ds| \\ &\qquad \ll (T^{2\phi(1-\alpha)}(\log T)^{\gamma})^{2b-2} x^{\alpha} \log^d x \int\limits_{-T}^{T} \frac{|\zeta(\alpha+it)|^4}{|\alpha+it|}\,dt \\ &\qquad \ll \sqrt{x}\, T^{(2b-2)\phi}(\log T)^{(2b-2)\gamma+5}(\log x)^d.\end{aligned}$$

We now estimate the integrals along D_1 and D_3. Here we have $\alpha \le \sigma \le 1+\eta$, $|x^s| = x^{\sigma}$, and

$$|E(s)| \le \tilde{J}\zeta^d(2\sigma) \ll \frac{1}{(2\sigma-1)^d} \ll \frac{1}{(2\alpha-1)^d} \ll \log^d x.$$

The integral along D_1 is found by averaging over U, $T/2 \le U \le T$:

$$\begin{aligned}(2.11)\qquad \left|\frac{1}{2\pi i}\int\limits_{D_1} F(s)\frac{x^s}{s}\,ds\right| &\le \frac{1}{T/2}\int\limits_{T/2}^{T}\int\limits_{\alpha}^{1+\eta} \frac{|F(s)|\,|x^s|}{|s|}\,|ds|\,dt \\ &= \frac{2}{T}\int\limits_{\alpha}^{1+\eta} x^{\sigma}\left(\int\limits_{T/2}^{T} \frac{|Z^{b+1}(s)E(s)|}{|s|}\,dt\right)d\sigma.\end{aligned}$$

We use the bounds (2.7)–(2.9) to estimate

$$\begin{aligned}(2.12)\qquad &\int\limits_{T/2}^{T} \frac{|Z^{b+1}(s)E(s)|}{|s|}\,dt \\ &\ll (\log x)^d \int\limits_{T/2}^{T} \frac{|\zeta(\sigma+it)|^{b+1}|L(\sigma+it,\chi)|^{b+1}}{|\sigma+it|}\,dt \\ &\ll \frac{(\log x)^d T \log^4 T (T^{2\phi(1-\sigma)}(\log T)^{\gamma})^{b-3}(T^{2\phi(1-\sigma)}(\log T)^{\gamma})^{b+1}}{T/2} \\ &\ll (\log x)^d T^{2\phi(1-\sigma)(2b-2)}(\log T)^{\gamma(2b-2)+4}.\end{aligned}$$

We substitute (2.12) into (2.11) to obtain

$$\begin{aligned}(2.13)\qquad &\left|\frac{1}{2\pi i}\int\limits_{D_1} F(s)\frac{x^s}{s}\,ds\right| \\ &\qquad \ll \frac{(\log x)^d(\log T)^{\gamma(2b-2)+4}}{T}\int\limits_{\alpha}^{1+\eta} x^{\sigma}T^{2\phi(1-\sigma)(2b-2)}\,d\sigma \\ &\qquad \ll \frac{(\log x)^d(\log T)^{\gamma(2b-2)+4}}{T}(\sqrt{x}\,T^{(2b-2)\phi}+x).\end{aligned}$$

We get the same estimate for the integral along D_3.

We choose T so that $T^{(4b-4)\phi} \ll x$, which gives $\log T \ll \log x$. We can now modify the estimate (2.13) to

$$\frac{1}{2\pi i}\int\limits_{D_1} F(s)\frac{x^s}{s}\,ds \ll \frac{x(\log x)^{(2b-2)\gamma+d+4}}{T},$$

and similarly for the integral along D_3. The integral along D_2, given in (2.10), becomes

$$\frac{1}{2\pi i}\int\limits_{D_2} F(s)\frac{x^s}{s}\,ds \ll \sqrt{x}\,T^{(2b-2)\phi}(\log x)^{(2b-2)\gamma+d+5}.$$

We balance these terms by choosing

$$T \asymp x^{\frac{1}{(4b-4)\phi+2}}(\log x)^{-((2b-2)\phi+1)}.$$

Hence

$$\sqrt{x}\,T^{(2b-2)\phi}(\log x)^{(2b-2)\gamma+d+5} \asymp \frac{x(\log x)^{(2b-2)\gamma+d+4}}{T} \asymp x^{\Phi}(\log x)^{A},$$

with Φ as in (1.4), and $A = (2b-2)\gamma + d + 4$. The powers of $\log x$ contribute to the factor of the form x^{ϵ}. ■

We now calculate the residue given in our contour integral estimation.

Lemma 2.4. *The residue in the statement of Lemma* 2.3 *can be written as*

$$\operatorname*{Res}_{s=1}[F(s)x^s/s] = xP_m(\log x),$$

where $P_m(z)$ is a polynomial in z of degree $b = 2^{m-1} - 1$, whose coefficients are expressed in terms of the derivatives of the function

$$V(s) = (s-1)^{b+1}F(s)/s \tag{2.14}$$

by

$$P_m(z) = \frac{1}{b!}\sum_{j=0}^{b} {}_b\mathrm{C}_j V^{(b-j)}(1)z^j.$$

Proof. Since $F(s) = Z^{b+1}(s)E(s)$, where the Dedekind zeta function $Z(s)$ has a single pole at $s = 1$, and the Euler product $E(s)$ is regular at $s = 1$, $V(s)$ is regular at $s = 1$, with power series expansion

$$V(s) = \sum_{n=0}^{\infty}\frac{V^{(n)}(1)}{n!}(s-1)^n.$$

We multiply (2.14) by x^s and rearrange to give

$$\frac{F(s)x^s}{s} = \frac{V(s)x^s}{(s-1)^{b+1}},$$

which we use to write the residue as a limit. The result of the lemma then follows by the usual rules of differentiation. ■

Proof of Theorem 1.1. Concatenating the results of Lemmas 2.2–2.4, we have

$$\sum_{n\le N} r^m(n) = xP_m(\log x) + O(x^{\Phi+\epsilon}) + O\bigg(\frac{x^{1+\epsilon}\log x}{T}\bigg). \tag{2.15}$$

By the choice of T in Lemma 2.3 the error terms combine to $O(x^{\Phi+\epsilon})$. Theorem 1.1 is expressed in terms of $N = x - 1/2$, so that

$$x = N(1 + O(1/N)), \qquad \log x = \log N + O(1/N), \tag{2.16}$$

and we pass easily from the expression (2.15) in terms of x to the statement (1.1) in terms of N.

The leading coefficient of $P_m(\log x)$ is $V(1)/b!$, where

$$V(1) = E(1)\Big(\operatorname*{Res}_{s=1}\Big)^{b+1} = E(1)(\pi/4)^{b+1}.$$

The leading coefficient of $P_m(\log x)$ is

$$c = (\pi/4)^{b+1}E/b!$$

in the notation of (1.2) and (1.3). ■

3. Proof of Theorem 1.2. We recall that $X_m(N)$ denotes the number of cyclic polygons with m integer vertices, centre at the origin, and circumradius at most $\sqrt{N}$. The circumradius is $\sqrt{n}$ for some integer n. Let $Y_m(n)$ be the number of such polygons inscribed in the circle $x^2 + y^2 = n$. Then $Y_m(n) = {}_r\mathrm{C}_m$, where $r = 4r(n)$ and $Y_m(n)$ can be expanded in terms of the signed Stirling numbers $s(m, j)$ of the first kind [2], to give

$$Y_m(n) = \frac{1}{m!}\sum_{j=1}^{m} s(m,j)r^j.$$

Hence

$$\begin{aligned} X_m(N) &= \sum_{n\le N} Y_m(n) = \sum_{n\le N}\frac{1}{m!}\sum_{j=1}^{m} s(m,j)r^j(n) \\ &= \frac{1}{m!}\sum_{j=1}^{m} 4^j s(m,j)\sum_{n\le N} r^j(n). \end{aligned} \tag{3.1}$$

Theorem 1.2 follows at once when we substitute the asymptotic expansion (1.1) of Theorem 1.1. The Φ term in the error exponent in (3.1) is formally the same as that of (1.4) with $b = 2^{m-1} - 1$. ■

4. Proof of Theorem 1.3. We indicate the necessary modifications to the proof of Theorem 1.1 to obtain Theorem 1.3.

Instead of the arithmetic function $r(n)$ given on primes p and prime powers p^k, we find expressions for $r^*(n,q)$ related to the primes p. We distinguish bad primes p with $p\,|\,q$ from good primes p with $p\nmid q$. Let $n=p^k$, where $p\geq 2$ is a prime, and $k\geq 1$ is an integer. Then

$$r^*(n,q)=\begin{cases} r(n) & \text{for all primes when } k=1,\\ r(n) & \text{for good primes } p\text{, when } k\geq 2,\\ 0 & \text{for } p=2 \text{ bad, when } k\geq 2,\\ 2 & \text{for bad } p\equiv 1 \bmod 4,\\ 0 & \text{for bad } p\equiv 3 \bmod 4.\end{cases}$$

We write the Dirichlet series $F(q,s)$ for $(r^*(n,q))^m$ as an Euler product

$$F(q,s)=\sum_{n=1}^{\infty}\frac{(r^*(n,q))^m}{n^s}=\prod_{p\,\text{prime}}\phi_p(q,s).$$

For good primes $p\nmid q$ the Euler factors are those in (2.1),

$$\phi_p(q,s)=\phi_p(s)=\begin{cases} G(1/2^s) & \text{for } p=2,\\ H(1/p^s) & \text{for } p\equiv 1 \bmod 4,\\ G(1/p^{2s}) & \text{for } p\equiv 3 \bmod 4.\end{cases}$$

For bad primes $p\,|\,q$ the Euler factors become

$$\phi_p(q,s)=\theta_p(s)=\begin{cases} 1+1/2^s & \text{for } p=2,\\ 1+2^m/(p^s-1) & \text{for } p\equiv 1 \bmod 4,\\ 1 & \text{for } p\equiv 3 \bmod 4.\end{cases}$$

We obtain a factorisation

$$F(q,s)=Z^{b+1}(s)E(q,s)=Z^{b+1}(s)E(s)\Psi(q,s),$$

where $\Psi(q,s)$ is a finite Euler product,

$$\Psi(q,s)=\prod_{p|q}\psi_p(s),$$

and $\psi_p(s)=\theta_p(s)/\phi_p(s)$, so that

$$\psi_p(s)=\begin{cases} 1-1/p^{2s} & \text{for } p\not\equiv 1 \bmod 4,\\ \dfrac{1+2^m/(p^s-1)}{H(1/p^s)} & \text{for } p\equiv 1 \bmod 4.\end{cases}\tag{4.1}$$

The most difficult case we consider is when $p\equiv 1 \bmod 4$. Instead of the Euler factor at good primes

$$H\left(\frac{1}{p^s}\right)=1+\frac{2^m}{p^s}+\frac{3^m}{p^{2s}}+\frac{4^m}{p^{3s}}+\cdots,$$

we have

$$1+\frac{2^m}{p^s-1}=1+\frac{2^m}{p^s}+\frac{2^m}{p^{2s}}+\frac{2^m}{p^{3s}}+\cdots.$$

Taking out the factor $Z^{b+1}(s)$ makes the Euler factor more complicated. At good primes the Euler factor becomes

$$\left(1-\frac{1}{p^s}\right)^{2^m}\left(1+\frac{2^m}{p^s}+\frac{3^m}{p^{2s}}+\frac{4^m}{p^{3s}}+\cdots\right)=1-\frac{d}{p^{2s}}+\frac{d_3}{p^{3s}}-\frac{d_4}{p^{4s}}+\cdots, \tag{4.2}$$

where $d=2^{m-1}(2^m+1)-3^m$ as in (2.6), and $d_3=4^m-6^m+(8^m-2^m)/3$.

At bad primes the Euler factor becomes

$$\left(1-\frac{1}{p^s}\right)^{2^m}\left(1+\frac{2^m}{p^s}+\frac{2^m}{p^{2s}}+\frac{2^m}{p^{3s}}+\cdots\right)=1-\frac{e}{p^{2s}}+\frac{e_3}{p^{3s}}-\frac{e_4}{p^{4s}}+\cdots, \tag{4.3}$$

where $e=2^{m-1}(2^m-1)$ and $e_3=(8^m+2^{m+1})/3-4^m$.

We consider the convergence of $E(q,s)$. Since $E(s)$ and the expressions (4.1)–(4.3) are convergent for $\sigma\geq 1/2$, and the finite Euler product $\Psi(q,s)$ does not affect convergence, $E(q,s)$ is convergent for $\sigma\geq 1/2$.

We consider the size of $E(q,s)$. Analogously to (2.5), we have

$$E(q,s)=\frac{J(q,s)}{\zeta^{j_1}(2s)L^{j_2}(s,\chi)},$$

where $j_1=(d+b)/2$ and $j_2=(d-b)/2$.

We take out the correct Euler factor $(1-1/p^{2s})^d$ for the good primes $p\equiv 1 \bmod 4$. At bad primes $p\equiv 1 \bmod 4$ we have a partially cancelled Euler factor

$$\frac{1-\dfrac{e}{p^{2s}}+\dfrac{e_3}{p^{3s}}-\dfrac{e_4}{p^{4s}}+\cdots}{\left(1-\dfrac{1}{p^{2s}}\right)^d}. \tag{4.4}$$

Our minimum value of σ is $1/2+1/\log x$, which gives $|p^{-2s}|\leq 1/p$. The modulus of the expression in (4.4) when $\sigma\geq 1/2$ is less than or equal to

$$\frac{\left(1+\dfrac{1}{\sqrt{p}}\right)^{2^m}\left(1+\dfrac{2^m}{\sqrt{p}-1}\right)}{\left(1-\dfrac{1}{p}\right)^d}.$$

We split the bad primes with $p\equiv 1$ mod 4 into small primes $p<M_1$ and large primes $p\geq M_1$, where $M_1=(2^m+1)^2$. We have

$$1+\frac{2^m}{\sqrt{p}-1}\leq\begin{cases}2 & \text{for } p\geq M_1,\\ 2^m & \text{for } 5\leq p<M_1.\end{cases}$$

We need to estimate the product $\Psi(q,s)$ over bad primes. Writing $\prod^*$ for a product over bad primes with $p \equiv 1 \bmod 4$, we have

$$\prod\nolimits^*\left(1+\frac{2^m}{\sqrt{p}-1}\right) \le \prod_{p<M_1}\nolimits^* 2^m \prod_{p\ge M_1}\nolimits^* 2 \le (2^m)^{2^{2m-1}+2^m} d(q) = O(q^\epsilon).$$

Also

$$\prod\nolimits^*\left(1+\frac{1}{\sqrt{p}}\right)^{2^m}\left(1-\frac{1}{p}\right)^{-d} \le (B(\epsilon))^\omega q^\epsilon,$$

where ω is the number of distinct prime factors of q and $B(\epsilon)$ is a constant depending on ϵ. We use $B(\epsilon) = 2^{B_2(\epsilon)}$ and $2^{\omega(q)} \le d(q)$ to obtain

$$(B(\epsilon))^\omega q^\epsilon = (2^{B_2(\epsilon)})^\omega q^\epsilon \le (d(q))^{B_2(\epsilon)} q^\epsilon = O(q^\epsilon).$$

The other factor is

$$\prod_{\substack{p\mid q\\ p\not\equiv 1 \bmod 4}}\left(1-\frac{1}{p^{2s}}\right) \le \prod_{\substack{p\mid q\\ p\not\equiv 1 \bmod 4}}\left(1-\frac{1}{p}\right) = O(q^\epsilon).$$

Thus, for $\sigma \ge 1/2$,

$$|E(q,s)| = |E(s)\Psi(q,s)| \ll q^\epsilon \log^d x.$$

We now truncate our contour integrals. The standard method of truncating the contour integral which defines the Mellin transform for a single term of a Dirichlet series is given in Lemma 2.1. We use this to produce an analogous result to that of Lemma 2.2 by applying the truncation to the series $F(q,s)$ term-by-term, so that for $x = N + 1/2$ and $\eta = 2/\log x$, as $N \to \infty$,

$$\sum_{n\le N}(r^*(n,q))^m = \frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} F(q,s)\frac{x^s}{s}\,ds + O\left(\frac{x^{1+\epsilon}\log x}{T}\right). \tag{4.5}$$

We estimate the contour integral in similar fashion to Lemma 2.3, choosing $T \ge 10$ so that, for large x,

$$\frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} F(q,s)\frac{x^s}{s}\,ds = \operatorname*{Res}_{s=1}\left[F(q,s)\frac{x^s}{s}\right] + O(q^\epsilon x^{\Phi+\epsilon}), \tag{4.6}$$

when $T = x^{1-\Phi}$, in the notation (1.4) for Φ. We calculate the residue in (4.6) in the same way as we did in the proof of Theorem 1.1. The residue can be written as

$$\operatorname*{Res}_{s=1}[F(q,s)x^s/s] = xP_{m,q}(\log x), \tag{4.7}$$

where $P_{m,q}(z)$ is a polynomial in z of degree $b = 2^{m-1}-1$, whose coefficients are expressed in terms of the derivatives of the function

$$V(q,s)=(s-1)^{b+1}F(q,s)/s$$

by

$$P_{m,q}(z)=\frac{1}{b!}\sum_{j=0}^{b}{}_b\mathrm{C}_j V^{(b-j)}(q,1)z^j. \tag{4.8}$$

Concatenating the results of (4.5)–(4.7), we have

$$\sum_{n\le N}(r^*(n,q))^m=xP_{m,q}(\log x)+O(q^\epsilon x^\Phi)+O\biggl(\frac{x^{1+\epsilon}\log x}{T}\biggr). \tag{4.9}$$

By the choice of T, $T=x^{1-\Phi}$, the error terms combine to $O(q^\epsilon x^{\Phi+\epsilon})$. Theorem 1.3 is expressed in terms of $N=x-1/2$, so that using (2.16) we can pass easily from the expression (4.9) in terms of x to the statement (1.5) of Theorem 1.3 in terms of N.

The leading coefficient of $P_{m,q}(\log x)$ is $c_q=V(q,1)/b!$. We have

$$V(q,1)=\frac{E(q,1)}{1}\Bigl(\lim_{s\to 1}(s-1)Z(s)\Bigr)^{b+1}=E(q,1)\biggl(\frac{\pi}{4}\biggr)^{b+1}.$$

Hence the leading coefficient $c_q=(\pi/4)^{b+1}E(q,1)/b!$ of $P_{m,q}(x)$ is as in (1.6), and we find an expression for $E(q,1)=E\Psi(q,1)$. We obtain

$$\Psi(q,1)=\prod_{\substack{p\mid q\\ p\not\equiv 1 \bmod 4}}\biggl(1-\frac{1}{p^2}\biggr)\prod_{\substack{p\mid q\\ p\equiv 1 \bmod 4}}\biggl(\frac{1+2^m/(p-1)}{H(1/p)}\biggr),$$

which completes the statement of Theorem 1.3. ∎

5. Proof of Lemma 1.4.

We now find an upper bound for the coefficients of the polynomial $P_{m,q}(z)$, and show that it depends only on $\log q$ and the number of distinct prime factors of q. We need an upper bound for the coefficients of the polynomial $P_{m,q}(z)$ in order to prove Lemma 1.4, when we are estimating a sum over q where the summand includes the polynomial $P_{m,q}(z)$.

LEMMA 5.1. *Consider the polynomial $P_{m,q}(z)$ with coefficients*

$$\frac{1}{b!}\sum_{j=0}^{b}{}_b\mathrm{C}_j V^{(b-j)}(q,1).$$

The upper bound for these coefficients is

$$B^\omega\sum_{\substack{j\\ j+k\le b}}\sum_{k}\frac{V^{(b-j-k)}(1)(\log q)^k}{k!j!(b-j-k)!}z^j,$$

where B is a constant given in the proof, so that the upper bound is dependent only on $\log q$ *and* $\omega = \omega(q)$, *the number of distinct prime factors of* q.

Proof. We define $P_{m,q}(z)$ by (4.8), and consider the derivatives

$$V^{(b-j)}(q,s) = \sum_{k=0}^{b-j} {}_{b-j}\mathrm{C}_k \Psi^{(k)}(q,s) V^{(b-j-k)}(s).$$

We rewrite $P_{m,q}(z)$ as

$$P_{m,q}(z) = \sum_{k} \frac{\Psi^{(k)}(q,1)}{k!} \sum_{\substack{j \\ j+k\le b}} \frac{V^{(b-j-k)}(1) z^j}{j!(b-j-k)!}. \tag{5.1}$$

Since q does not appear in the definition of $V(s)$, q does not appear in the second sum of (5.1). The coefficient of z^j in $P_{m,q}(z)$ is given by this sum, multiplied by the Dirichlet polynomial

$$\sum_{k\le b} \frac{\Psi^{(k)}(q,1)}{k!},$$

where $j + k \le b$. Thus only $\Psi^{(k)}(q,1)$ depends on q. We now estimate $\Psi^{(k)}(q,s)$ at $s = 1$.

The value of $\Psi(q,s)$ does not depend on what power of p divides q, only on whether p divides q. We let $q = q_1 \ldots q_\omega$ and $q_a = p_a^{r_a}$ for $a = 1, \ldots, \omega$; then

$$\Psi(q,s) = \prod_{a=1}^{\omega} \psi(q_a,s) = \prod_{a=1}^{\omega} \psi(p_a,s).$$

We find the kth derivative of $\Psi(q,s)$ in terms of $\psi(p_a,s)$,

$$\Psi^{(k)}(q,s) = \sum_{\substack{k_1 \\ k_1+\cdots+k_\omega=k}} \cdots \sum_{k_\omega} \prod_{a=1}^{\omega} \left(\frac{d}{ds}\right)^{k} \psi(p_a,s). \tag{5.2}$$

We now find the kth derivative of $\psi(p,s)$. We have

$$\psi(p,s) = \begin{cases} P_1(1/p^s) & \text{for } p \equiv 1 \bmod 4, \\ P_2(1/p^s) & \text{for } p \not\equiv 1 \bmod 4, \end{cases}$$

where, for $M = 2^m$,

$$P_1\left(\frac{1}{p^s}\right) = 1 + \sum_{t=1}^{M} \frac{(-1)^{t-1}(t-1)\,{}_M\mathrm{C}_t}{p^{ts}}, \qquad P_2\left(\frac{1}{p^s}\right) = 1 - \frac{1}{p^{2s}}.$$

We find the kth derivative of $P_1(1/p^s)$ to be

$$\begin{aligned}(5.3)\qquad \left(\frac{d}{ds}\right)^k P_1\left(\frac{1}{p^s}\right) &= (-\log p)^k \sum_{t=1}^{M} \frac{(-1)^{t-1} t^k (t-1)\,{}_M\mathrm{C}_t}{p^{ts}}\\ &= (-\log p)^k P_3\left(\frac{1}{p^s}\right).\end{aligned}$$

We expand $P_3(1/p^s)$ to obtain

$$-2^k \frac{e_2}{p^{2s}} + 3^k \frac{e_3}{p^{3s}} + \cdots - M^k \frac{e_M}{p^{Ms}},$$

where the coefficients e_i are defined by (4.3). Next we find the kth derivative of $P_2(1/p^s)$,

$$(5.4)\qquad \left(\frac{d}{ds}\right)^k P_2\left(\frac{1}{p^s}\right) = -\frac{(-2\log p)^k}{p^{2s}}.$$

We estimate the derivatives of (5.3) and (5.4) at $s = 1$. We find

$$\left|\left(\frac{d}{ds}\right)^k P_1\left(\frac{1}{p^s}\right)\right|_{s=1} = \left|(-\log p)^k P_3\left(\frac{1}{p^s}\right)\right|_{s=1} = (\log p)^k \left|P_3\left(\frac{1}{p}\right)\right|,$$

and

$$\left|P_3\left(\frac{1}{p}\right)\right| = \left|\sum_{t=1}^{M} \frac{(-1)^{t-1} t^k (t-1)\,{}_M\mathrm{C}_t}{p^t}\right| \le \sum_{t=1}^{M} \frac{t^k (t-1)\,{}_M\mathrm{C}_t}{p^t}.$$

Now as $p \equiv 1 \bmod 4$, we have $p \ge 5$, so that

$$\sum_{t=1}^{M} \frac{t^k (t-1)\,{}_M\mathrm{C}_t}{p^t} \le \sum_{t=1}^{M} \frac{t^k (t-1)\,{}_M\mathrm{C}_t}{5^t},$$

and thus

$$(5.5)\qquad \left|\left(\frac{d}{ds}\right)^k P_1\left(\frac{1}{p^s}\right)\right|_{s=1} \le (\log p)^k \sum_{t=1}^{M} \frac{t^k (t-1)\,{}_M\mathrm{C}_t}{5^t}.$$

By the definition of $P_2(1/p^s)$, we have $p \not\equiv 1$ mod 4 so that $p^2 \ge 4$, hence

$$(5.6)\qquad \left|\left(\frac{d}{ds}\right)^k P_2\left(\frac{1}{p^s}\right)\right|_{s=1} = \frac{(2\log p)^k}{p^2} \le 2^{k-2} (\log p)^k.$$

We now establish which of the estimates (5.5) and (5.6) is larger. The coefficient of $(\log p)^k$ in (5.5) is a sum whose first term is

$$\frac{2^k\,{}_M\mathrm{C}_2}{5^2} = \frac{2^{k+m-1}(2^m-1)}{5^2}.$$

This is already larger than the coefficient 2^{k-2} of $(\log p)^k$ in (5.6), as $m \ge 3$.

Let

$$B = \sum_{t=1}^{M} \frac{t^k (t-1)\,{}_M\mathrm{C}_t}{5^t}.$$

The kth derivatives of $P_1(1/p^s)$ and $P_2(1/p^s)$ at $s = 1$ are both bounded by $B(\log p)^k$, and therefore $|\psi^{(k)}(p,1)| \le B(\log p)^k$.

We use this with $p = p_a$ and $s = 1$ in (5.2) to find

$$\begin{aligned}(5.7)\quad \Psi^{(k)}(q,1) &= \sum_{\substack{k_1 \\ k_1+\cdots+k_\omega=k}} \cdots \sum_{k_\omega} \prod_{a=1}^{\omega} \left(\frac{d}{ds}\right)^k \psi(p_a,1) \\ &\le \sum_{\substack{k_1 \\ k_1+\cdots+k_\omega=k}} \cdots \sum_{k_\omega} \prod_{a=1}^{\omega} B(\log p_a)^k \le B^\omega (\log p_1 + \cdots + \log p_\omega)^k \\ &= B^\omega(\log(p_1+\cdots+p_\omega))^k = B^\omega(\log q)^k.\end{aligned}$$

We use the estimate $\Psi^{(k)}(q,1) \le B^\omega(\log q)^k$ of (5.7) in (5.1) to find our upper bound

$$P_{m,q}(z) \le B^\omega \sum_{\substack{j \\ j+k\le b}} \sum_{k} \frac{V^{(b-j-k)}(1)(\log q)^k}{k!j!(b-j-k)!} z^j,$$

which involves only $\log q$ and $\omega = \omega(q)$, the number of distinct prime factors of q, as required. ∎

Proof of Lemma 1.4. Let (x,y) be an integer point. Suppose that $(x,y) \equiv (a,b) \bmod q$, with $0 \le a < q$, $0 \le b < q$, so that there exist integers (x_1,y_1) with $x = qx_1 - a$ and $y = qy_1 - b$. The point (x,y) lies on the circle $x^2+y^2 = n$ if and only if the point (x_1,y_1) lies on the circle

$$(x - a/q)^2 + (y - b/q)^2 = \frac{n}{q^2}.$$

We call the integer points (x,y) on the circle $x^2+y^2 = n$ with highest common factor $(x,y,q) = 1$ the *primitive points*. Recall that r^* is the number of integer points on the circle $x^2+y^2 = n$ with highest common factor $(x,y,q) = 1$, so that r^* is the total number of primitive points.

Let

$$\sum_a \sum_b{}'$$

denote the sum over pairs of integers (a,b) with $0 \le a < q$, $0 \le b < q$ and highest common factor $(a,b,q) = 1$. Let r^*_{ab} count the primitive points

$(x, y) \equiv (a, b) \bmod q$, so we have

$$r^* = \sum_a {\sum_b}' r^*_{ab}.$$

We call $(a, b) \bmod q$ a *good residue class* if $r^*_{ab} \geq m$; otherwise if $r^*_{ab} \leq m - 1$ we call $(a, b) \bmod q$ a *bad residue class*. Let B be the number of bad residue classes, and let A be the total number of primitive points in the bad residue classes. Then $A \leq (m-1)B \leq (m-1)f(q) < r^*$ for $f(q)$ defined in (1.7). Let G be the number of good residue classes, and K the total number of primitive points in the good residue classes. Then there are $G = f(q) - B$ good residue classes containing $K = r^* - A$ primitive points.

Let

$$C(x) = {}_x\mathrm{C}_m = \frac{x}{m!}(x-1)\cdots(x-m+1).$$

From each good residue class we can pick primitive points in $C(r^*_{ab})$ ways. The total number of cyclic polygons with m integer point vertices constructed in this way is

$$\sum_{\substack{a \\ (a,b)\,\text{good}}} {\sum_b}' C(r^*_{ab}).$$

To determine a lower bound for this sum we need to use Jensen's inequality (see Hardy, Littlewood and Pólya [3, Chapter 2] or Mitrinović [12]).

Jensen's inequality. *Let $\varphi(x)$ be a convex real function satisfying $\varphi''(x) \geq 0$ on a closed interval $[a, b]$. Then for $x_1, \ldots, x_n$ on $[a, b]$ we have*

$$\sum_{i=1}^{n} \varphi(x_i) \geq n\varphi\biggl(\frac{1}{n}\sum_{i=1}^{n} x_i\biggr).$$

The zeros of $C(x)$ lie in the closed interval $[0, m-1]$, so the zeros of $C'(x)$ and $C''(x)$ lie in the open interval $(0, m-1)$. The interval for x will be the closed interval $[m-1, r^*]$, and bad residue classes occur when $r^*_{ab} \in [0, m-2]$, giving $C(r^*_{ab}) = 0$ and $r^*_{ab} \notin [m-1, r^*]$.

We cannot apply Jensen's inequality immediately because of the presence of bad residue classes. Schinzel [14] tells us that there must exist some residue class containing $x = r^*_{ab}$ points, with $x \geq r^*/f(q)$.

Let $r^* \geq (m-1)f(q)(f(q)+1)$, so that

$$\frac{r^*}{(B+1)f(q)} \geq \frac{r^*}{f(q)(f(q)+1)} \geq m - 1.$$

Then

$$C(x) \geq (B+1)P\biggl(\frac{x}{B+1}\biggr) = \frac{x}{120}\biggl(\frac{x}{B+1} - 1\biggr)\cdots\biggl(\frac{x}{B+1} - m + 1\biggr).$$

We replace the B values of $x = r^*_{ab}$, corresponding to bad residue classes, and the one value for which $C(x) = 0$, corresponding to the residue class with no primitive points, with $B+1$ values all equal to $r^*_{ab}/(B+1)$. For the other residue classes we do not need to replace any values. We now have the sum

$$\sum_{\substack{a \\ (a,b)\,\text{good}}} \sum_{b}{}' C(r^*_{ab}).$$

We apply Jensen's inequality to this sum to obtain

$$\sum_{\substack{a \\ (a,b)\,\text{good}}} \sum_{b}{}' C(r^*_{ab}) \ge \Big(\sum_{a \bmod q} \sum_{b \bmod q} 1\Big) C\left(\frac{\sum_{a \bmod q} \sum_{b \bmod q} r^*_{ab}}{\sum_{a \bmod q} \sum_{b \bmod q} 1}\right) = GC\Big(\frac{K}{G}\Big).$$

The worst case we have to consider has the K primitive points belonging to the good residue classes (a,b) split evenly between all of the residue classes (a,b), that is, between all of the $f(q)$ residue classes (a,b). This means that each residue class will be good, hence $K = r^*$ and $G = f(q)$, so that

$$V_m(n,q) = \sum_{\substack{a \\ (a,b)\,\text{good}}} \sum_{b}{}' C(r^*_{ab}) \ge f(q) C\Big(\frac{r^*}{f(q)}\Big) \ge f(q)\,{}_l\mathrm{C}_m,$$

with $l = [r^*/f(q)]$, the integer part of $r^*/f(q)$. If we have an even split between residue classes, then $r^*/f(q)$ is an integer and we have $l = r^*/f(q)$, but when $r^*/f(q)$ is not an integer, we need the more general definition for l. Hence we have shown that $V_m(n,q) \ge f(q)\,{}_l\mathrm{C}_m$, and we are done. ■

6. Proof of Theorem 1.5. We bound the number of cyclic polygons with m integer point vertices with radius $r \le R$. Let $V_m(n,q)$ be the number of cyclic polygons with m integer point vertices centred in the unit square with fixed radius $r = \sqrt{n}/q$, and centre of the form $(a/q, b/q)$, where the highest common factor (a,b,q) equals 1. Let $W_m(R)$ be the number of cyclic polygons with m integer point vertices centred in the unit square with radius $r \le R$. Then

$$W_m(R) = \sum_q \sum_n V_m(n,q) \tag{6.1}$$

with $q \le 6(R+1)^2$ and $n \le q^2R^2$, and these bounds are independent of m.

In (6.1) we have $q \le 6(R+1)^2$. However, large values of q complicate our summation of $V_m(n,q)$ over q, so we prefer to have very small values of q. We can restrict to small values of q, since we are calculating a lower bound. We choose q such that $f(q) < r^*$. Since the maximum value of $f(q)$ is q^2, we therefore choose $q^2 < r^* = 4r^*(n,q)$.

The root mean square size estimate for $r^*(n,q)$ is bounded for $n \le N$, and $r^*(n,q) \le \sqrt{\log N}/2$ in root mean square. We use the root mean square size of $r^*(n,q)$ to restrict our values of q. We have radius $r \le R$ and we replace N with R^2 to get $q^2 \le (8\log R)^{1/2}$. This is independent of m, the number of integer point vertices of our cyclic polygon. Thus let $q < Q$, where $Q = 2(\log R)^{1/4}$. Then we have

$$W_m(R) \ge \sum_{q<Q} \sum_{n \le q^2R^2} f(q)\, {}_l\mathrm{C}_m \tag{6.2}$$

with $f(q)$ defined in (1.7), and $l = r^*/f(q)$ for $r^* = 4r^*(n,q)$. We interpret ${}_l\mathrm{C}_m$ as 0 for $l \le m-1$.

We use the expansion of ${}_l\mathrm{C}_m$ as a function of l to obtain

$${}_l\mathrm{C}_m \ge \frac{l^m}{m!} - O(l^{m-1}).$$

We substitute this into (6.2) to get

$$W_m(R) \ge \sum_{q<Q} \sum_{n \le q^2R^2} f(q)\frac{l^m}{m!} - O\Big(\sum_{q<Q} \sum_{n \le q^2R^2} f(q) l^{m-1}\Big). \tag{6.3}$$

We consider the first sum in (6.3), our main term:

$$\begin{aligned} \sum_{q<Q} \sum_{n \le q^2R^2} f(q)\frac{l^m}{m!} &= \frac{4^m}{m!} \sum_{q<Q} \sum_{n \le q^2R^2} \frac{(r^*(n,q))^m}{(f(q))^{m-1}} \\ &\ge \frac{4^m}{m!} \sum_{q<Q} \frac{1}{q^{2m-2}} \sum_{n \le q^2R^2} (r^*(n,q))^m, \end{aligned} \tag{6.4}$$

since $f(q) \le q^2$.

We omit the constant factor $4^m/m!$ for ease of notation, and consider the term from (6.4),

$$\sum_{q<Q} \frac{1}{q^{2m-2}} \sum_{n \le q^2R^2} (r^*(n,q))^m. \tag{6.5}$$

We found in Theorem 1.3 that, as $N \to \infty$,

$$\sum_{n \le N} (r^*(n,q))^m = NP_{m,q}(\log N) + O(q^\epsilon N^{\Phi+\epsilon}), \tag{6.6}$$

where $P_{m,q}(x)$ is a polynomial of degree $b = 2^{m-1} - 1$, whose coefficients depend on q, and the term Φ in the exponent, given in (1.4) of Theorem 1.1, is less than 1.

In (6.5) we have $N = q^2R^2$ and we use the expression for the sum over $n \le N$ of $(r^*(n,q))^m$ in (6.6) to replace the sum of (6.5) with

$$\begin{aligned}(6.7)\qquad &\sum_{q<Q} \frac{q^2R^2\ P_{m,q}(2\log qR)}{q^{2m-2}} + O\Big(\sum_{q<Q} \frac{q^{\epsilon}(qR)^{2\Phi+2\epsilon}}{q^{2m-2}}\Big)\\ &= R^2\sum_{q<Q}\frac{P_{m,q}(2\log qR)}{q^{2m-4}} + O\Big(R^{2\Phi+2\epsilon}\sum_{q<Q}\frac{q^{2\Phi+3\epsilon}}{q^{2m-2}}\Big) = R^2\mathcal{A} + \mathcal{B}, \quad \text{say.}\end{aligned}$$

We have $\Phi < 1$ and we choose ϵ such that $2\Phi + 3\epsilon \le 2$ in $\mathcal{B}$. The error term $\mathcal{B}$ is the same size as the sum $\sum 1/q^{\beta}$, with $\beta = 2m-4$, which converges over q with $m \ge 4$. Hence $B = O(R^{2\Phi+2\epsilon})$.

We consider the sum $\mathcal{A}$ of (6.7), which, with $\beta = 2m-4$, can be written as

$$(6.8)\qquad \sum_{q<Q}\frac{P_{m,q}(2\log qR)}{q^{\beta}} = \sum_{q=1}^{\infty}\frac{P_{m,q}(2\log qR)}{q^{\beta}} + O\Big(\sum_{q\ge Q}\frac{P_{m,q}(2\log qR)}{q^{\beta}}\Big).$$

The polynomial $P_{m,q}$ of degree b has numerical coefficients involving both m and q. However, using Lemma 5.1, we found an upper bound for the coefficients of the polynomial $P_{m,q}(z)$ that depends only on $\log q$ and $\omega(q)$. Since $q < Q$, $\omega(q)$ is bounded and there exists an absolute constant C with

$$P_{m,q}(2\log qR) \le C(\log q + \log R)^b$$

for every q such that $1 \le q \le Q$ and $R \ge 10$. Since $m \ge 4$, the exponent β of q also satisfies $\beta \ge 4$. Hence, by the Integral Test [16], the error term from (6.8) becomes

$$\begin{aligned}(6.9)\qquad O\Big(\sum_{q\ge Q}\frac{P_{m,q}(2\log qR)}{q^{\beta}}\Big) &= O\Big(\int_{Q-1}^{\infty}\frac{(\log q + \log R)^b}{q^{\beta}}\,dq\Big)\\ &= O\Big(\frac{\log^b R}{Q^{\beta-1}}\Big).\end{aligned}$$

The leading term of the polynomial $P_{m,q}(2\log qR)$ in the main term of (6.8) is

$$\frac{1}{b!}V(q,1)(2\log qR)^b = \frac{2^b}{b!}V(1)\Psi(q,1)(\log q + \log R)^b.$$

We let $M = 2^m$ and write

$$\Psi(q,s) = \prod_{\substack{p\mid q\\ p\not\equiv 1 \bmod 4}}\Big(1-\frac{1}{p^{2s}}\Big)\prod{}^{*}\Big(1-\frac{1}{p^{2s}}\Big)^{M}\Big(1+\frac{M}{p^s-1}\Big) = \sum_{\substack{d=1\\ p\mid d\Rightarrow p\mid q}}^{\infty}\frac{e(d)}{d^s}.$$

The coefficients $e(d)$ in this sum are 0 unless d is powerful. This series converges absolutely at $s = 1$.

Thus the main term of (6.8) is given by the sum

$$\sum_{q=1}^{\infty} \frac{P_{m,q}(2\log qR)}{q^{\beta}} = \sum_{q=1}^{\infty} \frac{2^b}{b!}\,\frac{V(1)\Psi(q,1)}{q^{\beta}}(\log q + \log R)^b$$

where added to the second sum is the sum over q of lower order terms of $P_{m,q}(2\log qR)$, which is greater than or equal to

$$\frac{2^b V(1)}{b!}\sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^{\beta}}(\log q + \log R)^b.$$

This is a polynomial in $\log R$ of degree b,

$$\begin{aligned}(6.10)\qquad &\frac{2^b V(1)}{b!}\sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^{\beta}}(\log q + \log R)^b \\ &\qquad = \frac{2^b V(1)}{b!}\sum_{i=0}^{b} {}_b\mathrm{C}_i \log^{b-i} R \sum_{q=1}^{\infty}\frac{\Psi(q,1)\log^i q}{q^{\beta}}.\end{aligned}$$

Since

$$\frac{d}{d\beta}\biggl(\frac{1}{q^{\beta}}\biggr) = \frac{-\log q}{q^{\beta}}, \qquad \biggl(-\frac{d}{d\beta}\biggr)\frac{1}{q^{\beta}} = \frac{\log q}{q^{\beta}},$$

the expression (6.10) becomes

$$\begin{aligned}(6.11)\qquad &\frac{2^b V(1)}{b!}\sum_{i=0}^{b} {}_b\mathrm{C}_i \log^{b-i} R \sum_{q=1}\Psi(q,1)\biggl(-\frac{d}{d\beta}\biggr)^i \frac{1}{q^{\beta}} \\ &\qquad = \frac{2^b V(1)}{b!}\sum_{i=0}^{b} {}_b\mathrm{C}_i \log^{b-i} R\biggl(-\frac{d}{d\beta}\biggr)^i \sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^{\beta}}.\end{aligned}$$

We have $0 < \Psi(q,1) < \mu d(q)$ where

$$\mu = \prod_{\substack{p\mid q\\ p\equiv 1 \bmod 4\\ p\le M-1}}\biggl(1 + \frac{M-1}{p}\biggr),$$

and $d(q)$ is the divisor function counting the positive divisors of q. Hence

$$\sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^{\beta}} < \mu\sum_{q=1}^{\infty}\frac{d(q)}{q^{\beta}},$$

and in (6.11),

$$(6.12)\qquad \biggl(-\frac{d}{d\beta}\biggr)^i \sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^{\beta}} < \biggl(-\frac{d}{d\beta}\biggr)^i \mu\sum_{q=1}^{\infty}\frac{d(q)}{q^{\beta}} = \mu\biggl|\biggl(\frac{d}{ds}\biggr)^i \zeta^2(s)\biggr|_{s=\beta}.$$

The sum over q in (6.11) is bounded by the result of (6.12), and since

$$\Psi(q,1) = \sum_{\substack{d=1\\ p\mid d\Rightarrow p\mid q}}^{\infty} \frac{e(d)}{d}$$

forms a convergent series of positive terms, $\Psi(q,1)$ converges to a positive constant $\mathcal{K}_i(\beta)$, involving the ith derivative of $\zeta^2(\beta)$. Therefore

$$\sum_{q=1}^{\infty} \frac{P_{m,q}(2\log qR)}{q^{\beta}} \ge w(\log R) = \frac{2^b V(1)}{b!} \sum_{i=0}^{b} {}_b\mathrm{C}_i \mathcal{K}_i(\beta) \log^{b-i} R, \tag{6.13}$$

where $w(\log R)$ is a polynomial of degree b.

Hence, using (6.9) and (6.13), the main sum $\mathcal{A}$ in (6.8) satisfies

$$\sum_{q<Q} \frac{P_m^*(2\log qR)}{q^{\beta}} \ge w(\log R) + O\biggl(\frac{\log^{\,b} R}{Q^{\beta-1}}\biggr).$$

Returning to the expression in (6.7), we have

$$R^2\mathcal{A} + \mathcal{B} \ge R^2 w(\log R) + R^2 O\biggl(\frac{\log^{\,b} R}{Q^{\beta-1}}\biggr) + O(R^{2\Phi+2\epsilon}).$$

Since $2\Phi + 2\epsilon < 2\Phi + 3\epsilon \le 2$, we find $2\Phi + 2\epsilon < 2$, which makes our error term $O(R^{2\Phi+2\epsilon}) = o(1)$. As the polynomials $P_{m,q}(x)$ and $w(x)$ have positive numerical leading coefficients,

$$O\biggl(\frac{\log^b R}{Q^{\beta-1}}\biggr) = O\biggl(\frac{w(\log R)}{Q^{\beta-1}}\biggr) = w(\log R) O\biggl(\frac{1}{Q^{\beta-1}}\biggr),$$

and $O(1/Q^{\beta-1}) = o(1)$ for our choice of $\beta = 2m-4$ with $m \ge 4$. We therefore have

$$R^2\mathcal{A} + \mathcal{B} \ge R^2 w(\log R)(1+o(1)) + o(1) = R^2 w(\log R)(1+o(1)).$$

We write the error term in (6.3) as

$$O\biggl(\sum_{q<Q} \frac{1}{(f(q))^{m-2}} (q^2 R^2 P_{m-1,q}(2\log qR) + O(q^{\epsilon}(qR)^{2\Phi+2\epsilon}))\biggr).$$

We ignore the $O(q^{\epsilon}(qR)^{2\Phi+2\epsilon})$ term. As $1/(f(q))^{m-2} = O(1/q^{2m-2})$, we are left with an error term of the same form as $\mathcal{A}$ in (6.7). Thus

$$O\biggl(R^2 \sum_{q<Q} \frac{P_{m-1,q}(2\log qR)}{q^{2m-4}}\biggr) = O(w_1(\log R)(1+o(1))),$$

where $w_1(\log R)$ is a polynomial of degree $b_{m-1} = 2^{m-2} - 1$. We conclude that

$$W_m(R) \ge \sum_{q<Q} \sum_{n<q^2R^2} V_m(n,q) \ge \frac{4^m}{m!} R^2 w(\log R)(1+o(1)). \ \blacksquare$$

This paper distills part of my PhD thesis at Cardiff University.

References

[1] M. Beck and S. Robins, *Computing the Continuous Discretely: Integer-Point Enumeration in Polyhedra*, Springer, New York, 2007.

[2] L. Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, Reidel, Dordrecht, 1974.

[3] G. H. Hardy, J. E. Littlewood and G. Pólya, *Inequalities*, 2nd ed., Cambridge Univ. Press, Cambridge, 1952.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, Oxford, 1979.

[5] M. N. Huxley, *Area, Lattice Points, and Exponential Sums*, Clarendon Press, Oxford, 1996.

[6] M. N. Huxley, *Exponential sums and lattice points III*, Proc. London Math. Soc. (3) 87 (2003), 591–609.

[7] M. N. Huxley, *Exponential sums and the Riemann zeta function V*, Proc. London Math. Soc. (3) 90 (2005), 1–41.

[8] M. N. Huxley and S. V. Konyagin, *Cyclic polygons of integer points*, Acta Arith. 138 (2009), 109–136.

[9] M. N. Huxley and N. Watt, *The number of ideals in a quadratic field. II*, Israel J. Math. 120 (2000), 125–153.

[10] M. N. Huxley and J. Žunić, *The number of configurations in lattice point counting I*, Forum Math. 22 (2010), 127–152.

[11] M. N. Huxley and J. Žunić, *The number of configurations in lattice point counting II*, submitted.

[12] D. S. Mitrinović, *Analytic Inequalities*, Springer, Berlin, 1970.

[13] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I: Classical Theory*, Cambridge Stud. Adv. Math. 97, Cambridge, Cambridge Univ. Press, 2007.

[14] A. Schinzel, *Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières*, Enseign. Math. (2) 4 (1958), 71–72.

[15] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, 2nd ed., Oxford Univ. Press, Oxford, 1986.

[16] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge Univ. Press, Cambridge, 2002.

[17] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. (2) 21 (1922), 235–255.

Shaunna M. Plunkett-Levin
School of Mathematics
Cardiff University
23 Senghennydd Road
Cardiff CF24 4AG, Wales, UK
E-mail: LevinSM@cardiff.ac.uk

Current address:
School of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW, UK
E-mail: sp0462@bristol.ac.uk

Received on 17.2.2012
and in revised form on 15.9.2012 (6981)