Annales Univ. Sci. Budapest., Sect. Comp. 26 (2006) 25-42

ON THE NUMBER OF PRIMITIVE INTEGER POINTS ON ELLIPTIC CONES IN ARITHMETIC PROGRESSION

P.D. Varbanets (Odessa, Ukraine)

1. Introduction and notations

Let $T_m(x)$ denote the number of points (u, v, w) with integer coordinates located on the elliptic cone

$$u^2 + mv^2, \qquad 0 < w \leq x, \tag{1}$$

where m is a positive squarefree integer.

Let $r_m(n)$ be the number of integer solutions of the equation $n = u^2 + mv^2$. Then

$$T_m(x) = \sum_{n \leq x} r_m(n^2).$$

In some cases there is a constant $g = g(m)$, such that $\frac{1}{g} r_m(n)$ is a multiplicative function. This true, if $m \equiv 1, 2 \pmod 4$ and the kind of the form $u^2 + mv^2$ is one-class. But this is not true in general.

If $m = 1$, then we have a circle cone and $T_1(x)$ is Pythagorean number triple (u, v, w) with condition $0 < w \leq x$. The asymptotic formula for $T_1(x)$ is obtained in [1, 2]. The primitive Pythagorean triples (u, v, w) are considered in [3-5]. W.Muller and W.Novak [6] investigated the number of primitive points (u, v, w) satisfying $u^2 + mv^2 = w^2$, $uv \leq x$, assuming the fulfilment of the Riemann conjecture for the zeta function.

The aim of this paper is to give an asymptotic formula for the number of primitive points on the elliptic cone $u^2 + pv^2 = w^2$, $0 < w \leq x$, $w \equiv l \pmod q$, where $l, q \in \mathbb{N}$, $(l, q) = 1$, p is a prime number.

Notations. As usual $\mathbb{Q}(\sqrt{d})$ is the extension field of Q generated by $\sqrt{d}$, $K(\sqrt{d})$ is the ring of integers in $\mathbb{Q}(\sqrt{d})$. $\langle \alpha_1, \dots, \alpha_k \rangle$ denotes the ideal generated by $\alpha_1, \dots, \alpha_k \in K(\sqrt{d})$, $\{\alpha, \beta\}$ denotes the ideal in $K(\sqrt{d})$ with basis α, β. If $a, b, \dots, c \in \mathbb{Z}$ then $(a, b, \dots, c)$ denotes their greatest common divisor.

$\sum\limits_{a \pmod q}{}'$ denotes that we sum over the integers $a \pmod q$ for which $(a, q) = 1$.

We define

$$\delta_q = \begin{cases} 1 & \text{if } n \equiv 0 \pmod q, \\ 0 & \text{otherwise.} \end{cases}$$

For some set $\{\dots\}$ we write $\sharp\{\dots\}$ to denote the number of elements of $\{\dots\}$.

As usual, $\mu(n)$ is the Moebius function, $\Gamma(z)$ is the Gamma function of Euler, $\left(\frac{-2}{a}\right)$ is the Jacobi symbol defined for odd a.

Furthermore, let $\exp(x) = e^x$, $e(x) = e^{2\pi i x}$, $e_q(x) = e\left(\frac{x}{q}\right)$ for $x \in \mathbb{R}$. If $(a, q) = 1$, then $\overline{a}$ is the residue class mod q for which $a\overline{a} \equiv 1 \pmod q$.

The Vinogradov symbol $X \ll Y$ means that $X = O(Y)$.

2. Results

Let $\rho(n)$ be the number of those coprime pairs $u, v \in \mathbb{Z}$ for which $n = u^2 + pv^2$ holds.

Lemma 1. *Let p be a prime, $p \equiv 3 \pmod 4$. Then*

$$\rho(n^2) = \begin{cases} 0, & \textit{if } p|n, \\ \rho(2n), & \textit{if } (n,p) = 1, \ n \textit{ even}, \\ \rho(n), & \textit{if } (n,p) = 1, \ n \textit{ odd}. \end{cases} \tag{2}$$

Proof. The assertion that $\rho(n^2) = 0$ if $p|n$, is clear. Assume that n is even, $n = 2k$. We shall prove that there is a one-to-one correspondence between the primitive representations of $4k$, and $4k^2$ by the form $u^2 + pv^2$. If $(u, v) = 1$ then clearly u, v are odd. Let u_1, v_1 be defined by

$$\begin{cases} u = 2u_1 + v_1, \\ v = v_1. \end{cases}$$

Then $(u,v)=1$ holds if and only if $(u_1,v_1)=1$, and uv is odd if and only if u_1v_1 is odd. There is a one-to-one correspondence between the solutions of $u^2+pv^2=4k$ and

$$u_1^2+u_1v_1+\frac{p+1}{4}v_1^2=k,$$

and that of the primitive solutions of them. Thus, it is enough to prove that the number of primitive solutions (3) and (4) are equal, where

$$u^2+uv+\frac{p+1}{4}v^2=k \qquad (v \text{ odd}), \tag{3}$$

$$u^2+uv+\frac{p+1}{4}v^2=k^2 \qquad (v \text{ odd}). \tag{4}$$

Let $\varphi(u,v)=au^2+buv+cv^2$, $d=b^2-4ac$, $(a,b,c)=1$. Let A be the ideal with basis $a, \dfrac{b+\sqrt{d}}{2}$ in $K(\sqrt{d})$ and norm $N(A)=a$. Then

$$\varphi(u,v)=\frac{1}{N(A)}\left(au+\frac{b+\sqrt{d}}{2}v\right)\left(au+\frac{b-\sqrt{d}}{2}v\right).$$

Therefore, if u,v is a primitive solution of (3) such that $v\equiv 1 \pmod 2$, then

$$k=u^2+uv+\frac{p+1}{4}v^2=\left(u+\frac{1+\sqrt{-p}}{2}v\right)\left(u+\frac{1-\sqrt{-p}}{2}v\right),$$

then

$$k^2=\left(u_1+\frac{1+\sqrt{-p}}{2}v_1\right)\left(u_1+\frac{1-\sqrt{-p}}{2}v_1\right)=u_1^2+u_1v_1\frac{p+1}{4}v_1^2,$$

$$u_1=u^2-\frac{p+1}{4}v^2, \qquad v_1=2uv+v^2.$$

The ideals $A=\left\{1,\dfrac{1+\sqrt{-p}}{2}\right\}$, $\overline{A}=\left\{1,\dfrac{1-\sqrt{-p}}{2}\right\}$ are coprimes, and it is easy to verify, from $(u,v)=1$ and v odd, it follows that $(u_1,v_1)=1$, $(v_1,2)=1$. Thus the primitive solution of equation (3) generates the primitive solution of (4). On the other hand, if (u_1,v_1) is a primitive solution of (4) with $v\equiv 1 \pmod 2$, then from the equations

$$\left(u+\frac{1+\sqrt{-p}}{2}v\right)\left(u+\frac{1-\sqrt{-p}}{2}v\right)=k^2, \quad v\equiv 1 \pmod 2,$$

and from the fact that A and $\overline{A}$ are coprimes, we obtain that A is the square of a principal ideal. Since the order of the group classes of ideals of $\mathbb{Q}(\sqrt{-p})$, $p \equiv 3 \pmod 4$ is an odd number (see [7], Th.4, Ch. V.4), and so A is a principal ideal, too,

$$A = \left\langle u + \frac{1+\sqrt{-p}}{2} v \right\rangle, \qquad \overline{A} = \left\langle u + \frac{1-\sqrt{-p}}{2} v \right\rangle,$$

u, v are fixed integers.

Then

$$k = \left(u + \frac{1+\sqrt{-p}}{2} v \right) \left(u + \frac{1-\sqrt{-p}}{2} v \right)$$

and

$$u_1 = u^2 + \frac{p+1}{4} v^2,$$
$$v_1 = 2uv + v^2,$$
$$v_1 \equiv v \pmod 2, \quad v \text{ odd}.$$

Thus every solution of (4) generates a solution of (3), uniquely. Thus, $\rho(n^2) = \rho(2n)$ if n =even, $(n,p) = 1$.

Assume now that $(n, 2p) = 1$. Let $n = u^2 + pv^2$, $(u, v) = 1$. Then the principal ideals $\langle u + \sqrt{-p}v \rangle$, $\langle u - \sqrt{-p}v \rangle$ are coprimes and

$$n^2 = (u + \sqrt{-p}v)^2 (u - \sqrt{-p}v)^2 = (u^2 - pv^2 + 2uv\sqrt{-p})(u^2 - pv^2 - 2uv\sqrt{-p}) =$$

$$= (u_1 + \sqrt{-p}v_1)(u - \sqrt{-p}v_1 = u_1^2 + pv_1^2,$$

where $u_1 = u^2 - pv^2$, $v_1 = 2uv$, $(u_1, v_1) = 1$.

Hence, a primitive solution of the equation

$$u^2 + pv^2 = n \tag{5}$$

generates a primitive solution of

$$u^2 + pv^2 = n^2 \tag{6}$$

if $(n, 2p) = 1$.

On the other hand, if

$$n^2 = u^2 + pv^2 = (u + \sqrt{-p}v)(u - \sqrt{-p}v), \qquad (u, v) = 1,$$

then, by the ideals $\langle u+\sqrt{-p}v\rangle$, $\langle u-\sqrt{-p}v\rangle$ are coprimes, we infer that $A^2 = \langle u+\sqrt{-p}v\rangle$, and A is a principal ideal, too.

Let $A = \left\langle u_0 + \frac{1+\sqrt{-p}}{2} v_0 \right\rangle$. Hence,

$$\left(u_0+\frac{v_0}{2}\right)^2 + p\left(\frac{v_0}{2}\right)^2 = n.$$

The numbers $\frac{v_0}{2}$, $u_0+\frac{v_0}{2}$ must be integers. Hence, $v_0 = 2v_0'$, $v_0' \in \mathbb{Z}$. Therefore the solution (u,v) corresponds to the solution (u_0+v_0') of equation (5). So, if $(n,2p)=1$, then $\rho(n^2)=\rho(n)$. The proof is completed.

Lemma 2. *Let p be a prime, $p\equiv 1 \pmod 4$, $d=4p$. Then there exists such a primitive quadratic form $\varphi(u,v)=au^2+buv+cv^2$ with discriminant -d, which is not equivalent to u^2+pv^2, such that*

$$\rho(n^2) = \begin{cases} 0 & \text{if} \quad (n,d)>1, \\ \rho(n)+\rho_\varphi(n) & \text{if} \quad (n,d)=1. \end{cases}$$

Here $\rho_\varphi(n)$ is the number of primitive representations of n by the form $\varphi(u,v)$.

Proof. The case $(n,d)>1$ is trivial. If $(n,2p)=1$ and $n^2=u^2+pv^2$, $(u,v)=1$, then n^2 is the norm of a principal ideal $\langle u+\sqrt{-p}v\rangle$. Since $\langle u+\sqrt{-p}v\rangle$, $\langle u-\sqrt{-p}v\rangle$, are coprime ideals, thus $\langle u+\sqrt{-p}v\rangle = A^2$, where A is an integral ideal. Thus, either A is a principal ideal $\langle u_0+\sqrt{-p}v_0\rangle$, or A belongs to such a class of ideals of the field $\mathbb{Q}(\sqrt{-p})$ which have order 2 in the group of classes of ideals. But, as we know, in this group there is only one class of order 2 (see [7], p. 328). Then

$$\rho(n^2)=\rho(n)+\rho_\varphi(n),$$

where $\varphi(u,v)=au^2+buv+cv^2$ is the positive definite quadratic form of discriminant $-4p$ which belongs to the class A (A^2 is a principal class), and such that $\varphi(u,v)$ represents n^2 primitively.

Lemma 3. *Let $\rho_2(n)$ be the number of primitive representations of n as u^2+2v^2. Then*

$$\rho_2(2^{2k})=0 \quad (k\ge 1), \qquad \rho_2(p^{2k}) = 2\left(1+\left(\frac{-2}{p}\right)\right)$$

if p is an odd prime, furthermore $\frac{1}{2}\rho_2(n^2)$ is a multiplicative function.

Proof. Let $r_2(n)$ be the number of representations of n in the form $n = u^2 + 2v^2$. Then

$$r_2(n) = 2 \sum_{\substack{d|n \\ d \text{ is odd}}} \left(\frac{-2}{d}\right)$$

and, hence, $\frac{1}{2} r_2(n)$ is a multiplicative function.

Next, if p prime, then we have

$$\rho_2\left(p^{2k}\right) = r_2\left(p^{2k}\right) - r_2\left(p^{2(k-1)}\right) = \begin{cases} 0 & \text{if } p = 2, \\ 2\left(1 + \left(\frac{-2}{p}\right)\right) & \text{if } p > 2. \end{cases}$$

Moreover, by

$$(u_1^2 + 2v_1^2)(u_2^2 + 2v_2^2) = (u_1u_2 - 2v_1v_2)^2 + 2(u_1v_2 + u_2v_1)^2$$

we infer that if $(u_1, v_1) = (u_2, v_2) = 1$ and $(u_1^2 + 2v_1^2, u_2^2 + 2v_2^2) = 1$, then $(u_1u_2 - 2v_1v_2, u_1v_2 + u_2v_1) = 1$. Hence, $\rho_2(n^2)$ is a multiplicative function.

Lemma 4. *Let $l, q \in \mathbb{N}$, $1 \le l \le q$. Then for $(a, q) = 1$*

$$\sum_{l_1, l_2 = 1}^{q} e_q(ul_1 + vl_2)\delta_q(l_1^2 + al_2^2 - l) \ll q^{\frac{1}{2}}(u, v, q)\tau(q).$$

Here $\tau(q)$ is the number of divisors of n.

Proof. We have

$$S(u, v, q) = \sum_{l_1, l_2 = 1}^{q} e_q(ul_1 + vl_2)\delta_q(l_1^2 + al_2^2 - l) =$$

$$= \frac{1}{q} \sum_{h=1}^{q} \sum_{l_1, l_2 = 1}^{q} e_q((l_1^2 + al_2^2 - l)h + ul_1 + vl_2) =$$

$$= \frac{1}{q} \sum_{d|q} \sum_{h (\mathrm{mod}\ \frac{q}{d})}{}' e_q(-hl) \sum_{l_1=1}^{q} e_q(dhl_1^2 + ul_1) \times$$

$$\times \sum_{l_2=1}^{q} e_q(adhl_2^2 + vl_2) \sum_{z_1, z_2 = 1}^{d} e_d(uz_1 + vz_2).$$

Now, by substituting the values of the Gaussian sums and using the known inequalities for Kloosterman sums (see [8]), we obtain
(7)

$$S(u,v,q) \ll \sum_{d|(u,v,q)} \left| \sum_{h(\text{mod } \frac{q}{d})}{}' e_{\frac{q}{d}}(-(hl+\overline{h}(u^2+a^2v^2))) \right| \ll q^{\frac{1}{2}}(u,v,q)^{\frac{1}{2}}\tau(q).$$

Let $g_1, g_2, h_1, h_2 \in \mathbb{R}$. Consider the Epstein zeta function [9]

$$Z_\varphi(g_1,g_2,h_1,h_2;s) = \sum_{(u,v)}{}^{*} e(h_1u+h_2v)(\varphi(u+g_1,v+g_2))^{-s}, \quad \operatorname{Re} s > 1,$$

where $\varphi(u,v)$ is the positive definite quadratic form and the asterix $*$ indicates that the summation runs over all integers u, v, for which $\varphi(u+g_1,v+g_2) \neq 0$.

Let $\varphi(u,v) = au^2+2buv+cv^2$, $D = ac-b^2 > 0$, and let $\Psi(u,v)$ be the inverse form to φ, that is $\Psi(u,v) = a'u^2+2b'uv+c'v^2$, where $a' = \dfrac{c}{D}$, $b' = -2\dfrac{b}{D}$, $c' = \dfrac{a}{D}$.

Lemma 5. *The function $Z(g_1,g_2,h_1,h_2;s)$, defined for* Re $s > 1$ *by (7), can be continued analytically over the whole s-plane. If $(g_1,g_2,h_1,h_2) \notin \mathbb{Z}^4$ then $Z_\varphi(g_1,g_2,h_1,h_2;s)$ is an entire function. If $(g_1,g_2,h_1,h_2) \in \mathbb{Z}^4$ then $Z_\varphi(g_1,g_2,h_1,h_2;s) = Z_\varphi(0,0,0,0;s)$ is a meromorphic function with a simple pole $s=1$, $\operatorname{res}_{s=1} Z_\varphi(0,0,0,0;s) = \dfrac{\pi}{\sqrt{D}}$.*

Moreover, the functional equation

$$\pi^{-s}\Gamma(s)Z_\varphi(g_1,g_2,h_1,h_2;s) =$$

$$= \frac{1}{\sqrt{D}} e(-(h_1g_1+h_2g_2))\pi^{-(1-s)}\Gamma(1-s)Z_\varphi(h_1,h_2,-g_1,-g_2;1-s)$$

holds.

Lemma 6. *Let the Dirichlet series*

$$\Phi(s) = \sum_{n=1}^{\infty} a_n\lambda_n^{-s}, \qquad \Psi(s) = \sum_{n=1}^{\infty} b_n\mu_n^{-s}, \qquad s = \sigma+it$$

be absolutely convergent for Re $s > 1$, *and assume that $\Phi(s), \Psi(s)$ can be continued analytically over the whole s-plane (except at the finite number of singular points), moreover the functional equation*

$$A^s\Gamma(ms+v)\Phi(s) = B^{-1}\Gamma(m(1-s)+v)\Psi(1-s)$$

(A, B are constant) holds.

Then, for every $\tau \in C$, $\arg\tau = \left(\frac{\pi}{2} - \frac{1}{t}\right)\operatorname{sign} t$ and for any fixed stripe $a \le \sigma \le b$ uniformly for $|t| \ge t_0, A, B, \tau$, the approximate functional equation

$$\Phi(s) = \sum_{\lambda_n \le x\log x} a_n\lambda_n^{-s} F\left(s, \frac{\lambda_n\tau^m}{A}\right) +$$

$$+\frac{B^{1-s}\Gamma(m(1-s)+v)}{A^s\Gamma(ms+v)} \sum_{\mu_n \le y\log y} b_n\mu_n^{s-1} F\left(1-s, \frac{\mu_n\tau^{-m}}{B}\right) +$$

$$+O\left(x^{-M} + y^{-M}\right) + \sum_{z\neq s} \operatorname{res}\left\{\left(\frac{A}{\tau^m}\right)^{z-s} \frac{\Gamma(mz+v)\Phi(z)}{z-s}\right\}$$

holds, where $M > 0$ is any fixed constant,

$$F(w, X) = \frac{1}{\Gamma(mw+v)}\frac{1}{2\pi}\int\limits_{(\Delta)} \Gamma(m(w+z)+v)\frac{X^z}{z}dz,$$

where Δ is so chosen that in the region $\operatorname{Re} s \ge \Delta$ there are no singularities of the integrand.

Moreover, we have uniformly for all parameters

$$F(w, X) =$$

$$= l + O\left(\exp\left(-\frac{|X|^{\frac{1}{m}}}{|t|}\right)\left(\frac{|X|}{|t|^m}\right)^{\operatorname{Re}\, w + \frac{1}{m}\operatorname{Re}\, v}\left(1 + \left|m\sqrt{|t|} - \frac{|X|^{\frac{1}{m}}}{\sqrt{|t|}}\right|^{-1}\right)\right),$$

where

$$l = \begin{cases} 1 & \text{if } \lambda_n \le x,\ \mu_n \le y, \\ 0 & \text{else,} \end{cases}$$

$x = m^m|\tau|^{-1}\cdot A|t|^m$, $y = m^m|\tau|\cdot B|t|^m$.

This lemma is a special case of Lavrik's theorem [10].

Lemma 7. *Let $\varphi(u,v)$ be a positive definite quadratic form $\varphi(u,v) = au^2 + 2buv + cv^2$, $D = ac - b^2 > 0$, and $Z_\varphi\left(\frac{l_1}{q}, \frac{l_2}{q}, 0, 0; s\right)$ be the Epstein zeta-function for φ. Then*

$$\int\limits_{-T}^{T} \left| \frac{1}{q^{2s}} \sum_{\substack{l_1,l_2 (\mathrm{mod}\ q)\\ \varphi(l_1,l_2)\equiv l(q)}} Z_\varphi\left(\frac{l_1}{q}, \frac{l_2}{q}, 0, 0; s\right) - \sum_{u,v\in B} \varphi(u,v)^{-s} \right|^2 \ll_\varepsilon T^{1+\varepsilon} D^{\frac{3}{2}} q^{-1+\varepsilon},$$

where B denotes the set of points (u,v) for which $\varphi(u,v) \equiv l \pmod q$ and $0 < \varphi(u,v) < 2q$.

Proof. We apply Lemma 6 for the Dirichlet series

$$\Phi(s) = \sum_{\substack{n=1\\ n\equiv l(q)}}^{\infty} a_n n^{-s}, \qquad \Psi(s) = \sum_{n-1}^{\infty} b_n n^{-s},$$

where

$$a_n = r_\varphi(n) = \sum_{\substack{(u,v)\in\mathbb{Z}^2\\ \varphi(u,v)=n}} 1, \qquad b_n = \frac{1}{q\sqrt{D}} \sum_{\substack{(u,v)\in\mathbb{Z}^2\\ D^2\psi(u,v)=n}} \sum_{\substack{l_1,l_2 (\mathrm{mod}\ q)\\ D\psi(l_1,l_2)=l(\mathrm{mod}\ q)n}} e_q(l_1u+l_2v)$$

with $A = \frac{q}{\pi}$, $B = DA$, $m = 1$, $v = 0$, $\arg\tau = \arg s$, $|\tau| = q^{-1}D^{-\frac{3}{2}}$, and then we repeat the reasonings in proofs of Lemmas 5 and 6 from [11].

Let $V_p(x,l,q)$ denote the number of the primitive integer points on a cone

$$u^2 + pv^2 - w^2 = 0, \quad w \equiv l \pmod q, \quad 0 < w \le x.$$

We shall suppose that $(l,q) = 1$. The general case can be considered similarly. We have

$$V_p(x,l,q) = \sum_{\substack{n\equiv l(\mathrm{mod}\ q)\\ n\le x}} \rho(n^2).$$

Let

$$F(s) = \sum_{\substack{n=1\\ n\equiv l(\mathrm{mod}\ q)}} \frac{\rho(n^2)}{n^s}, \qquad \mathrm{Re}\, s > 1.$$

First consider the case $p \equiv 3 \pmod 4$. By Lemma 1 we have

$$F(s) = \sum_{\substack{n=1\\(n,p)=1\\n\equiv l(\mathrm{mod}\ q)}} \frac{\rho(n^2)}{n^s} = \sum_{\substack{n=1\\(n,2p)=1\\n\equiv l(\mathrm{mod}\ q)}}^{\infty} \frac{\rho(n)}{n^s} + \sum_{\substack{n=1\\(n,p)=1\\2n\equiv l(\mathrm{mod}\ q)}}^{\infty} \frac{\rho(4n)}{(2n)^s}.$$

If $q \equiv 0 \pmod 2$ then the second sum is empty. We have

$$\sum_{\substack{n=1\\(n,2p)=1\\n\equiv l(\mathrm{mod}\ q)}}^{\infty} \frac{\rho(n)}{n^s} = \tag{8}$$

$$= \sum_{\substack{(u,v)=1\\(u^2+pv^2,2p)=1}} \frac{\delta_q(u^2+pv^2-l)}{(u^2+pv^2)^s} = \sum_{\substack{u,v=1\\(u^2+pv^2,2p)=1}}^{\infty} \frac{\delta_q(u^2+pv^2-l)}{(u^2+pv^2)^s} \sum_{d|(u,v)} \mu(d) =$$

$$= {\sum_{a(\mathrm{mod}\ q)}}' \sum_{\substack{d\equiv a(q)\\(d,2p)=1}} \frac{\mu(d)}{d^{2s}} \sum_{\substack{n=1\\(n,2p)=1\\n\equiv a^{-2}l(q)}} \frac{r_p(n)}{n^s}.$$

Moreover,

$$\sum_{\substack{n=1\\2n\equiv l(\mathrm{mod}\ q)}} \frac{\rho(4n)}{(2n)^s} = \tag{9}$$

$$= 2^s {\sum_{a(\mathrm{mod}\ q)}}' \sum_{\substack{d=1\\(d,p)=1\\d\equiv a(\mathrm{mod}\ q)}}^{\infty} \frac{\mu(d)}{d^{2s}} \left(\sum_{\substack{n=1\\(n,p)=1\\4n\equiv 2\overline{a}^2 l(q)}}^{\infty} \frac{r_p(4n)}{(4n)^s} - \frac{1}{4^s} \sum_{\substack{n=1\\(n,p)=1\\4n\equiv 2\overline{a}^2 l(q)}}^{\infty} \frac{r_p(n)}{n^s} \right).$$

We have $r_p(2n) = 0$ if $n \equiv 1 \pmod 2$. Hence,

$$\sum_{\substack{n=1\\(n,p)=1\\4n\equiv 2\overline{a}^2 l(q)}}^{\infty} \frac{r_p(n)}{n^s} = \sum_{\substack{(n,2p)=1\\4n\equiv 2\overline{a}^2 l(q)}} \frac{r_p(n)}{n^s} + \sum_{\substack{(n,p)=1\\4n\equiv 2\overline{a}^2 l(q)}} \frac{r_p(4n)}{(4n)^s}. \tag{10}$$

Now from (8)-(10) for $p \equiv 3 \pmod 4$, Re $s > 1$ we obtain that

$$F(s) = {\sum_{a\ (\mathrm{mod}\ q)}}' \sum_{\substack{d\equiv a(q)\\(d,2p)=1}} \frac{\mu(d)}{d^{2s}} \sum_{\substack{(n,2p)=1\\n\equiv \overline{a}^2 l(q)}} \frac{r_p(n)}{n^s} +$$

$$+(2^s-2^{-s})\sum_{a \pmod q}{}' \sum_{\substack{d=1\\(d,p)=1\\d\equiv a(q)}}^{\infty}\frac{\mu(d)}{d^{2s}}\sum_{\substack{n=1\\(n,p)=1}}^{\infty}\frac{r_p(4n)}{(4n)^s}\cdot\delta_q(4n-2\overline{a}^2l)- \tag{11}$$

$$-2^{-s}\sum_{a \pmod q}{}' \sum_{\substack{d=1\\(d,p)=1\\d\equiv a \pmod q}}^{\infty}\frac{\mu(d)}{d^{2s}}\sum_{\substack{n=1\\(n,2p)=1}}^{\infty}\frac{r_p(n)}{n^s}\cdot\delta_q(4n-2\overline{a}^2l).$$

Now, if $(n,2p)=1$, then in the representation $n=u^2+pv^2$ the numbers u,v should have different parity and hence,

$$\sum_{\substack{n\equiv l\ (q)\\(n,2p)=1}}\frac{r_p(n)}{n^s}=$$

$$=\sum_{l_1,l_2 (\mathrm{mod}\ q)}\left(\sum_{\substack{u,v=-\infty\\2u\equiv l_1(q)\\2v+1\equiv l_2(q)}}^{\infty}\frac{1-p^{-s}}{((2u)^2+p(2v+1)^2)^s}+\right.$$

$$\left.+\sum_{\substack{u,v=-\infty\\2u+1\equiv l_1(q)\\2v\equiv l_2(q)}}\frac{1-p^{-s}}{((2u+1)^2+p(2v)^2)^s}\right)\times\delta_q(l_1^2+pl_2^2-l)=$$

$$=\frac{1-p^{-s}}{q_1^{2s}}\times \tag{12}$$

$$\times\sum_{l_1,l_2(\mathrm{mod}\ q)}\left(Z\left(\frac{l_1}{q_1},\frac{l_2-1}{q_1},0,0;s\right)+Z\left(\frac{l_1-1}{q_1},\frac{l_2}{q_1},0,0;s\right)\right)\delta_q(l_1^2+pl_2^2-l),$$

where

$$q_1=\begin{cases}2q & \text{if } q \text{ is odd,}\\ q & \text{if } q \text{ is even.}\end{cases}$$

If $u^2+pv^2=4n$, $(n,p)=1$ then $u\equiv v \pmod 2$, and hence, for $q\equiv$ $\equiv 1 \pmod 2$ we have

$$\sum_{\substack{n=l\\(n,p)=1}}^{\infty}\frac{r_p(4n)}{(4n)^s}= \tag{13}$$

$$= \frac{1-p^{-s}}{(2q)^{2s}} \sum_{l_1,l_2 (\mathrm{mod}\ q)} \left(Z\left(\frac{l_1}{q_1}, \frac{l_2}{q_1}, 0, 0; s\right) + \right.$$

$$\left. + Z\left(\frac{l_1+1}{q_1}, \frac{l_2+1}{q_1}, 0, 0; s\right)\right) \delta_q(l_1^2 + pl_2^2 - l),$$

(here $Z(g_1, g_2, h_1, h_2; s)$ is the Epstein zeta-function for the quadratic form $u^2 + pv^2$).

In the case $p \equiv 1 \pmod 4$ we use Lemma 2:

$$\sum_{\substack{n=1 \\ n\equiv l (\mathrm{mod}\ q)}}^{\infty} \frac{\rho(n^2)}{n^s} = \sum_{\substack{n=1 \\ (n,2p)=1 \\ n\equiv l (\mathrm{mod}\ q)}}^{\infty} \frac{\rho(n^2)}{n^s} = \sum_{\substack{n=1 \\ (n,2p)=1 \\ n\equiv l (\mathrm{mod}\ q)}}^{\infty} \frac{\rho(n)}{n^s} + \sum_{\substack{n=1 \\ (n,2p)=1 \\ n\equiv l (\mathrm{mod}\ q)}}^{\infty} \frac{\rho_\varphi(n)}{n^s},$$

where $\rho_\varphi(n)$ is the number of primitive representations of n by the form $\varphi(u,v) = au^2 + buv + cv^2$, where φ belongs to the A of a quadratic form with a discriminant $-4p$ and class order 2.

But, as we have shown earlier

$$\sum_{\substack{(n,2p)=1 \\ n\equiv l(q)}} \frac{\rho(n)}{n^s} = \sum_{a (\mathrm{mod}\ q)}{}' \sum_{\substack{d\equiv a(q) \\ (d,2p)=1}} \frac{\mu(d)}{d^{2s}} \sum_{(n,2p)=1} \frac{r_p(n)}{n^s} \cdot \delta_q(n - \overline{a}^2 l) =$$

$$(14) \qquad = \sum_{a (\mathrm{mod}\ q)}{}' \sum_{\substack{d=1 \\ d\equiv a(q) \\ (d,2p)=1}}^{\infty} \frac{\mu(d)}{d^{2s}} \frac{1-p^{-s}}{q^{2s}} \times$$

$$\times \sum_{l_1,l_2 (\mathrm{mod}\ q)} \left(Z\left(\frac{l_1+1}{q_1}, \frac{l_2}{q_1}, 0, 0; s\right) + Z\left(\frac{l_1}{q_1}, \frac{l_2+1}{q_1}, 0, 0; s\right)\right) \delta_q(l_1^2 + pl_2^2 - l),$$

$$(15) \qquad \sum_{\substack{(n,2p)=1 \\ n\equiv l(q)}} \frac{\rho_\varphi(n)}{n^s} = \sum_{a (\mathrm{mod}\ q)}{}' \sum_{\substack{d\equiv a(q) \\ (d,2p)=1}} \frac{\mu(d)}{d^{2s}} \sum_{(n,2p)=1} \frac{r_\varphi(n)}{n^s} \cdot \delta_q(n - \overline{a}^2 l),$$

where $r_\varphi(n)$ is the number of representations of n by form ϕ.

In the class of forms equivalent to the quadratic form $\varphi(u,v)$ always can be found a quadratic primitive form $Au^2 + Buv + Cv^2$ such that $A \equiv C \pmod 2$ and $(A,p) = 1$. Moreover, from $B^2 - 4AC = -4p$ we infer $B = 2B'$, $B' \in Z$.

Thus, if $(A,p)=1$, $A\equiv 0 \pmod 2$ then from $n=Au^2+2B'uv+Cv^2$ it follows that $(n,2)=1$, if and only if $(v,2)=1$.

Hence,

$$\sum_{\substack{n=1\\(n,2p)=1\\n\equiv l(q)}}^{\infty} \frac{r_\varphi(n)}{n^s} = \sideset{}{^*}\sum_{\substack{u,v=-\infty\\(v,2)=1}}^{\infty} \frac{\delta_q(Au^2+B'uv+Cv^2)}{(Au^2+B'uv+Cv^2)^s} =$$

$$= A^s \sideset{}{^*}\sum_{\substack{u,v=-\infty\\(Au+B'v,p)=1\\(v,2)=1}}^{\infty} \frac{\delta_q((Au+B'v)^2+pv^2-l)}{((Au+B'v^2)+pv^2)^s} = \tag{16}$$

$$= A^s \sideset{}{^*}\sum_{u,v=-\infty}^{\infty} \frac{\delta_q(Au+B'(2v+1)^2+p(2v+1)^2-l)}{(Au+B'(2v+1)^2+p(2v+1)^2)^s} -$$

$$-A^s \sum_{\substack{u,v=-\infty\\Au+B'(2v+1)\equiv 0(p)}} \frac{\delta_q((Au+B'v)^2+pv^2-l)}{((Au+B'v)^2+pv^2)^s} =$$

$$= \frac{1-p^{-s}}{q_1^{2s}} \left(\sum_{\substack{l_1,l_2 \pmod q\\ \varphi_1(l_1,l_2)\equiv l(q)}} Z_{\varphi_1}\left(\frac{l_1}{q_1}, \frac{l_2+1}{q_1}, 0, 0; s\right) - \right.$$

$$\left. -p^{-s} \sum_{\substack{l_1,l_2 \pmod q\\ 4\varphi_2(l_1,l_2)\equiv l(q)}} Z_{\varphi_2}\left(\frac{l_1+1}{q_1}, \frac{l_2}{q_1}, 0, 0; s\right)\right),$$

where $\varphi_1(u,v)=Au^2+2B'uv+4Cv^2$, $\varphi_2(u,v)=\hat{A}U^2+\hat{B}uv+Cv^2$, and the form φ_2 can be obtained from the form φ_1 by using the substitution

$$\begin{cases} u = A'B'v', \\ v = v', \end{cases} \qquad AA' \equiv -1 \pmod p.$$

It is obvious that $AC-B'^2=p$, $\hat{A}\hat{C}-\frac{1}{4}\hat{B}^2=p^3$.

Further, if $(A,p)=1$, $A\equiv 1 \pmod 2$ then similarly we have

$$\sum_{\substack{n=1\\(n,2p)=1\\n\equiv l(q)}} \frac{r_\varphi(n)}{n^s} = \tag{17}$$

$$= \frac{1-p^{-s}}{q_1^{2s}} \left\{ \sum_{\substack{l_1, l_2 (\mathrm{mod}\ q) \\ \varphi_3(l_1,l_2)\equiv l(q)}} Z_{\varphi_3}\left(\frac{l_1+1}{q_1}, \frac{l_2}{q_1}, 0, 0; s\right) - \right.$$

$$\left. -p^{-s} \sum_{\substack{l_1, l_2 (\mathrm{mod}\ q) \\ \varphi_4(l_1,l_2)\equiv l(q)}} Z_{\varphi_4}\left(\frac{l_1}{q_1}, \frac{l_2+\frac{l+2AA''}{p}}{q_1}, 0, 0; s\right) \right\},$$

where $\varphi_3(u,v) = 4Au^2 + 2Buv + Cv^2$, $\varphi_4(u,v) = \hat{A}u^2 + \hat{B}uv + \hat{C}v^2$, and φ_4 can be obtained from $Au^2 + Buv + Cv^2$ by the substitution

$$\begin{cases} u = 2A''B'u' + 2pv', \\ v = u', \end{cases}$$

$2AA'' \equiv -1 \pmod p$, $\hat{A}\hat{C} - \frac{1}{4}\hat{B}^2 = 4p^3$.

In the case $p = 2$ by Lemma 3 we have

$$\sum_{n=1}^{\infty} \frac{1}{2}\rho_2(n^2)\chi_q(n)n^{-s} = \prod_{p\equiv 1,3 (\mathrm{mod}\ 8)} \left(1 + \frac{2\chi_q(p)}{p^s} + \frac{2\chi_q^2(p)}{p^{2s}} + \ldots\right) =$$

$$= \prod_{p\equiv 1,3 (\mathrm{mod}\ 8)} \left(\frac{1-p^{-2s}\chi_q^2(p)}{(1-p^{-s}\chi_q(p))^2}\right),$$

where χ_q is the Dirichlet character mod q.

And thus

$$\text{(18)} \qquad \sum_{\substack{n=1 \\ (n,2)=1}}^{\infty} \rho_2(n^2)\delta_q(n-1)n^{-s} = \frac{2}{\varphi(q)} \sum_{\chi_q} \overline{\chi}_q(l) \frac{L(s,\chi_{8q}^0)L(s,\chi_{8q})}{L(2s,\chi_q^0)(1-2^{-2s})},$$

where $\chi_{8q} = \chi_8\chi_q$, $\chi_{8q}^0 = \chi_8^0\chi_q$, χ_8^0 is a principal character mod 8.

Now from the expressions (11)-(13) we have

Theorem 1. *Let $l, q \in \mathbb{N}$, $(l,q) = 1$ and let p be a prime, $p \equiv 3 \pmod 4$. Then for the number $V_p(x,l,q)$ of primitive integer points on the cone $u^2+pv^2 = = w^2$, $0 < w \le x$, under condition $w \equiv l \pmod q$, the asymptotic formula*

$$V_p(x,l,q) = c_0(q)\frac{\sqrt{p}}{p+1} x \frac{I_p(l,q)}{q^2} \prod_{\substack{p|q \\ p \text{ is prime}}} (1-p^{-2})^{-1} + O\left(x^{\frac{1}{2}}\tau(q)\log^2 x\right)$$

holds,

$$c_0(q) = \begin{cases} 7 & \text{if } q \equiv 1 \pmod 2, \\ 16 & \text{if } q \equiv 0 \pmod 2, \end{cases}$$

where $I_p(l,q)$ *is the number of solutions of the congruence*

$$u^2 + pv^2 \equiv l \pmod q.$$

Proof. For the Dirichlet series $F(s) = \sum\limits_{n=1}^{\infty} \rho(n^2)\delta_q(n-l)n^{-s}$ we have

$$V_p(x,l,q) = \sum_{n\le x} \rho(n^2)\delta_q(n-l) = \frac{1}{2\pi i}\int\limits_{c-iT}^{c+iT} F(s)\frac{x^s}{s}ds + O\left(\frac{x\log x}{Tq}\right) + O_\varepsilon(x^\varepsilon),$$

where $c = 1 + (\log x)^{-1}$, $T > 1$, $\varepsilon > 0$.

We split the solutions (l_1, l_2) of the solutions of the congruence $l_1^2 + pl_2^2 \equiv \equiv l \pmod q$, $0 < l_1, l_2 \le q$, into two classes, K_1 and K_2. We shall write $(l_1, l_2 \in K_1$ if $l_1^2 + pl_2^2 > q$ and $(l_1, l_2) \in K_2$ otherwise. It is clear that $\sharp\{(l_1,l_2) \in \in K_2\} \ll q^\varepsilon$. From the expressions (11)-(13) follows that we need to find upper bounds for the integral of type

$$\frac{1}{2\pi i}\int\limits_{c-iT}^{c+iT} \left(\sum_{a \pmod q}{}' \sum_{(d,2p)=1} \mu(d)\delta_q(d-a)d^{-2s} \times \right.$$

$$\left. \times \sum_{l_1,l_2=1}^{q} Z\left(\frac{l_1+g_1}{q_1}, \frac{l_2+g_2}{q_1}, 0, 0; s\right) \delta_q(l_1^2 + pl_2^2 - l)\frac{x^s}{s}\right)$$

$(g_1, g_2 \in \{0, 1\})$.

Summing over d we can truncate till $d \le Y$ with error $\ll \dfrac{x}{q}\dfrac{\log T}{Y}$. After truncating we shift the contour of integration to the line $\mathrm{Re}\, s = \frac{1}{2}$. Write

$$Z\left(\frac{l_1+g_1}{q_1}, \frac{l_2+g_2}{q_1}, 0, 0; s\right) =$$

$$= \left[Z\left(\frac{l_1+g_1}{q_1}, \frac{l_2+g_2}{q_1}, 0, 0; s\right) - \left(\left(\frac{l_1+g_1}{q_1}\right)^2 + p\left(\frac{l_2+g_2}{q_1}\right)^2\right)^{-s}\right] +$$

$$+\left(\left(\frac{l_1+g_1}{q_1}\right)^2+p\left(\frac{l_2+g_2}{q_1}\right)^2\right)^{-s}$$

for $(l_1+g_1, l_2+g_2)\in K_2$, and then we apply Lemma 7. Let us set $Y=x, T=x^{\frac{1}{2}}$ and calculate $\operatorname*{res}_{s=1}\left(F(s)\frac{x^s}{s}\right)$. If $q\equiv 1 \pmod 2$ then

$$\operatorname*{res}_{s=1}\left(F(s)\frac{x^s}{s}\right)=$$

$$=x\left\{\sum_{a(\bmod\ q)}{}'\left[\sum_{(d,2p)=1}\frac{\mu(d)}{d^2}\delta_q(d-a)I_p(l,q)\frac{2\pi}{\sqrt{p}}\frac{1-\frac{1}{p}}{q_1^2}\left(\frac{1}{1-\frac{1}{4}}\frac{1}{4}-\frac{1}{8}\right)\right]+\right.$$

$$\left.+\sum_{(d,2p)=1}\frac{\mu(d)}{d^2}\delta_q(d-a)I_p(l,q)\frac{2\pi}{\sqrt{p}}\frac{1-\frac{1}{p}}{q_1^2}\right\}=\frac{7x\sqrt{p}}{p+1}\frac{I_p(l,q)}{q^2}\prod_{p|q}(1-p^{-2})^{-1}.$$

If $q\equiv 0 \pmod 2$ then

$$\operatorname*{res}_{s=1}\left(F(s)\frac{x^s}{s}\right)=$$

$$=\frac{1-\frac{1}{p}}{q^2}I_p(l,q)\frac{2\pi}{\sqrt{p}}x\sum_{(d,2p)=1}\frac{\mu(d)}{d^2}\delta_q(d-a)=\frac{16\sqrt{p}x}{\pi(p+1)}\frac{I_p(l,q)}{q^2}\prod_{p|q}(1-p^{-2})^{-1}.$$

The proof is completed.

Similarly from (14)-(17) we infer

Theorem 2. *Let p be a prime, $p\equiv 1 \pmod 4$, and let $0<l\le q$, $(l,q)=1$. Then*

$$V_p(x,l,q)=\frac{8\sqrt{p}x}{\pi(p+1)}\frac{I_p(l,q)}{q_1^2}\prod_{p|q}(1-p^{-2})^{-1}+O\left(x^{\frac{1}{2}}\tau(q)\log^2 x\right).$$

From the expression (18) we obtain

Theorem 3. *Let $l,q\in\mathbb{N}$, $0<l\le q$, $(l,q)=1$. Then*

$$V_2(x,l,q)=c_1(q)\frac{\sqrt{8}}{\pi}\frac{I_2(l,q)}{q^2}x\prod_{\substack{p|q\\ q^2}}\frac{p-1}{p+1}+O\left(x^{\frac{1}{2}}\tau(q)\log^2 x\right),$$

where

$$c_1(q) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 2, \\ 2 & \text{if } q \equiv 0 \pmod 2. \end{cases}$$

Remark. The error terms can be improved by using known results on the zerofree domains of the Riemann zeta function and the that of the Dirichlet function $L(s, \chi_q)$.

References

[1] **Бабаев Г.,** *Распределение целых точек на алгебраических поверхностях,* Душанбе, 1966.

[2] **Стронина М.,** Целые точки на круговых конусах, *Известия вузов. Математика,* (8) (1969), 112-116.

[3] **Lambek I. and Moser L.,** On the distribution of Pythagorean triangles, *Pacific J. Math.,* **5** (1955), 73-83.

[4] **Wild R.E.,** On the number of primitive Pythagorean triangles with area less than n, *Pacific J. Math.,* **5** (1955), 85-91.

[5] **Müller W., Nowak W. and Menzer H.,** On the number of primitive Pythagorean triangles, *Ann. Sci. Math. Quebec,* **12** (1989), 263-273.

[6] **Müller W. and Nowak W.,** Lattice points in planar domains: Applications of Huxley's "discrete Hardy-Littlewood method", *Number-theoretic analysis III.,* Lecture Notes in Mathematics **1452**, Springer Verlag, 1990, 139-164.

[7] **Боревич З.И. и Шафаревич И.Р.,** *Теория чисел,* Наука, Москва, 1964. (Borevich Z.I. and Shafarevich I.R., *Number theory,* Academic Press, 1966.)

[8] **Малышев А.,** О представлении целых чисел положительными квадратичными формами, *Труды Матем. института АН СССР,* **65** (1962), 3-212.

[9] **Epstein P.,** Zur Theorie allgemeiner Zeta-funktionen, *Math. Ann.,* **56** (1903), 615-644.

[10] **Лаврик А.,** Приближенное функциональное уравнение для функций Дирихле, *Изв. АН СССР,* **32** (1) (1968), 134-149.

[11] **Varbanets P. and Zarzycki P.,** Divisors of the Gaussian integers in an arithmetic progression, *J. Number Theory,* **33** (1989), 152-169.

(Received March 2, 2004)

Varbanets P.D.
Department of Computer Algebra and Discrete Mathematics
Odessa National University
ul. Dvoryanskaya 2.
65000 Odessa, Ukraine