ACTA ARITHMETICA
XC.2 (1999)

On divisors whose sum is a square

by

Wolfgang Jenkner (Wien)

1. Introduction. We are interested in the arithmetic function

$$a(n) = \#\{(x,y) \in \mathbb{N} \times \mathbb{N}_0 \mid x^4 - y^2 = 4n,\ (x,y) = 1\}.$$

It is related to the family of elliptic curves $E_n : \eta^2 = \xi^3 + n\xi$ $(n \in \mathbb{N})$ by means of the birational transformation $E_n \to \overline{E}_n$ given by

$$\begin{cases} \overline{\xi} = \frac{\eta}{\xi}, \\ \overline{\eta} = \frac{\eta^2 - 2\xi^3}{\xi^2} \end{cases} \tag{1}$$

with $\overline{E}_n : \overline{\xi}^4 - \overline{\eta}^2 = 4n$ (cf. [4], 64.X, §6). We assume $\overline{\xi} > 0$, so that we can write

$$\overline{\xi} = \frac{\overline{x}}{\overline{z}}, \quad \overline{\eta} = \frac{\overline{y}}{\overline{z}}$$

with $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}, \overline{x} > 0, \overline{z} > 0$ and $(\overline{x}, \overline{y}, \overline{z}) = 1$. It is easy to see that there are $x, z \in \mathbb{N}$ with $(x,z) = 1$ so that

$$\overline{z} = z^2, \quad \overline{x} = xz.$$

So we have to deal with the equation

$$x^4 - y^2 = 4nz^4 \quad \text{with } (x,z) = 1. \tag{2}$$

Note that for x, y, z satisfying this equation, the condition $(x,z) = 1$ is equivalent to $((x^2 - y)/2, (x^2 + y)/2, z) = 1$, which implies

$$(x^2 - y)/2 = p^4 d, \quad (x^2 + y)/2 = q^4 t$$

with $pq = z$, $(p,q) = 1$, $dt = n$ and $p^4 d + q^4 t = x^2$ for some positive integers p, q, d, t.

In fact, this is just a special case of a classical method for determining the rank of certain elliptic curves over $\mathbb{Q}$ (see [2]); in particular, for square-free n, $a(n)$ and the rank r_n of E_n are related by the inequality $2^{r_n + 1} \geq a(n)$.

1991 *Mathematics Subject Classification*: 11D25, 11G05, 11N25.

Some aspects of the closely related arithmetic function counting all lattice points (not just the primitive ones) (x, y) with $x^4 - y^2 = 4n$ are described in [1]. An asymptotic expansion for its arithmetic mean is a special case of the results in [3].

In the following section we will consider the slightly more general case of the function

$$a_\lambda(n) = \#\{(x, y) \in \mathbb{N} \times \mathbb{N}_0 \mid \lambda^2 x^4 - y^2 = 4n,\ (x, y) = 1\}$$

for some fixed $\lambda \in \mathbb{N}$.

2. The arithmetic mean. Our goal in this section is to establish the following result.

PROPOSITION 1. *Let* $T \geq 1$. *Then*

$$\sum_{n \leq T} a_\lambda(n) = C \frac{(4T)^{3/4}}{\lambda^{1/2}} + O(T^{1/2} \log(T/\lambda + e))$$

with

$$C = \frac{1}{3} \cdot \frac{1}{\zeta(2)} \cdot \frac{1}{6} \cdot \frac{\Gamma(1/4)\Gamma(1/2)}{\Gamma(3/4)} = \frac{\Gamma(1/4)^2}{3\sqrt{2}\,\pi^{5/2}}.$$

Proof. In order not to encumber the notation, we write out the proof only for $\lambda = 1$. Setting $S = 4T$, we may express the sum as

$$\sum_{x \leq \sqrt{S}} \#\{y \in \mathbb{N}_0 \mid x^4 - S \leq y^2 < x^4,\ x \equiv y \bmod 2,\ (x, y) = 1\}.$$

As usual, we can dispense with the last condition by means of the Möbius function, which gives

$$\sum_n \mu(n) \sum_{x \leq \sqrt{S}/n} \#\{y \in \mathbb{N}_0 \mid n^2 x^4 - S/n^2 \leq y^2 < n^2 x^4,\ xn \equiv yn \bmod 2\}.$$

In order to eliminate the annoying congruence, we observe that for the principal character $\chi \bmod 2$ and $a, b \in \mathbb{N}_0$,

$$(1 - \chi(a))(1 - \chi(b)) + \chi(a)\chi(b) = \begin{cases} 1 & \text{if } a \equiv b \bmod 2, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

In view of this relation, we find it convenient to consider sums

$$\sum_n \mu(n)\chi_1(n) \sum_{x \leq \sqrt{S}/n} \chi_2(x) \sum_{n^2 x^4 - S/n^2 \leq y^2 < n^2 x^4} \chi_3(y),$$

where χ_i $(i = 1, 2, 3)$ are the principal characters mod $N_i \in \mathbb{N}$ (however, with a view to applying (3), we need only $N_i \in \{1, 2\}$).

Splitting the last sum, we get

$$\sum_{n\le S^{1/4}}\mu(n)\chi_1(n)\sum_{x\le S^{1/4}/n}\chi_2(x)\sum_{y<nx^2}\chi_3(y)$$
$$+\sum_{n\le S^{1/2}}\mu(n)\chi_1(n)\sum_{S^{1/4}/n<x\le S^{1/2}/n}\chi_2(x)\sum_{\sqrt{n^2x^4-S/n^2}\le y<nx^2}\chi_3(y),$$

which gives after a routine calculation involving Euler's summation formula and some trivial estimations

$$I\frac{\phi(N_2)\phi(N_3)}{\zeta(2)N_2N_3\prod_{p\mid N_1}(1-1/p^2)}S^{3/4}+O(S^{1/2}\log S),$$

where

$$I=\frac{1}{3}+\int_1^\infty(t^2-\sqrt{t^4-1})\,dt=\frac{1}{6}\cdot\frac{\Gamma(1/4)\Gamma(1/2)}{\Gamma(3/4)}. \ \blacksquare$$

3. The quadratic mean. From now on, we restrict our attention to the case $\lambda=1$.

PROPOSITION 2. *Let* $T\ge 2$. *Then*

$$\sum_{n\le T}a(n)(a(n)-1)\ll T^{1/2}(\log T)^5.$$

Proof. In view of what was said in the introduction, we have to count the quadruples (d_1,t_1,d_2,t_2) with $\{d_1,t_1\}\ne\{d_2,t_2\}$ such that d_1+t_1 and d_2+t_2 are squares and $d_1t_1=d_2t_2$. The last condition is equivalent to

$$\frac{d_1}{t_2}=\frac{d_2}{t_1}=\frac{a}{b}$$

for some relatively prime a and b, which means that there exist s and t such that

$$\begin{cases} d_1=sa, & d_2=ta,\\ t_2=sb, & t_1=tb.\end{cases}$$

As a result, we have to count the quadruples (a,b,s,t) with

$$\begin{cases} abst\le T,\\ sa+tb=\square, \quad ta+sb=\square,\\ a\ne b, \quad s\ne t.\end{cases}$$

Note that if such a quadruple satisfies these conditions the same holds for (b,a,s,t), (a,b,t,s) and (s,t,a,b), which implies in particular that we can assume $a>b$, $s>t$ and $ab\le st$.

Let $\nu \in \mathbb{N}$ be a square. First, we count the sextuples (a,b,s,t,x,y) of natural numbers satisfying

$$(4)\qquad \begin{cases} stab \le T, \\ sa+tb = \nu x^2, \\ sb+ta = \nu y^2, \\ (sa,tb) = (sb,ta) = 1, \\ s > t, \quad a > b, \\ ab \le \sqrt{T}, \\ (x,y) = 1, \quad x \ne y. \end{cases}$$

Obviously, $(\nu, stab) = 1$ and the two linear equations in s and t of (4) show that $\nu \mid (a^2 - b^2)$. Putting $m = (a^2-b^2)/\nu$ and actually solving these equations, we get

$$(5)\qquad s = \frac{ax^2 - by^2}{m}, \quad t = \frac{ay^2 - bx^2}{m}.$$

So the problem of counting the sextuples satisfying (4) is reduced to finding all solutions (a,b,x,y) of the following system of congruences:

$$(6)\qquad \begin{cases} a^2 \equiv b^2 \bmod \nu, \\ ax^2 \equiv by^2 \bmod m, \\ ay^2 \equiv bx^2 \bmod m. \end{cases}$$

Let a and b be fixed. In view of $(a,b)=1$, the definition of m implies

$$(a,m) = (b,m) = 1,$$

and so (6) shows

$$(x,m) = (y,m) = 1,$$

and, in fact, the last two congruences of (6) are equivalent. Thus, we are left with the problem of counting solutions $(\varrho \bmod m, x, y)$ satisfying congruences $\bmod m$

$$\begin{cases} \varrho^2 \equiv b/a, \\ y \equiv \varrho x. \end{cases}$$

The number of solutions of the first of these congruences equals 0 or the number of residue classes $\tau \bmod m$ with

$$\tau^2 \equiv 1 \bmod m.$$

Writing this as the equivalent system of congruences modulo powers of the various prime numbers dividing m, we find that this number is $\ll 2^{\omega(m)}$, where $\omega(m)$ denotes the number of different primes dividing m. Now, for each $\varrho \bmod m$ we have to count all possible (x,y). We begin with the simple observation that for all $T>0, B>A>0$ the number of such pairs satisfying

$$(x,y) = 1, \quad 0 < x \le T, \quad A \le y/x \le B$$

is at most $1 + (B - A)T^2$. Namely, let K be this number and suppose $K > 1$. Dividing the interval $[A, B]$ in the $K - 1$ successive intervals of length $(B - A)/(K - 1)$, we find two pairs (x, y) and (x', y') such that

$$0 < \frac{y}{x} - \frac{y'}{x'} \le \frac{B - A}{K - 1}.$$

But then this difference

$$\frac{yx' - y'x}{xx'}$$

actually equals at least T^{-2}, which proves the assertion. Now, assuming that ϱ is a positive member of its residue class, we can write

$$y = \varrho x - zm \tag{7}$$

with $z > 0$ since $y < x$. Further, $(x, y) = 1$ implies $(z, x) = 1$. Remembering (5), we see that the condition $abst \le T$ is equivalent to

$$f\left(\frac{y^2}{x^2}\right) \le \frac{4T}{x^4\nu^2},$$

where we have set

$$f(t) = \frac{4ab}{(a^2 - b^2)^2}(a - bt)(at - b).$$

This function is increasing in $[b/a, 1]$ and $f(1) = 4ab/(a + b)^2$.

We have to consider two cases.

First case:

$$\frac{4T}{x^4\nu^2} \ge \frac{4ab}{(a + b)^2} \quad \text{or} \quad x \le \left(\frac{T}{ab}\right)^{1/4}\left(\frac{a + b}{\nu}\right)^{1/2}.$$

In this case, we have to count the relatively prime (x, y) such that

$$\left(\frac{b}{a}\right)^{1/2} < \frac{y}{x} \le 1,$$

which means

$$(\varrho - 1)\frac{\nu}{a^2 - b^2} \le \frac{z}{x} < \left(\varrho - \left(\frac{b}{a}\right)^{1/2}\right)\frac{\nu}{a^2 - b^2}.$$

The preceding considerations show that this number is at most

$$\left(\frac{T}{ab}\right)^{1/2}\left(\frac{a + b}{\nu}\right)\left(1 - \left(\frac{b}{a}\right)^{1/2}\right)\frac{\nu}{a^2 - b^2} + 1$$
$$= \frac{T^{1/2}}{ab^{1/2}(a^{1/2} + b^{1/2})} + 1 \le \frac{T^{1/2}}{a^{3/2}b^{1/2}} + 1.$$

Second case:

$$\frac{4T}{x^4\nu^2} < \frac{4ab}{(a+b)^2} \quad \text{or} \quad x > \left(\frac{T}{ab}\right)^{1/4}\left(\frac{a+b}{\nu}\right)^{1/2}.$$

We have to count the (x,y) such that

$$\left(\frac{b}{a}\right)^{1/2} < \frac{y}{x} \le t^{1/2},$$

where t is the smaller solution of the quadratic equation

$$f(t) = \frac{4T}{x^4\nu^2},$$

which means

$$\begin{aligned} 0 &< \frac{y}{x} - \left(\frac{b}{a}\right)^{1/2} \\ &< \left(\frac{a^2+b^2-(a^2-b^2)(1-4Tx^{-4}\nu^{-2})^{1/2}}{2ab}\right)^{1/2} - \left(\frac{b}{a}\right)^{1/2}, \end{aligned}$$

this expression being

$$\begin{aligned} &< \frac{\frac{a^2+b^2-(a^2-b^2)(1-4Tx^{-4}\nu^{-2})^{1/2}}{2ab} - \frac{b}{a}}{2\left(\frac{b}{a}\right)^{1/2}} \\ &= \frac{(a^2-b^2)}{4a^{1/2}b^{3/2}}(1-(1-4Tx^{-4}\nu^{-2})^{1/2}) \le \frac{(a^2-b^2)}{4a^{1/2}b^{3/2}} \cdot \frac{4T}{x^4\nu^2}. \end{aligned}$$

Substituting (7), we find

$$0 < \left(\varrho - \frac{b^{1/2}}{a^{1/2}}\right)\frac{\nu}{a^2-b^2} - \frac{z}{x} < \frac{1}{a^{1/2}b^{3/2}} \cdot \frac{T}{x^4\nu},$$

and so there are at most

$$\frac{1}{a^{1/2}b^{3/2}} \cdot \frac{4T}{u^2\nu} + 1$$

suitable (x,z) with $u \le x \le 2u$ for some

$$u \ge u_0 := \left(\frac{T}{ab}\right)^{1/4}\left(\frac{a+b}{\nu}\right)^{1/2}.$$

Now putting $u_i := 2^i u_0$ for $1 \le i \le N$, we sum up over intervals $u_i \le x \le u_{i+1}$. We have to choose N such that $u_N \ge (2T)^{1/2}\nu^{-1/2}$ or $N \ge (4\log 2)^{-1}\log T$. Since

$$\frac{1}{a^{1/2}b^{3/2}} \cdot \frac{4T}{u_0^2\nu} = \frac{4T^{1/2}}{b(a+b)} \le \frac{4T^{1/2}}{ba}$$

we find that the total number of suitable (x,z) (and hence (x,y)) is

$$\ll \frac{T^{1/2}}{ab} + \log T.$$

Now, returning to the original problem and remembering that ν is a square μ^2, we have to estimate

$$\sum_{ab\le T^{1/2}} \sum_{\mu^2 \mid a^2-b^2} \left(\frac{T^{1/2}}{ab} + \log T\right) 2^{\omega((a^2-b^2)/\mu^2)}.$$

Fortunately, denoting by $d(n)$ the number of divisors of a positive integer n, we have

$$\sum_{\mu^2\mid n} 2^{\omega(n/\mu^2)} = d(n)$$

since both sides of the equation are multiplicative and the assertion is easily checked for powers of primes.

Let

$$D_b(t) = \sum_{b<a\le t} d(a^2-b^2),$$

where it is understood that the sum runs over a with $(a,b)=1$. This sum is

$$\begin{aligned} &\ll \sum d(a-b)d(a+b) \\ &\le \Big(\sum d(a-b)^2\Big)^{1/2} \Big(\sum d(a+b)^2\Big)^{1/2} \le \sum_{n\le 2t} d(n)^2. \end{aligned}$$

A well-known estimate shows (for $t\ge 2$, say) that this sum is $\ll t(\log t)^3$. So we have

$$\begin{aligned} \sum_{ab\le T^{1/2}} d(a^2-b^2) &= \sum_{b\le T^{1/4}} D_b\left(\frac{T^{1/2}}{b}\right) \\ &\ll T^{1/2}(\log T)^3 \sum_{b\le T^{1/4}} \frac{1}{b} \ll T^{1/2}(\log T)^4. \end{aligned}$$

On the other hand,

$$\begin{aligned} \sum_{ab\le T^{1/2}} \frac{d(a^2-b^2)}{ab} &= \sum_{b\le T^{1/4}} \frac{1}{b} \sum_{a\le T^{1/2}b^{-1}} \frac{d(a^2-b^2)}{a} \\ &= \sum_{b\le T^{1/4}} \frac{1}{b} \int_b^{T^{1/2}b^{-1}} \frac{1}{t}\, dD_b(t). \end{aligned}$$

Integration by parts and trivial estimates show that the integral is $\ll (\log T)^4$, so the whole expression does not exceed $O((\log T)^5)$. Putting everything together, we have finished the proof of Proposition 2. ∎

We conclude by pointing out that this and the preceding proposition immediately imply

COROLLARY 3.

$$\#\{n \le T \mid a(n) \ne 0\} = C(4T)^{3/4} + O(T^{1/2}(\log T)^5).$$

References

[1] D. Clark, *An arithmetical function associated with the rank of elliptic curves*, Canad. Math. Bull. 34 (1991), 181–185.

[2] J. Coates, *Elliptic curves and Iwasawa theory*, in: Modular Forms, R. Rankin (ed.), Halsted Press, New York, 1984.

[3] W. Jenkner, *Asymptotic aspects of the Diophantine equation* $p^k x^{nk} - z^k = l$, preprint.

[4] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

Institut für Mathematik
Universität Wien
Strudlhofgasse 4
1090 Wien, Austria
E-mail: wolfgang@mat.univie.ac.at

Received on 22.5.1998
and in revised form on 30.9.1998 (3389)