LATTICE POINTS ON ELLIPSES

J.Cilleruelo and A.Córdoba

Departamento de Matemáticas. Universidad Autónoma de Madrid

Madrid 28049. España

I.- Introduction.

Given a square free positive integer d one may consider the arithmetical function $r_d(n) = \#\{n = x^2 + dy^2/x, y \in Z\}$ which can also be described as the number of lattice points on the ellipse $x^2 + dy^2 = n$ and it has a natural interpretation inside the ring of algebraic integers of the field $Q(\sqrt{-d})$. The main purpose of this paper is to analyse closely this function in connection with the distribution of lattice points on "small arcs " of those ellipses.

Let us denote by h_2 the number of elements of order two in the class field group of $Q(\sqrt{-d})$, then we may state our main result:

Theorem 1. *On the ellipse $x^2 + dy^2 = n$, an arc of length $n^{\frac{1}{4}-\frac{1}{8[\frac{m+h_2}{2h_2+2}]+4}}$ contains, at most, m lattice points.*

In other words, for every $\epsilon > 0$, there exists a finite constant C_ϵ such that given an arc of length $n^{\frac{1}{4}-\epsilon}$ on the ellipse $x^2 + dy^2 = n$ it contains no more than C_ϵ lattice points. The particular case $m = h_2 + 2$, which corresponds to arcs of length $n^{\frac{1}{6}}$ is not difficult to prove by geometric arguments based on curvature considerations. However, the general case is of a much more intricate arithmetical nature.

Similary to the case of gaussian integers one has estimates of the form $r_d(n) = O(n^\epsilon)$ and $\limsup_{n\to\infty} \frac{r_d(n)}{(\log n)^\epsilon} = \infty$ for every $\epsilon > 0$. Therefore, in view of the theorem, one may asks what happens for arcs whose length is n^α, $\frac{1}{2} >$

$\alpha \geq \frac{1}{4}$; this remains an open question which we have not been able to answer with the methods introduced to prove theorem 1. There is a relationship between upper bounds estimates for lattice points on arcs, restriction lemmas of Fourier series and integrals and L^p-properties of certain gaussian sums (see [1], [2],[7],[10],[11] and [12]). The existence of this connection has stimulated this research whose first published result [1] contains the case $d = -1$.

Another interesting question is to analyse how "well distributed" are the lattice points on these ellipses when $r_d(n)$ is large enough. In the next theorem we answer that question in the following sense: we consider the quantity $\mathcal{D}_d(n) = \mathcal{S}_d(n)/(\frac{\pi n}{\sqrt{d}})$, for $r_d(n) \geq 4$, where $\mathcal{S}_d(n)$ denotes the area of the polygon whose vertexs are the lattice points on the ellipse $x^2 + dy^2 = n$. Clearly these lattice points will be "better distributed" if $\mathcal{D}_d(n)$ is close enough to the number 1. We have the following theorem

Theorem 2.

a) $|\mathcal{D}_d(n) - 1| << e^{12\sqrt{d}} \left(\frac{\log\log n}{\log n} \right)^2$ *for infinitely many integers* n.

b) For every $\epsilon > 0$ *and for every integer* k*, there exists an ellipse* $x^2+dy^2 = n$ *such that all its lattice points are placed an the arcs* $|\frac{y}{x}| < \epsilon$ *and the number of them is greater than* k*.*

c) The set $\{\mathcal{D}_d(n), r_d(n) \geq 4\}$ *is dense in the interval* $\begin{cases} [\frac{2}{\pi}, 1] \text{ if } d = 1 \\ [\frac{3\sqrt{3}}{2\pi}, 1] \text{ if } d = 3 \\ [0, 1] \text{ for } d \neq 1, 3. \end{cases}$

In general one cannot expect a much better estimate than a) because it is easy to show that $|\mathcal{D}_d(n) - 1| >> \dfrac{1}{dr_d^2(n)}$, and it is a well known that $r_d(n) = O(n^\epsilon)$ for every $\epsilon > 0$.

Obviously estimates a) and b) yield respectively

$$\limsup_{n\to\infty} \frac{\mathcal{S}_d(n)}{\frac{\pi}{\sqrt{d}} n} = 1, \qquad \liminf_{\substack{n\to\infty \\ r_d(n)\geq 4}} \frac{\mathcal{S}_d(n)}{\frac{\pi}{\sqrt{d}} n} = 0$$

II.- Proofs.

[A] Preliminary results and notation.

For the sake of simplicity we shall discuss the details when $d \not\equiv -1 \pmod 4$. The straightforward modifications of the arguments to cover the case $d \equiv -1 \pmod 4$ are left to the reader.

To each representation $n = a^2 + db^2$ we shall associate the lattice point (a, b) on the ellipse $x^2 + dy^2 = n$, the point $(a, b\sqrt{d})$ on the circle $z^2 + w^2 = n$ and the algebraic integer $a + b\sqrt{-d}$ in $Q(\sqrt{-d})$ whose norm is precisely $N(a + b\sqrt{-d}) = a^2 + db^2 = n$.

Given a rational prime p we shall consider the principal ideal $< p >$ in the ring A of algebraic integers of the quadratic field $Q(\sqrt{-d})$. It is well known that $< p >$ may be a prime ideal or may have a descomposition $< p >= \wp_1\wp_2$ as a product of two, not necessarily differents, prime ideals $\wp_j$.

The Kronecker symbol (d/p) describes the situation: $(d/p) = +1$ if $< p >= \wp_1\wp_2$, $\wp_1 \neq \wp_2$; $(d/p) = -1$ if $< p >$ is prime and $(d/p) = 0$ if $< p >= \wp^2$. The fundamental theorem of arithmetic yields

$$n = \prod_{(d/p)=-1} q_k^{\tilde\beta_k} \prod_{(d/p_j)=1 \text{ or } 0} p_j^{\alpha_j}$$

which produces the unique factorization

$$< n >= \prod < q_k >^{\tilde\beta_k} \prod \wp_{j,1}^{\alpha_j}\wp_{j,2}^{\alpha_j}.$$

Obviously each representation of $n = x^2 + dy^2$ corresponds to a descomposition of the principal ideal $< n >=< x + y\sqrt{-d} >< x - y\sqrt{-d} >$ with norm

$$N[< x + y\sqrt{-d} >] = N[< x - y\sqrt{-d} >] = n.$$

In such a situation the factors must to be of the form:

$$< x + y\sqrt{-d} >= \prod < q_k >^{\frac{\tilde\beta_k}{2}} \prod \wp_{j,1}^{\gamma_j}\wp_{j,2}^{\alpha_j-\gamma_j}$$

$$< x - y\sqrt{-d} >= \prod < q_k >^{\frac{\tilde\beta_k}{2}} \prod \wp_{j,1}^{\alpha_j-\gamma_j}\wp_{j,2}^{\gamma_j}, \quad 0 \le \gamma_j \le \alpha_j$$

which yields the condition that $\tilde\beta_k = 2\beta_k$ must be even. Therefore we shall concentrate our attention in all the products

$$\prod < q_k >^{\beta_k} \prod \wp_{j,1}^{\alpha_j-\gamma_j}\wp_{j,2}^{\gamma_j}, \qquad 0 \le \gamma_j \le \alpha_j$$

and we will characterize those among them which correspond to principal ideals.

Let us denote by $E_1, ..., E_h$ the elements of the group of ideal classes in $Q(\sqrt{-d})$ where $E_1 = I$ is the unity i.e. the class of principal ideals. Therefore, modulo the unities of the ring A, there will be as many representations of the form $n = x^2 + dy^2$ as sets of integers $\gamma_j, \quad 0 \leq \gamma_j \leq \alpha_j$ such that

$$\prod < q_k >^{\beta_k} \prod \wp_{j,1}^{\gamma_j} \wp_{j,2}^{\alpha_j - \gamma_j} \in E_1$$

that is $\prod E_{\nu(j)}^{2\alpha_j - \gamma_j} = E_1$, where we have used $E_{\nu(j)}$ for the class of the ideal $\wp_{j,1}$.

Let us denote by $\mathcal{U}$ the number of unities of the ring A, i.e.

$$\mathcal{U} = \begin{cases} 4 & \text{if } d = 1 \\ 6 & \text{if } d = 3 \\ 2 & \text{in the remainder cases.} \end{cases}$$

and let us write the product

$$\mathcal{U} \prod E_{\nu(j)}^{-\alpha_j} \prod \left\{ E_1 + E_{\nu(j)}^2 + ... + (E_{\nu(j)}^2)^{\alpha_j} \right\} = \sum_{m=1}^{h} a_m E_m$$

Then we have:

Lemma 3. *The first coefficient a_1 is precisely the number of representations of the integer n by the quadratic form $x^2 + dy^2$.*

Let us remark that the other coefficients have a similar interpretation in terms of lattice points on the ellipses associated to the quadratic forms corresponding to the other elements of the class group.

Corollary 4.

a) If $h = 1$ then $r_d(n) = 0$ if one of the β's is odd and $r_d(n) = \mathcal{U} \prod (1+\alpha_j)$ if every β_k is even.

b) If every element of the class group, except the unity, has order two then:

$$r_d(n) = \begin{cases} 0 \text{ if there is an odd exponent } \beta_k \text{ or if } \prod E_{\nu(j)}^{\alpha_j} \neq E_1 \\ \mathcal{U} \prod (1 + \alpha_j) \text{ in other case.} \end{cases}$$

c) There exists a finite constant $C(d)$ such that if all the exponents $\tilde{\beta}_k$ are even then we can find $m \leq C(d)$ in such a way that the number mn has, at least, $\left[\dfrac{\mathcal{U} \prod (1 + \alpha_j)}{h} \right]$ different representations.

The proofs of parts *a)* and *b)* are immediate. To see *c)* let us observe first that
$\sum_{i=1}^{h} a_i = \mathcal{U}\prod(1+\alpha_j)$ and, therefore, there exists a_i so that $a_i \geq \left[\frac{\mathcal{U}\prod(1+\alpha_j)}{h}\right]$.
If it happens that $i=1$ then there is nothing to prove and we may take $m=1$. If $i \neq 1$ then we choose a prime p so that $< p >= \wp_1\wp_2$, $\wp_1 \in E_i^{-1}$ and take $m = p$.

[B] The angular representation.

Let (x^s, y^s) be a lattice point on the ellipse $x^2 + dy^2 = n$ with $< \alpha^s >=< x^s + y^s\sqrt{-d} >$ as its associated principal ideal.

Using the notation introduced in the preceding section we may write:

$$< \alpha^s >= \prod < q_k >^{\beta_k} \prod \wp_{j,1}^{\gamma_j^s} \wp_{j,2}^{\alpha_j-\gamma_j^s}, \quad 0 \leq \gamma_j^s \leq \alpha_j,$$

in such a way that $\prod E_{\nu(j)}^{2\gamma_j^s-\alpha_j} = E_1$, where $\wp_{j,1}, \wp_{j,2}$ will not be necessarily principal, but one can find a positive integer n_j/h such that $E_{\nu(j)}^{n_j} = E_1$ and, therefore, the ideals $\wp_{j,1}^{n_j}, \wp_{j,2}^{n_j}$ became principal. That is, there exists algebraic integers $\omega_{j,1}, \omega_{j,2}$ in the ring A so that $\wp_{j,1}^{n_j} =< \omega_{j,1} >, \wp_{j,2}^{n_j} =< \omega_{j,2} >$.

Let us consider the ring B of algebraic integers of the field $Q(\sqrt{-d}, \omega_{j,1}^{1/n_j}, \omega_{j,2}^{1/n_j})$. Then we know that $\wp_{j,1}, \wp_{j,2}$ have extensions $\tilde{\wp}_{j,1}, \tilde{\wp}_{j,2}$ respectively, which are principal ideals in the ring B. More concretely,

$$\tilde{\wp}_{j,1} = B\omega_{j,1}^{1/n_j} =< \omega_{j,1}^{1/n_j} > \qquad \tilde{\wp}_{j,2} = B\omega_{j,2}^{1/n_j} =< \omega_{j,2}^{1/n_j} >$$

which implies

$$< p_j >= Bp_j = \tilde{\wp}_{j,1}\tilde{\wp}_{j,2} =< (\omega_{j,1}\omega_{j,2})^{1/n_j} >$$

and since $Ap_j = \tilde{\wp}_{j,1}\tilde{\wp}_{j,2} \cap A$ we may write

$$\omega_{j,1}^{1/n_j} = \sqrt{p_j}e^{2\pi i\Phi_j} \quad \omega_{j,2}^{1/n_j} = \sqrt{p_j}e^{-2\pi i\Phi_j}$$

for an appropiate angle Φ_j, $-\pi < \Phi_j \leq \pi$.

In general, the ideal

$$\prod < q_k >^{\beta_k} \prod \wp_{j,1}^{\gamma_j} \wp_{j,2}^{\alpha_j-\gamma_j^s} =< (\prod q_k^{\beta_k} \prod p_j^{\alpha_j/2}) e^{2\pi i \sum (2\gamma_j^s-\alpha_j)\Phi_j} >$$

is a principal ideal when considered in the ring of integers of the field $Q(\sqrt{-d}, \omega_{1,1}^{1/n_1}, \omega_{1,2}^{1/n_1}, ...)$. However, if it happens that $\prod E_{\nu(j)}^{2\gamma_j^s-\alpha_j} = E_1$, then it is also principal in the ring A of algebraic integers of $Q(\sqrt{-d})$. Therefore we have proved the following.

Lemma 5. *The integers $x^s + y^s\sqrt{-d}$ corresponding to the different representations of $n = (x^s)^2 + d(y^s)^2$ are given by the formula:*

$$\sqrt{n} e^{2\pi i \sum \lambda_j \Phi_j}$$

where the angles Φ_j corresponds to rational primes p_j such that $(d/p_j) = 1$ or 0 and have been defined above, while the rational integers λ_j satisfy the relations $-\alpha_j \le \lambda_j \le \alpha_j$, $\lambda_j \equiv \alpha_j \pmod 2$, $\prod E_{\nu(j)}^{\lambda_j} = E_1$.

[C] End of the proof of Theorem 1.

Let us consider an arc Γ of length $n^{\alpha/2}$, on the ellipse $x^2+dy^2 = n$, which contains $m+1$ lattice points and let $< \alpha^j >=< a_j+b_j\sqrt{-d} >$, $j = 1, ..., m+1$ be the corresponding principal ideals. To each pair of them $< \alpha^s >, < \alpha^t >$ we may associate the angle

$$\Psi^{s,t} = \frac{1}{2}\left\{ \sum_j \lambda_j^s \Phi_j - \sum_j \lambda_j^t \Phi_j \right\}$$

We have:

$$|\Psi^{s,t}| = |\sum_j \frac{\lambda_j^s - \lambda_j^t}{2} \Phi_j| < \sqrt{d} n^{\frac{\alpha-1}{2}}$$

where $\dfrac{\lambda_j^s - \lambda_j^t}{2} \in Z$ for each j because $\lambda_j^s \equiv \lambda_j^t \equiv \alpha_j \pmod 2$.

The elements of the class group given by the products $\prod_j E_{\nu(j)}^{\frac{\lambda_j^s-\lambda_j^t}{2}}$ have, at most, order two because

$$\left[\prod_j E_{\nu(j)}^{\frac{\lambda_j^s-\lambda_j^t}{2}} \right]^2 = \prod_j E_{\nu(j)}^{\lambda_j^s} \prod_j E_{\nu(j)}^{-\lambda_j^t} = E_1^2 = E_1.$$

Therefore, if h_2 denotes the number of elements of the class group of $Q(\sqrt{-d})$ whose order is two, then, among the products $\prod_j E_{\nu(j)}^{\frac{\lambda_j^1-\lambda_j^t}{2}}$, $2 \leq t \leq$ $\leq m+1$ there are, at least, $\left[\dfrac{m+h_2}{h_2+1}\right]$ which are equal.

Let us denote by I the set of those t's. For them we consider the products

$$\prod_j E_{\nu(j)}^{\frac{\lambda_j^s-\lambda_j^t}{2}}, \quad 1 < s < t, \quad s,t \in I$$

We have

$$\prod_j E_{\nu(j)}^{\frac{\lambda_j^s-\lambda_j^t}{2}} = \prod_j E_{\nu(j)}^{\frac{\lambda_j^s-\lambda_j^1}{2}} \prod_j E_{\nu(j)}^{\frac{\lambda_j^1-\lambda_j^t}{2}} = E_1.$$

for each pair $s,t \in I$.

Therefore, the angle $\sum_j \dfrac{\lambda_j^s-\lambda_j^t}{2}\Phi_j$ will correspond to a representation

$$x^2+dy^2 = \prod_j p_j^{\frac{|\lambda_j^s-\lambda_j^t|}{2}}.$$

The least favourable case (i.e. $y=1$) yields the estimate:

$$\frac{\sqrt{d}}{\left(\prod p_j^{\frac{|\lambda_j^s-\lambda_j^t|}{2}}\right)^{1/2}} < |\Psi^{s,t}| < \sqrt{d}n^{\frac{\alpha-1}{2}}$$

which implies the inequality

$$\prod p_j^{-\frac{|\lambda_j^s-\lambda_j^t|}{4}} < n^{\frac{\alpha-1}{2}}.$$

Our next step is to multiply all together these inequalities obtanied for such pairs (s,t). We get

$$(*) \qquad \prod_j p_j^{-\frac{1}{4}\sum_{s,t}|\lambda_j^s-\lambda_j^t|} \leq n^{\frac{\alpha-1}{2}\binom{\left[\frac{m+h_2}{h_2+1}\right]}{2}}.$$

Let us now recall the fact that $-\alpha_j \leq \lambda_j^s \leq \alpha_j$ and observe that in order to estimate $\sum |\lambda_j^s - \lambda_j^t|$ the worst possible situation occurs when half of the λ_j^s are equal to $-\alpha_j$ and the other half to α_j. Therefore

$$\sum_{s,t} |\lambda_j^s - \lambda_j^t| \leq \frac{1}{2}\alpha_j \left\{ \left[\frac{m+h_2}{h_2+1}\right]^2 - \delta\left(\left[\frac{m+h_2}{h_2+1}\right] - 1\right)\right\}$$

where

$$\delta(a) = \begin{cases} 0 \text{ if } a \text{ is odd} \\ +1 \text{ if } a \text{ is even.} \end{cases}$$

We substitute this estimate in (*) and we use the fact $\prod p_j^{\alpha_j} = \dfrac{n}{\prod q_k^{2\beta_k}} <$ n to finish the proof of the theorem.

[D] Proof of theorem 2.

We are proving the general case $d \neq 1, 3$. The particular case $d = 1$ was studied in [5] and the case $d = 3$ only needs some straightforward technical variations whose details are left to the reader.

a) For each integer k let us consider

$$n_k = \prod_{1 \leq m < k(d)} (dm^2+1) \quad \text{and} \quad \Phi^l = \sum_{m=1}^{l} \arctan\frac{1}{m\sqrt{d}} - \sum_{m=l+1}^{k(d)} \arctan\frac{1}{m\sqrt{d}}$$

where $k(d) = [ke^{4\sqrt{d}}]$.

By lemma 5, each angle $\dfrac{\Phi^l}{2\pi}$ determines a lattice point (a_l, b_l) on the ellipse $x^2 + dy^2 = n_k$, i.e. a point $(a_l, b_l\sqrt{d})$ on the circle $x^2 + y^2 = n_k$.

In general we don't know if the ideals $< i\sqrt{d}m + 1 >$ are primes or not and, obviously, we can not expect that the lattice points described above are all the lattice points on the ellipse.

However, let us observe that $\Phi^l - \Phi^{l-1} = \arctan\dfrac{1}{l\sqrt{d}} \leq 2\arctan\dfrac{1}{k\sqrt{d}}$ and

$$\sum_{k<l<k(d)} 2\arctan\frac{1}{l\sqrt{d}} > 2\pi.$$

Then, the distance between two neighbour points on the circle is smaller than

$$2\sqrt{n_k}\arctan\frac{1}{k\sqrt{d}}.$$

The quanty $\dfrac{\mathcal{S}_d(n_k)}{\pi n_k/\sqrt{d}}$ can be evaluated by the quotien $\dfrac{\mathcal{S}'_d(n_k)}{\pi n_k}$ where $\mathcal{S}'_d(n_k)$ is the area of the polygon whose vertices are the corresponding points on the circle $x^2+y^2=n_k$.

An easy geometric argument allows us to estimate the area $\mathcal{S}''_d(n_k)$ of the circle's region not included in the polygon whose vertices are $\sqrt{n_k}e^{i\Phi^l}$, $k<l<k(d)$. We have

$$0<\pi n_k-\mathcal{S}'_d(n_k)<\mathcal{S}''_d(n_k)<$$

$$k(d)\left(\frac{n_k}{2}\big(2\arctan\frac{1}{k\sqrt{d}}\big)-\frac{1}{2}\big(2\sqrt{n_k}\sin\arctan\frac{1}{k\sqrt{d}}\big)\big(\sqrt{n_k}\cos\arctan\frac{1}{k\sqrt{d}}\big)\right)=$$

$$=k(d)n_k\left(\arctan\frac{1}{k\sqrt{d}}-\frac{1}{2}\sin\big(2\arctan\frac{1}{k\sqrt{d}}\big)\right)=$$

$$=k(d)n_k\left(\arctan\frac{1}{k\sqrt{d}}-\frac{1}{2}\big(2\arctan\frac{1}{k\sqrt{d}}+O(\frac{1}{k^3d^{\frac{3}{2}}})\big)\right)=\frac{k(d)n_k}{k^3d^{\frac{3}{2}}}$$

Now, let us observe that $k(d)>>\dfrac{\log n_k}{\log\log n_k}$. Then, if we divide by n_k and made the sustitution $k=k(d)e^{-12\sqrt{d}}$ we obtain:

$$0<\left|1-\frac{S'_d(n_k)}{\pi n_k}\right|<<\left(\frac{\log\log n_k}{\log n_k}\right)^2e^{12\sqrt{d}}$$

b) In reference [5], in order to prove the theorem for $d=1$, a result about the angular equidistribution of the primes $a+bi\in Z(i)$ is used. Here we need the more general result (see, for example ref [9], pages 374-375):

Theorem A. *Let h be the class-number of $Q(\sqrt{-d})$. If $N(\alpha,\beta,x)$ denotes the number of prime ideals $<a+b\sqrt{-d}>$ such that $\alpha<\arctan\frac{a}{b\sqrt{d}}<\beta$ and $\sqrt{a^2+db^2}\le x$, then*

$$N(\alpha,\beta,x)=\left(\frac{(\beta-\alpha)\mathcal{U}}{2\pi h}+o(1)\right)\frac{x}{\log x}.$$

where $\mathcal{U}$ is the number of units of the ring of integers.

Corolary B. *For each $\alpha \in [0, 2\pi)$ and for every $\epsilon > 0$, there exists an ideal prime $< a + b\sqrt{-d} >$, $a + b\sqrt{-d} = \sqrt{a^2 + db^2}e^{i\Phi}$ such that $|\Phi - \alpha| < \epsilon$.*

Taking $\alpha = 0$ we can find, for each $\epsilon > 0$ and for each integer k, a prime ideal $< a_{\epsilon,k} + db_{\epsilon,k} >$ such that $|\Phi_{\epsilon,k}| < \frac{\epsilon}{k}$.

Let $n_k = \left(a_{\epsilon,k}^2 + db_{\epsilon,k}^2\right)^k$. Acording with lemma 5, all the points $(a, b\sqrt{d})$ on the circle are given by the formula

$$\sqrt{n_k}e^{i\gamma\Phi_{\epsilon,k}}$$

where γ runs over the set $\{\gamma \in Z; |\gamma| \leq k, \gamma \equiv k \pmod 2\}$.

To finish the proof of b) we observe that the $r_d(n) = \mathcal{U}(k+1) > k$ and $|\gamma\Phi_{\epsilon,k}| < \epsilon$ in all the cases.

c) We remember that $\mathcal{S}_d(n)/(\frac{\pi n}{\sqrt{d}}) = \mathcal{S}'_d(n)/\pi n$. Let $\alpha \in [0, 1]$, then there exists $\beta \in (0, \frac{\pi}{4})$ such that the area of the dotted region is $\pi\alpha n_k$.

The idea is to look for circles such that the polygons with vertices in the corresponding points $(a, b\sqrt{d})$ are close enough to the region described above.

Let us consider $\frac{\beta}{2^2}, \frac{\beta}{2^3}, ..., \frac{\beta}{2^k}$ and $\epsilon = \frac{\beta}{2^{2k}}$. Acording to lemma A, for each $j = 2, 3, ..., k$ we can find a prime
$a_j + \sqrt{-d}b_j = \sqrt{p_j}e^{2\pi i\Phi_j}$ such that $|2\pi\Phi_j - \frac{\beta}{2^j}| < \epsilon$.

We choose $n_k = \prod_{j=2}^{k} p_j^2$. The points $(a, b\sqrt{d})$ on the circle $x^2 + y^2 = n_k$ are given by the formula

$$\sqrt{n_k} e^{2\pi i \{\sum_{j=2}^{k} \gamma_j \Phi_j\}}$$

where γ_j takes the values $-2, 0$ or 2.

All the integers r, $0 \le r < 2^{k-1}$ can be written in the form

$$r = a_0(r)2^0 + a_1(r)2^1 + \cdots + a_{k-2}(r)2^{k-2}.$$

where the $a_j(r)$ takes values 0 or 1.

For every r we choose $\gamma_j^r = 2a_{k-j}(r)$ and we have

$$\sum_{j=1}^{k} \gamma_j^r \Phi_j = 2\sum_{j=2}^{k} \frac{\beta a_{k-j}(r)2^{k-j}}{2^k} + O(\frac{k\beta}{2^{2k}}) = \frac{\beta r}{2^{k-1}} + O(\frac{k\beta}{2^{2k}}).$$

Then, for each r, $0 \le r < 2^{k-1}$ there exists a point $(a_r, b_r\sqrt{d})$ on the circle $x^2 + y^2 = n_k$, $a_r + b_r\sqrt{-d} = \sqrt{n_k} e^{2\pi i \Phi_r}$, such that

$$\left|2\pi\Phi_r - \frac{\beta r}{2^{k-1}}\right| < \epsilon' \qquad \epsilon' = \frac{k\beta}{2^{2k}}$$

Then, $|2\pi\Phi_{r-1} - 2\pi\Phi_r| < \dfrac{\beta}{2^{k-1}} + 2\epsilon', \qquad r = 1, ..., 2^{k-1} - 1$ and

$$|2\pi\Phi_{2^{k-1}-1} - \beta| < \frac{\beta}{2^{k-1}} + \epsilon'.$$

Futhermore there are no lattice points on the arcs

$$\sqrt{n_k} e^{i\theta + \pi t}, \qquad \beta + \epsilon < \theta < \pi - \beta - \epsilon, \quad t = 0, 1.$$

Now, with the same geometric argument used in the proof of b) and making $k \to \infty$ we obtain c).

References.

[1] J.Cilleruelo and A.Córdoba. *Trigonometrics polynomials and lattice points.* Proceedings of the A.M.S. Vol 115. N 4 (1992)

[2] J.Cilleruelo and A.Córdoba. *$B_2[\infty]$-sequences whose terms are squares.* Acta Arithmetica. Vol LXI.3 (1992)

[3] J.Cilleruelo y A.Córdoba. *La Teoría de los Números.* Ed. Mondadori. Madrid, 1992.

[4] J.Cilleruelo. *Arcs containing no three lattice points.* Acta Arithmetica. Vol LIX.1 (1991).

[5] J.Cilleruelo. *The distribution of the lattice points on circles.* To appear in "Journal of Number Theory".

[6] J.Cilleruelo. *$B_2[g]$-sequences whose terms are squares.* Preprint.

[7] A.Córdoba. *Traslation invariant perators.* Proceedings of the seminary held at the Escorial. June. 1974.

[8] Y.Meyer. *Algebraic Numbers and Harmonic Analysis.* Noth-Holland.

[9] Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Springer-Verlag.

[10] W.Rudin. *Trigonometric series with gaps.* Journal of Mathematics and Mechanis, Vol 9. N 2 (1960).

[11] A.Zygmund. *A Cantor-Lebesgue theorem for double trigonometric series.* Studia Math. 64. (1975)

[12] A.Zygmund. *On Fourier coefficients and transform of functions of two variables.* Studia Math. (1974), 189-202.