and

$$x^p = [-(rr_1)^{p^n} + (ss_1)^{p^n} + p^{mp^n-n+1}(tt_1)^{p^n}]/2 \equiv -r^{p^n} \pmod{p^{3n}},$$
$$y^p = [(rr_1)^{p^n} - (ss_1)^{p^n} + p^{mp^n-n+1}(tt_1)^{p^n}]/2 \equiv -s^{p^n} \pmod{p^{3n}},$$

so we obtain

$$x^p \equiv x \pmod{p^{3n}}, \qquad y^p \equiv y \pmod{p^{3n}}.$$

Noticing that

$$z = (r^{p^n} + s^{p^n} - p^{mp^n-n}t^{p^n})/2 \equiv 0 \pmod{p^{3n}},$$

we also have

$$z^p \equiv z \pmod{p^{3n}}.$$

That completes the proof of the theorem.

**References**

[1] T. Azuhata, *On Fermat's Last Theorem*, Acta Arith. 45 (1985), 19–27.
[2] K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. Ser. AI, 1946, No. 33, 60 pages.
[3] —, *Abschätzungen für eventuelle Lösungen der Gleichung in Fermatschen Problem*, Ann. Univ. Turku, Ser. A 1 (1953), 3–9.
[4] K. Inkeri and A. J. van der Poorten, *Some remarks on Fermat's conjecture*, Acta Arith. 36 (1980), 107–111.
[5] M. Moriya, *Über die Fermatsche Vermutung*, J. Reine Angew. Math. 169 (1933), 92–97.
[6] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, 1978, 225–240.
[7] C. C. Stewart, *A note on the Fermat equation*, Mathematika 224 (1977), 130–132.
[8] H. S. Vandiver, *A property of cyclotomic integers and its relation to Fermat's Last Theorem*, Ann. of Math. 21 (1919), 73–80.

MATHEMATICS DEPARTMENT
THE UNIVERSITY OF BRITISH COLUMBIA
121-1984 Mathematics Road
Vancouver, B.C.
Canada, V6T 1Y4

*Received on 2.5.1990*
*and in revised form on 21.8.1990* (2036)

ACTA ARITHMETICA
LIX.1 (1991)

# Arcs containing no three lattice points

by

JAVIER CILLERUELO (Madrid)

**1. Introduction.** In [1], A. Córdoba and myself developed a method to study the location of lattice points on circles centered at the origin. There we proved the following theorem:

THEOREM A. *On a circle of radius R centered at the origin, an arc whose length is not greater than*

$$\sqrt{2}R^{1/2-1/(4[m/2]+2)}$$

*contains at most m lattice points.*

We could not decide whether the exponent

$$\frac{1}{2} - \frac{1}{4[m/2]+2}$$

is sharp for each $m$. In particular, we do not know if the number of lattice points on arcs of length $R^{1/2}$ is bounded uniformly in $R$ or not. Probably it is not.

Obviously, Theorem A is sharp for $m = 1$. The case $m = 2$ was first proved by A. Schinzel and used by Zygmund [2] to prove a Cantor–Lebesgue theorem in two variables.

It is not too hard to prove that the exponent 1/3 cannot be improved.

In this paper we get the best constant $C$, such that an arc of length $CR^{1/3}$ cannot contain three lattice points.

THEOREM 1. (i) *On a circle of radius R centered at the origin, an arc whose length is not greater than* $2\sqrt[3]{2}R^{1/3}$ *contains at most two lattice points.*

(ii) *For every* $\varepsilon > 0$, *there exist infinitely many circles* $x^2+y^2 = R_n^2$ *with arcs of length* $2\sqrt[3]{2}R_n^{1/3}+\varepsilon$ *containing three lattice points.*

**2. Preliminary lemma and notation.** Let us denote by $r(n)$ the number of representations of the integer $n$ as a sum of two squares, i.e. $r(n)$ is the number of lattice points on the circle $x^2+y^2 = n$. Therefore we shall associate lattice points with Gaussian integers: $a^2+b^2 = n$ determines a Gaussian integer

$a+bi=\sqrt{n}e^{2\pi i\Phi}$ for a suitable angle $\Phi$. If
$$n=2^{v}\prod_{p_j\equiv 1\,(4)} p_j^{\alpha_j}\prod_{q_k\equiv 3(4)} q_k^{\beta_k}$$
is the prime factorization of the integer $n$, then $r(n)=0$ unless all the exponents $\beta_k$ are even. In that case we have $r(n)=4\prod(1+\alpha_j)$.

A prime $p_j\equiv 1$ (4) can be represented as a sum of two squares, $p_j=a^2+b^2$, $0<a<b$, in only one way. Then, for each $p_j$, the angle $\Phi_j$, such that $a+bi=\sqrt{p_j}e^{2\pi i\Phi_j}$ is well defined.

With this notation we proved in [1] the following lemma:

LEMMA. *If*
$$n=2^{v}\prod_{p_j\equiv 1\,(4)} p_j^{\alpha_j}\prod_{q_k\equiv 3\,(4)} q_k^{2\beta_k}$$
*then the Gaussian integers corresponding to the* $4\prod(1+\alpha_j)$ *lattice points on the circle* $x^2+y^2=n$ *are given by the formula*
$$\sqrt{n}\exp\{2\pi i(\sum_j \gamma_j\Phi_j+t/4)\}$$
*where* $\Phi_j$ *is the angle corresponding to* $p_j$, $\gamma_j$ *runs over the set* $\{\gamma\in\mathbf{Z};\ |\gamma|\leqslant\alpha_j,\ \gamma\equiv\alpha_j\ (2)\}$, $t$ *takes the values* 0, 1, 2, 3 *and*
$$\Phi_0=\begin{cases}0 & \text{if } v \text{ is even,}\\ 1/8 & \text{if } v \text{ is odd.}\end{cases}$$

**3. Proof of Theorem 1.** (i) Let us suppose that for the integer
$$n_0=2^{v}\prod_{p_j\equiv 1\,(4)} p_j^{\alpha_j}\prod_{q_k\equiv 3\,(4)} q_k^{2\beta_k}$$
there is an arc, on the circle of radius $R_0=\sqrt{n_0}$ centered at the origin, which contains three lattice points and whose length is $2\sqrt[3]{2}R_0^{1/3}$.

The previous lemma implies that the same must be true for the circle of radius $R=\sqrt{n}$ where $n=\prod_{p_j\equiv 1\,(4)}p_j^{\alpha_j}$.

Let $v_1$, $v_2$, $v_3$ be three such lattice points. By the lemma, they have representations of the form
$$\sqrt{n}\exp\{2\pi i(\sum_j \gamma_j^s+t^s/4)\}\qquad (s=1,2,3),$$
$\gamma_j^s\in\{\gamma\in\mathbf{Z};\ |\gamma|\leqslant\alpha_j,\ \gamma\equiv\alpha_j\ (2)\}$, $t^s\in\{0,1,2,3\}$.

For each pair $v_s\neq v_{s'}$ of such points, let us consider the quantity
$$\Psi^{s,s'}=\sum_j\Phi_j\{\gamma_j^s-\gamma_j^{s'}\}+\frac{t^s-t^{s'}}{4}=2\left\{\sum_j\Phi_j\frac{\gamma_j^s-\gamma_j^{s'}}{2}+\frac{t^s-t^{s'}}{8}\right\}$$
and observe that $\gamma_j^{s,s'}=(\gamma_j^s-\gamma_j^{s'})/2$ takes always integer values.



We can write
$$\frac{t^s-t^{s'}}{8}=\frac{\delta(s,s')}{8}+\frac{t^{s,s'}}{4}$$
where $t^{s,s'}$ is an integer and
$$\delta(s,s')=\begin{cases}0 & \text{if } t^s\not\equiv t^{s'}\ (2),\\ 1 & \text{if } t^s\equiv t^{s'}\ (2).\end{cases}$$
Now, the angles $\Psi^{s,s'}/2$ correspond to a representation as a sum of two squares of
$$2^{\delta(s,s')}\prod_j p_j^{|\gamma_j^{s,s'}|}=n_{s,s'}^2+m_{s,s'}^2,\qquad 1\leqslant n_{s,s'}\leqslant m_{s,s'}.$$
Then
$$\frac{\Psi^{s,s'}}{2}=\frac{1}{2\pi}\arctan\frac{n_{s,s'}}{m_{s,s'}}$$
where
$$\arctan\frac{n_{s,s'}}{m_{s,s'}}\geqslant\arctan\frac{1}{m_{s,s'}}>\frac{1}{\sqrt{m_{s,s'}^2+1}}\geqslant\frac{1}{\sqrt{2^{\delta(s,s')}\prod p_j^{|\gamma_j^{s,s'}|}}}.$$
And we have
$$\frac{\Psi^{1,2}}{2}\frac{\Psi^{1,3}}{2}\frac{\Psi^{2,3}}{2}>\frac{1}{(2\pi)^3\sqrt{2^{\delta(1,2)+\delta(1,3)+\delta(2,3)}\prod p_j^{|\gamma_j^{1,2}|+|\gamma_j^{1,3}|+|\gamma_j^{2,3}|}}}.$$
The maximum value of
$$|\gamma_j^{1,2}|+|\gamma_j^{1,3}|+|\gamma_j^{2,3}|=\frac{|\gamma_j^1-\gamma_j^2|}{2}+\frac{|\gamma_j^1-\gamma_j^3|}{2}+\frac{|\gamma_j^2-\gamma_j^3|}{2}$$
is obtained when $\gamma_j^1=\gamma_j^2=\alpha_j$ and $\gamma_j^3=-\alpha_j$. Therefore $|\gamma_j^{1,2}|+|\gamma_j^{1,3}|+|\gamma_j^{2,3}|\leqslant 2\alpha_j$. Also we can observe that $\delta(1,2)+\delta(1,3)+\delta(2,3)\leqslant 2$. Thus we get
$$\Psi^{1,2}\Psi^{1,3}\Psi^{2,3}>1/2\pi^3R^2.$$
On the other hand, if $P_1$, $P_2$, $P_3$ are three points of the interval [0, 1], we have
$$|P_1-P_2|\,|P_1-P_3|\,|P_2-P_3|\leqslant 1/4.$$
This implies that for three lattice points on an arc of length $2\sqrt[3]{2}R^{1/3}$, we have
$$\Psi^{1,2}\Psi^{1,3}\Psi^{2,3}\leqslant\frac{1}{4}\left(\frac{2\sqrt[3]{2}R^{1/3}}{2\pi R}\right)^3=\frac{1}{2\pi^3R^2}$$
and we get a contradiction.

(ii) For each $n$ we consider the circle $x^2+y^2 = R_n^2$ where

$$R_n^2 = 16n^6+4n^4+4n^2+1.$$

We can see that

$$16n^6+4n^4+4n^2+1 = (4n^3-1)^2+(2n^2+2n)^2$$
$$= (4n^3)^2+(2n^2+1)^2 = (4n^3+1)^2+(2n^2-2n)^2.$$

The three lattice points

$$(4n^3-1,\ 2n^2+2n),\quad (4n^3,\ 2n^2+1),\quad (4n^3+1,\ 2n^2-2n)$$

are on an arc of length

$$R_n\left\{\arctan\frac{2n^2+2n}{4n^3-1}-\arctan\frac{2n^2-2n}{4n^3+1}\right\} = R_n\arctan\frac{16n^4+4n^2}{16n^6+4n^4-4n^2-1}$$
$$= 2\sqrt[3]{2}R_n^{1/3}+o(1)$$

and the theorem follows.

**References**


[1] J. Cilleruelo and A. Córdoba, *Trigonometric polynomials and lattice points*, Proc. Amer. Math. Soc., to appear.

[2] A. Zygmund, *A Cantor–Lebesgue theorem for double trigonometric series*, Studia Math. 43 (1972), 173–178.



DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD AUTÓNOMA DE MADRID
28049 Madrid, España



*Received on 17.5.1990*
*and in revised form on 27.7.1990* (2048)



ACTA ARITHMETICA
LIX.1 (1991)


# Sur une classe d'extensions non ramifiées


par

A. Movahhedi (Limoges)


Soient $K$ un corps de nombres, $\theta$ un élément primitif de $K$ sur $\boldsymbol{Q}$: $K = \boldsymbol{Q}(\theta)$. Notons $\varphi$ le polynôme minimal de $\theta$ sur $\boldsymbol{Q}$. Supposons que le corps $L$ de décomposition de $\varphi$ soit une $S_n$-extension (1) de $\boldsymbol{Q}$. Alors Elstrodt, Grunewald et Mennicke [1] ont montré que si le discriminant $D(\varphi)$ du polynôme $\varphi$ est sans facteur carré, la $A_n$-extension (2) $L/\boldsymbol{Q}(\sqrt{D(\varphi)})$ est non ramifiée en toutes les places finies. Yamamura [7] et Osada [4] ont généralisé ce résultat en montrant que la condition "le groupe de Galois $G(L/\boldsymbol{Q})$ est $S_n$" est une conséquence de l'hypothèse "$D(\varphi)$ est sans facteur carré". Enfin Nakagawa [3] a obtenu le même résultat en remplaçant l'hypothèse "$D(\varphi)$ est sans facteur carré" par l'hypothèse moins forte "le discriminant $D_{K/\boldsymbol{Q}}$ de l'extension $K/\boldsymbol{Q}$ est sans facteur carré", en retrouvant ainsi un théorème de Scholz [5] datant de 1937. Notre but est de généraliser ce résultat. Nous remarquons en particulier que, contrairement à ce que pourraient laisser penser les articles cités ci-dessus, le problème de la non-ramification de $L/\boldsymbol{Q}(\sqrt{D(\varphi)})$ est largement indépendant du groupe de Galois de $L/\boldsymbol{Q}$.

L'auteur remercie F. Laubie pour son aide dans la réalisation de ce travail.

Fixons d'abord quelques notations. Soient $k$ un corps de nombres et $K$ une extension finie de $k$ de degré $n$. Soit $\{b_i\}_{1\leqslant i\leqslant n}$ une base de $K/k$. Le discriminant de cette base est un élément non nul de $k$ dont la classe modulo $k^{*2}$ est indépendante du choix de la base choisie. Ceci nous fournit donc une extension quadratique ou triviale $F$ de $k$ contenue dans la clôture normale $L$ de $K$ sur $k$.

Pour un idéal premier $\mathfrak{q}$ de $K$, on écrit $\mathfrak{q} = \mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_g^{e_g}$ la décomposition de $\mathfrak{q}$ en produit de puissance d'idéaux premiers $\mathfrak{p}_i$ de $K$ deux à deux distincts. On note $f_i$ le degré résiduel de $\mathfrak{p}_i$ de sorte qu'on a $n = \sum_{i=1}^{g} e_i f_i$.

Théorème 1. *Supposons $F \neq k$ et $\mathfrak{q}$ ramifié dans $K/k$.*

1) *Dans le cas où $\mathfrak{q}$ ne divise pas 2, pour que l'extension $L/F$ soit non*

(1) Par $S_n$-extension nous entendons une extension galoisienne dont le groupe de Galois est le groupe symétrique $S_n$ de degré $n$.

(2) $A_n$ est le sous-groupe alterné de $S_n$.