HAL
open science

Integral points on circles

A Schinzel, M Skalba

To cite this version:

A Schinzel, M Skalba. Integral points on circles. Hardy-Ramanujan Journal, 2019, Atelier Digit_Hum, pp.140 - 142. 10.46298/hrj.2019.5116 . hal-01986718

HAL Id: hal-01986718

https://hal.science/hal-01986718

Submitted on 19 Jan 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Hardy-Ramanujan Journal 41 (2018), 140-142 submitted 03/10/2018, accepted 23/11/2018, revised 26/11/2018

Integral points on circles

A. Schinzel and M. Skałba

In memory of S. Srinivasan

Abstract. Sixty years ago the first named author gave an example [Sch58] of a circle passing through an arbitrary number of integral points. Now we shall prove: *The number N of integral points on the circle $(x-a)^2+(y-b)^2=r^2$ with radius $r=\frac{1}{n}\sqrt{m}$, where $m,n\in\mathbb{Z}$, $m,n>0$, $\gcd(m,n^2)$ squarefree and $a,b\in\mathbb{Q}$ does not exceed $r(m)/4$, where $r(m)$ is the number of representations of m as the sum of two squares, unless $n|2$ and $n\cdot(a,b)\in\mathbb{Z}^2$; then $N\le r(m)$.*

Keywords. sums of two squares, Gaussian integers

2010 Mathematics Subject Classification. 11D25, 11D09.

Sixty years ago the first named author gave an example [Sch58] of a circle passing through an arbitrary number of integral points. If the center of a circle is not a rational point (i.e. not both coordinates are rational numbers) then it passes through no more than 2 rational points. In fact, the equation of the perpendicular bisector of a segment joining two rational points has rational coefficients, hence the circumcenter of a triangle with rational vertices has to be rational as well. From now on we will consider only circles

$$(x-a)^2+(y-b)^2=r^2, \tag{0.1}$$

with $a,b\in\mathbb{Q}$ and we shall prove

Theorem 0.1. *The number N of integral points on the circle (0.1) with radius $r=\frac{1}{n}\sqrt{m}$, where $m,n\in\mathbb{Z}$, $m,n>0$, $\gcd(m,n^2)$ squarefree does not exceed $r(m)/4$, where $r(m)$ is the number of representations of m as the sum of two squares, unless $n|2$ and $n\cdot(a,b)\in\mathbb{Z}^2$; then $N\le r(m)$.*

Lemma 0.2. *Assume that $\beta,\gamma_1,\gamma_2\in\mathbb{Z}[i]$ and $c\in\mathbb{N}$ satisfy*

$$N(\gamma_1)=N(\gamma_2)=c^2, \tag{0.2}$$

$$\beta\gamma_1\equiv\beta\gamma_2 \pmod{c}, \tag{0.3}$$

$$\text{if a rational prime } t \text{ divides } c \text{ then } t\not|\beta\gamma_1 \text{ and } t\not|\beta\gamma_2. \tag{0.4}$$

Then $\gamma_1\sim\gamma_2$ in $\mathbb{Z}[i]$.

Proof. We assume from the beginning that $\gamma_1\ne\gamma_2$.

1. Case $\gcd(\beta,c)\sim 1$**:** We can divide the congruence (0.3) by β and obtain

$$\gamma_1-\gamma_2=c\delta \quad \text{with } \delta\in\mathbb{Z}[i],\ \delta\ne 0.$$

Further

$$N(\gamma_1)+N(\gamma_2)-\gamma_1\overline{\gamma_2}-\gamma_2\overline{\gamma_1}=c^2N(\delta).$$

If we put $\gamma_1\overline{\gamma_2}=f+gi$ with $f,g\in\mathbb{Z}$ then by equation (0.2) we obtain

$$2f=(2-N(\delta))c^2.$$

We thank episciences.org for providing open access hosting of the electronic journal *Hardy-Ramanujan Journal*

Hence

$$f = \frac{u}{2} \cdot c^2 \quad \text{with } u \in \mathbb{Z},\ u \leq 1.$$

Because

$$f^2 + g^2 = N(\gamma_1 \overline{\gamma_2}) = c^4 \quad \text{by (0.2)}$$

one obtains

$$g^2 = c^4 - f^2 = c^4(1 - \frac{u^2}{4}).$$

It follows $u \in \{-2, -1, 0, 1\}$ but $u \in \{-1, 1\}$ would lead to $g \notin \mathbb{Q}$. Hence $u \in \{0, -2\}$.
If $u = 0$ then $f = 0$, $g = \pm c^2$ hence

$$\gamma_1 \overline{\gamma_2} = \pm c^2 i \quad \text{what gives } \gamma_1 c^2 = \pm c^2 i \gamma_2,$$

and finally $\gamma_1 = \pm i \gamma_2$.
If $u = -2$ then $f = -c^2$,$g = 0$ hence $\gamma_1 \overline{\gamma_2} = -c^2$ and $\gamma_1 = -\gamma_2$.

2. Case $N(\gcd(\beta, c)) = d > 1$**:** We adopt inductive method and assume that the assertion of lemma holds for $N(\gcd(\beta, c)) < d$. Let π be a prime element of the ring $\mathbb{Z}[i]$ satisfying $\pi | \beta$ and $\pi | c$. By condition (0.4) (and (0.2)) $N(\pi) = p$ is a rational prime of the form $4k + 1$.
By (0.2) $\pi | \gamma_1$ or $\overline{\pi} | \gamma_1$, but the latter is excluded by (0.4), hence $\pi^{2l} || \gamma_1$ where $p^l || c$. In the same way $\pi^{2l} || \gamma_2$. Rewrite the initial equality

$$\beta \gamma_1 - \beta \gamma_2 = \delta c \quad \text{with } \delta \in \mathbb{Z}[i], \delta \neq 0$$

in the form

$$\beta \frac{\gamma_1}{\pi^{2l}} - \beta \frac{\gamma_2}{\pi^{2l}} = \frac{\delta \overline{\pi}^{2l}}{p^l} \cdot \frac{c}{p^l}$$

where all fractions are algebraic integers. Using the inductive assumption finishes the proof of lemma.

Proof of Theorem. The considered circle (0.1) is given by the equation

$$(x - a)^2 + (y - b)^2 = \frac{m}{n^2}. \tag{0.5}$$

Put $a = A/C, b = B/C$, where $A, B, C \in \mathbb{Z}$, $C > 0$, $(A, B, C) = 1$. It follows that $n | C$ and hence $C = nc$ with $c \in \mathbb{N}$. The number N of integral points on the circle (0.5) satisfies

$$N = \text{card}\{(x, y) \in \mathbb{Z}^2 | (Cx - A)^2 + (Cy - B)^2 = c^2 m\}.$$

Each solution $(x, y) \in \mathbb{Z}^2$ to the equation

$$(Cx - A)^2 + (Cy - B)^2 = c^2 m \tag{0.6}$$

is encoded by the equality

$$(Cx - A) + (Cy - B)i = \beta \cdot \gamma \tag{0.7}$$

with $\beta, \gamma \in \mathbb{Z}[i]$ and $N(\beta) = m$, $N(\gamma) = c^2$.
Assume now to the contrary that the number of solutions $(x, y) \in \mathbb{Z}^2$ to the equation (0.6) exceeds $r(m)/4$. It follows that there exist $\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{Z}[i]$ satisfying

$$\beta_1 \sim \beta_2,\ N(\beta_1) = N(\beta_2) = m,\ N(\gamma_1) = N(\gamma_2) = c^2,$$

$$\gamma_1 \beta_1 \equiv \gamma_2 \beta_2 \pmod{c} \text{ and } \gamma_1 \beta_1 \neq \gamma_2 \beta_2.$$

Adjusting γ_1, γ_2 for a unit (if necessary) we may assume that there are $\beta, \gamma_1, \gamma_2 \in \mathbb{Z}[i]$ satisfying

$$N(\beta) = m,\ N(\gamma_1) = N(\gamma_2) = c^2,\ \beta \gamma_1 \equiv \beta \gamma_2 \pmod{c},\ \gamma_1 \neq \gamma_2.$$

Now we infer by Lemma that

$$\gamma_2 \in \{-\gamma_1, i\gamma_1, -i\gamma_1\}.$$

((0.4) is fulfilled by the assumption $(A, B, C) = 1$.) In all above cases we get

$$2\beta\gamma_1 \equiv 0 \pmod{c}.$$

For $c > 2$ this contradicts the condition $(A, B, C) = 1$. In case $c = 2$, for any integers A, B and $C \equiv 0 \pmod 2$ the conditions $(A, B, C) = 1$ and

$$(Cx - A)^2 + (Cy - B)^2 = 4m$$

are incompatible. Concluding: $N > r(m)/4$ is possible only for $c = 1$. In case $c = 1$, $C = n$ and by (0.6) one gets $N \leq r(m)$. It remains to deduce $n|2$ from $N > r(m)/4$. It follows from the last inequality that there exist integers x_1, x_2, y_1, y_2 and $k \in \{1, 2, 3\}$ satisfying

$$(nx_2 - A) + (ny_2 - B)i = i^k[(nx_1 - A) + (ny_1 - B)i]$$

hence

$$(1 - i^k)(A + Bi) \equiv 0 \pmod{n}.$$

It follows $n|(2A, 2B)$ and since $(A, B, n) = 1$ we infer that $n|2$.

Remark. The number $1/4$ in our theorem is optimal and here is an example. Let m be of the form $3k + 2$ and satisfying $r(m) > 0$. The equality $m = x^2 + y^2$ implies $x \equiv \pm 1 \pmod 3$, $y \equiv \pm 1 \pmod 3$. It follows that $(x - 1/3)^2 + (y - 1/3)^2 = m/9$ has $r(m)/4$ integer solutions.

References

[Sch58] A. Schinzel, Sur l'existence d'un cercle passant par un nombre donne de points aux coordonnees entieres, *Enseignement Math.* **4** (1958), 71-72; A. Schinzel, *Selecta*, vol.1, 17.

A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Sniadeckich 8
00-656 Warszawa, Poland *e-mail*: schinzel@impan.pl

M. Skałba
Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland *e-mail*: skalba@mimuw.edu.pl