A NUMBER THEORETIC QUESTION ARISING IN THE GEOMETRY OF PLANE CURVES AND IN BILLIARD DYNAMICS

VAN CYR

ABSTRACT. We prove that if $\rho \neq 1/2$ is a rational number between zero and one, then there is no integer $n > 1$ such that

$$n \tan(\pi\rho) = \tan(n\pi\rho).$$

This proves a conjecture due to E. Gutkin which he formulated in connection with mathematical billiards. It also may be viewed as a rigidity result for the circle in the theory of bicycle curves.

1. INTRODUCTION

A famous conjecture of Ulam says that the round ball is the only compact surface that is able to float in a liquid in neutral equilibrium in any orientation. A related problem is to classify which regular infinite cylinders are able to float in equilibrium in any orientation; in this case the relevant question is which convex plane curves can be the cross-section of such a cylinder.

This second problem has recently been studied in two seemingly different contexts: plane geometry and mathematical billiards. In both cases, the classification problem leads naturally to the following number theoretic question: for given $\rho \in (0, 1)$, does there exist an integer $n > 1$ satisfying $n \tan(\pi\rho) = \tan(n\pi\rho)$.

We will briefly describe how this question arises.

1.1. Bicycle Curves.

A closed, convex, unit speed plane curve $\Gamma : S^1 \to \mathbb{R}^2$ of perimeter length 2π is called a *bicycle curve* (of rotation number ρ) if $\|\Gamma(t+\rho)-\Gamma(t)\|$ is constant for all t (see the end note in [6] for a list of papers dealing with bicycle curves). A theorem of Auerbach [1] shows that Γ is a bicycle curve if and only if its image is the cross section of an infinite cylinder that floats in neutral equilibrium in any orientation if and only if it is a bicycle curve (although he does not use this terminology and to the author's knowledge, the connection was first pointed out in [6]).

In attempting to classify the non-circular bicycle curves, Tabachnikov [6] studied conditions under which the circle can be infinitesimally perturbed as a bicycle curve of rotation number ρ. He obtained a theorem [6, Theorem 7] which says that the circle admits a non-trivial infinitesimal deformation as a smooth plane bicycle curve of rotation number ρ if and only if ρ is a root of the equation $n \tan(\pi\rho) = \tan(n\pi\rho)$ for some integer $n \geq 2$. In light of our Theorem 1, the circle is rigid as a bicycle

Date: March 29, 2011.

2010 *Mathematics Subject Classification.* 11R18, 53A04, 37E99.

Key words and phrases. Cyclotomic field, bicycle curve, mathematical billiards.

curve of any rational rotation number (except $\rho = 1/2$ where any curve of constant width is a bicycle curve).

We remark that a similar trigonometric equation was obtained by Tabachnikov to determine the rigidity of the polygonal analog of a bicycle curve (an (n,k)-bicycle polygon: see [6]). In [2], R. Connelly and B. Csikós studied solutions to the equation and were able to classify the first-order flexible bicycle polygons.

1.2. **Mathematical Billiards.** In [3], E. Gutkin studied the billiard map inside the cross section of an infinite cylinder that floats in neutral equilibrium in any orientation. He showed (using Fourier analysis) that if Γ is the boundary of a regular, noncircular billiard table, then a necessary condition for Γ to have a constant angle caustic is that $n\tan(\pi\rho) = \tan(n\pi\rho)$ for some integer $n > 1$ and some $\rho \in \mathbb{R}$.

He further obtained a conditional theorem (which now follows from Theorem 1) that if Γ is a regular billiard table (that is not a curve of constant width) that has a caustic of constant type, then the restriction of the billiard map to this caustic is an irrational rotation.

2. Statement of Results

Our main result is the following.

Theorem 1. *If $\rho \in (0,1) \cap \mathbb{Q} \setminus \{\frac{1}{2}\}$, then there is no integer $n > 1$ such that*

$$n\tan(\pi\rho) = \tan(n\pi\rho).$$

We obtain Theorem 1 as a consequence of the following two lemmas.

Lemma 2. *Suppose $\rho \in (0,1) \setminus \{\frac{1}{2}\}$. If there exists an integer $n > 1$ such that*

$$n\tan(\pi\rho) = \tan(n\pi\rho), \tag{1}$$

then

$$\frac{\sin((n-1)\pi\rho)}{\sin((n+1)\pi\rho)} = \frac{n-1}{n+1}. \tag{2}$$

Lemma 3. *If $\rho \in (0,1) \cap \mathbb{Q} \setminus \{\frac{1}{2}\}$ and $k, m \in \mathbb{Z}$ are such that $\sin(m\pi\rho) \neq 0$, then*

$$\frac{\sin(k\pi\rho)}{\sin(m\pi\rho)}$$

is either -1, 0, 1 or irrational.

Proof of Theorem 1. By Lemma 2, any such n, ρ would have to satisfy (2). Since $n > 1$ we know

$$\frac{n-1}{n+1} \notin \{-1, 0, 1\},$$

and so the pair $k := n-1$, $m := n+1$ would contradict Lemma 3 (that $\sin((n+1)\pi\rho) \neq 0$ follows from (2)). □

3. Proof of Lemma 2

The proof of this lemma is elementary and the result was already known (see [4] for example). We include it only for completeness.

For $z \in \mathbb{C} \setminus \left\{\frac{(2k+1)\pi}{2} : k \in \mathbb{Z}\right\}$,

$$\tan(z) = \frac{i(e^{-iz} - e^{iz})}{e^{-iz} + e^{iz}}.$$

By assumption $|\tan(\pi\rho)| < \infty$, so if n satisfies (1) then $|\tan(n\pi\rho)| < \infty$. So our original equation can be rewritten as

$$n\frac{i(e^{-i\pi\rho} - e^{i\pi\rho})}{e^{-i\pi\rho} + e^{i\pi\rho}} = \frac{i(e^{-in\pi\rho} - e^{in\pi\rho})}{e^{-in\pi\rho} + e^{in\pi\rho}}.$$

This reduces to

$$ni(e^{-i\pi\rho} - e^{i\pi\rho})(e^{-in\pi\rho} + e^{in\pi\rho}) = i(e^{-in\pi\rho} - e^{in\pi\rho})(e^{-i\pi\rho} + e^{i\pi\rho}),$$

which further simplifies to

$$(n-1)\big(e^{-i(n+1)\pi\rho} - e^{i(n+1)\pi\rho}\big) = (n+1)\big(e^{-i(n-1)\pi\rho} - e^{i(n-1)\pi\rho}\big). \tag{3}$$

Since $n > 1$ we know $(n-1)(n+1) \neq 0$, so if $e^{-i(n+1)\pi\rho} - e^{i(n+1)\pi\rho} = 0$ then $e^{-i(n-1)\pi\rho} - e^{i(n-1)\pi\rho} = 0$. But if $e^{-i(n-1)\pi\rho} = e^{i(n-1)\pi\rho}$, then

$$e^{-i(n+1)\pi\rho} = e^{-i(n-1)\pi\rho}e^{-2\pi i\rho} = e^{i(n-1)\pi\rho}e^{-2\pi i\rho} \neq e^{i(n-1)\pi\rho}e^{2\pi i\rho} = e^{i(n+1)\pi\rho}$$

which is a contradiction (here we used $\rho \neq \frac{1}{2}$). So we can divide in (3) to get

$$\frac{n-1}{n+1} = \frac{e^{-i(n-1)\pi\rho} - e^{i(n-1)\pi\rho}}{e^{-i(n+1)\pi\rho} - e^{i(n+1)\pi\rho}} = \frac{\left(\frac{e^{i(n-1)\pi\rho} - e^{-i(n-1)\pi\rho}}{2i}\right)}{\left(\frac{e^{i(n+1)\pi\rho} - e^{-i(n+1)\pi\rho}}{2i}\right)} = \frac{\sin((n-1)\pi\rho)}{\sin((n+1)\pi\rho)}.$$

□

4. Proof of Lemma 3

In this section we set $\omega_n := e^{2\pi i/n}$ to be a primitive n^{th} root of unity and $\mathbb{Q}(\omega_n)$ the n^{th} cyclotomic field. We need the following two well known facts (e.g. [5]):

(1) $|\mathbb{Q}(\omega_n) : \mathbb{Q}| = \phi(n)$ (Euler's ϕ-function);
(2) $\mathbb{Q}(\omega_n) = Span\{1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}\}$.

4.1. **Basic strategy of the proof.** We want to show that if $\rho = \frac{p}{q}$ and $\sin(k\pi\rho) = \lambda\sin(m\pi\rho)$ then $\lambda \in \{-1, 0, 1\}$. Since $\sin(k\pi\rho), \sin(m\pi\rho) \in \mathbb{Q}(\omega_{2q})$, our main tool is the following simple (but useful) observation.

Lemma 4. *Let $\mathcal{B}$ be a basis for a finite dimensional $\mathbb{Q}$-vector space V and suppose $u, v \in V$ are vectors whose coordinates (relative to $\mathcal{B}$) all come from the set $\{-1, 0, 1\}$. If $u = \lambda v$ for some $\lambda \in \mathbb{Q}$, then $\lambda \in \{-1, 0, 1\}$.*

We will prove Lemma 3 by (explicitly) constructing a basis $\mathcal{B}$ for $\mathbb{Q}(\omega_{2q})$ in which, for every integer ℓ, $i\Im(\omega_{2q}^{\ell})$ is of the type described in Lemma 4.

4.2. **Motivating case.** Here we will prove Lemma 3 in the special case that the denominator of ρ is an odd prime (see Corollary 6). This subsection is not necessary to prove Lemma 3, but is included to demonstrate the main idea of the proof.

Lemma 5. *If n is an odd prime and we define*

$$\begin{aligned} A_n &:= \{\ \Re(\omega_n),\ \Re(\omega_n^2), \ldots,\ \Re(\omega_n^{(n-1)/2})\} \\ B_n &:= \{i\Im(\omega_n), i\Im(\omega_n^2), \ldots, i\Im(\omega_n^{(n-1)/2})\}, \end{aligned}$$

then $A_n \cup B_n$ is a basis for $\mathbb{Q}(\omega_n)$ over $\mathbb{Q}$.

Proof. First note that $\omega_n^k \in Span(A_n \cup B_n)$ for every $k = 1, 2, \ldots, n$ (sum the geometric series $\omega_n + \omega_n^2 + \cdots + \omega_n^{n-1} = -1$ to see the $k = n$ case). Next $|A_n \cup B_n| = n - 1 = \phi(n)$ (since n is prime). Any spanning set with $\phi(n)$ elements is a basis. □

Since $|\mathbb{Q}(\omega_{2n}) : \mathbb{Q}(\omega)| = \phi(2n) = \phi(n) = |\mathbb{Q}(\omega_n) : \mathbb{Q}|$, $A_n \cup B_n$ is also a basis for $\mathbb{Q}(\omega_{2n})$ over $\mathbb{Q}$.

Corollary 6 (Lemma 3 for an odd prime). *If n is an odd prime and $k_1, k_2 \in \mathbb{Z}$ are such that $\sin\left(\frac{k_2\pi}{n}\right) \neq 0$, then*

$$\frac{\sin\left(\frac{k_1\pi}{n}\right)}{\sin\left(\frac{k_2\pi}{n}\right)} \tag{4}$$

is either $-1, 0, 1$ or irrational.

Proof. If $\sin\left(\frac{k_1\pi}{n}\right) = 0$, we are done. Otherwise find $0 < \tilde{k}_1 \leq \tilde{k}_2 \leq \frac{n-1}{2}$ such that

$$\begin{aligned} i\sin\left(\frac{k_1\pi}{n}\right) &= \pm i\Im(\omega_{2n}^{\tilde{k}_1}) \\ i\sin\left(\frac{k_2\pi}{n}\right) &= \pm i\Im(\omega_{2n}^{\tilde{k}_2}). \end{aligned}$$

If (4) is a rational number, say $i\Im(\omega_{2n}^{\tilde{k}_1}) = i\lambda\Im(\omega_{2n}^{\tilde{k}_2})$ for some $\lambda \in \mathbb{Q}$, then $\lambda \in \{-1, 0, 1\}$ by Lemma 4 (applied to the basis constructed in Lemma 5). □

4.3. **Prime Powers.** Here we generalize Lemma 5 to the case where the denominator of ρ is a prime power.

Lemma 7. *If $n = p^k$ is an odd prime power and we define (for integers t)*

$$\begin{aligned} A_{p^k} &:= \{\ \Re(\omega_n^t) : 1 \leq t \leq \phi(n)/2\} \\ B_{p^k} &:= \{i\Im(\omega_n^t) : 1 \leq t \leq \phi(n)/2\}, \end{aligned}$$

then $A_n \cup B_n$ is a basis for $\mathbb{Q}(\omega_n)$ over $\mathbb{Q}$. Moreover for any integer t, all coefficients of the vectors $\Re(\omega_n^t)$ and $i\Im(\omega_n^t)$ (with respect to this basis) are contained in the set $\{-1, 0, 1\}$.

Proof. The set $A_n \cup B_n$ contains exactly $\phi(n) = p^{k-1}(p-1)$ many elements so to prove the first claim it suffices to show that $Span\{A_n \cup B_n\} = \mathbb{Q}(\omega_n)$, or simply that $\omega_{p^k}^t \in Span\{A_n \cup B_n\}$ for every integer $t \in [0, p^k - 1]$.

It is immediate that if $1 \leq t \leq \frac{p^{k-1}(p-1)}{2}$, then $\omega_{p^k}^{\pm t} \in Span\{A_n \cup B_n\}$ (recall that $\Re(\omega_n^{-t}) = \Re(\omega_n^t)$ and $\Im(\omega_n^{-t}) = -\Im(\omega_n^t)$). That is, the only integers $t \in [1, p^k - 1]$ for which we have not yet verified that $\omega_{p^k}^t \in Span\{A_n \cup B_n\}$ are those satisfying

$$\frac{p^{k-1}(p-1)}{2} < t < \frac{p^{k-1}(p-1)}{2} + p^{k-1}.$$

If $0 < s < p^{k-1}$, then there is precisely one $r \in [0, (p-1)/2)$ so that

$$t_s := rp^{k-1} + s \in \left(\frac{p^{k-1}(p-1)}{2}, \frac{p^{k-1}(p-1)}{2} + p^{k-1}\right).$$

On the other hand, for any s,

$$\omega_{p^{k+1}}^s + \omega_{p^{k+1}}^{p^{k-1}+s} + \omega_{p^{k+1}}^{2p^{k-1}+s} + \cdots + \omega_{p^{k+1}}^{(p-1)p^{k-1}+s} = 0 \tag{5}$$

(divide both sides by $\omega_{p^{k+1}}^s$ and sum the geometric series). In light of (5) and our previous verification that $\omega_n^t \in Span\{A_n \cup B_n\}$ for every $t \equiv s \pmod{p^{k-1}}$ (except t_s itself), we see $\omega_n^{t_s} \in Span\{A_n \cup B_n\}$. It remains only to see that $1 = \omega_n^0 \in Span\{A_n \cup B_n\}$. This follows because from (5) with $s = 0$ and the observation that $rp^{k-1} \notin \left(\frac{p^{k-1}(p-1)}{2}, \frac{p^{k-1}(p-1)}{2} + p^{k-1}\right)$ for any integer r.

The second claim follows from the previous two paragraphs. □

Lemma 8. *If $n = 2^k$ and we define (for integers t)*

$$\begin{aligned} A_{2^k} &:= \{\ \Re(\omega_n^t) : 0 \le t < 2^{k-2}\} \\ B_{2^k} &:= \{i\Im(\omega_n^t) : 0 < t \le 2^{k-2}\}, \end{aligned}$$

then $A_n \cup B_n$ is a basis for $\mathbb{Q}(\omega_n)$ over $\mathbb{Q}$. Moreover for any integer t, all coefficients of the vectors $\Re(\omega_n^t)$ and $i\Im(\omega_n^t)$ (with respect to this basis) are contained in the set $\{-1, 0, 1\}$.

Proof. As before, the number of elements in $A_{2^k} \cup B_{2^k}$ is $2^{k-1} = \phi(2^k)$ so it suffices to see that $\omega_n^t \in Span(A_{2^k} \cup B_{2^k})$ for every $0 \le t < 2^k$.

It is immediate that $\omega_n^t \in Span(A_{2^k} \cup B_{2^k})$ for $0 \le t \le 2^{k-2}$ (note that $\Re(\omega_n^{2^{k-2}}) = \Im(\omega_n^0) = 0$). This describes the set of all (2^k)-th roots of unity in the positive quadrant in $\mathbb{C}$. The set of all roots of $x^{2^k} - 1$ is symmetric about the real and imaginary axes, so $\omega_n^t \in Span(A_{2^k} \cup B_{2^k})$ for every t.

Again, the second claim is by construction. □

4.4. **General Result.** Finally we are ready to prove Lemma 3 in full generality. We begin with some notation: if $S_1, S_2, \ldots, S_n$ are (nonempty) subsets of $\mathbb{C}$, define

$$S_1 S_2 \cdots S_n := \{\alpha_1 \alpha_2 \cdots \alpha_n \in \mathbb{C} : \alpha_i \in S_i\}.$$

Lemma 9. *If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization of an integer n (for ease of notation, set $q_i := p_i^{e_i}$) and we define, for $1 \le i \le k$ and $0 \le j \le 1$,*

$$D_i^j = \begin{cases} A_{q_i} & \text{if } j = 0 \\ B_{q_i} & \text{if } j = 1 \end{cases}$$

and set

$$D_n := \bigcup_{(j_1, \ldots, j_k) \in \{0,1\}^k} D_1^{j_1} \cdots D_k^{j_k},$$

then D_n is a basis for $\mathbb{Q}(\omega_n)$ over $\mathbb{Q}$. Moreover for any integer t, all coefficients of the vectors $\Re(\omega_n^t)$ and $i\Im(\omega_n^t)$ (with respect to this basis) are contained in the set $\{-1, 0, 1\}$.

Proof. It is immediate that D_n is a basis for $\mathbb{Q}(\omega_n)$, but it remains to see that all coefficients (with respect to the basis D_n) of the vectors $\Re(\omega_n^t)$ and $i\Im(\omega_n^t)$ are in the set $\{-1, 0, 1\}$.

Suppose $0 \le t < n$ and write

$$t = s_1(n/q_1) + s_2(n/q_2) + \cdots + s_k(n/q_k),$$

where $0 \le s_i < q_i$ for $i = 1, 2, \ldots, k$. Then $\omega_n^t = \omega_{q_1}^{s_1} \omega_{q_2}^{s_2} \cdots \omega_{q_k}^{s_k}$. Write

$$\begin{aligned} \Re(\omega_{q_i}^{s_i}) &= \lambda_{i,1} \Re(\omega_{q_i}) + \lambda_{i,2} \Re(\omega_{q_i}^2) + \cdots + \lambda_{i,\phi(q_i)/2} \Re(\omega_{q_i}^{\phi(q_i)/2}) \\ \Im(\omega_{q_i}^{s_i}) &= \mu_{i,1} \Im(\omega_{q_i}) + \mu_{i,2} \Im(\omega_{q_i}^2) + \cdots + \mu_{i,\phi(q_i)/2} \Im(\omega_{q_i}^{\phi(q_i)/2}), \end{aligned}$$

where $\lambda_{i,j}, \mu_{i,j} \in \{-1, 0, 1\}$ (possible by Lemmas 7 and 8). Then $\Re(\omega_n^t)$ and $i\Im(\omega_n^t)$ are both sums of expressions of the form

$$\pm \delta_1 \delta_2 \cdots \delta_k \mathcal{G}_1 \mathcal{G}_2 \cdots \mathcal{G}_k,$$

where $\mathcal{G}_i \in A_{q_i} \cup B_{q_i}$ and $\delta_i \in \{\lambda_{i,1}, \ldots, \lambda_{i,\phi(q_i)/2}, \mu_{i,1}, \ldots, \mu_{i,\phi(q_i)/2}\}$. The result follows. □

Proof of Lemma 3. Let $\rho \in (0,1) \cap \mathbb{Q} \setminus \{\frac{1}{2}\}$ and suppose $k, m \in \mathbb{Z}$ are such that $\sin(m\pi\rho) \neq 0$. If $\sin(k\pi\rho)/\sin(m\pi\rho) = \lambda \in \mathbb{Q}$ then, by Lemmas 4 and 9, $\lambda \in \{-1, 0, 1\}$. $\square$

References

[1] H. Auerbach, *Sur un problem de M. Ulam concernant l'equilibre des corps flottants.* Studia. Math. **7** (1938), 121–142.

[2] R. Connelly and B. Csikós, *Classification of first-order flexible regular bicycle polygons.* Studia Sci. Math. Hungar. **46**, no. 1 (2009), 37–46.

[3] E. Gutkin, *Capillary floating and the billiard ball problem.* (2010) arXiv: 1012.2448.

[4] E. Gutkin, *Billiard tables of constant width and dynamical characterizations of the circle*, Abstract, Penn State Workshop, 1993.

[5] P. Morandi, "Field and Galois Theory." Graduate Texts in Mathematics **167**. Springer-Verlag, New York (1996).

[6] S. Tabachnikov, *Tire track geometry: variations on a theme.* Israel J. Math. **151** (2006), 1–28.

Department of Mathematics, Northwestern University, Evanston, IL 60208 USA
E-mail address: cyr@math.northwestern.edu