On the "Reducibility" of Arctangents of Integers

E. Kowalski

On a number of occasions (see [5], [4]), this Monthly has mentioned a problem originally due to J.C.P Miller concerning relations (with integer coefficients) among numbers of the type $\arctan m$, where $m \geqslant 1$. The best-known instance is

$$\arctan(239) = 4\arctan(5) - 5\arctan(1),$$

which is equivalent to the formula

$$\frac{\pi}{4} = \arctan(1) = 4\arctan\Big(\frac{1}{5}\Big) - \arctan\Big(\frac{1}{239}\Big)$$

used by J. Machin (1706) to compute π. Which integers $m \geqslant 1$ are expressible as sums of values $\arctan k$ with $k < m$? We say that $\arctan m$ (or m itself) is *reducible*[1] if we can write

$$\arctan m = \sum_{j=1}^{k} n_j \arctan m_j \tag{1}$$

with n_j in $\mathbf{Z}$ and $1 \leqslant m_j < m$, and that $\arctan m$ is *irreducible* otherwise.[2]

Todd established the following criterion [5]:

Lemma 1. *Let $m \geqslant 1$ be an integer. Then $\arctan m$ is reducible if and only if all prime divisors p of m^2+1 satisfy $p < 2m$.*

For instance, $239^2+1 = 2\cdot 13^4$. Numbers of the type m^2+1 arise here because $\arctan m = \arg(1+im)$ and $|1+im|^2 = m^2+1$.

The question under consideration is to count reducible (or irreducible) arctangents:

Problem 2. *Let $N(x)$ be the number of integers $m \leqslant x$ such that $\arctan m$ is irreducible. What is the behavior of $N(x)$ as $x \to +\infty$?*

It is easy to show that there are infinitely many reducible arctangents, as well as infinitely many irreducible ones: see [5] for elementary proofs. Moreover, in [5] and elsewhere, the conjecture is made that in fact there is a positive density of irreducible arctangents. To be precise:

Conjecture 3. *$N(x) \sim (\log 2)x$ as $x \to +\infty$.*

This is discussed a bit further in [1] with some numerical and theoretical evidence. In this note we point out the link of Conjecture 3 with the recent very deep work of Duke, Friedlander, and Iwaniec [2] on roots of quadratic congruences modulo primes and give some more support (heuristic and theoretical) for the conjecture, showing also that it is undoubtedly a very hard problem.

The condition $p \mid n^2+1$ that occurs in Lemma 1 means that n is a root of the quadratic congruence $X^2+1 = 0 \pmod p$. We recall Fermat's classical theorem that this congruence has two solutions if $p \equiv 1 \pmod 4$ (if ν is one, the other is $-\nu$), none if $p \equiv 3 \pmod 4$ and one if $p = 2$ (see, for instance, [7] for a proof). If $\nu^2 = -1 \pmod p$, then the *fractional part* $\{\tilde{\nu}/p\}$ of $\tilde{\nu}/p$, where $\tilde{\nu}$ is any integer congruent to ν modulo p, is well-defined in $[0,1]$.

According to the lemma, $\arctan m$ is *irreducible* if and only if there *exists* a prime p such that $p \mid m^2+1$ and $p \geqslant 2m$. This prime p is then unique, since $p \leqslant q$ implies $pq \geqslant 4m^2 > m^2+1$. Thus one can write

$$\begin{aligned} N(x) &= \sum_{1\leqslant m\leqslant x} \sum_{\substack{p\mid m^2+1\\ 2m\leqslant p}} 1 = \sum_{p\leqslant x^2+1} \Big(\sum_{\substack{m\leqslant \min(x,p/2)\\ m^2\equiv -1 \pmod p}} 1\Big) \\ &= \sum_{p\leqslant 2x} \sum_{\substack{m\leqslant p/2\\ m^2\equiv -1 \pmod p}} 1 + \sum_{2x<p\leqslant x^2+1} \sum_{\substack{m\leqslant x\\ m^2\equiv -1 \pmod p}} 1 \\ &= N'(x) + M(x). \end{aligned}$$

[1] In [5], m itself is said to be reducible.

[2] One can show that considering coefficients n_j in $\mathbf{Q}$ would not lead to any new results (see [5]).

For fixed p the sum over m in $N'(x)$ is 1 if $p \equiv 1 \pmod 4$ (or $p = 2$) and 0 otherwise. (Since $m \leqslant p/2$, m is known from its reduction modulo p, namely, as the root $m \leqslant p/2$ of $m^2 + 1 \equiv 0 \pmod p$, if it exists, which is precisely when $p \equiv 1 \pmod 4$ or when $p = 2$.) Thus

$$N'(x) = 1 + \pi(2x; 4, 1) = \frac{x}{\log 2x} + o\Big(\frac{x}{\log x}\Big) \tag{2}$$

as $x \to +\infty$ by the Prime Number Theorem in this arithmetic progression.
As to $M(x)$, we can rewrite it as

$$M(x) = \Big|\Big\{(p, \nu) \mid 2x < p \leqslant x^2 + 1,\ \nu^2 + 1 \equiv 0 \pmod p \text{ and } \Big\{\frac{\nu}{p}\Big\} \leqslant \frac{x}{p}\Big\}\Big|. \tag{3}$$

From this formula it is clear that the estimation of $M(x)$ depends on the distribution of the roots ν of the quadratic congruence $X^2 + 1 = 0 \pmod p$ modulo prime numbers. Duke, Friedlander, and Iwaniec have recently proved that those roots are *equidistributed* in $[0, 1]$ (see [2]):

Theorem 4. *For any real numbers α and β satisfying $0 \leqslant \alpha < \beta \leqslant 1$,*

$$\Big|\Big\{(p, \nu) \mid p \leqslant x,\ \nu^2 + 1 \equiv 0 \pmod p \text{ and } \alpha \leqslant \Big\{\frac{\nu}{p}\Big\} \leqslant \beta\Big\}\Big| \sim (\beta - \alpha)\frac{x}{\log x}$$

as $x \to +\infty$.

Heuristically one is thus led to expect that for a given prime p such that $p \equiv 1 \pmod 4$ the "probability" that ν satisfies the inequality in (3) is x/p, which leads to the expectation that

$$M(x) \approx \sum_{2x < p \leqslant x^2 + 1} \frac{x}{p} \approx x \log \frac{\log(x^2 + 1)}{\log 2x} \approx (\log 2)x,$$

since

$$\sum_{p \leqslant x} \frac{1}{p} = \log\log x + O(1).$$

In (3), however, one of the end points of the interval depends on p and tends to zero as $p \to +\infty$, so Theorem 4 does not apply. We prove the following:

Proposition 5. *For any $\varepsilon > 0$, $N(x) \geqslant \dfrac{(2 - \varepsilon + o(1))x}{\log x}$ as $x \to +\infty$.*

Proof. In view of (2) we have to show that

$$M(x) \geqslant (1 - \varepsilon + o(1))\frac{x}{\log x}$$

as $x \to +\infty$. But for any fixed $A > 2$ and $x > A$ we have

$$M(x) \geqslant \Big|\Big\{(p, \nu) \mid 2x < p < Ax,\ \nu^2 + 1 \equiv 0 \pmod p \text{ and } \Big\{\frac{\nu}{p}\Big\} \leqslant \frac{1}{A}\Big\}\Big|$$

According to the theorem of Duke, Friedlander, and Iwaniec,

$$\begin{aligned}\Big|\Big\{(p, \nu) \mid 2x < p < Ax,\ \nu^2 + 1 \equiv 0 \pmod p \text{ and } \Big\{\frac{\nu}{p}\Big\} \leqslant \frac{1}{A}\Big\}\Big| &\geqslant (1 + o(1))\Big\{\frac{Ax}{A\log Ax} - \frac{2x}{A\log 2x}\Big\} \\ &\geqslant (1 + o(1))\frac{(1 - 2/A)x}{\log x}\end{aligned}$$

as $x \to +\infty$. Taking A sufficiently large, we get the result claimed. □

Obtaining a nontrivial upper bound for $M(x)$ (the trivial bound is $M(x) \leqslant x$), on the other hand, is much more difficult, especially since in (3) one has to consider primes as large as x^2. The proof of Theorem 4 is based on the Weyl criterion for equidistribution and involves two steps: first a sieving part, then an estimate for "Weyl sums" over integers $n \leqslant x$ divisible by a fixed integer d (rather large compared with x) derived from the spectral theory of automorphic forms. For the discrepancy analysis that suggests itself as an approach to (3), the latter part might still be sufficient, but the sieving part would require a considerable strengthening that for the present seems quite difficult. The proof of Theorem 4 is presented in great detail (in French) in the lecture notes [3].

It is quite hard to construct tables of integers m such that $\arctan m$ is irreducible, for the criterion of Lemma 1 (the best known) requires the factoring of $m^2 + 1$.

We also mention that another seemingly unexpected application of the Duke–Friedlander–Iwaniec result is discussed in [6, sec. 7]: it concerns a special case of a generalization of Grothendieck's conjecture

about the link between rational solutions of linear differential equations with rational coefficients and solvability modulo p for almost all p.

References

[1] S. D. Chowla and J. Todd, The density of reducible integers, *Canadian J. Math.* **1** (1949) 297–299.

[2] W. Duke, J. Friedlander, and H. Iwaniec, Equidistribution of roots of a quadratic congruence to prime moduli, *Ann. of Math. (2)* **141** (1995) 423–441.

[3] E. Kowalski, Un cours de théorie analytique des nombres, in preparation, draft of book available on the web at `http://www.math.u-bordeaux.fr/~kowalski/dea/index.html`

[4] O. Taussky, Sums of squares, *Amer. Math. Monthly* **77** (1970) 805–830.

[5] J. Todd, A problem on arc tangent relations, *Amer. Math. Monthly* **56** (1949) 517–528.

[6] M. van der Put, Grothendieck's conjecture for the Risch equation $y' = ay+b$, *Indag. Mathem., N.S.* **12** (2001) 113–124.

[7] D. Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, *Amer. Math. Monthly* **97** (1990) 144.

Université Bordeaux I - A2X, 351, cours de la Libération, 33405 Talence Cedex, France
E-mail address: `emmanuel.kowalski@math.u-bordeaux1.fr`