On a Problem of Ruderman

M. Ram Murty and V. Kumar Murty

Abstract. In 1974, Harry Ruderman proposed the following problem in the problem section of this MONTHLY: if $m > n \geq 0$ are integers such that $2^m - 2^n$ divides $3^m - 3^n$, then show that $2^m - 2^n$ divides $x^m - x^n$ for all natural numbers x. This problem is still open. We prove that there are only finitely many pairs of natural numbers m, n such that $2^m - 2^n$ divides $3^m - 3^n$. Since the proof involves the Schmidt subspace theorem, our bounds on m and n are ineffective. We discuss how an effective version of the *abc* conjecture can be used to derive effective bounds on m and n.

1. INTRODUCTION. In 1974, Harry Ruderman [**12**] proposed Problem E2468 in the problems section of this MONTHLY: Suppose that $m > n \geq 0$ are integers such that $2^m - 2^n$ divides $3^m - 3^n$. Show that $2^m - 2^n$ divides $x^m - x^n$ for all natural numbers x. This problem has remained unsolved for quite a long time and is still unsolved. In 1976, some remarks by W. Vélez [**14**] were published in which he noted that the pairs $(m, n) =$

$$(2, 1), (3, 1), (4, 2), (5, 1), (5, 3), (6, 2), (7, 3), \quad (1)$$
$$(8, 2), (8, 4), (9, 3), (14, 2), (15, 3), (16, 4)$$

had the property that $(2^m - 2^n) \mid (x^m - x^n)$ for all integers $x \geq 1$. To this, we can add $(m, n) = (1, 0)$ to get a total of fourteen such pairs. In his remarks, Vélez [**14**] showed that if we write for $k \geq 2$,

$$2^k - 1 = \prod_{i=1}^{r} p_i^{e_i},$$

with p_i distinct primes, $e_i \geq 1$, and $k = 2^s t$ with t odd, then

$$2^n(2^k - 1) \text{ divides } x^n(x^k - 1), \quad x = 1, 2, 3, \ldots$$

if and only if

(a) $\phi(p_i^{e_i})$ divides k and

(b) $e_i \leq n \leq s + 2$,

for $1 \leq i \leq r$.

A year later, in 1977, some more remarks were published [**6**] and attributed to "The Mod Set Stanford University" and Carl Pomerance (independently). These remarks cited an old paper of Schinzel [**13**] in which he proved that if $k \neq 1, 2, 4, 6, 12$, then $2^k - 1$ has a prime factor $p \geq 2k + 1$. In view of Vélez's theorem stated above, this implies that $m - n$ has only five possible values in the conclusion of Ruderman's problem. Indeed, by Vélez's theorem, any prime divisor p_i of $k = m - n$ must satisfy $p_i - 1$ divides k, so that $p_i \leq k + 1$. But by Schinzel's theorem, there is a prime factor which does not satisfy this inequality for $k \neq 1, 2, 4, 6$, or 12.

doi:10.4169/amer.math.monthly.118.07.644

If we let A be the set of pairs (n, k) such that $2^n(2^k - 1)$ divides $x^n(x^k - 1)$ for all positive integers x, then these remarks show that there are only five possible values for k. Since for $x = 3$, we see that 2^n divides $3^k - 1$, we deduce that n is also bounded. A quick calculation allows us to deduce that (1) gives all such possible pairs (apart from the trivial $(1, 0)$). As in [**6**], if we let B be the set of pairs (n, k) for which $2^n(2^k - 1)$ divides $3^n(3^k - 1)$, then clearly $A \subseteq B$, and Ruderman's problem is to show that $A = B$. The authors in [**6**] comment that a computer search showed there is no pair $(n, k) \in B$ with $13 \leq k \leq 1900$.

The problem resurfaced again in 1981 in Guy's monograph [**5**], where the question of classifying pairs (a, b) such that $(2^a - 2^b)$ divides $(x^a - x^b)$ for all positive integers x is attributed to Selfridge. In 1985, Sun and Zhang [**9**] published a paper answering this question, apparently unaware of the problem's history in this MONTHLY.

In spite of these remarks and results, the original question of Ruderman remains unanswered. Indeed, in the light of the theorems stated above, the following question arises: are there only finitely many pairs (m, n) such that $(2^m - 2^n)$ divides $(3^m - 3^n)$ with $m > n \geq 0$? If so, are they given by (1)?

The purpose of this note is to answer the first question. We invoke a result that makes essential use of Schmidt's subspace theorem, which is ineffective. Consequently, we are unable to answer the second question. We will prove:

Theorem 1. *There are only finitely many pairs (m, n) with $m > n \geq 0$ such that $2^m - 2^n$ divides $3^m - 3^n$.*

The Schmidt subspace theorem is one of the landmark theorems of the 20th century and is a sweeping generalization of Roth's theorem in the theory of Diophantine approximation. We will not discuss the subspace theorem here but refer the reader to [**4**] and [**15**] for an exposition of some remarkable applications of it. We merely record here one of these applications due to Bugeaud, Corvaja, and Zannier [**3**]. To this end, it is convenient to introduce the notation $f(n) \ll g(n)$ to mean that there is a constant C such that $f(n) \leq Cg(n)$. Then the result in [**3**] is: for any $\epsilon > 0$,

$$\gcd(2^n - 1, 3^n - 1) \ll 2^{\epsilon n}, \tag{2}$$

where the implied ineffective constant depends on ϵ. Of course, a similar result is valid with 2 and 3 replaced by two coprime numbers a and b, with the implied constant depending on ϵ, a, and b (see [**3**]).

In the last section, we address the question of effectivity and discuss the role of the abc conjecture in this context.

2. PRELIMINARIES. The following lemma from elementary number theory is a key ingredient in our proof.

Lemma 2. *Let p be an odd prime. If g is a primitive root (mod p^2), then g is a primitive root (mod p^α) for every $\alpha \geq 2$.*

Proof. See p. 102 of [**7**]. ∎

Corollary 3. 2 is a primitive root (mod 3^α) for every $\alpha \geq 1$.

Proof. Since 2 is a primitive root (mod 9), the result follows from the lemma. ∎

3. PROOF OF THE THEOREM. Fix ϵ with $0 < \epsilon < 1$. From the relation

$$2^n(2^{m-n} - 1) \mid 3^n(3^{m-n} - 1),$$

we deduce that $2^{m-n} - 1 = ab$, where $a = 3^r$ (for some $r \geq 0$) and b divides $(3^{m-n} - 1)$. Thus, b divides $\gcd(2^{m-n} - 1, 3^{m-n} - 1)$. By (2), $b \ll 2^{\epsilon(m-n)}$. Consequently,

Q: ran in some equations here to facilitate paging

$$a \gg 2^{(1-\epsilon)(m-n)}.$$

Since $a = 3^r$ and $a \mid (2^{m-n} - 1)$, we deduce

$$2^{m-n} \equiv 1 \pmod{3)^r}.$$

If $m - n$ is sufficiently large, then by Corollary 3, 2 is a primitive root (mod 3^r) and so $\phi(3^r)$ divides $(m - n)$. Since $\phi(3^r) = 2 \cdot 3^{r-1}$ we deduce that

$$2^{(1-\epsilon)(m-n)} \ll a \leq 3(m - n)/2,$$

so that $m - n$ is bounded. Since 2^n divides $(3^{m-n} - 1)$ also, we find n is bounded and consequently, m is bounded. This completes the proof.

4. RELATIONS TO THE *abc* CONJECTURE. For notational convenience, we define the radical of n, denoted $\mathrm{rad}(n)$, to be the product of the distinct prime divisors of n. Now, the abc conjecture is simple to state: for any $\epsilon > 0$, there is a constant $\kappa(\epsilon)$ such that for any mutually coprime A, B, C satisfying $A + B = C$, we have

$$\max(|A|, |B|, |C|) \leq \kappa(\epsilon)(\mathrm{rad}(ABC))^{1+\epsilon}.$$

We refer the reader to [**8**] and [**2**] for the history and status of this conjecture. Effective versions of this conjecture have been suggested by Baker [**1**], inspired by his theory of linear forms in logarithms. Namely, he conjectures that there is an effectively computable absolute constant K such that for any $\eta > 0$,

$$\max(|A|, |B|, |C|) \leq K \left(\prod_{p \mid ABC} p/\eta \right)^{1+\eta}. \tag{3}$$

We remark that setting $\eta = 1$, (3) implies that there are only finitely many triples A, B, C with a given radical satisfying $A + B = C$, and these can be effectively bounded.

It is also evident that if (2) is replaced by

$$\gcd(2^n - 1, 3^n - 1) \ll 2^{\delta n}, \tag{4}$$

for some $\delta < 1$, our proof still works. However, even this weaker result seems to be beyond the reach of elementary methods (see [**3**]). The substantially weaker estimate

$$\gcd(2^n - 1, 3^n - 1) \leq \frac{2^n}{3n}$$

would suffice for our purposes.

An inequality of the form (4) can be deduced from the *abc* conjecture. Since there are effective versions of this conjecture, this opens up the way to prove that the bound in our main theorem can be made effective modulo the *abc* conjecture. Below, we will prove two theorems that suggest how some "weaker results" would lead to an effective resolution of the Ruderman problem.

We first give a mild revision of (3).

Theorem 4. *Let A, B, C be mutually coprime nonzero integers satisfying $A + B = C$. Let $N = \mathrm{rad}(ABC)$ be such that $N > \exp(e^e)$. Assuming conjecture (3), we have*

$$\max(|A|, |B|, |C|) \leq K N^{1+\frac{4 \log\log\log N}{\log\log N}}.$$

Proof. The upper bound in (3) can be rewritten as

$$K N \exp\left(\eta \log N - \omega(N)(1+\eta)\log\eta\right), \tag{5}$$

where $\omega(N)$ is the number of distinct prime factors of N. We can bound $\omega(N)$ using Ramanujan's bound [**10**]: for $N \geq 3$,

$$\omega(N) < \frac{c \log N}{\log\log N}$$

for some absolute constant c. According to Robin [**11**], $c = 1.3841$ is large enough. We now choose

$$\eta = \frac{\log\log\log N}{\log\log N},$$

and proceed to bound (5). Since $N > \exp(e^e)$, we see that $\eta > 0$. If $\eta \geq 1$, then

$$\eta \log N - \omega(N)(1+\eta)\log\eta \leq \eta \log N$$

and we are done. If $\eta < 1$, then

$$\begin{aligned}\eta \log N + \omega(N)(1+\eta)\log\frac{1}{\eta} &\leq \eta \log N + \frac{2c \log N}{\log\log N}\log\log\log N \\ &= \frac{(2c+1)(\log\log\log N)\log N}{\log\log N},\end{aligned}$$

and we are done since $2c + 1 < 4$. ∎

Thus we have the following modification of (3): for any $\epsilon > 0$, there is an effectively computable $K(\epsilon)$ such that if $A + B = C$ with A, B, and C mutually coprime, then

$$\max(|A|, |B|, |C|) < K(\epsilon)\left(\prod_{p|ABC} p\right)^{1+\epsilon}. \tag{6}$$

Indeed, we need only observe that

$$\frac{4 \log\log\log N}{\log\log N} \tag{7}$$

tends to zero as N tends to infinity. Hence there is an $N_0(\epsilon) > \exp(e^e)$ so that for $N = \mathrm{rad}(ABC) \geq N_0(\epsilon)$, (7) is less than ϵ. Consequently, we deduce (6) with $K(\epsilon) = K$ if $N \geq N_0(\epsilon)$. If $N < N_0(\epsilon)$, then by our earlier remark, there are only finitely many triples A, B, C with $A + B = C$ having a given radical, and these can be effectively determined. Hence, by enlarging K to a suitable $K(\epsilon)$, we deduce (6).

Theorem 5. *Assuming the abc conjecture as formulated in* (6), we have for any $\epsilon > 0$,

$$\gcd(2^n - 1, 3^n - 1) \ll 3^{(n/2)(1+\epsilon)},$$

where the implied constant depends effectively on ϵ.

Proof. Let $d = \gcd(2^n - 1, 3^n - 1)$. Writing $2^n - 1 = dU$ and $3^n - 1 = dV$, with $(U, V) = 1$, we have $U(3^n - 1) = V(2^n - 1)$ which leads to the equation

$$U3^n - V2^n = U - V.$$

We apply the *abc* conjecture to this equation, with $A = U3^n$, $B = -V2^n$, and $C = U - V$, noting that all the summands are mutually coprime. Applying the *abc* conjecture with $\epsilon/2$ instead of ϵ, we get

$$U3^n \ll [\mathrm{rad}(UV(U - V))]^{1+\epsilon/2} \leq [U\,\mathrm{rad}(V(U - V))]^{1+\epsilon/2}.$$

After canceling a factor of U from both sides and using the fact that $U \leq dU = 2^n - 1 < 3^n$, we get

$$3^n \ll U^{\epsilon/2}[\mathrm{rad}(V(U - V))]^{1+\epsilon/2} \leq 3^{n\epsilon/2}[\mathrm{rad}(V(U - V))]^{1+\epsilon/2}.$$

Therefore

$$3^{n(1-\epsilon/2)} \ll [\mathrm{rad}(V(U - V))]^{1+\epsilon/2}.$$

Raising both sides of this inequality to the power $1/(1 + \epsilon/2)$, we get

$$\mathrm{rad}(V(U - V)) \gg 3^{n(1-\epsilon/2)/(1+\epsilon/2)} \geq 3^{n(1-\epsilon)}.$$

Now

$$\mathrm{rad}(V(U - V)) = \mathrm{rad}(V)\mathrm{rad}(U - V) \leq V(V - U) \leq V^2.$$

Thus,

$$V^2 \gg 3^{n(1-\epsilon)}.$$

Therefore $V \gg 3^{(n/2)(1-\epsilon)}$. Thus, $3^n \geq dV \gg d\,3^{(n/2)(1-\epsilon)}$, which implies $d \ll 3^{(n/2)(1+\epsilon)}$. ∎

We remark that a similar method can be applied to treat $\gcd(a^n - 1, b^n - 1)$ for a and b coprime integers. Assuming the *abc* conjecture, one can deduce that for $a < b$,

$$\gcd(a^n - 1, b^n - 1) \ll [\max(\sqrt{b}, b/\sqrt{a})]^{n(1+\epsilon)}.$$

If the effective version (3) of the *abc* conjecture is assumed, then the m and n in Theorem 1 are effectively bounded.

One can actually deduce Theorem 1 from a weaker result. Suppose we have that for r sufficiently large, there is a prime p satisfying $p \mid (2^r - 1)$ and $p \nmid (3^r - 1)$. Then one can derive a bound for Ruderman's problem. This too seems to be out of bounds of existing knowledge.

Theorem 6. *Assume the abc conjecture. Then for r sufficiently large, there is a prime p such that* $p \mid (2^r - 1)$ *and* $p \nmid (3^r - 1)$.

Proof. Applying the *abc* conjecture to the equation $(2^r - 1) + 1 = 2^r$, we find

$$\operatorname{rad}(2^r - 1) \gg 2^{(1-\epsilon)r},$$

for any $\epsilon > 0$, with the implied constant depending on ϵ. Now suppose that for every prime $p \mid (2^r - 1)$, we have $p \mid (3^r - 1)$. Then $\operatorname{rad}(2^r - 1) \mid (3^r - 1)$. Hence

$$\gcd(2^r - 1, 3^r - 1) \geq \operatorname{rad}(2^r - 1) \gg 2^{(1-\epsilon)r}.$$

But by (2), we have that the gcd is bounded by $2^{\epsilon r}$. Since we may take any ϵ positive, we choose $\epsilon < 1/2$ to derive a bound on r. Thus, for sufficiently large r, there is a prime p such that $p|(2^r - 1)$ and $p \nmid (3^r - 1)$. ∎

If one could establish an effective version of this theorem, then the Ruderman problem could be resolved effectively. It is clear that (3) would imply an effective version of the previous theorem.

ACKNOWLEDGMENTS. We thank the referees for their helpful comments on an earlier version of this paper. Research of both authors was partially supported by NSERC Discovery grants.

REFERENCES

1. A. Baker, Logarithmic forms and the *abc* conjecture, in *Number Theory: Diophantine, Computational and Algebraic Aspects, Eger—1996*, K. Győry, A. Pethö, and V. T. Sós, Proc. Intl. Conf., de Grutyer, Berlin, 1998, 37–44.
2. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, Cambridge, 2006.
3. Y. Bugeaud, P. Corvaja, and U. Zannier, An upper bound for the GCD of $a^n - 1$ and $b^n - 1$, *Math. Z.*, no. 1, **243** (2003) 79–84. doi:10.1007/s00209-002-0449-z
4. P. Corvaja and U. Zannier, Some new applications of the subspace theorem, *Compos. Math.* **131** (2002) 319–340. doi:10.1023/A:1015594913393
5. R. K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer-Verlag, New York, 1994.
6. The Mod Set Stanford University and C. Pomerance, Remarks on #2468, *Amer. Math. Monthly* **84** (1977) 59–60. doi:10.2307/2318318
7. I. Niven, H. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley, New York, 1991.
8. J. Oesterlé, Nouvelles approches du "théorème" de Fermat, Séminaire Bourbaki, vol. 1987/88, Exp. No. 694, *Astérisque* **161–162** (1988) 165–186.
9. Q. Sun and M. Z. Zhang, Pairs where $2^a - 2^b$ divides $n^a - n^b$ for all n, *Proc. Amer. Math. Soc.* **93** (1985) 218–220. doi:10.1090/S0002-9939-1985-0770523-6
10. S. Ramanujan, Highly composite numbers, *Proc, London Math. Soc. Ser. 2* **14** (1915) 347–400; reprinted in *Collected Papers of Srinivasa Ramanujan*, G. H. Hardy, P. V. Seshu Aiyar, and B. M. Wilson, eds., AMS Chelsea, Providence, RI, 1962.
11. G. Robin, Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n, *Acta Arith.* **42** (1983) 367–389.
12. H. Ruderman, Problem E2468, *Amer. Math. Monthly* **81** (1974) 405. doi:10.2307/2319015
13. A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Camb. Phil. Soc.* **58** (1962) 555–562. doi:10.1017/S0305004100040561

14. W. Y. Vélez, Remarks on E 2468, *Amer. Math. Monthly* **83** (1976) 288–289. doi:10.2307/2318231
15. U. Zannier, *Some Applications of Diophantine Approximation to Diophantine Equations*, Forum Editrice Universitaria Udinese, Udine, Italy, 2003; available at http://www.forumeditrice.it/percorsi/scienza-e-tecnica/varsia/some-applications-of-diophantine-approximation-to-diophantine-equations.

Department of Mathematics, Queen's University, Kingston, Ontario, K7L 3N6, Canada
murty@mast.queensu.ca

Department of Mathematics, University of Toronto, Toronto, Ontario, M5S 2E4, Canada
murty@math.toronto.edu

Cyclic Absolute Differences of Integers

Alan F. Beardon

Abstract. We give an elementary proof of the convergence, or nonconvergence, to zero in the "four numbers game."

1. INTRODUCTION. Let $(a_1, \ldots, a_n)$ be a sequence of integers, where $n \geq 2$, and let θ be the map

$$\theta : (a_1, \ldots, a_n) \mapsto (|a_1 - a_2|, \ldots, |a_{n-1} - a_n|, |a_n - a_1|).$$

The problem (attributed to Enrico Ducci in the late 1800s) is to discuss the iteration of θ. It is clear that, after one or more applications of θ, each term in the sequence will be nonnegative, and that, after the first application of θ, $\max\{a_1, \ldots, a_n\}$ will not increase when we apply θ. These facts imply that, regardless of the initial sequence, repeated applications of θ will eventually produce a periodic list of sequences. Beyond this the following result is well known.

Theorem 1. *Every sequence* $(a_1, \ldots, a_n)$ *eventually maps to* $(0, \ldots, 0)$ *under repeated applications of* θ *if and only if* $n = 2^m$ *for some integer* m.

The problem has a long history (see, for example, [**1**], [**2**], [**4**], [**5**], [**6**], and [**7**]), and the first proof of Theorem 1 seems to have appeared in 1937 [**3**]. The usual proofs of Theorem 1 involve expanding a sum of matrices by the binomial theorem over the field $\mathbb{Z}_2$, or using polynomial rings. However, since the problem can be understood by people with only a minimal background in mathematics, it seems desirable to have a proof of Theorem 1 that is completely elementary, and significantly less demanding than the usual proofs. The sole purpose of this article is to provide such a proof. The ideas that we use are in the literature but not, as far as we know, collected together in this way. In particular, the argument in Section 2 occurs briefly, and in a different context, in [**6**] but, for completeness, we include the argument here.

We write $\mathbf{a} = (a_1, \ldots, a_n)$, and so on, and $\mathbf{0} = (0, \ldots, 0)$. All sequences in this paper will be assumed to have nonnegative integral components, and the sequence $\mathbf{a}$

doi:10.4169/amer.math.monthly.118.07.650