On a variation of a congruence of Subbarao

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
duje@math.hr

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

December 17, 2010

To the memory of Alf van der Poorten

Abstract

Here, we study positive integers n such that $n\phi(n) \equiv 2 \pmod{\sigma(n)}$, where $\phi(n)$ and $\sigma(n)$ are the Euler function and the sum of divisors function of the positive integer n, respectively. We give a general ineffective result showing that there are only finitely many such n whose prime factors belong to a fixed finite set. When this finite set consists only of the two primes 2 and 3 we use continued fractions to find all such positive integers n.

1 Introduction

We write $\phi(n)$ and $\sigma(n)$ for the Euler function and the sum of divisors function of the positive integer n, respectively. There are many open problems concerning the characterization of the positive integers n fulfilling certain congruences involving $\phi(n)$ and $\sigma(n)$. For example, a known open problem due to Lehmer asks if there are any composite integers n such that $n \equiv 1 \pmod{\phi(n)}$ (see [7]). A different problem due to Subbarao concerns finding composite integers n such that $n\sigma(n) \equiv 2 \pmod{\phi(n)}$ (see [9]). See also section **B37** in [4] for other problems and results of a similar kind.

In this paper, we study a congruence similar to Subbarao's congruence, namely

$$n\phi(n) \equiv 2 \pmod{\sigma(n)}. \tag{1}$$

Congruence (1) was recently proposed and investigated by Díaz in [3]. It is easy to see that prime numbers n satisfy (1). In [3], it was shown that the only positive integers n which are prime powers of exponent $a \geq 1$ satisfying (1) are $n = 8,\ 9$. It was also shown that if n is a composite integer satisfying (1) and if we put

$$k := \frac{n\phi(n) - 2}{\sigma(n)},$$

then n can be bounded in terms of k. This follows from the minimal order $\phi(n) \gg n/\log\log n$ of the Euler function, as well as the maximal order $\sigma(n) \ll n\log\log n$ of the sum of divisors function, which together imply that

$$k = \frac{n\phi(n) - 2}{\sigma(n)} \gg \frac{n\phi(n)}{\sigma(n)} \gg \frac{n}{(\log\log n)^2},$$

yielding that $n \ll k(\log\log k)^2$.

Here, we prove two results about congruence (1). First, we let $\mathcal{P} = \{p_1, \ldots, p_k\}$ be a finite set of primes and let $\mathcal{S}_{\mathcal{P}} = \{p_1^{a_1} \cdots p_k^{a_k} \ :\ a_i \geq 0\}$ be the set of all positive integers whose prime factors belong to $\mathcal{P}$. Our first result is the following:

Theorem 1 *For any finite set of primes $\mathcal{P}$ there are only finitely many positive integers $n \in \mathcal{S}_{\mathcal{P}}$ satisfying congruence (1).*

For a positive integer n let $P(n)$ be the largest prime factor of n. Theorem 1 has the following immediate corollary.

Corollary 1 *We have $P(n) \to \infty$ as n goes to infinity through solutions of congruence (1).*

The proof of Theorem 1 uses a result of Hernández and Luca [6] whose proof uses Schmidt's Subspace Theorem and finiteness results about the number of non-degenerate solutions to $\mathcal{S}$–unit equations. As such, it is ineffective. That is, given $\mathcal{P}$, we do not know how to write down a specific upper bound depending on $\mathcal{P}$ on the largest solution $n \in \mathcal{S}_{\mathcal{P}}$ of congruence (1). Our next result is an effective version of Theorem 1 when $\mathcal{P} = \{2, 3\}$. Quite likely, our method of proof extends to all sets $\mathcal{P}$ consisting of only two primes but we have not worked out the details of such an extension.

Theorem 2 *If $\mathcal{P} = \{2, 3\}$, then the only $n \in \mathcal{S}_{\mathcal{P}}$ satisfying congruence* (1) *are $n = 1, 2, 3, 8, 9$.*

2 The proof of Theorem 1

Let us comment on the situation when $n = p^a$ for some $a \geq 2$. Put $D := \sigma(p^a) = (p^{a+1} - 1)/(p - 1)$. Then $p^{a+1} \equiv 1 \pmod D$. But also $n\phi(n) \equiv 2 \pmod D$, or $p^{2a-1}(p-1) \equiv 2 \pmod D$. Hence, $p^{2(a+1)}(p-1) \equiv 2p^3 \pmod D$. Using also $p^{a+1} \equiv 1 \pmod D$, we get that $2p^3 \equiv p - 1 \pmod D$. Thus, $D \mid 2p^3 - p + 1$. The expression $2p^3 - p + 1$ is never 0 when p is a prime, so $D \leq 2p^3 - p + 1$. Thus,

$$p^{a+1} - 1 \leq (p-1)(2p^3 - p + 1).$$

If $a \geq 4$, we then get that $p^5 - 1 \leq p^{a+1} - 1 \leq (p-1)(2p^3 - p + 1)$, which is impossible for $p \geq 2$. Thus, $a \in \{2, 3\}$. If $a = 2$, we then get $p^2 + p + 1 \mid 2p^3 - p + 1$, which leads to $p^2 + p + 1 \mid p - 3$. This is possible only when $p = 3$, which gives the solution $n = 9$. If $a = 3$, we then get $p^3 + p^2 + p + 1 \mid 2p^3 - p + 1$, which leads to $p^3 + p^2 + p + 1 \mid 2p^2 + 3p + 1$. Thus, $p^3 \leq p^2 + 2p$, so $p \leq 2$. This leads to the solution $n = 8$ to congruence (1).

Now let $\mathcal{P} = \{p_1, \ldots, p_k\}$. We assume that $p_1 < p_2 < \cdots < p_k$. There is no loss of generality in assuming that $\mathcal{P}$ consists of all primes $p \leq p_k$. Hence, p_j is just the jth prime number. Now say $n = p_{i_1}^{a_1} \cdots p_{i_s}^{a_s} \in \mathcal{S}_{\mathcal{P}}$ satisfies congruence (1), where $1 \leq i_1 < \cdots < i_s \leq k$ and a_j are positive for $j = 1, \ldots, s$. There is no loss of generality in assuming that $s \geq 2$. Put $u_j := p_{i_j}^{a_j+1}$ for $j = 1, \ldots, s$ and put $v := n\phi(n)/2 = p_{i_1}^{2a_1-1} \cdots p_s^{2a_s-1}(p_{i_1} - 1) \cdots (p_{i_s} - 1)/2$. Observe that u_j and v are all members of $\mathcal{S}_{\mathcal{P}}$ for $j = 1, \ldots, s$. Moreover, u_j and v are multiplicatively independent because u_j is a prime power and v has at least two distinct prime factors, namely p_{i_1} and p_{i_2}. Let j be such that $u_j = \max\{u_t \ : \ 1 \leq t \leq s\}$. We may assume that

$a_j \geq 3$, otherwise $u_t \leq p_k^3$, for all $i = 1, \ldots, s$, so we have only finitely many possibilities for n. Then

$$v < p_{i_1}^{2a_1} \cdots p_{i_s}^{2a_s} < u_1^2 \cdots u_s^2 < u_j^{2k},$$

giving that $u_j > v^{1/2k}$. Since $(u_j - 1)/(p_{i_j} - 1)$ divides $2(v-1)$, it follows that

$$\gcd(u_j - 1, v - 1) \geq \frac{u_j - 1}{2(p_{i_j} - 1)} > u_j^{1/2} > v^{1/4k},$$

where we used the fact that $a_j \geq 3$. However, a result of Hernández and Luca from [6] asserts that if $\varepsilon > 0$ is fixed, then there are only finitely many pairs of elements (u, v) in $\mathcal{S}_{\mathcal{P}}$ such that

$$\gcd(u - 1, v - 1) < \max\{u, v\}^{\varepsilon},$$

and such that u and v are multiplicatively independent. Note that $u_j < v$ for $a_j \geq 3$. Since we have already established that u_j and v are multiplicatively independent, the above result applied with $\varepsilon := 1/4k$ gives us only finitely many possibilities for v. Hence, only finitely many possibilities for $n\phi(n)$, and in particular for n, which is what we wanted to prove. The theorem is therefore proved.

3 Proof of Theorem 2

We assume that $n = 2^a 3^b$, where a and b are positive integers. Let $M := 2^{a+1} - 1$, $N := (3^{b+1} - 1)/2$. Then $2^{a+1} \equiv 1 \pmod{M}$ and $3^{b+1} \equiv 1 \pmod{N}$. But we also have $n\phi(n) \equiv 2 \pmod{MN}$, which gives $2^{2a}3^{2b-1} \equiv 2 \pmod{MN}$. Thus, $2^{2(a+1)}3^{2(b+1)} \equiv 216 \pmod{MN}$. Since $2^{a+1} \equiv 1 \pmod{M}$, we get that $3^{2(b+1)} \equiv 216 \pmod{M}$. Also, since $3^{b+1} \equiv 1 \pmod{N}$, we get that $2^{2(a+1)} \equiv 216 \pmod{N}$. Since M divides $2^{2(a+1)} - 1$ and N divides $3^{2(b+1)} - 1$, we get that both M and N divide

$$2^{2(a+1)} + 3^{2(b+1)} - 217.$$

Let us now show that a and b are both even and that M and N are coprime. Let $D := \gcd(M, N)$. Then $2^{a+1} \equiv 3^{b+1} \equiv 1 \pmod{D}$, so D divides $1 + 1 - 217 = -215 = -5 \times 43$. But if 5 divides M, then $4 \mid a+1$, so, in particular, $2 \mid a+1$, which implies that $3 \mid M$. This leads to $3 \mid n\phi(n) - 2 = 2^{2a}3^{2b-1} - 1$, which is false. Hence, D cannot be a multiple of 5 and $a+1$ is odd, therefore a is even. If 43 divides M, then $2^{a+1} \equiv 1 \pmod{43}$, which implies again that $a+1$ is even, which is a contradiction. Hence, M and N are coprime and a is even. Let us show that b is also even. If not, then $b+1$ is even, so $3^{b+1}-1$ is a multiple of 8. Thus, $4 \mid N \mid 2^{2a}3^{2b-1}-2$, which is impossible. Hence, $b+1$ is odd and therefore both M and N are odd. Since MN divides $2^{2(a+1)}+3^{2(b+1)}-217$ and this last number is even, we get that this last number is a multiple of $2MN=(2^{a+1}-1)(3^{b+1}-1)$. Let $x:=2^{a+1}$ and $y:=3^{b+1}$. We get the equation

$$x^2+y^2-217=c(x-1)(y-1) \tag{2}$$

with some positive integer c. Since a and b are even, we have the following congruences: $x\equiv 0 \pmod 8$, $y\equiv 3 \pmod 8$, $y^2\equiv 9 \pmod{16}$, $x\equiv 2 \pmod 3$, $x^2\equiv 1 \pmod 3$, $y\equiv 0 \pmod 3$. Using these congruences, from (2), we conclude that $c\equiv 0 \pmod 8$ and $c\equiv 0 \pmod 3$; i.e., $c\equiv 0 \pmod{24}$.

We shall next "diagonalize" the equation (2). Namely, let

$$X:=cy-c-2x, \tag{3}$$

$$Y:=cy-c-2y. \tag{4}$$

Then

$$(c+2)Y^2-(c-2)X^2-(-860c+1736)=-4(c-2)(x^2+y^2-217-c(x-1)(y-1))=0.$$

Hence, we get the Pellian equation

$$(c+2)Y^2-(c-2)X^2=-860c+1736. \tag{5}$$

From (5), we see that X/Y is good rational approximation of the irrational number $\sqrt{\frac{c+2}{c-2}}$. More precisely, we have

$$\left|\frac{X}{Y}-\sqrt{\frac{c+2}{c-2}}\right|=\frac{860c-1736}{(\sqrt{c+2}Y+\sqrt{c-2}X)\sqrt{c-2}Y}\le\frac{860(c-2)}{\sqrt{c^2-4}Y^2}<\frac{860}{Y^2}.$$

The rational approximation of the form

$$\left|\frac{X}{Y}-\sqrt{\frac{c+2}{c-2}}\right|<\frac{860}{Y^2} \tag{6}$$

is not good enough to conclude that $\frac{X}{Y}$ is a convergent of continued fraction expansion of $\sqrt{\frac{c+2}{c-2}}$, but by Worley's theorem [10, Theorem 1] (see also [1, Theorem 1]), we know that

$$\frac{X}{Y}=\frac{rp_{k+1}\pm up_k}{rq_{k+1}\pm uq_k},$$

for some $k \geq -1$ and nonnegative integers r and u such that $ru < 2 \times 860 = 1720$. Since c is even, we have the following continued fraction expansion

$$\sqrt{\frac{c+2}{c-2}} = [1, \overline{(c-2)/2,\, 2}]$$

(see e.g. [5]). Let $X = d(rp_{k+1} \pm up_k)$, $Y = d(rq_{k+1} \pm uq_k)$, where $d^2ru < 1720$. Then, by [2, Lemma], we have

$$(c+2)Y^2 - (c-2)X^2 = d^2(-1)^k(u^2t_{k+1} + 2rus_{k+1} - r^2t_{k+2}), \qquad (7)$$

where $\{s_k\}_{k\geq -1}$ and $\{t_k\}_{k\geq -1}$ are sequences of integers appearing in the continued fraction algorithm for quadratic irrational $\sqrt{\frac{c+2}{c-2}}$. From [5], we learn that $s_k = c-2$, $t_{2k} = c-2$, $t_{2k+1} = 4$. Let us check whether it is possible that the expression on the right hand side of (7) is identically equal to the right hand side of (5); i.e., to $-860c+1736$. For k even, we get $d^2((4u^2-2ru+2r^2)+c(2ruc-r^2))$, while for k odd, we get $-d^2(c(u^2+2ru)-(4r^2+4ru+2u^2))$. Comparing these two expression with $-860c+1736$, we first see that $d=1$ or $d=2$, and then that in both cases the resulting system of two equations has no integers solutions.

It remains to consider all possible triples of integers d, r, u satisfying $d^2ru < 1720$, and check whether the corresponding right–hand sides of (7) have nonempty integer intersection with $-860c+1736$, and lastly compute the corresponding positive integer c. There are many such c's (the largest is 739586), but only three of them satisfy the condition $c \equiv 0 \pmod{24}$. These c's are 48, 288 and 23328.

Let us solve the corresponding three Pellian equations. The equations are:

$$\begin{aligned} 25Y^2 - 23X^2 &= -19772, &(8)\\ 145Y^2 - 143X^2 &= -122972, &(9)\\ 11665Y^2 - 11663X^2 &= -10030172. &(10)\end{aligned}$$

Using bounds for the fundamental solutions of Pellian equations (see e.g. [8]), we find that all solutions of equation (8) are given by $(X_0, X_1) = (58, 192)$ or $(192, 58)$, $X_k = 48X_{k-1} - X_{k-2}$ for all $k \geq 2$ and $(Y_0, Y_1) = (48, 182)$ or $(182, 48)$, $Y_k = 48Y_{k-1} - Y_{k-2}$ for all $k \geq 2$. Assume now that for X, Y defined by (3) and (4) there exists an index k such that $X = X_k$ and $Y = Y_k$. Then $(X, Y) \equiv (10, 0), (0, 38), (0, 10)$ or $(38, 0) \pmod{48}$. But on the other hand, $X \equiv 0 \pmod{16}$, $Y \equiv 0 \pmod{6}$, and none of these four pairs satisfies this condition.

Completely analogous arguments apply to other two equations, since both other c's are also divisible by 24. The fundamental solutions of (9) are $(X_0, X_1) = (38, 1992)$, $(Y_0, Y_1) = (24, 1978)$, and we get $(X, Y) \equiv (14, 0)$, $(0, 10), (0, 14)$ or $(10, 0) \pmod{24}$, while the fundamental solutions of (10) are $(X_0, X_1) = (218, 23112)$, $(Y_0, Y_1) = (216, 23110)$, and we get $(X, Y) \equiv (2, 0), (0, 22), (0, 2)$ or $(22, 0) \pmod{24}$. In both cases, none of the pairs modulo 24 satisfies the conditions $X \equiv 0 \pmod{16}$, $Y \equiv 0 \pmod{6}$. This completes the proof of Theorem 2.

References

[1] A. Dujella, Continued fractions and RSA with small secret exponents, *Tatra Mt. Math. Publ.* **29** (2004), 101–112.

[2] A. Dujella and B. Jadrijević, A family of quartic Thue inequalities, *Acta Arith.* **111** (2004), 61–76.

[3] M. Díaz, Two variations of Subbarao's problem, *Preprint*, 2010.

[4] R. Guy, Unsolved problems in Number Theory, Springer-Verlag New York, Second Edition, 1994.

[5] B. He, B. Jadrijevic and A. Togbé, Solutions of a class of quartic Thue inequalities, *Glas. Mat. Ser. III* **44** (2009), 309–321.

[6] S. H. Hernández and F. Luca, On the largest prime factor of $(ab + 1)(ac + 1)(bc + 1)$, *Bol. Soc. Math. Mexicana* **9** (2003), 235–244.

[7] D. H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.* **38** (1932), 745–751.

[8] T. Nagell, Introduction to Number Theory, Almqvist, Stockholm; Wiley, New York, 1951.

[9] M. V. Subbarao, On two congruences for primality, *Pacific J. Math.* **52** (1974), 261–268.

[10] R. T. Worley, Estimating $|\alpha - p/q|$, *J. Austral. Math. Soc. Ser. A* **31** (1981), 202–206.