A Variation of a Congruence of Subbarao for $n = 2^{\alpha}5^{\beta},\ \alpha \geq 0, \beta \geq 0$

29th Journées Arithmétiques JA 2015
Debrecen, Hungary

Sanda Bujačić[1]

[1]Department of Mathematics
University of Rijeka, Croatia

Simple Characterization of Prime Numbers

- Wilson's theorem is a well known characterization of prime numbers.
- There is probably no other characterization of prime numbers in the form of a congruence simple as Wilson's theorem, but there are many open problems concerning the characterization of positive integers fulfilling certain congruences and involving functions φ and σ, where $\varphi(n)$ and $\sigma(n)$ stand for the Euler totient function and the sum of positive divisors function of the positive integer n, respectively.

Previous Results

- In 1932 D. H. Lehmer [5] was dealing with the congruence of the form
$$n - 1 \equiv 0 \pmod{\varphi(n)}. \tag{1}$$
- This problem is known as Lehmer's totient problem. Despite the fact that the congruence (1) is satisfied by every prime number, Lehmer's totient problem is an open problem because it is still not known whether there exists a composite number that satisfies it.
- Lehmer proved that, if there exists a composite number that satisfies the congruence (1), then it must be odd, square-free and it must have at least seven distinct prime factors.

Previous Results

- In 1944, F. Schuh [7] improved Lehmer's result and showed that such composite number must have at least eleven distinct prime factors.
- M. V. Subbarao was considering the congruence of the form

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

- He proved [8] that the only composite numbers that satisfy the congruence (2) are numbers $4, 6$ and 22.

Previous Results

- A. Dujella and F. Luca were dealing with the congruence of the form
$$n\varphi(n) \equiv 2 \pmod{\sigma(n)}, \tag{3}$$
which is a variation of the congruence of Subbarao (2).
- They proved [4] that there are only finitely many positive integers that satisfy the congruence (3) and whose prime factors belong to a fixed finite set (ineffective result).

- We deal with the variation of the congruence of Subbarao (3) and try to answer the question which positive integers n of the form
$$n = 2^\alpha 5^\beta,\ \alpha \geq 0,\ \beta \geq 0,$$
satisfy the congruence (3).

- Let $\mathcal{P} = \{p_1, \ldots, p_k\}$ be a finite set of prime numbers and let

  $$\mathcal{S}_{\mathcal{P}} = \{p_1^{a_1} \cdot \cdots \cdot p_k^{a_k} \mid a_i \geq 0,\ i = 1, \ldots, k\}$$

  be the set of all positive integers whose prime factors belong to the set $\mathcal{P}$.

Theorem (B.)

If $\mathcal{P} = \{2, 5\}$, then the only positive integers $n \in \mathcal{S}_{\mathcal{P}}$ that satisfy the congruence (3) are $n = 1, 2, 5, 8$.

Proof for prime numbers

- The congruence (3) is satisfied for all the prime numbers, or more precisely,

$$p(p-1) \equiv 2 \pmod{(p+1)}.$$

  Hence, 2 and 5 satisfy the congruence (3).
- The remaining part of the proof deals with the composite numbers of the form $n = 2^\alpha 5^\beta, \ \alpha \geq 0, \ \beta \geq 0$.

Proof for $n = 2^\alpha, \ \ \alpha \geq 2$

- Let $\beta = 0$ which implies dealing with the positive integers of the form $n = 2^\alpha, \ \ \alpha \geq 2$.
- We define
$$D := \sigma(2^\alpha) = 2^{\alpha+1} - 1.$$
- Because of the congruence (3), we obtain
$$2^\alpha \cdot 2^\alpha \left(1 - \frac{1}{2}\right) \equiv 2 \pmod{D},$$
$$2^{2(\alpha+1)} \equiv 2^4 \pmod{D},$$
$$(2^{\alpha+1} - 1)(2^{\alpha+1} + 1) - 15 \equiv 0 \pmod{D}.$$

Proof for $n = 2^\alpha, \ \alpha \geq 2$

- The condition

$$D \mid ((2^{\alpha+1} - 1)(2^{\alpha+1} + 1) - 15)$$

  is satisfied if and only if $D \mid 15$, or more precisely, if and only if

$$(2^{\alpha+1} - 1) \mid 15.$$

- For $\alpha \geq 2$, $(2^{\alpha+1} - 1) \mid 15$ is satisfied only when $\alpha = 3$.
- Hence, $n = 2^3$ is the only positive integer of the form $n = 2^\alpha, \ \alpha \geq 2$, that satisfies the variation of congruence of Subbarao (3).

Proof for $n = 5^\beta$, $\beta \geq 2$

- Let $\alpha = 0$, we deal with the positive integers of the form $n = 5^\beta$, $\beta \geq 2$.
- We define

$$D := \sigma(5^\beta) = \frac{5^{\beta+1} - 1}{4}.$$

- Because of (3), we obtain

$$5^{2\beta-1} \cdot 2^2 \equiv 2 \pmod{D},$$

$$5^{2(\beta+1)} \cdot 2^2 \equiv 5^3 \cdot 2 \pmod{D}.$$

Proof for $n = 5^{\beta},\ \ \beta \geq 2$

- Using
$$5^{\beta+1} \equiv 1 \pmod{D},$$
the previous congruence implies
$$D \mid 246,$$
which is not possible for $\beta \geq 2$.
- Consequently, the positive integers of the form $n = 5^{\beta},\ \ \beta \geq 2$, do not satisfy the congruence (3).

Proof for $n = 2^\alpha 5^\beta,\ \alpha \geq 2,\ \beta \geq 2$

- The remaining part of the proof deals with the most general case, or more precisely, with the positive integers of the form

$$n = 2^\alpha 5^\beta,\ \alpha \geq 2,\ \beta \geq 2.$$

- We start by defining $M := 2^{\alpha+1} - 1$ and $N := \frac{5^{\beta+1}-1}{4}$. As in the previous cases, we use congruences

$$2^{\alpha+1} \equiv 1 \pmod{M}$$

and

$$5^{\beta+1} \equiv 1 \pmod{N}.$$

Proof for $n = 2^\alpha 5^\beta,\ \alpha \geq 2,\ \beta \geq 2$

- We get
$$2^{2\alpha+1} \cdot 5^{2\beta-1} \equiv 2 \pmod{MN} \tag{4}$$
from the congruence (3).
- Multiplying (4) by $2 \cdot 5^3$, we can easily obtain
$$2^{2(\alpha+1)} \cdot 5^{2(\beta+1)} \equiv 500 \pmod{MN}.$$

Proof for $n = 2^\alpha 5^\beta,\ \alpha \geq 2,\ \beta \geq 2$

- Since $2^{\alpha+1} \equiv 1 \pmod{M}$, we get that
$$5^{2(\beta+1)} \equiv 500 \pmod{M}.$$
- Analogously, because of $5^{\beta+1} \equiv 1 \pmod{N}$, we conclude
$$2^{2(\alpha+1)} \equiv 500 \pmod{N}.$$
- For $M \mid (2^{\alpha+1} - 1)$, we have
$$M \mid (2^{2(\alpha+1)} - 1).$$
Similarily,
$$N \mid (5^{2(\beta+1)} - 1).$$

Proof for $n = 2^\alpha 5^\beta,\ \alpha \geq 2,\ \beta \geq 2$

- We get
$$M, N \mid (2^{2(\alpha+1)} + 5^{2(\beta+1)} - 501). \tag{5}$$
- Our next step is to show that α and β are even numbers and M and N are coprime.
- Let $G := \gcd(M, N)$, then
$$2^{\alpha+1} \equiv 5^{\beta+1} \equiv 1 \pmod{G}.$$
- Because of (5), we conclude $G \mid -499$.
- Number 499 is a prime number, so $G = 1$ or $G = 499$.

Proof for $n = 2^\alpha 5^\beta,\ \alpha \geq 2,\ \beta \geq 2$

- For start, we can assume $G = 499$. This implies that $499 \mid M$, or, more precisely, $499 \mid (2^{\alpha+1} - 1)$.
- The order of 2 modulo 499 is 166, so $166 \mid (\alpha + 1)$.
- Especially, $2 \mid (\alpha + 1)$. Hence, α is an odd number.

Proof for $n = 2^\alpha 5^\beta,\ \alpha \geq 2,\ \beta \geq 2$

- We can notice that M can be expressed as

$$M = 2^{\alpha+1} - 1 = 2^{2k} - 1,$$

for $k \in \mathbb{N}$.

- Obviously, $3 \mid M$.
- Hence, $3 \mid (n\varphi(n) - 2)$, or, specifically, $3 \mid (2^{2\alpha+1} \cdot 5^{2\beta-1} - 2)$, which is not possible.
- As a consequence, we conclude $499 \nmid M$, so $G = 1$. We have proved that $\alpha + 1$ is an odd number which implies that α is an even number.

Proof for $n = 2^\alpha 5^\beta,\ \alpha \geq 2,\ \beta \geq 2$

- We show that β is an even number, also. On the contrary, we assume that β is an odd number.
- In that case, we write

$$5^{\beta+1} - 1 = 5^{2k} - 1,$$

for $k \in \mathbb{N}$.
- Obviously, $24 \mid (5^{2k} - 1)$, and because of $6 \mid N$ and $N \mid (2^{2\alpha+1} \cdot 5^{2\beta-1} - 2)$, we get $6 \mid (2^{2\alpha+1} \cdot 5^{2\beta-1} - 2)$, which is not possible.
- Hence, β is an even number, which automatically implies that N is an odd number.
- We have proved that M and N are odd and coprime numbers.

α, β are even numbers

- As a consequence of (5), we may notice

$$MN \mid (2^{2(\alpha+1)} + 5^{2(\beta+1)} - 501).$$

- On the other hand, we have

$$4MN = (2^{\alpha+1} - 1)(5^{\beta+1} - 1),$$

and obviously $2^{2(\alpha+1)} + 5^{2(\beta+1)} - 501 \equiv 0 \pmod 4$.

Properties of the number c

Let $x := 2^{\alpha+1}$ and $y := 5^{\beta+1}$. The initial problem is now represented by the equation

$$x^2 + y^2 - 501 = c(x-1)(y-1), \tag{6}$$

for some $c \in \mathbb{N}$.

Properties of the number c

- Since numbers α and β are even, the following congruences hold
$$x \equiv 0 \pmod 8, \;\; x^2 \equiv 0 \pmod 8$$
and
$$y \equiv 5 \pmod 8, \;\; y^2 \equiv 1 \pmod 8.$$
- Using these congruences, from (6), we get $4c \equiv 4 \pmod 8$ which is satisfied for
$$c \equiv 1 \pmod 2. \tag{7}$$

Properties of the number c

- We also notice that congruences

$$x \equiv 2 \pmod 3, \quad x^2 \equiv 1 \pmod 3$$

and

$$y \equiv 2 \pmod 3, \quad y^2 \equiv 1 \pmod 3$$

are satisfied. From (6) we easily get

$$c \equiv 2 \pmod 3. \tag{8}$$

Properties of the number c

- We also conclude that

$$x \equiv 3 \pmod 5, \ x^2 \equiv 4 \pmod 5 \quad \text{for } \alpha \equiv 2 \pmod 4,$$

$$x \equiv 2 \pmod 5, \ x^2 \equiv 4 \pmod 5 \quad \text{for } \alpha \equiv 0 \pmod 4.$$

- Obviously,

$$y \equiv y^2 \equiv 0 \pmod 5.$$

- From (6), we obtain

$$c \equiv 1 \pmod 5, \ \text{for } \alpha \equiv 2 \pmod 4,$$

or

$$c \equiv 2 \pmod 5, \ \text{for } \alpha \equiv 0 \pmod 4. \tag{9}$$

Properties of the number c

- Let $t = 2^\alpha \cdot 5^{\beta-1}$. We get that

$$5t^2 = 2^{2\alpha} \cdot 5^{2\beta-1}.$$

- According to (4), we conclude $5t^2 \equiv 1 \pmod{M}$, which implies $\left(\frac{5}{M}\right) = \left(\frac{M}{5}\right) = 1$.
- In this case $M \equiv 1, 4 \pmod{5}$.
- Since $M = 2^{\alpha+1} - 1$, we get

$$2^{\alpha+1} - 1 \equiv 1 \pmod{5}$$

or

$$2^{\alpha+1} - 1 \equiv 4 \pmod{5}.$$

Properties of the number c

- The first congruence is satisfied when $\alpha \equiv 0 \pmod 4$, while the second possibility is satisfied when $\alpha \equiv 3 \pmod 4$.
- The second possibility is excluded since we deal with the positive integers α that are even numbers.
- Consequently, we consider only positive integers c that satisfy the congruence
$$c \equiv 2 \pmod 5.$$
- Taking into account congruences (7), (8) and (9) and using Chinese Remainder Theorem, we determine that required positive integers c satisfy

$$c \equiv 17 \pmod{30} \tag{10}$$

Pellian equations

- We "diagonalize" the equation (6) as in [4].
- Let

$$X := cy - c - 2x, \tag{11}$$
$$Y := cy - c - 2y. \tag{12}$$

- Then

$$(c+2)Y^2 - (c-2)X^2 - (-1996c + 4008) =$$
$$= -4(c-2)(x^2 + y^2 - 501 - c(x-1)(y-1)) = 0.$$

- This method has resulted with the Pellian equation of the form

$$(c+2)Y^2 - (c-2)X^2 = -1996c + 4008. \tag{13}$$

Pellian equations

- Let $X = 0$. In this case, the Pellian equation (13) becomes

$$Y^2 = \frac{-1996c + 4008}{c + 2}.$$

- The only integer solution of the above equation is $Y = \pm 2$ for $c = 2$. Since $c = 2$ does not satisfy the congruence (10), in our case Y is not the solution of (13).

Pellian equations

- Let $Y = 0$. The initial Pellian equation (13) is of the form

$$X^2 = \frac{1996c - 4008}{c - 2}.$$

- The right-hand side of the equation is an integer for $c = 1, 3, 4, 6, 10, 18$. Those numbers do not satify the congruence (10). Since none of these numbers is a perfect square, there does not exist a solution X of the Pellian equation (13).

Pellian equations

- Now we deal with the general case.
- Let (X, Y) be a solution of the equation (13) in positive integers.
- In this case, $\frac{X}{Y}$ is a good rational approximation of the irrational number $\sqrt{\frac{c+2}{c-2}}$. More precisely,

$$\left|\frac{X}{Y} - \sqrt{\frac{c+2}{c-2}}\right| = \frac{1996c - 4008}{(\sqrt{c+2}Y + \sqrt{c-2}X)\sqrt{c-2}Y} \leq$$

$$\leq \frac{1996(c-2)}{\sqrt{c^2 - 4Y^2}} < \frac{1996}{Y^2}.$$

Pellian equations

- The rational approximation of the form

$$\left| \frac{X}{Y} - \sqrt{\frac{c+2}{c-2}} \right| < \frac{1996}{Y^2} \tag{14}$$

  is not good enough to conclude that $\frac{X}{Y}$ is a convergent of continued fraction expansion of $\sqrt{\frac{c+2}{c-2}}$.
- We use Worley and Dujella's theorem from [9], or [2].

Pellian equations

Theorem (Worley, Dujella)

Let α be an irrational number and let $a, b \neq 0$ be coprime nonzero integers satisfying the inequality

$$\left|\alpha - \frac{a}{b}\right| < \frac{H}{b^2},$$

where H is a positive real number. Then

$$(a, b) = (rp_{m+1} \pm sp_m, \ \ rq_{m+1} \pm sq_m),$$

for $m, r, s \in \mathbb{N}_0$ such that $rs < 2H$, where $\frac{p_m}{q_m}$ is m–th convergent from continued fraction expansion of irrational number α.

Pellian equations

- According to Worley and Dujella's theorem we get that every solution (X, Y) of the Pellian equation (13) is of the form

$$X = \pm d(rp_{k+1} + up_k), \quad Y = \pm d(rq_{k+1} + uq_k)$$

for some $k \geq -1$, $u \in \mathbb{Z}$, r nonnegative positive integer and $d = \gcd(X, Y)$ for which the inequality

$$|ru| < 2 \cdot \frac{1996}{d^2}$$

holds.

Pellian equations

In order to determine all the integer solutions of the Pellian equation (13), we also use Lemma from [3].

Lemma (Dujella, Jadrijević)

Let $\alpha\beta$ be a positive integer which is not a perfect square and let p_k/q_k be the k-th convergent of continued fraction expansion of $\sqrt{\frac{\alpha}{\beta}}$. Let the sequences $(s_k)_{k\geq -1}$ and $(t_k)_{k\geq -1}$ be the sequences of integers appearing in the continued fraction expansion of $\frac{\sqrt{\alpha\beta}}{\beta}$. Then

$$\alpha(rq_{k+1}+uq_k)^2-\beta(rp_{k+1}+up_k)^2 = (-1)^k(u^2t_{k+1}+2rus_{k+2}-r^2t_{k+2}). \tag{15}$$

Pellian equations

- Applying Lemma 3, it is easy to conclude that we obtain

$$(c+2)Y^2 - (c-2)X^2 = d^2(-1)^k(u^2 t_{k+1} + 2rus_{k+2} - r^2 t_{k+2}), \tag{16}$$

  where $(s_k)_{k\geq -1}$ and $(t_k)_{k\geq -1}$ are sequences of integers appearing in the continued fraction expansion of the quadratic irrationality $\sqrt{\frac{c+2}{c-2}}$.
- Our next step is to determine the continue fraction expansion of $\sqrt{\frac{c+2}{c-2}}$, where c is a positive and odd integer.

Pellian equations

- From the continued fraction expansion, we get

$$\begin{gathered}
s_0 = 0, \ \ t_0 = c - 2, \ \ a_0 = 1, \\
s_1 = c - 2, \ \ t_1 = 4, a_1 = \frac{c-3}{2}, \\
s_2 = c - 4, \ \ t_2 = 2c - 5, \ \ a_2 = 1, \\
s_3 = c - 1, \ \ t_3 = 1, \ \ a_3 = 2c - 2, \\
s_4 = c - 1, \ \ t_4 = 2c - 5, \ \ a_4 = 1, \\
s_5 = c - 4, \ \ t_5 = 4, \ \ a_5 = \frac{c-3}{2}, \\
s_6 = c - 2, \ \ t_6 = c - 2, \ \ a_6 = 2,
\end{gathered}$$

hence

$$\sqrt{\frac{c+2}{c-2}} = \left[1; \overline{\frac{c-3}{2}, 1, 2c-2, 1, \frac{c-3}{2}, 2}\right], \quad c \ \text{odd integer}.$$

Pellian equations

- The length l of the period of the continued fraction expansion of $\sqrt{\frac{c+2}{c-2}}$ is $l = 6$, so we consider the equation (16) for $k = 0, 1, 2, 3, 4, 5$ and determine all the positive integers c that satisfy the congruence (10).
- From (13) and (16) we get

$$d^2(-1)^k(u^2 t_{k+1} + 2rus_{k+2} - r^2 t_{k+2}) = -1996c + 4008. \quad (17)$$

- Obviously, d can be $d = 1$ or $d = 2$ for all $k = 0, 1, 2, 3, 4, 5$.

Pellian equations

- Our goal is to determine all positive integers c that satisfy the congruence (10), that are of the form (18) and for which the triples (d, r, u) satisfy the conditions $d \in \mathbb{N},\ \ r \in \mathbb{N},\ \ u \in \mathbb{Z},\ \ u \neq 0$ and the inequality

$$d^2|ru| < 3992.$$

- It is useful to mention that the latter condition implies that $d \leq 63$.

Pellian equations

- An algorithm for generating triples (d, r, u) that satisfy the inequality
$$d^2|ru| < 3992$$
is created.
- This algorithm plugs these triples (d, r, u) into formulas for c-s for every $k = 0, 1, 2, 3, 4, 5$.
- It checks if the obtained numbers are positive integers and if these positive integers satisfy the congruence (10).

Pellian equations

- Let $k = 0$. From the equation

$$d^2(-1)^k(u^2t_{k+1} + 2rus_{k+2} - r^2t_{k+2}) = -1996c + 4008,$$

we obtain

$$d^2(4u^2 + 2(c-4)ru - r^2(2c-5)) = -1996c + 4008.$$

Pellian equations

For start, we deal with the cases when $d = 1$ and $d = 2$. For $d = 1$ we get the system of two equations

$$\begin{cases} 4u^2 - 8ru + 5r^2 = 4008, \\ 2ru - 2r^2 = -1996, \end{cases}$$

that does not have integer solutions. For $d = 2$ we get the system

$$\begin{cases} 4u^2 - 8ru + 5r^2 = 1002, \\ 2ru - 2r^2 = -499, \end{cases}$$

which also does not have integer solutions.

Pellian equations

Generally, for $k = 0$ and for all values of d, from

$$d^2(-1)^k(u^2 t_{k+1} + 2rus_{k+2} - r^2 t_{k+2}) = -1996c + 4008,$$

we obtain that the positive integer c is of the form

$$c = \frac{4008 - 4d^2u^2 + 8d^2ru - 5d^2r^2}{1996 + 2d^2ru - 2d^2r^2}. \tag{18}$$

Pellian equations

For $k = 1$ the equation (17) becomes

$$-d^2(u^2(2c-5) + 2ru(c-1) - r^2) = -1996c + 4008.$$

For $d = 1$ we get the system of two equations of the form

$$5u^2 + 2ru + r^2 = 4008, \ \ 2u^2 + 2ru = 1996,$$

while for $d = 2$ we obtain

$$5u^2 + 2ru + r^2 = 1002, \ \ 2u^2 + 2ru = 499.$$

There are no integer solutions for both systems.
Generally, c is represented by

$$c = \frac{5d^2u^2 + 2d^2ru + d^2r^2 - 4008}{2d^2u^2 + 2d^2ru - 1996}.$$

Pellian equations

For $k = 2$ we get

$$d^2(u^2 + 2ru(c-1) - r^2(2c-5)) = -1996c + 4008.$$

For $d = 1$ we obtain the following system of two equations

$$u^2 - 2ru + 5r^2 = 4008, \ \ 2ru - 2r^2 = -1996$$

which does not have integer solutions. For $d = 2$ the system

$$u^2 - 2ru + 5r^2 = 1002, \ \ 2ru - 2r^2 = -499$$

also has no integer solutions.
The positive integer c is of the form

$$c = \frac{d^2u^2 - 2d^2ru + 5d^2r^2 - 4008}{2d^2r^2 - 2d^2ru - 1996}.$$

Pellian equations

For $k = 3$ we get

$$-d^2(u^2(2c-5) + 2ru(c-4) - 4r^2) = -1996c + 4008.$$

For $d = 1$ and $d = 2$ we obtain the following systems respectively

$$5u^2 + 8ru + 4r^2 = 4008,\ \ 2u^2 + 2ru = 1996$$

and

$$5u^2 + 8ru + 4r^2 = 1002,\ \ 2u^2 + 2ru = 499.$$

Like in previous cases, these systems do not have integer solutions. The positive integer c is of the form

$$c = \frac{5d^2u^2 + 8d^2ru + 4d^2r^2 - 4008}{2d^2u^2 + 2d^2ru - 1996}.$$

Pellian equations

Analogously, for $k = 4$ we get

$$d^2(4u^2 + 2ru(c-2) - r^2(c-2)) = -1996c + 4008.$$

For $d = 1$ we obtain

$$4u^2 - 4ru + 2r^2 = 4008, \ \ 2ru - r^2 = 1996,$$

while for $d = 2$ we get

$$4u^2 - 4ru + 2r^2 = 1002, \ \ 2ru - r^2 = 499.$$

Both systems do not have integer solutions. Generally,

$$c = \frac{4d^2u^2 - 4d^2ru + 2d^2r^2 - 4008}{d^2r^2 - 2d^2ru - 1996}.$$

Pellian equations

Finally, for $k = 5$ we get

$$-d^2(u^2(c-2) - r^2(c-2)) = -1996c + 4008.$$

For $d = 1$ we obtain the following system of equations

$$2u^2 - 2r^2 = 4008, \ \ r^2 - u^2 = -1996,$$

and for $d = 2$ we get

$$2u^2 - 2r^2 = 1002, \ \ r^2 - u^2 = 499.$$

Both systems of equations do not have integer solutions. Generally,

$$c = \frac{2d^2u^2 - 2d^2r^2 - 4008}{d^2u^2 - d^2r^2 - 1996}. \tag{19}$$

Pellian equations

We gather all the possible positive integers $c \equiv 17 \pmod{30}$ that we get for $k = 0, 1, 2, 3, 4, 5$. We obtain

$$c \in \{17, 227, 497, 647, 857, 2537, 3107, 4937\}.$$

We set a Pellian equation of the form (13) for every obtained positive integer c.

Pellian equations

The Pellian equations are

$$
\begin{aligned}
19Y^2 - 15X^2 &= -29924, \quad \text{for} \quad c = 17,\\
229Y^2 - 225X^2 &= -449084, \quad \text{for} \quad c = 227,\\
499Y^2 - 495X^2 &= -988004, \quad \text{for} \quad c = 497,\\
649Y^2 - 645X^2 &= -1287404, \quad \text{for} \quad c = 647,\\
859Y^2 - 855X^2 &= -1706564, \quad \text{for} \quad c = 857,\\
2539Y^2 - 2535X^2 &= -5059844, \quad \text{for} \quad c = 2537,\\
3109Y^2 - 3105X^2 &= -6197564, \quad \text{for} \quad c = 3107,\\
4937Y^2 - 4935X^2 &= -9850244, \quad \text{for} \quad c = 4937.
\end{aligned}
$$

Pellian equations

- In order to determine whether these Pellian equations have integer solutions (X, Y), we use Dario Alpern's quadratic two integer variable equation solver [1].

Pellian equations

We assumed that X, Y are of the form

$$X := cy - c - 2x,$$
$$Y := cy - c - 2y.$$

- X satisfies the following congruences

$$X \equiv 0 \pmod 4, \ X \equiv 1 \pmod 3, \ X \equiv 4 \pmod 5,$$

$$\text{hence, } X \equiv 4 \pmod{60}.$$

We set $X = 60i + 4, \ i \in \mathbb{Z}$.

- Analogously, for Y we have

$$Y \equiv 2 \pmod 4, \ Y \equiv 1 \pmod 3, \ Y \equiv 3 \pmod 5,$$

hence, $Y \equiv 58 \pmod{60}$. We set $Y = 60j + 58, \ j \in \mathbb{Z}$.

Pellian equations

Additionally, we know that

$$Y = cy - c - 2y = c(y-1) - 2y \equiv -2 \pmod{(c-2)}.$$

- Using mentioned congruences and online calculator [1] we get that none of the mentioned Pellian equations has integer solutions (X, Y).
- Consequently, there does not exist a positive integer of the form $n = 2^\alpha 5^\beta$, $\alpha \geq 2$, $\beta \geq 2$ that satisfies the variation of congruence of Subbarao. So, the only numbers that satisfy the mentioned congruence are numbers $1, 2, 5, 8$.

□

References

[1] D. Alpern, Quadratic Diophantine equation solver, `http://www.alpertron.com.ar`

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

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

[4] A. Dujella and F. Luca, *On a variation of a congruence of Subbarao*, J. Aust. Math. Soc. **93** (2012), 85–90.

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

[6] The PARI Group, PARI/GP version `2.7.0`, Bordeaux, 2014, `http://pari.math.u-bordeaux.fr/`

[7] F. Schuh, *Do there exist composite numbers m for which $\varphi(m) \mid (m-1)$ (Dutch)*, Mathematica Zupten B, **13** (1944), 102–107.

[8] M. V. Subbarao, *On two congruences for primality*, Pacific J. Math. **54** (1974), 261–268.

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

Thank you for your attention!