

On Erdős–Wood’s conjecture

S SUBBURAM¹ and R THANGADURAI^{2,*}

¹Institute of Mathematical Sciences, C.I.T. Campus, 4th Cross Street, Taramani,
Chennai 600 113, India

²Harish-Chandra Research Institute, Chhatnag Road, Jhansi, Allahabad 211 019, India

*Corresponding author.

E-mail: ssrammaths@gmail.com; thanga@hri.res.in

MS received 20 August 2013

Abstract. In this article, we prove that infinite number of integers satisfy Erdős–Woods conjecture. Moreover, it follows that the number of natural numbers $\leq x$ satisfies Erdős–Woods conjecture with $k = 2$ is at least $cx/(\log x)$ for some positive constant $c > 2$.

Keywords. Erdős–Wood’s conjecture; exponential diophantine equations.

2010 Mathematics Subject Classification. 11N25, 11E12.

1. Introduction

For a given natural number $n \geq 2$, we let the radical of n ,

$$\text{rad}(n) = \{p : p|n, p \text{ is a prime number}\}$$

to be the set of all distinct prime divisors of n . In 1981, the Erdős–Woods conjecture was made by Woods [7] and is as follows.

Conjecture 1 [7]. There exists an integer k such that if

$$\text{rad}(n + i) = \text{rad}(m + i) \text{ holds for all } i = 1, 2, \dots, k,$$

then $n = m$.

This conjecture is known as the Erdős–Woods conjecture, since Woods made this conjecture after working on a number of problems and conjectures by Erdős of a similar form in his Ph.D. thesis [7].

Clearly, this conjecture $k = 1$ is not true. Also, it is not true for $k = 2$ as Erdős gave the following counter examples: Note that if $n = 74$ and $m = 1214$, then $\text{rad}(n + 1) = \{3, 5\} = \text{rad}(m + 1)$ and $\text{rad}(n + 2) = \{2, 19\} = \text{rad}(m + 2)$; yet $n < m$. Indeed, for any integer $h \geq 2$, we have

$$\text{rad}(2^h - 2) = \text{rad}(2^h(2^h - 2)), \text{rad}(2^h - 1) = \text{rad}(2^h(2^h - 2) + 1).$$

So, $k \geq 3$ is necessary in the Erdős–Wood’s conjecture to be true for all integers n . The main question is whether $k = 3$ is sufficient or not?

In 1989, Balasubramanian *et al.* [1] proved that

$$\log k \leq c\sqrt{(\log n)(\log \log n)},$$

for a given n , where $c > 0$ is an effectively computable constant. By assuming ABC conjecture, in 1993, Langevin [3] proved that $k = 3$ is sufficient for all integers $n > C$, where C is an absolute constant. Assuming the truth of the Hall's conjecture, it is known that $k \leq 20$. Recently, Rundle [5], in his thesis, gave a new proof of Langevin's result.

In this article, we prove the following theorems.

Theorem 1. *Let $p \geq 5$ be a prime number. Then the Erdős–Wood's conjecture is true with $k = 2$ for $n = p - 2$.*

COROLLARY 1.1

Let $p \geq 5$ be a prime number. Then the Erdős–Wood's conjecture is true with $k = 3$ for $n = p - 3$.

Theorem 2. *Let p and q be odd prime numbers such that $p \nmid (q - 1)$. Then the Erdős–Wood's conjecture is true with $k = 2$ for $n = q^p - 2$.*

COROLLARY 2.1

Let p and q be odd prime numbers such that $p \nmid (q - 1)$. Then the Erdős–Wood's conjecture is true with $k = 3$ for $n = q^p - 3$.

Theorem 3. *Let p be any prime number and s be any positive integer. Suppose that $p^s - 1$ is a square-free integer, then there is no integer $m > n = p^s - 2$ satisfying $\text{rad}(m + 1) = \text{rad}(n + 1)$ and $\text{rad}(m + 2) = \text{rad}(n + 2)$.*

COROLLARY 3.1

Let p be any prime number and s be any positive integer. Suppose that $p^s - 1$ is a square-free integer, then there is no integer $m > n = p^s - 3$ satisfying $\text{rad}(m + i) = \text{rad}(n + i)$ for $i = 1, 2, 3$.

Theorem 4. *Let $a \geq 1$ be any integer and p is any odd prime. If $p^a + 2 = q^b$, a power of prime q , then $n = p^a - 1$ satisfies the Erdős–Wood's conjecture with $k = 3$.*

Put $a = 1$ and $b = a$ in Theorem 4. Then we have the following corollary.

COROLLARY 4.1

Let p be a prime such that $p + 2 = q^a$, where q is a prime and $a \geq 1$ is an integer. Then $n = p - 1$ satisfy Erdős–Wood's conjecture with $k = 3$.

Remark 1. The above corollary includes the case that $n = p - 1$, where p is a twin prime. Conjecturally, there are infinitely many twin primes that exist; but, as of now, it is unknown.

2. Proof of Theorem 1 and Corollary 1.1

Proof of Theorem 1. Let $n = p - 2$, where $p \geq 5$ is an odd prime number. Let

$$n + 1 = p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r},$$

where q_1, q_2, \dots, q_r are distinct prime numbers and $\alpha_1, \alpha_2, \dots, \alpha_r$ are positive integers. Suppose that there is an integer m such that

$$\text{rad}(m + 1) = \text{rad}(n + 1) = \{q_1, q_2, \dots, q_r\}$$

and

$$\text{rad}(m + 2) = \text{rad}(n + 2) = \{p\}.$$

Then

$$m + 1 = q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} \quad \text{and} \quad m + 2 = p^\alpha,$$

where $\alpha, a_1, a_2, \dots, a_r$ are positive integers. If $\alpha = 1$, then $n = m$. So we assume that $\alpha > 1$. Now,

$$1 = (m + 2) - (m + 1) = p^\alpha - q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}.$$

This implies that

$$q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} + 1 = p^\alpha.$$

Since $p = q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} + 1 := \ell + 1$, we have

$$\begin{aligned} q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} + 1 &= (\ell + 1)^\alpha \\ &= \ell^\alpha + \alpha \ell^{\alpha-1} + \cdots + \alpha \ell + 1 \\ &= \ell[\ell^{\alpha-1} + \alpha \ell^{\alpha-2} + \cdots + \alpha] + 1. \end{aligned}$$

Therefore, ℓ divides LHS. Hence for some non-negative integers b_1, b_2, \dots, b_r , we have

$$\frac{q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}}{\ell} = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}.$$

Therefore

$$\ell^{\alpha-1} + \alpha \ell^{\alpha-2} + \cdots + \alpha = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}.$$

Since $\alpha > 1$ is an integer, we let $\alpha = q_1^{c_1} q_2^{c_2} \cdots q_r^{c_r} B$, where c_1, c_2, \dots, c_r are nonnegative integers and B is some positive integer such that $q_i \nmid B$. So

$$\ell^{\alpha-1} + (q_1^{c_1} q_2^{c_2} \cdots q_r^{c_r} B) \ell^{\alpha-2} + \cdots + q_1^{c_1} q_2^{c_2} \cdots q_r^{c_r} B = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}. \quad (1)$$

From this, we observe that for each $i = 1, 2, \dots, r$, we have

$$b_i = 0 \Leftrightarrow c_i = 0.$$

Next we show that for every $j \leq \alpha - 1$, we have

$$q_i^{c_i} \mid \binom{\alpha}{j-1} \ell^{\alpha-j}.$$

Clearly, for each $i = 1, 2, \dots, r$, we have, $q_i | \ell$. Let $1 \leq j \leq \alpha - 1$ be a fixed integer. If $\alpha - j \geq c_i$, then $q_i^{c_i}$ divides $\ell^{\alpha-j}$ and hence

$$q_i^{c_i} \left| \binom{\alpha}{j-1} \ell^{\alpha-j}.$$

Let $\alpha - j \leq c_i$. Since

$$\binom{\alpha}{j-1} = \binom{\alpha}{\alpha - (j-1)},$$

we rewrite this as

$$\binom{\alpha}{j-1} = \frac{\alpha}{\alpha - (j-1)} \binom{\alpha-1}{\alpha-j}.$$

Since $1 \leq j \leq \alpha - 1$, $\binom{\alpha-1}{\alpha-j}$ is an integer. So if $q_i \nmid (\alpha, \alpha - (j-1))$, then

$$q_i^{c_i} \left| \binom{\alpha}{j-1}.$$

If $q_i | (\alpha, \alpha - (j-1))$, then we denote the non-negative integer $s = \text{ord}_{q_i}(R)$, if $q_i^s \parallel R$. Then

$$\text{ord}_{q_i}(\alpha, \alpha - (j-1)) \leq \log_{q_i}(\alpha - (j-1)).$$

Therefore

$$q_i^{c_i - \log_{q_i}(\alpha - (j-1))} \left| \binom{\alpha}{j-1}.$$

This implies that

$$q_i^{c_i + [\alpha_i(\alpha-j) - \log_{q_i}(\alpha - (j-1))]} \left| \binom{\alpha}{j-1} \ell^{\alpha-j}.$$

Now, to prove the claim, we need to prove that $\alpha_i(\alpha - j) - \log_{q_i}(\alpha - (j-1)) \geq 0$. If possible, we assume that

$$\alpha_i(\alpha - j) < \log_{q_i}(\alpha - (j-1)).$$

That is,

$$q_i^{\alpha_i(\alpha-j)} < \alpha - (j-1).$$

Since $q_i \geq 2$, we get

$$2^{\alpha-j} < \alpha - j + 1,$$

which is a contradiction to $1 \leq j \leq \alpha - 1$. Therefore $\alpha_i(\alpha - j) - \log_{q_i}(\alpha - (j-1)) \geq 0$. Thus,

$$q_i^{c_i} \left| \binom{\alpha}{j-1} \ell^{\alpha-j} \quad \text{for all } j = 1, 2, \dots, \alpha - 1.$$

Hence, from (1), we get

$$\ell^{\alpha-1} + [q_1^{c_1} q_2^{c_2} \cdots q_r^{c_r}]A = q_1^{b_1} \cdots q_r^{b_r},$$

for some positive integer A such that $(A, q_1 q_2 \cdots q_r) = 1$. Since $\alpha - 1 \geq 1$, it follows from the above equation that

$$b_i = c_i \quad \text{for all } i = 1, 2, \dots, r.$$

Then (1) implies that $B = 1$ and $\ell = 0$, a contradiction. Hence the theorem. \square

Proof of Corollary 1.1. Let $p \geq 5$ be a prime and $n = p - 3$. If there is an integer m such that

$$\text{rad}(m + 1) = \text{rad}(n + 1), \text{rad}(m + 2) = \text{rad}(n + 2) = \text{rad}(p - 1)$$

and

$$\text{rad}(m + 3) = \text{rad}(n + 3) = \{p\}.$$

Note that $n' = n + 1 = p - 2$. By Theorem 1, we know that n' satisfies Erdős–Wood’s conjecture with $k = 2$. We see that $n + 1 = m + 1$ and hence $n = m$. \square

3. Proof of Theorem 2

Given that p and q are odd prime numbers such that $p \nmid (q - 1)$ and $n = q^p - 2$. Then let

$$n + 1 = q^p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r},$$

where q_1, q_2, \dots, q_r are distinct prime numbers and $\alpha_1, \alpha_2, \dots, \alpha_r$ are positive integers. Suppose that there is an integer m such that

$$\text{rad}(m + 1) = \text{rad}(n + 1) = \{q_1, q_2, \dots, q_r\}$$

and

$$\text{rad}(m + 2) = \text{rad}(n + 2) = \{q\}.$$

Then let

$$m + 1 = q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} \quad \text{and} \quad m + 2 = q^\alpha,$$

where $\alpha, a_1, a_2, \dots, a_r$ are positive integers. Therefore

$$q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} + 1 = q^\alpha.$$

Without loss of generality, we assume that $m > n$. Then we get $\alpha > p$. Let $\alpha = ps + x$ for some integer x such that $0 \leq x < p$. Then

$$q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} + 1 = q^{ps+x} = (q^p)^s q^x.$$

We shall prove that $x = 0$. Suppose $x \geq 1$. Since

$$q^p = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r} + 1 := \ell + 1,$$

we have

$$\begin{aligned} q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} + 1 &= q^x (\ell + 1)^s \\ &= q^x (\ell^s + s\ell^{s-1} + \cdots + s\ell + 1) \\ &= q^x \ell [\ell^{s-1} + s\ell^{s-2} + \cdots + s] + q^x. \end{aligned}$$

This implies that

$$q^x - 1 = [q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}] - q^x \ell [\ell^{s-1} + s\ell^{s-2} + \cdots + s].$$

From this we observe that

$$q_1 q_2 \cdots q_r | q^x - 1.$$

Therefore

$$q_1 q_2 \cdots q_r | \gcd(q^x - 1, q^p - 1) = q^{(x,p)} - 1 = q - 1.$$

Then there exists an integer z such that

$$q - 1 = q_1 q_2 \cdots q_r z.$$

That is,

$$q = 1 + q_1 q_2 \cdots q_r z.$$

Since

$$q^p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r},$$

we have

$$q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r} = (1 + q_1 q_2 \cdots q_r z)^p - 1.$$

This implies

$$q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r} = (q_1 q_2 \cdots q_r z)^p + \cdots + \binom{p}{2} (q_1 q_2 \cdots q_r z) + p.$$

Since $q_1 q_2 \cdots q_r z$ divides LHS (as it divides $q - 1$) and all the terms except the last term, we conclude that it divides p ; but $p \nmid (q - 1)$. Hence this is impossible. Therefore, $x = 0$. Thus, we let $\alpha = ps$ and hence

$$1 + q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r} = q^\alpha = q^{ps} = (q^p)^s = (\ell + 1)^s.$$

If $s > 1$, by the way of the proof of Theorem 1, we get a contradiction. So $s = 1$. That is, $m = n$. This proves the theorem. \square

4. Proof of Theorem 3 and Corollary 3.1

Proof of Theorem 3. Given that, for an prime p , the integer $p^s - 1$ is square-free. Let $p^s - 1 = 2^\epsilon q_1 q_2 \cdots q_r$, where q_i 's are distinct odd primes and $\epsilon = 0$ if $p = 2$ and $\epsilon = 1$ if $p \geq 3$.

Let $n = p^s - 2$ be the given integer. Suppose there exists an integer m such that $m > n$ and $\text{rad}(m+1) = \text{rad}(n+1) = \{2^\epsilon, q_1, \dots, q_r\}$ and $\text{rad}(m+2) = \text{rad}(n+2) = \{p\}$. Since $m > n$, we get $m+2 > n+2 = p^s$ and hence $m+2 = p^\alpha$, where $\alpha > s$. By letting $m+1 = 2^a q_1^{a_1} \dots q_r^{a_r}$, we get

$$1 = m+2 - (m+1) = p^\alpha - 2^a q_1^{a_1} \dots q_r^{a_r} \implies p^\alpha = 2^a q_1^{a_1} \dots q_r^{a_r} + 1,$$

where $a_i \geq 1$ and $a \geq 0$ are integers.

Claim. s divides α .

Suppose $\alpha = ts + x$, where $1 \leq x < s$ and for some integer $t \geq 1$. Then

$$p^\alpha = p^x p^{st} = 2^a q_1^{a_1} \dots q_r^{a_r} + 1.$$

Since $p^s = 2^\epsilon q_1 q_2 \dots q_r + 1 := \ell + 1$, we see that

$$2^a q_1^{a_1} \dots q_r^{a_r} + 1 = p^x (\ell + 1)^t = p^x \ell^t + \dots + p^x t \ell + p^x.$$

Hence

$$p^x - 1 = 2^a q_1^{a_1} \dots q_r^{a_r} - p^x \ell^t - \dots - t \ell p^x.$$

Since ℓ divides the RHS, ℓ divides LHS. That is, $(p^s - 1)$ divides $(p^x - 1)$, which is a contradiction to the assumption that $1 \leq x < s$. Therefore, we get $x = 0$ and hence α is a multiple of s .

Let $\alpha = s\beta$ for some integer $\beta \geq 1$. Therefore, we have $m+2 = (n+2)^\beta$. That is, we have

$$\begin{aligned} 2^a q_1^{a_1} \dots q_r^{a_r} + 1 &= p^\alpha = (p^s)^\beta = (\ell + 1)^\beta \\ &= \ell^\beta + \beta \ell^{\beta-1} + \dots + \beta \ell + 1. \\ \implies 2^{a-1} q_1^{a_1-1} \dots q_r^{a_r-1} &= \ell^{\beta-1} + \beta \ell^{\beta-2} + \dots + \beta \end{aligned}$$

If $a = 1 = a_1 = a_2 = \dots = a_r$, then, clearly, we have $m+1 = n+1$ and we are done. Therefore, without loss of generality, we assume that $a > 1$ (if $a_i > 1$ for some i , then the same proof works analogously). That is, 2 divides LHS of the equation. Since $2|\ell$, we see that $2|\beta$ also. Suppose $2^c || \beta$ for some integer $c \geq 1$.

Claim. 2^c divides $\binom{\beta}{j} \ell^{\beta-j}$ for every $j = 1, 2, \dots, \beta$.

Since $2|\ell$ and $\binom{\beta}{j}$ is an integer, we see that 2^c divides $\ell^{\beta-j}$ for all $\beta - j \leq c - 1$. Therefore, we consider $j \geq \beta - c$. In this case, $c \geq \beta - j$. Also,

$$\binom{\beta}{j} = \binom{\beta}{\beta - j} = \frac{\beta(\beta - 1)(\beta - 2) \dots (\beta - (\beta - j) + 1)}{1 \cdot 2 \cdot \dots \cdot (\beta - j)}.$$

Since $\beta \equiv 0 \pmod{2^c}$, we see that $\beta - 2y \equiv -2y \pmod{2^c}$ for all $2y \leq \beta - j - 1$. Therefore, except the last term $\beta - j$ (when it is even) in the denominator and the first term β in the numerator, the power of 2 cancels each other. If $\beta - j$ is even, then the power of 2 dividing $\beta - j$ cancels with the power of 2 dividing β . However, in this case, the integer $\ell^{\beta-j}$ has extra $2^{\beta-j}$ apart from the power of 2 of $\beta/(\beta - j)$ and with both together, we get 2^c divides $\binom{\beta}{j} \ell^{\beta-j}$. Hence the claim.

Suppose $c \leq a - 1$ (the other case $c \geq a - 1$ is similar). Then, by canceling both the sides 2^c , we can make the RHS an odd integer. If $c < a - 1$, then LHS would be even, a contradiction to RHS is odd. This would imply that $a - 1 = c$. That is, $2^{a-1} \parallel \beta$. Now, we have

$$q_1^{a_1-1} \cdots q_r^{a_r-1} = \frac{1}{2^{a-1}} (\ell^{\beta-1} + \cdots + \beta).$$

If $a_i > 1$ for some i , then, as $q_i \mid \ell$, we see that $q_i \mid \beta$ also. Let $q_i^{c_i} \parallel \beta$. Then by canceling $q_i^{c_i}$ on both sides, we conclude that $c_i = a_i - 1$. Otherwise, in the LHS, there will be a factor of q_i which will not divide the RHS, a contradiction. Hence we conclude that

$$2^{a-1} q_1^{a_1-1} q_2^{a_2-1} \cdots q_r^{a_r-1} \text{ divides } \beta.$$

However, from the equation, it is clear that β is smaller than $2^{a-1} q_1^{a_1-1} q_2^{a_2-1} \cdots q_r^{a_r-1}$ which forces

$$\beta = 2^{a-1} q_1^{a_1-1} q_2^{a_2-1} \cdots q_r^{a_r-1}.$$

This implies that the other terms in the RHS must be zero which is possible only when $\beta - 1 = 0$. That is, $\beta = 1$ and hence $a = 1 = a_1 = a_2 = \cdots = a_r$. Thus, $m = n$ follows. \square

Proof of Corollary 3.1. If $n = p^s - 3$, then $n + 1$ satisfies Theorem 3 and $n + 1 = m + 1$ and hence the corollary. \square

5. Proof of Theorem 4

We need the following results which deals with the integral solutions of the exponential diophantine equation.

Theorem 4.1 [4]. *The integral solutions of*

$$2^x + 3^y = 5^z$$

are given by $(x, y, z) = (1, 1, 1)$ and $(4, 2, 2)$.

Theorem 4.2 ([6], cf. Lemma 6). *Let $p, q \geq 5$ be two distinct primes. Then the equation*

$$p^x + 2^y = q^z$$

has at most one integral solution $(x, y, z) \in \mathbb{N}^3$.

For more related results, we refer to [2].

Proof of Theorem 4. Given that $n = p^a - 1$, where p is a prime and $p^a + 2 = q^b$ for some prime q . Suppose there exists an integer m such that

$$\text{rad}(m + 1) = \text{rad}(n + 1) = \{p\}, \text{rad}(m + 2) = \text{rad}(n + 2) = \text{rad}(p^a + 1)$$

and

$$\text{rad}(m + 3) = \text{rad}(n + 3) = \{q\}.$$

Therefore, we get

$$m + 1 = p^\alpha \quad \text{and} \quad m + 3 = q^\beta$$

for some integers $\alpha \geq 1$ and $\beta \geq 1$. Then

$$2 = m + 3 - m - 1 = q^\beta - p^\alpha \implies q^\beta = p^\alpha + 2.$$

By Theorem 4.2, the equation $p^x + 2^y = q^z$ has at most one integral solution (x, y, z) . Since, by assumption, we have

$$2 = n + 3 - n - 1 = q^b - p^a \implies p^a + 2 = q^b,$$

we see that $(x, y, z) = (a, 1, b)$ is an integral solution of the above equation. Therefore, we conclude that $\alpha = a$ and $\beta = b$ and so $m = n$. \square

References

- [1] Balasubramanian R, Shorey T N and Waldschmidt M, On the maximal length of two sequences of consecutive integers with the same prime divisors, *Acta Math. Hungar.* **54(3–4)** (1989) 225–236
- [2] Cao Z F, A note on the Diophantine equation $a^x + b^y = c^z$, *Acta Arith.* **XCLI** (1999) 85–93
- [3] Langevin M, Cas dégalite pour le theoreme de Mason et applications de la conjecture (abc) . (Extremal cases for Mason’s theorem and applications of the (abc) conjecture), *C. R. Acad. Sci., Paris, Ser. I* **317(5)** (1993) 441–444
- [4] Nagell T, Sur une classe d’équations exponentielles, *Ark. Mat.* **3** (1958) 569–582
- [5] Rundle R J, Generalization of Ruderman’s problem to imaginary quadratic fields, Ph.D. Thesis (2012) (Canada: Queen’s University)
- [6] Scott R, On the equations $p^x - b^y = c$ and $a^x + b^y = c^z$, *J. Number Theory* **44** (1993) 153–165
- [7] Woods A R, Some problems in logic and number theory, and their connections, Ph. D. Thesis (1981) (University of Manchester)

COMMUNICATING EDITOR: B V Rajarama Bhat