Prime n solutions of the Brocard’s Problem

Devansh Singh (✉ ds0324549@gmail.com )
I.E.T. Lucknow

Research Article

Keywords: Laplace Transform, Brocard’s Problem, s, f (t).

Posted Date: December 30th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-1217305/v1

License: ☑️ This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License
Prime n solutions of the Brocard’s Problem

Devansh Singh*

B.Tech. M.E.

Department of Mechanical Engineering,

Institute of Engineering and Technology, Lucknow, Uttar Pradesh, India

ds0324549@gmail.com, 8787011853, ORCID- 0000-0002-4947-8297

Keywords- Laplace Transform, Brocard’s Problem, s, f (t).

MSC Classification- 44A10, 11D45

Abbreviations- L[f(t)] = ∫₀^∞ e^{-st} f(t) dt, where s>0. L[f(t)] is called Laplace transform of f(t). ‘∀’ means “for all”, ‘:’ means “such that”, ‘≡’ means “congruent to”, “parity” means even or odd.

Abstract- In this paper on the [1]“Brocard’s Problem”, I have worked on case when n is prime and n divides m-1. Necessary conditions on m are given in Theorem and Corollaries.

I used necessary and sufficient condition of primes. Assuming that n is prime and divides m-1, I applied Inverse Laplace Transform on the obtained equation and got a polynomial function which is easier to deal with. I worked with zero of the polynomial function and got lower bound of p which was not useful as p tends to infinity, but solving quartic equation which I have given at the end could give significant upper, lower bounds of p.

What would happen to those upper, lower bounds if p tends to infinity?

Introduction- [1]“Brocard’s Problem” asks for (n, m): n! + 1 = m^2, where (m, n) are natural numbers and n! is factorial of n; is a Diophantine equation in 2 variables. It was posed by “Henri Brocard” in 1876 and 1885, and independently in 1913 by “Srinivasa Ramanujan”. Only 3 solutions of the problem have been found so far which are (4, 5), (5, 11), (7, 71). There may be more solutions but none has
been found up to $n \leq 10^{15}$. Overholt (1993) showed that there are only finitely many solutions provided that the “abc conjecture” is true.

We will try to find solutions where $n$ is prime and divides $m-1$. We will use Wilson’s theorem on prime numbers, it is a necessary and sufficient condition for primality. According to the Wilson’s Theorem, $p$ is prime number iff $(p−1)! \equiv −1 \pmod{p}$. [4]

**Theorem 1** - $m$ in $p! + 1 = m^2$ – (eqn. 1), is $\frac{p(p^2-1)}{2} + 1$, where ‘a’ is odd.

**Proof** - 1) Using Wilson’s Theorem on prime we can write $(p - 1)! = pq’ + p-1$, where $p$ is odd prime and $q’$ is an even natural number.

2) Using assumption that $p$ divides $m-1$ we can write $m = pq + 1$ – (eqn. 2). On squaring $m$ we get: $m^2 = p^2q^2 + 1 + 2pq = p! + 1$. Solving this equation we get $pq^2 + 2q = (p-1)! – (eqn. 3)$, where $q$ is an even natural number.

From above 1) and 2) - $(p-1)! = pq^2 + 2q = pq’ + p-1$. Solving this equation we get: $p(q’ - q^2 + 1) = 2q + 1$. Let $a = q’ - q^2 + 1$, where ‘a’ is odd then $q = \frac{p(p-1)}{2}$.

After substituting value of $q$ from above, eqn. 2 can be rewritten as:

$m = \frac{p(p^2-1)}{2} + 1$.

Eqn. 1 can be rewritten as: $(p − 1)! = \left(\frac{p(p-1)}{2}\right)\left(\frac{p(p-1)}{2} + 2\right)$

Let $s = \frac{p(p-1)}{2}$ then again rewriting eqn. 1 as: $p! = s^2 + 2s$ - (eqn. 4)

**Corollary 1.1** - $a \equiv r \pmod{4}$, where $r \equiv p \pmod{4}$.

**Proof** - ∴ $(p − 1)! = \left(\frac{p(p-1)}{4}\right)(p(p-1) + 4)$. (From proof of Theorem 1.1)

∴ $4(p−1)! = (p(a - 1))(p(pa - 1) + 4)$.

Taking mod 4 on both sides, we get: $p(pa − 1)^2 \equiv 0 \pmod{4}$. 
\[ \therefore p \equiv 1 \pmod{4} \text{ or } p \equiv 3 \pmod{4} \therefore (pa - 1)^2 \equiv 0 \pmod{4}. \]

So, \( pa \equiv 1 \pmod{4} \) and so, \( a \equiv r \pmod{4} \), where \( r \equiv p \pmod{4} \).

**Corollary 1.2** \( \frac{p+a-2r}{4} \) is even when \( m \equiv 1 \pmod{4} \) and \( \frac{p+a-2r}{4} \) is odd when \( m \equiv 3 \pmod{4} \).

**Proof** \( \because m = \frac{p(pa-1)}{2} + 1 \) (Theorem 1) and \( a \equiv r \pmod{4} \), where \( r \equiv p \pmod{4} \) (Corollary 1.1); we get: \( m = \frac{(4Q_1+r)((4Q_1+r)(4Q_2+r)-1)}{2} + 1 \), where \( p = 4Q_1 + r \) and \( a = 4Q_2 + r \).

1.) For \( r=1 \): \( m = \frac{(4Q_1+1)((4Q_1+3)(4Q_2+3)-1)}{2} + 1 = 32Q_1^2Q_2 + 16Q_1Q_2 + 8Q_1^2 + 2Q_1 + 2Q_2 + 1. \)

2.) For \( r=3 \): \( m = \frac{(4Q_1+3)((4Q_1+3)(4Q_2+3)-1)}{2} + 1 = 32Q_1^2Q_2 + 48Q_1Q_2 + 24Q_1^2 + 34Q_1 + 18Q_2 + 13. \)

From 1.) and 2.) above, we get \( m \equiv (2(Q_1 + Q_2) + 1)(mod \ 4). \)

i. \( 1 \equiv (2(Q_1 + Q_2) + 1)(mod \ 4) \Rightarrow 0 \equiv 2(Q_1 + Q_2)(mod \ 4) \Rightarrow Q_1 + Q_2 \text{ is even} \Rightarrow Q_1 \text{ and } Q_2 \text{ are of same parity.} \)

ii. \( 3 \equiv (2(Q_1 + Q_2) + 1)(mod \ 4) \Rightarrow 2 \equiv 2(Q_1 + Q_2)(mod \ 4) \Rightarrow 1 \equiv (Q_1 + Q_2)(mod \ 4) \text{ or } 3 \equiv (Q_1 + Q_2)(mod \ 4) \Rightarrow (Q_1 + Q_2) \text{ is odd} \Rightarrow Q_1 \text{ and } Q_2 \text{ are of opposite parity.} \)

**Corollary 1.3** ‘\( a \)’ increases with increase in \( p \).

**Proof**

<table>
<thead>
<tr>
<th>a</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
</tr>
</tbody>
</table>

(a, p) for known values of p.
m from Theorem 1.1 = \( \frac{p(p-1)}{2} + 1 = \sqrt{p!} + 1 \). So, \( a = \frac{2\sqrt{p!} + 1 + 1}{p^2} \approx \frac{2\sqrt{p!}}{p^2} \).

\[ p! \approx \left( \frac{p}{e} \right)^p \sqrt{2\pi p}. \text{[3]} \]

\[ a \approx 2 \left( \frac{p}{e} \right)^{\frac{p}{2}} \frac{\sqrt{2\pi p}}{e^2} \text{ is increasing for } p > 5. \]

**Applying Inverse Laplace Transform on equation 4:** We can apply inverse Laplace transform on equation to get a function which is simpler to deal with than its predecessor.

First comparing 4\(^{th}\) eqn. with: \( L[f^2(t)] = s^2L[f(t)] - sf(0) - f^1(0) \), where \( L[f(t)] \) is Laplace Transform of \( f(t) \) and \( f^n(t) \) is \( n \)\(^{th}\) derivative of \( f(t) \). After comparison we get: \( L[f(t)] = 1, f(0) = -2, f^1(0) = 0 \) and \( p! = s^{p+1}L[t^p] = L[f^2(t)] \) (as \( L[t^n] = n!/s^{n+1} \)).

Let \( f^2(t) = s^{p+1}t^p \) then \( f^1(t) = \frac{s^{p+1}t^{p+1}}{p+1} + c_1. \)

\[ \because f^1(0) = 0, \therefore c_1 = 0. \]

\[ \therefore f(t) = \frac{s^{p+1}t^{p+1}}{(p+1)(p+2)} + c_2. \]

\[ \therefore f(0) = -2, \therefore c_2 = -2. \]

\[ \therefore f(t) = \frac{s^{p+1}t^{p+2}}{(p+1)(p+2)} - 2, \text{ for } t \in [0, \infty). \]

**Existence of \( L[f(t)] \):**

[2] Sufficient conditions for existence of \( L[f(t)] \):

1) \( f(t) \) is piecewise-continuous on \([0, \infty)\).

2) \( f(t) \) is of exponential order \( c \) if there exist positive real numbers \( M, c \): \( f(t) \leq M e^{ct} \) for all \( t > t_0 > 0 \).

We have:
a) \( f(t) \) is piecewise-continuous on \([0, \infty)\).

b) \( f(t) = \frac{s^{p+1}t^{p+2}}{(p+1)(p+2)} - 2 < \frac{s^{p+1}e^{(p+2)t}}{(p+1)(p+2)} \) for \( \forall \ t > 0 \). There exist positive real numbers \( M, c \) such that \( f(t) \leq Me^{ct} \) for all \( t > 0(t_0) \), where \( M = \frac{s^{p+1}}{(p+1)(p+2)} \) and \( c = p + 2 \). \( \therefore \) \( f(t) \) is of exponential order ‘c’.

So, \( L[f(t)] \) exists for \( s = \frac{p(pa-1)}{2} > c \).

Let \( t = \varepsilon: f(\varepsilon) = 0 \) then \( \varepsilon = (\frac{\sqrt{2s(p+1)(p+2)}}{s^{p+1}})^{1/p+2} \).

\( \therefore s > \frac{1}{\varepsilon} = \left( \frac{s^{p+1}}{2(p+1)(p+2)} \right)\frac{1}{p+2} = \frac{s^{1-1/p+2}}{(2(p+1)(p+2))^{1/p+2}} > \frac{s^{3/4}}{(2(p+1)(p+2))^{1/4}} \text{ (i)} \)

\( \Rightarrow \frac{1}{\varepsilon^4} > \frac{s^3}{2(p+1)(p+2)}. \) After rearranging we get: \( 2(p+1)(p+2) > s^3 \varepsilon^4 > s^2 \varepsilon^4 > s \varepsilon^4 \). \( \text{(ii)} \)

Using \( 2(p+1)(p+2) > s \varepsilon^4 \) for simplicity, substituting value of \( s = \frac{p(pa-1)}{2} \), and after rearranging we get: \( p^2(\varepsilon^4 - 4) - p(\varepsilon^4 + 12) - 8 < 0 \).

Due to Corollary 1.3:

\( e^{a^{1/4}} = a^{1/4} \left( \frac{2^{p+2}(p+1)(p+2)}{(p(pa-1))^{p+1}} \right)^{1/p+2} = \frac{2((p+1)(p+2))^{1/p+2}}{a^{0.75} \frac{1}{p+2} (p-\frac{1}{a})^{1-\frac{1}{p+2}} p^{1-\frac{1}{p+2}}} \) decreases with increase in \( a \). For \( a = 1 \), \( (e^{a^{1/4}})^4 = 0.00468831446 < 4 \).

Solving above inequality and due to above reasoning, we get: \( p \geq \frac{\sqrt{\Delta-(12+\varepsilon^4)}}{2(4-\varepsilon^4)} \), where \( \Delta = \varepsilon^8 + \varepsilon^4(24 + 32a) + 16 \).

**Theorem 2**- If there are infinitely many solutions of \( p! = s^2 + 2s \) then

\( \lim_{a \to \infty} e^{a^{1/4}} = 0, \lim_{a \to \infty} e = 0 \) and conversely.

**Proof**- If there are infinitely many solutions of \( p! = s^2 + 2s \) then \( \lim_{a \to \infty} e^{a^{1/4}} = \lim_{a \to \infty} \frac{2(p+1)(p+2)}{s^{p+1}}^{1/p+2}, \) where \( s = \frac{p(pa-1)}{2} \).
\[ \lim_{a \to \infty} e^{1/4} = \lim_{a \to \infty} a^{1/4} \left( \frac{2^{p+2}(p+1)(p+2)}{(p(pa-1))^{p+1}} \right)^{1/p+2} = \lim_{a \to \infty} \frac{2((p+1)(p+2))^{1/p+2}}{0.75 - \frac{1}{p+2}(p-\frac{1}{a})^{1-p+2} p^{1-p+2}} = 0 \]

\[ \therefore \lim_{a \to \infty} e^{1/4} = 0 \text{ so does } \lim_{a \to \infty} e = 0. \text{ Similarly } \lim_{a \to \infty} e^x = 0 \text{ if } \frac{1}{p+2} + x \leq 1 \text{ otherwise it is infinite.} \]

\[ \therefore \lim_{a \to \infty} \sqrt{\Delta} = \frac{\sqrt{\Delta - (12+e^4)}}{2(4ae^4)} (\Delta = e^8 + e^4(24 + 32a) + 16) = -1 \]

\[ \Rightarrow -1 \leq \lim_{p \to \infty} p \text{ which is not useful.} \]

\[ 2(p+1)(p+2) > s^2 e^4. \]

From (i) inequality above theorem 1.2, we have \( s > \frac{1}{e} \), where \( s = \frac{p(pa-\_)}{2} \).

\[ p^2ae - pe - 2 > 0 \Rightarrow p > \frac{e + \sqrt{e^2 + 8ae}}{2ae}. \]

\[ \therefore \lim_{e \to 0} \frac{e + \sqrt{e^2 + 8ae}}{2ae} = \infty. \therefore p > \infty. \text{ So, converse of the theorem is also true.} \]

Or \( e \to 0 \leftrightarrow p \to \infty. \)

*From (ii) inequality, above theorem 1.2, we have: \( 2(p+1)(p+2) > s^2 e^4 \) or \( 2(p+1)(p+2) > s^2 e^3 \) (if we put \( p = 1 \)). If we expand this inequality in terms of \( p \) and \( a \), we will get 4\(^{th}\) degree polynomial inequality in \( p \).

Though solving 4\(^{th}\) degree polynomial equation is time consuming but there are chances that we may get significant information on upper bounds and lower bounds of \( p \) which we cannot get in \( 2(p+1)(p+2) > s e^4 \) or \( 2(p+1)(p+2) > s e^2. \)

**Result-** \( \frac{p+a-2r}{4} = Q_1 + Q_2 \) is even when \( m \equiv 1 \text{ (mod 4) \ and } \frac{p+a-2r}{4} = Q_1 + Q_2 \) is odd when \( m \equiv 3 \text{ (mod 4). Also:} \)

1) If \( 1 \equiv p \text{ (mod 4), then } m = 32Q_1^2Q_2 + 16Q_1Q_2 + 8Q_1^2 + 2Q_1 + 2Q_2 + 1. \)
2) If \( 3 \equiv p \text{ (mod 4), then } m = 32Q_1^2Q_2 + 48Q_1Q_2 + 24Q_1^2 + 34Q_1 + 18Q_2 + 13. \)
References


* All data generated or analysed during this study are included in this article.*