Brocard's Problem 4th Solution Search Utilizing Quadratic Residues

Robert D. Matson

Abstract

In 1876, Henri Brocard[1] first posed the problem of finding integer solutions to the Diophantine equation $n! + 1 = m^2$ beyond $n = 4$, 5 and 7. In 1935, Hansraj Gupta[2] claimed that calculations of $n!$ up to $n = 63$ gave no further solutions. In 2000, Bruce Berndt and William Galway[3] performed the first extensive computer search for a solution with n up to 10^9 but found none. The purpose of this paper is to report on recent calculations (2016) that extend the lower limit on any fourth solution to the Brocard Problem by three orders of magnitude to $n > 1$ trillion.

Algorithmic Approach

The basic algorithmic approach used for testing large values of n was the same as that outlined by Berndt & Galway utilizing test primes, P_i, and the Legendre symbol $\left(\frac{a}{P_i}\right)$, where $a = n! + 1$. If the Legendre symbol $\left(\frac{n!+1}{P_i}\right)$ for a given P_i equals 1, then $n! + 1$ is a quadratic residue modulo P_i, and therefore n *may* be a solution. If instead it equals -1 for any prime, then that n cannot be a solution. (The Legendre symbol is 0 if $(n! + 1)$ is a multiple of P_i, in which case n may still be a solution. However, the values of P_i used here are all greater than 10^{12}, so the probability that $n! + 1 = 0$ mod P_i is extremely low.)

The explicit formula for computing the Legendre symbol is:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}\ (mod\ p)$$

Since the P values here are large, exponentiation-by-squaring and Montgomery modular multiplication were utilized to efficiently compute the Legendre symbol. The probability that the Legendre symbol will be -1 for a given pair of integers is very nearly 50%, so the key to proving that a given $n! + 1$ is not a perfect square is to test against a sufficient number of primes that a Legendre symbol result of -1 is sure to be found for one of them. For instance, if testing is carried out against 40 primes, the probability of a given *n* passing all 40 tests is approximately one in 2^{40}, or about one in a trillion. Note that if such an *n* should be found, it does <u>not</u> mean it is a solution to Brocard's Problem – it is a necessary condition, but not a sufficient one. However, in the range $7 < n < 1 \times 10^{12}$, no *n* passed more than 39 tests.

Since the goal was to eventually search all n values up to 1 trillion, the 40 test primes chosen were the first 40 primes greater than 1 trillion, shown in Table 1:

Prime #	**Prime**	**Prime #**	**Prime**
1	1,000,000,000,039	21	1,000,000,000,547
2	1,000,000,000,061	22	1,000,000,000,561
3	1,000,000,000,063	23	1,000,000,000,609
4	1,000,000,000,091	24	1,000,000,000,661
5	1,000,000,000,121	25	1,000,000,000,669
6	1,000,000,000,163	26	1,000,000,000,721
7	1,000,000,000,169	27	1,000,000,000,751
8	1,000,000,000,177	28	1,000,000,000,787
9	1,000,000,000,189	29	1,000,000,000,789
10	1,000,000,000,193	30	1,000,000,000,799
11	1,000,000,000,211	31	1,000,000,000,841
12	1,000,000,000,271	32	1,000,000,000,903
13	1,000,000,000,303	33	1,000,000,000,921
14	1,000,000,000,331	34	1,000,000,000,931
15	1,000,000,000,333	35	1,000,000,000,933
16	1,000,000,000,339	36	1,000,000,000,949
17	1,000,000,000,459	37	1,000,000,000,997
18	1,000,000,000,471	38	1,000,000,001,051
19	1,000,000,000,537	39	1,000,000,001,083
20	1,000,000,000,543	40	1,000,000,001,123

Table 1. First 40 primes greater than 1 trillion used for Brocard Problem search.

Results

The first *n* < 1 trillion to pass 38/40 prime tests was 208,463,325,489. The first *n* to pass 39/40 prime tests was 246,433,859,065. (Additional n's to pass 39 prime tests were 704,282,301,652 and 728,972,865,656. Testing to *n* = 1 trillion took approximately 16 months on a single core of a 64-bit Dell Optiplex 790 with an i7-2600 running at 3.4 GHz. As mentioned above, no *n* was found that passed all 40 prime tests, so there is no Brocard Problem solution for $7 < n \le 10^{12}$.

References

[1] H. Brocard, *Question 166*, Nouv. Corresp. Math. **2** (1876), 287.

[2] H. Gupta, *On a Brocard-Ramanujan problem*, Math. Student **3** (1935), 71.

[3] B. Berndt and W. Galway, *The Brocard-Ramanujan Diophantine Equation* $n! + 1 = m^2$, The Ramanujan Journal **4**, 41-42.