# BRAZILIAN PRIMES WHICH ARE ALSO SOPHIE GERMAIN PRIMES

**Jon Grantham**
*Institute for Defense Analyses/Center for Computing Sciences, Bowie, Maryland*
grantham@super.org

**Hester Graves**
*Institute for Defense Analyses/Center for Computing Sciences, Bowie, Maryland*
hkgrave@super.org

*Received: 6/6/19, Revised: 12/9/19, Accepted: 4/23/20, Published: 5/8/20*

**Abstract**

We disprove a conjecture of Schott that no Brazilian prime is a Sophie Germain prime. We compute all counterexamples up to $10^{46}$. We prove conditional asymptotics for the number of Brazilian Sophie Germain primes up to $x$.

## 1. Introduction

The term "Brazilian numbers" comes from the 1994 Iberoamerican Mathematical Olympiad [8] in Fortaleza, Brazil, in a problem proposed by the Mexican math team.[1]. They became a topic of lively discussion on the forum mathematiques.net. Bernard Schott [5] summarized the results in the standard reference on Brazilian numbers.

**Definition 1.** A *Brazilian number* $n$ is an integer whose base-$b$ representation has all the same digits for some $1 < b < n-1$.

In other words, $n$ is Brazilian if and only if $n = m\left(\frac{b^q-1}{b-1}\right) = mb^{q-1}+\cdots+mb+m$, with $q \geq 2$. These numbers are A125134 in the Online Encyclopedia of Integer Sequences (OEIS).

A *Brazilian prime* (or "prime repunit") is a Brazilian number that is prime; by necessity, $m = 1$ and $q \geq 3$. See A085104 in the OEIS for the sequence of Brazilian primes. In 2010, Schott [5] conjectured that no Brazilian prime is also a Sophie Germain prime.

[1]The term appears as "sensato" in the original problem [6]. The authors are puzzled by the discrepancy with [8].

Sophie Germain discovered her eponymous primes while trying to prove Fermat's Last Theorem; her work was one of the first major steps towards a proof.

**Definition 2.** A *Sophie Germain prime* is a prime $p$ such that $2p+1$ is also prime.

Germain showed that if $p$ is such a prime, then there are no non-zero integers $x, y, z$, not divisible by $p$, such that $x^p + y^p = z^p$. If $p$ is a Sophie Germain prime, then we say that $2p+1$ is a *safe prime*.

It is conjectured that there are infinitely many Sophie Germain primes, but the claim is still unproven. The Bateman-Horn conjecture [1] implies that the number of Sophie Germain primes less than $x$ is asymptotic to $2C\frac{x}{\log^2 x}$, where $C = \prod_{p>2} \frac{p(p-2)}{(p-1)^2} \approx 0.660161$.

See [3] for further information about Sophie Germain primes.

## 2. Enumerating Counterexamples

To aid our search, we use a few lemmas.

**Lemma 1.** *If $p = \frac{b^q-1}{b-1}$ is a Brazilian prime, then $q$ is an odd prime.*

*Proof.* Recall $x^q - 1$ is divisible by the $m$th cyclotomic polynomial $\Phi_m(x)$ for $m|q$; therefore $p$ can only be prime if $q$ is also prime. Note that $q > 2$ because $b < p-1$, so $q$ is an odd prime. □

The preceding lemma is also Corollary 4.1 of Schott [5].

**Lemma 2.** *If $p$ is a Brazilian prime and a Sophie Germain prime, then $p \equiv q \equiv 2 \pmod 3$ and $b \equiv 1 \pmod 3$.*

*Proof.* If $p$ is a Sophie Germain prime, then 3 cannot divide the safe prime $2p+1$, so $p$ cannot be congruent to 1 (mod 3). The number 3 is not Brazilian, so $p \neq 3$ and thus $p \equiv 2 \pmod 3$.

If $3|b$, then

$$p = b^{q-1} + b^{q-2} + \cdots + b + 1 \equiv 1 \pmod 3,$$

which is a contradiction. Lemma 1 states that $q$ is an odd prime, so if $b \equiv 2 \pmod 3$, then $p \equiv 1 \pmod 3$, a contradiction. We conclude that $b \equiv 1 \pmod 3$, so that $q \equiv p \pmod 3$, and therefore $q \equiv 2 \pmod 3$. □

For $q = 5$, we use a modification of the technique described in [7] to compute a table of length-5 Brazilian primes up to $10^{46}$. We will describe this computation in full in a forthcoming paper [2]. Of these, 104890280 are Sophie Germain primes.

The smallest is $28792661 = 73^4 + 73^3 + 73^2 + 73 + 1$. We very easily prove the primality of Sophie German primes with the Pocklington-Lehmer test.

For $q \geq 11$, we very quickly enumerate all possibilities for $b \leq 10^{46/(q-1)}$. We find 22 Brazilian Sophie Germain primes for $q = 11$, and none for larger $q$. (We have $q < \log_2 10^{46} + 1 < 154$.) The smallest is

$$14781835607449391161742645225951 = 1309^{10} + 1309^9 + \cdots + 1309 + 1.$$

While we disprove Schott's conjecture, we do have a related proposition.

**Proposition 1.** *The only Brazilian prime which is a safe prime is* 7*.*

*Proof.* If $p = b^{q-1} + \cdots + b + 1$ is a safe prime, then $\frac{p-1}{2} = \frac{1}{2}(b^{q-1} + \cdots + b)$ must also be prime. This expression, however, is divisible by $\frac{b(b+1)}{2}$, which is only prime when $b = 2$ and $p = 7$. □

The list of Brazilian Sophie Germain primes is A306845 in the OEIS. The first few counterexamples were also discovered by Giovanni Resta and Michel Marcus; see the comments for A085104.

## 3. Conditional Results

The infinitude of Brazilian Sophie Germain primes, as well as the asymptotic number of them, is the consequence of well-known conjectures.

**Proposition 2.** *Assuming Schnizel's Hypothesis H, there are infinitely many Brazilian Sophie Germain primes.*

*Proof.* Recall that Hypothesis H [4] says that any set of polynomials, whose product is not identically zero modulo any prime, is simultaneously prime infinitely often. Take our two polynomials to be $f_0(x) = x^4 + x^3 + x^2 + x + 1$ and $f_1(x) = 2x^4 + 2x^3 + 2x^2 + 2x + 3$. Then $f_0(b)$ is Brazilian and $f_1(b) = 2f_0(b) + 1$. Rather than checking congruences, it suffices to note the existence of the above primes of this form to see that the conditions of Hypothesis H are satisfied. □

The Bateman-Horn Conjecture [1] implies a more precise statement about the number of Brazilian Sophie Germain primes.

**Proposition 3.** *For an odd prime $q$, let $\Phi_q(x)$ be the $q$th cyclotomic polynomial. Assuming the Bateman-Horn Conjecture, the number of values of $b < x$ such that $\Phi_q(b)$ and $2\Phi_q(b) + 1$ are simultaneously prime is $0$ or $\sim C_q \frac{x}{\log^2 x}$, for some positive constant $C_q$, depending on whether $\Phi_q(b)(2\Phi_q(b) + 1)$ is identically zero modulo some prime $p$.*

*Proof.* This follows immediately from the Bateman-Horn conjecture, with $C_q = \left(\prod_p \frac{1-N(p)/p}{(1-1/p)^2}\right)/q^2$, where $N(p)$ is the number of roots of $\Phi_q(b)(2\Phi_q(b)+1)$ modulo $p$. □

**Corollary 1.** *Assuming the Bateman-Horn Conjecture, the number of Brazilian Sophie Germain primes up to $x$ is $\sim C\frac{x^{1/4}}{\log^2 x}$, for some $C$.*

*Proof.* To find the number of Brazilian Sophie Germain primes less than $y$ of the form $\Phi_q(b)$ for a fixed $q$, we apply the preceding proposition, substituting $x = y^{1/(q-1)}$, and get $\sim C'_q \frac{y^{1/(q-1)}}{\log^2 y}$, with $C'_q = C_q(q-1)^2$. We sum over all $q \equiv 2 \pmod 3$ and notice that the $q = 5$ term dominates. We can thus take $C = C'_5$. □

**Acknowledgement.** Thanks to Enrique Treviño for helping track down the reference in [6], and to the referee for helpful comments.

## References

[1] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962), 363–367.

[2] J. Grantham and H. Graves, Goldbach variations, in preparation, 2020.

[3] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[4] A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208; erratum 5 (1958), 259.

[5] B. Schott, Les nombres brésiliens, *Quadrature* (2010), 30–38.

[6] E. Wagner, G. T. de Araujo Moreira Carlos, P. Fauring, F. Gutiérrez, and A. Wykowski, *10 Olimpíadas Iberoamericanas de Matemática*, OEI, Madrid, 1996.

[7] M. Wolf, Some conjectures on primes of the form $m^2 + 1$, *J. Comb. Number Theory* **5** (2013), 103–131.

[8] R. E. Woodrow, The Olympiad corner, *Crux Mathematicorum* **24** (1998), 385–395.