Brazilian Primes

Jon Grantham
Hester Graves

Institute for Defense Analyses
Center for Computing Sciences
Bowie, Maryland

April 2019

Primes of the form $x^2 + x + 1$

- Last year at SERMON, I talked about computations of primes of the form $x^2 + 1$ for $x < 2.5 \times 10^{14}$.
- Previously, computed for $x < 10^{12.5}$ by Gerbicz and Wolf.
- This led to questions about other prime values of cyclotomic polynomials.

Primes of the form $x^2 + x + 1$

- Last year at SERMON, I talked about computations of primes of the form $x^2 + 1$ for $x < 2.5 \times 10^{14}$.
- Previously, computed for $x < 10^{12.5}$ by Gerbicz and Wolf.
- This led to questions about other prime values of cyclotomic polynomials.
- Let's ignore the cases $k = 1$ and $k = 2$ for now.

Primes of the form $x^2 + x + 1$

- Last year at SERMON, I talked about computations of primes of the form $x^2 + 1$ for $x < 2.5 \times 10^{14}$.
- Previously, computed for $x < 10^{12.5}$ by Gerbicz and Wolf.
- This led to questions about other prime values of cyclotomic polynomials.
- Let's ignore the cases $k = 1$ and $k = 2$ for now.
- For $k = 3$, the previous published computation appears to be up to 1.21×10^9, by Poletti (1929).
- It was easy to modify the $x^2 + 1$ code to compute a table up to 10^{12}.
- Fun fact: $\phi_3(x - 1) = \phi_6(x)$, so we have done the $k = 6$ case.

An Interlude about Luigi Poletti

- Luigi Poletti (1864-1967) was an banker from Pontremoli in Italy who stumbled across a book of Derrick Lehmer at age 47.
- He spoke at the 1928 ICM.
- After World War II, he served on a commission to rebuild French science.
- He wrote original poems in and translated Dante into his native dialect (Pontremolese).
- There is a Via Luigi Poletti in Pontremoli.

An Interlude about Luigi Poletti

- Luigi Poletti (1864-1967) was an banker from Pontremoli in Italy who stumbled across a book of Derrick Lehmer at age 47.
- He spoke at the 1928 ICM.
- After World War II, he served on a commission to rebuild French science.
- He wrote original poems in and translated Dante into his native dialect (Pontremolese).
- There is a Via Luigi Poletti in Pontremoli.
- We are going to call primes of the form $x^2 + x + 1$ "Poletti primes".

Brazilian Primes

- Brazilian Primes are primes that are all 1s (repunits) in some base $b > 1$ (of length q at least 3).
- For primes $q > 2$, primes represented by the qth cyclotomic polynomial are Brazilian primes.
- Originated at the 1994 Iberoamerican Mathematical Olympiad in Fonseca, Brazil, in a problem proposed by the Mexican math team.
- First studied by Schott (2010).
- Thanks to Hester for translating from the French.

$k = 5$

- It is possible to modify the existing algorithm to compute primes of the form $x^4 + x^3 + x^2 + x + 1$.
- But to compute up to $x < B$, we need to sieve up to B^2.
- So the running time is now $O(B^2 \log B \log\log B)$.
- In other words, a table for $B < 10^6$ would take as long as our $k = 3$ table for $B < 10^{12}$.

A better algorithm

- If we sieve up to B, we get numbers of the form $x^4 + x^3 + x^2 + x + 1$ which are B-rough.
- Heuristically, there should be $O(x/\log x)$ of these. (Buchstab)
- Need a fast way to distinguish primes from composites.

A better algorithm

- If we sieve up to B, we get numbers of the form $x^4 + x^3 + x^2 + x + 1$ which are B-rough.
- Heuristically, there should be $O(x/\log x)$ of these. (Buchstab)
- Need a fast way to distinguish primes from composites.
- The Pocklington–Lehmer test on N runs in $O(\log^2 N)$ time if you can fully factor a piece of $N-1$ of size $N^{1/2}$.
- Here, $N = x^4 + x^3 + x^2 + x + 1$, so $N - 1 = x^4 + x^3 + x^2 + x = x(x+1)(x^2+1)$. So you can!
- We can still generate a list up to B in time $O(B \log B \log\log B)$
- So verified up to 10^{12}.

A Conjecture

- Schott conjectured that there are no Brazilian Sophie Germain primes.
- Recall that a Sophie Germain prime is a prime p such that $2p + 1$ is also prime.
- If p is a Sophie Germain prime, then we say that $2p + 1$ is a “safe” prime.
- It is straightforward to show that if p is a Brazilian prime, then q is an odd prime.

A Lemma

- **If p is a Brazilian Sophie Germain prime, $p \equiv q \equiv 2 \pmod 3$ and $b \equiv 1 \pmod 3$.**
- If p is a Sophie Germain prime, then 3 cannot divide the safe prime $2p + 1$, so p cannot be congruent to $1 \pmod 3$.
- 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.
- 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 $q \equiv 2 \pmod 3$.

Finding Counterxamples

- So the key to looking for counterexamples is to look in our $k = 5$ list, not our list of Poletti primes.
- We find $28792661 = 73^4 + 73^3 + 73^2 + 73 + 1$ as the smallest example, and $104, 890, 302$ examples up to 10^{46}.

Finding Counterxamples

- So the key to looking for counterexamples is to look in our $k = 5$ list, not our list of Poletti primes.
- We find $28792661 = 73^4 + 73^3 + 73^2 + 73 + 1$ as the smallest example, and $104,890,302$ examples up to 10^{46}.
- (There are $104,890,282$ examples up to 10^{46}.)
- There are only 20 other Brazilian Sophie Germain primes up to 10^{46}, all of length 11.

Finding Counterxamples

- So the key to looking for counterexamples is to look in our $k = 5$ list, not our list of Poletti primes.
- We find $28792661 = 73^4 + 73^3 + 73^2 + 73 + 1$ as the smallest example, and $104,890,302$ examples up to 10^{46}.
- (There are $104,890,282$ examples up to 10^{46}.)
- There are only 20 other Brazilian Sophie Germain primes up to 10^{46}, all of length 11.
- The first few counterexamples were discovered independently by Giovanni Resta and Michel Marcus.

Finding Counterxamples

- So the key to looking for counterexamples is to look in our $k = 5$ list, not our list of Poletti primes.
- We find $28792661 = 73^4 + 73^3 + 73^2 + 73 + 1$ as the smallest example, and $104,890,302$ examples up to 10^{46}.
- (There are $104,890,282$ examples up to 10^{46}.)
- There are only 20 other Brazilian Sophie Germain primes up to 10^{46}, all of length 11.
- The first few counterexamples were discovered independently by Giovanni Resta and Michel Marcus.
- See A306845 in the On-Line Encyclopedia of Integer Sequences.

Conditional Results

- Recall that Schinzel's Hypothesis H says that any set of polynomials, whose product is not identically zero modulo any prime, is simultaneously prime infinitely often.
- Assuming Hypothesis H, there are infinitely many Brazilian Sophie Germain primes.

Conditional Results

- Recall that Schinzel's Hypothesis H says that any set of polynomials, whose product is not identically zero modulo any prime, is simultaneously prime infinitely often.
- Assuming Hypothesis H, there are infinitely many Brazilian Sophie Germain primes.
- Assuming the Bateman–Horn conjecture, the number of Brazilian Sophie Germain primes is $\sim C\frac{x^{1/4}}{\log x^2}$, for some C.
- (Look at the $k = 5$ case, and show that it dominates the others.)

A Related Proposition

- **Proposition:** The only Brazilian prime which is a safe prime is 7.
- 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 $p = 7$.

Future Work

- Extend tables?
- $k = 7$ requires use of Brillhart–Lehmer–Selfridge test (factorization of $N - 1$ up to $N^{1/3}$).
- Find application of Konyagin–Pomerance (which works with $N^{3/10}$).