Episode III: German Conjectures, an Italian Poet and Brazilian Primes

Jon Grantham

Institute for Defense Analyses
Center for Computing Sciences
Bowie, Maryland

February 2019

Episode I: Primes of the form $x^2 + 1$

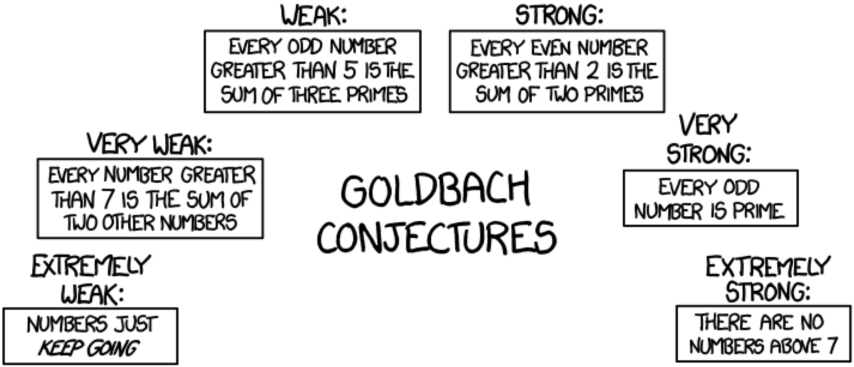
- At MASON I, I presented computations of primes of the form $x^2 + 1$ for $x < 2.5 \times 10^{14}$.
- Using a modified version of the sieve of Eratosthenes, you can compute for $x < B$ in time $O(B \log B \log\log B)$.
- The picture got more complicated for parallel computation.

- Let A be the set of numbers a for which $a^2 + 1$ is prime. Then every $a \in A$ $(a > 1)$ can be written in the form $a = b + c$, for $b, c \in A$.

Episode II: Goldbach's Other Other Conjecture

- Let A be the set of numbers a for which $a^2 + 1$ is prime. Then every $a \in A$ $(a > 1)$ can be written in the form $a = b + c$, for $b, c \in A$.
- This comes from a October 1, 1742 letter from Goldbach to Euler.
- At MASON II, I presented joint work with Hester Graves which verified this conjecture for $a < 2.5 \times 10^{14}$.

obxkcd



- At MASON II, I said, "I will never talk about this and not include this comic." So I guess I'm stuck.
-

Episode III: Cyclotomic Goldbach

- *Conjecture:* Let $\phi_k(x)$ be the kth cyclotomic polynomial.
- Let A_k be the set of positive integers such that $\phi_k(x)$ is prime.
- Then any (sufficiently large) positive (even) integer can be written as the sum of two elements in A_k.

Episode III: Cyclotomic Goldbach

- *Conjecture:* Let $\phi_k(x)$ be the kth cyclotomic polynomial.
- Let A_k be the set of positive integers such that $\phi_k(x)$ is prime.
- Then any (sufficiently large) positive (even) integer can be written as the sum of two elements in A_k.
- When $k = 1$ or $k = 2$, this implies the more famous Goldbach conjecture.
- When $k = 4$, this implies a stronger form of the less famous Goldbach conjecture.
- (In both of these cases "sufficiently large" is overkill, but "even" is needed.)

Episode III: Cyclotomic Goldbach

- *Conjecture:* Let $\phi_k(x)$ be the kth cyclotomic polynomial.
- Let A_k be the set of positive integers such that $\phi_k(x)$ is prime.
- Then any (sufficiently large) positive (even) integer can be written as the sum of two elements in A_k.
- When $k = 1$ or $k = 2$, this implies the more famous Goldbach conjecture.
- When $k = 4$, this implies a stronger form of the less famous Goldbach conjecture.
- (In both of these cases "sufficiently large" is overkill, but "even" is needed.)
- This formulation was prompted by an excellent question someone asked at MASON II.

What about $k = 3$?

- Now we are talking about the question of computation of primes of the form $x^2 + x + 1$.
- The largest published computation I could find was 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} and verify the conjecture.
- Still no exceptions, but all odd numbers greater than 1 are also represented as $a + b$ where $a^2 + a + 1$ and $b^2 + b + 1$ are prime.
- 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.

$k = 5$

- 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 $x^4 + x^3 + x^2 + 1$ 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 $x^4 + x^3 + x^2 + 1$ 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}.
- List of exceptions: $5, 6, 10, 11, 16, 21, 27, 33, 38, 49, 82, 484$.

Brazilian Primes

- Brazilian Primes are primes that are all 1s (repunits) in some base (of length at least 3).
- For primes $k > 2$, primes represented by the kth cyclotomic polynomial are Brazilian primes.
- First introduced by Schott (2010).
- Thanks to Hester for translating from the French.
- A number of interesting questions we hope to study.

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 $N^{3/10}$.
- This undoubtedly generalizes to arbitrary polynomials. Is there any fun there?
- Conditional proofs of cyclotomic Goldbach?