Young Mathematicians Conference 2018
The Ohio State University, August 10-12

Frequency of Elliptic Carmichael Numbers

Alice Lin (adlin@princeton.edu)
Calvin Yost-Wolff (calvinyw@mit.edu)
Boise State University [Mentor:Liljana Babinkostova]

Abstract of Report Talk: Efficiently distinguishing prime and composite numbers is a fundamental problem in number theory and cryptography. A Fermat pseudoprime is a composite number N which satisfies Fermat's Little Theorem for a specific base b: $b^{N-1} \equiv 1 \bmod N$. A Carmichael number N is a Fermat pseudoprime for all b with $\gcd(b, N) = 1$. In 2012, J. Silverman introduced elliptic pseudoprimes and elliptic Carmichael numbers, which are elliptic-curve analogues of Fermat pseudoprimes and Carmichael numbers.

Using techniques from analytic number theory, we provide probabilistic bounds for whether a fixed integer N is an elliptic Carmichael number for a randomly chosen elliptic curve with good reduction at every prime factor of N. For any N with a prime factor $p > N^{c \log(2)/\log\log N}$, $p^2 \nmid N$, we show that the probability that N is a Carmichael number for a random curve E is $\mathcal{O}\left(p^{-1/2+1.538/c+\epsilon}\right)$. We improve bounds given by J. Schlage-Puchta for the probability that a fixed N is an elliptic Carmichael number for a random curve when the largest prime factor p of N with $p^2 \nmid N$ is greater than $\log(N)^{f(N)}$ for some increasing, diverging function f or when $\omega(N)$, the number of distinct prime factors of N, is greater than $\left(\frac{1}{2} + \epsilon\right) \frac{\log N}{\log\log N}$ for any $\epsilon > 0$. Among other bounds, we show the probability N is a strong elliptic Carmichael number is $\mathcal{O}\left(\log(\omega(N))/3^{\omega(N)}\right)$.

[Joint work with Dylan Fillmore, Philip Lamkin]

Received: July 23, 2018