Elliptic curves from a statistical point of view

Avram Gottschlich

Abstract

In this thesis, we examine two statistical questions about groups of points on an elliptic curve E. We first look at the group of rational points on an elliptic curve to determine an upper bound on the number of $n \leq x$ for which $n \mid D_n$, where D_n is a sequence generated from the various $[n]\mathbf{P}$ for $\mathbf{P}$ a rational non-torsion point on E. This is based on work by Silverman and Stange. Our second question has to do with the size of the rank of the elliptic curve $E_d : y^2 + xy = x^3 - t^d$ over the function field $\mathbb{F}_q(t)$, d a positive integer, q a prime power. Specifically, a result of Ulmer gives a formula for the rank assuming d has certain properties; we focus on the set of numbers with those properties in particular. We establish an unconditional lower bound and a GRH-dependent upper bound for what the rank normally is, extending work of Pomerance and Shparlinski. In addition, let S be a set of primes with relative density α; let U be the set of integers n with all of their prime factors contained in S. We also consider normal values for the Carmichael lambda function $\lambda(d)$ and $\ell_q(d)$ (the order of q in $(\mathbb{Z}/d\mathbb{Z})^\times$) for $d \in U$, the latter of which is GRH-dependent.