PACIFIC JOURNAL OF MATHEMATICS
Vol. 131, No. 1, 1988

PRIMALITY OF THE NUMBER OF POINTS ON AN ELLIPTIC CURVE OVER A FINITE FIELD

NEAL KOBLITZ

Given a fixed elliptic curve E defined over Q having no rational torsion points, we discuss the probability that the number of points on E mod p is prime as the prime p varies. We give conjectural asymptotic formulas for the number of $p \leq n$ for which this number is prime, both in the case of a complex multiplication and a non-CM curve E. Numerical evidence is given supporting these formulas.

1. Let E be an elliptic curve defined over the field $\mathbf{Q}$ of rational numbers which has no rational torsion points. Motivated by an analogy with a classical question about finite fields (see §2) and by cryptographic applications (where certain public key cryptosystems use an elliptic curve whose group of points mod p has order divisible by a very large prime, see [**6**]), we ask the question: As the prime p varies, what is the probability that the number of points on E mod p is prime? After recalling analogous questions in classical number theory, in §3 we give a conjectural answer to this question in the case of elliptic curves without complex multiplication, and present some numerical evidence supporting the conjecture. In §4 we give a conjectural asymptotic formula in the case of CM curves, and decribe some supporting evidence.

2. In Hardy and Littlewood's paper [**4**] about the Goldbach conjecture and related questions, they give a conjectural asymptotic formula for half the number of twin primes (primes p for which $p + 2$ is prime) less than n:

$$(1) \quad C_2\frac{n}{(\log n)^2}, \quad \text{where } C_2 = \prod_{\text{primes } l\geq 3}\left(1 - \frac{1}{(l-1)^2}\right) \approx 0.660164.$$

The same heuristics lead to the identical asymptotic formula for a slightly different question (not considered in the Hardy-Littlewood paper): For how many primes $5 \leq p \leq n$ is $(p-1)/2$ prime? It should be recalled, by the way, that, as in the case of twin primes, no one has even been able to prove that there are infinitely many p such that both p and $(p-1)/2$ are prime.