Michigan Math. J. 62 (2013), 491–505

On the Lang–Trotter and Sato–Tate Conjectures on Average for Polynomial Families of Elliptic Curves

IGOR E. SHPARLINSKI

1. Introduction

1.1. BACKGROUND. For a prime p, we denote by $\mathbb{F}_p$ the finite field with p elements.

Given an elliptic curve $\mathbf{E}$ over $\mathbb{Q}$ and a prime p we use $\mathbf{E}(\mathbb{F}_p)$ to denote the set of the $\mathbb{F}_p$-rational points of the reduction of $\mathbf{E}$ modulo p, provided that p does not divide the discriminant $\Delta(\mathbf{E})$ of $\mathbf{E}$, together with a point at infinity. This set forms an *abelian group* under an appropriate composition rule and satisfies the *Hasse bound*:

$$|\#\mathbf{E}(\mathbb{F}_p) - p - 1| \le 2\sqrt{p}; \tag{1}$$

see [35] for background on elliptic curves.

Accordingly, we denote by $\Pi^{\mathrm{LT}}(\mathbf{E}, t; x)$ the number of primes $3 < p \le x$ (with $p \nmid \Delta(\mathbf{E})$) for which $\#\mathbf{E}(\mathbb{F}_p) = p + 1 - t$. The *Lang–Trotter conjecture* asserts that if $\mathbf{E}$ does not have complex multiplication then the asymptotic formula

$$\Pi^{\mathrm{LT}}(\mathbf{E}, t; x) \sim c(\mathbf{E}, t)\frac{\sqrt{x}}{\log x}, \quad x \to \infty, \tag{2}$$

holds for some explicitly given constant $c(\mathbf{E}, t) \ge 0$ depending only on $\mathbf{E}$ and t. Furthermore, the usual interpretation of the value $c(\mathbf{E}, t) = 0$ is $\Pi^{\mathrm{LT}}(\mathbf{E}, t; x) = O(1)$.

Since the Lang–Trotter conjecture (2) remains widely open (see [13; 14; 15; 26; 28; 29; 30; 32; 37]), it is natural to obtain its analogues "on average" over various interesting families of curves. As one example, for integers a and b such that $4a^3 + 27b^2 \ne 0$, we denote by $\mathbf{E}_{a,b}$ the elliptic curve defined by the *affine Weierstraß equation,*

$$\mathbf{E}_{a,b} : Y^2 = X^3 + aX + b,$$

and put

$$\Pi^{\mathrm{LT}}_{a,b}(t; x) = \Pi^{\mathrm{LT}}(\mathbf{E}_{a,b}, t; x).$$

Fouvry and Murty [17] initiated the study of $\Pi^{\mathrm{LT}}_{a,b}(t; x)$ and similar quantities on average, and they showed that the asymptotic formula

Received April 30, 2012. Revision received October 10, 2012.
This work was supported in part by ARC Grant no. DP1092835.