Michigan Math. J. 56 (2008)

Distribution of Modular Inverses and Multiples of Small Integers and the Sato–Tate Conjecture on Average

Igor E. Shparlinski

1. Introduction

1.1. Motivation

A rather old conjecture asserts that if $m = p$ is prime then, for any fixed $\varepsilon > 0$ and sufficiently large p, for every integer a there are integers x and y with $|x|, |y| \le p^{1/2+\varepsilon}$ and such that $a \equiv xy \pmod p$; see [14; 16; 17; 18] and references therein. The question has probably been motivated by the following observation. Using the Dirichlet pigeon-hole principle, one can easily show that, for every integer a, there exist integers x and y with $|x|, |y| \le 2p^{1/2}$ and with $a \equiv y/x \pmod p$. Unfortunately, this is known only with $|x|, |y| \ge Cp^{3/4}$ for some absolute constant $C > 0$, which is due to Garaev [15].

On the other hand, it has been shown in the series of works [14; 16; 17; 18] that the congruence $a \equiv xy \pmod p$ is solvable for all but $o(m)$ values of $a = 1, \dots, m-1$, where x and y are significantly smaller than $m^{3/4}$. In particular, it is shown by Garaev and Karatsuba [17] for x and y in the range $1 \le x, y \le m^{1/2}(\log m)^{1+\varepsilon}$. Certainly this result is very sharp. Indeed, it has been observed by Garaev [14] that well-known estimates for integers with a divisor in a given interval immediately imply that, for any $\varepsilon > 0$, almost all residue classes modulo m are *not* of the form $xy \pmod m$ with $1 \le x, y \le m^{1/2}(\log m)^{\kappa-\varepsilon}$, where

$$\kappa = 1 - \frac{1 + \log\log 2}{\log 2} = 0.08607\dots.$$

One can also derive from [10] that, for any $\varepsilon > 0$, the inequality

$$\max\{|x|, |y| : xy \equiv 1 \pmod m\} \ge m^{1/2}(\log m)^{\kappa/2}(\log\log m)^{3/4-\varepsilon}$$

holds:

- for all positive integers $m \le M$, except for possibly $o(M)$ of them;
- for all prime $m = p \le M$, except for possibly $o(M/\log M)$ of them.

Similar questions about the ratios x/y have also been studied; see [14; 17; 28].

Received December 5, 2006. Revision received July 5, 2007.
This work was supported in part by ARC grant DP0556431.