**Michigan Math. J. 59 (2010), 313–328**

# On the Divisibility of Fermat Quotients

JEAN BOURGAIN, KEVIN FORD,
SERGEI V. KONYAGIN, & IGOR E. SHPARLINSKI

## 1. Introduction

For a prime $p$ and an integer $a$ the *Fermat quotient* is defined as

$$q_p(a) = \frac{a^{p-1} - 1}{p}.$$

It is well known that divisibility of Fermat quotients $q_p(a)$ by $p$ has numerous applications, which include Fermat's last theorem and squarefreeness testing; see [6; 7; 8; 16].

In particular, the smallest value $\ell_p$ of $a$ for which $q_p(a) \not\equiv 0 \pmod p$ plays a prominent role in these applications. In this direction, Lenstra [16, Thm. 3] has shown that

$$\ell_p \le \begin{cases} 4(\log p)^2 & \text{if } p \ge 3, \\ (4e^{-2} + o(1))(\log p)^2 & \text{if } p \to \infty; \end{cases} \tag{1}$$

see also [7]. Granville [9, Thm. 5] has shown that in fact

$$\ell_p \le (\log p)^2 \tag{2}$$

for $p \ge 5$.

A very different proof of a slightly weaker bound $\ell_p \le (4 + o(1))(\log p)^2$ has been obtained by Ihara [12] as a by-product of the estimate

$$\sum_{\substack{\ell^k < p \\ \ell \in \mathcal{W}(p)}} \frac{\log \ell}{\ell^k} \le 2 \log\log p + 2 + o(1) \tag{3}$$

as $p \to \infty$, where the summation is taken over all prime powers up to $p$ of primes $\ell$ from the set

$$\mathcal{W}(p) = \{\ell \text{ prime} : \ell < p,\ q_p(\ell) \equiv 0 \pmod p\}.$$

However, the proof of (3) given in [12] is conditional on the extended Riemann hypothesis.

It has been conjectured by Granville [8, Conj. 10] that

$$\ell_p = o((\log p)^{1/4}). \tag{4}$$

Received December 22, 2008. Revision received August 14, 2009.