# Accepted Manuscript


The $p$-adic valuations of Weil sums of binomials

Daniel J. Katz, Philippe Langevin, Lee Sangman, Yakov Sapozhnikov

PII: S0022-314X(17)30222-6
DOI: http://dx.doi.org/10.1016/j.jnt.2017.05.020
Reference: YJNTH 5785

To appear in: *Journal of Number Theory*

Received date: 22 October 2016
Revised date: 20 March 2017
Accepted date: 1 May 2017

Please cite this article in press as: D.J. Katz et al., The $p$-adic valuations of Weil sums of binomials, *J. Number Theory* (2017), http://dx.doi.org/10.1016/j.jnt.2017.05.020

# The $p$-Adic Valuations of Weil Sums of Binomials

Daniel J. Katz[a,1,*], Philippe Langevin[b], Sangman Lee[a,1], Yakov Sapozhnikov[a,1]

[a]Department of Mathematics, California State University, 18111 Nordhoff Street, Northridge, CA 91330, United States
[b]Institut de Mathématiques de Toulon, Université de Toulon, Avenue de l'Université, 83957 La Garde Cedex, France

## Abstract

We investigate the $p$-adic valuation of Weil sums of the form $W_{F,d}(a) = \sum_{x \in F} \psi(x^d - ax)$, where $F$ is a finite field of characteristic $p$, $\psi$ is the canonical additive character of $F$, the exponent $d$ is relatively prime to $|F^\times|$, and $a$ is an element of $F$. Such sums often arise in arithmetical calculations and also have applications in information theory. For each $F$ and $d$ one would like to know $V_{F,d}$, the minimum $p$-adic valuation of $W_{F,d}(a)$ as $a$ runs through the elements of $F$. We exclude exponents $d$ that are congruent to a power of $p$ modulo $|F^\times|$ (degenerate $d$), which yield trivial Weil sums. We prove that $V_{F,d} \leq (2/3)[F\colon \mathbb{F}_p]$ for any $F$ and any nondegenerate $d$, and prove that this bound is actually reached in infinitely many fields $F$. We also prove some stronger bounds that apply when $[F\colon \mathbb{F}_p]$ is a power of 2 or when $d$ is not congruent to 1 modulo $p-1$, and show that each of these bounds is reached for infinitely many $F$.

*Keywords:* Weil sum, character sum, finite field, valuation, $p$-divisibility
*2010 MSC:* Primary: 11L40, 11L07, 11L05, 11T23, Secondary: 11T71, 05D99

*corresponding author
*Email addresses:* daniel.katz@csun.edu (Daniel J. Katz), langevin@univ-tln.fr (Philippe Langevin), sangman.lee.145@my.csun.edu (Sangman Lee), yakov.sapozhnikov.473@my.csun.edu (Yakov Sapozhnikov)

[1]The work of Katz, Lee, and Sapozhnikov on this paper was supported in part by the National Science Foundation under Grant DMS 1500856.