

# 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>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



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

Daniel J. Katz<sup>a,1,\*</sup>, Philippe Langevin<sup>b</sup>, Sangman Lee<sup>a,1</sup>, Yakov  
Sapozhnikov<sup>a,1</sup>

<sup>a</sup>*Department of Mathematics, California State University, 18111 Nordhoff Street,  
Northridge, CA 91330, United States*

<sup>b</sup>*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  $V_{F,d} \leq (2/3)[F : \mathbb{F}_p]$  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  $[F : \mathbb{F}_p]$  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)

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

Download English Version:

<https://daneshyari.com/en/article/5772646>

Download Persian Version:

<https://daneshyari.com/article/5772646>

[Daneshyari.com](https://daneshyari.com)