

involve

a journal of mathematics

The average order of elements
in the multiplicative group of a finite field

Yilan Hu and Carl Pomerance



The average order of elements in the multiplicative group of a finite field

Yilan Hu and Carl Pomerance

(Communicated by Kenneth S. Berenhaut)

We consider the average multiplicative order of a nonzero element in a finite field and compute the mean of this statistic for all finite fields of a given degree over their prime fields.

1. Introduction

For a cyclic group of order n , let $\alpha(n)$ denote the average order of an element. For each $d \mid n$, there are exactly $\varphi(d)$ elements of order d in the group (where φ is Euler's function), so

$$\alpha(n) = \frac{1}{n} \sum_{d \mid n} d\varphi(d).$$

It is known [von zur Gathen 2004] that

$$\frac{1}{x} \sum_{n \leq x} \alpha(n) = \frac{3\zeta(3)}{\pi^2} x + O((\log x)^{2/3} (\log \log x)^{4/3}).$$

We are interested here in obtaining an analogous result where n runs over the orders of the multiplicative groups of finite fields. Let p denote a prime number. We know that up to isomorphism, for each positive integer k , there is a unique finite field of p^k elements. The multiplicative group for this field is cyclic of size $p^k - 1$. We are concerned with the average order of an element in this cyclic group as p varies. We show the following results.

Theorem 1. *For each positive integer k there is a positive constant K_k such that the following holds. For each number $A > 0$, each number $x \geq 2$, and each positive*

MSC2010: 11B05, 11B75.

Keywords: average multiplicative order, finite field.

This paper is based on Hu's 2010 Dartmouth honors thesis, written under the direction of Pomerance. Both authors gratefully acknowledge Florian Luca, who suggested the problem. Pomerance was supported in part by NSF grant DMS-1001180.

integer k with $k \leq (\log x)/(2 \log \log x)$, we have

$$\frac{1}{\pi(x)} \sum_{p \leq x} \frac{\alpha(p^k - 1)}{p^k - 1} = K_k + O_A \left(\frac{1}{\log^A x} \right).$$

This theorem in the case $k = 1$ appears in [Luca 2005]. Using Theorem 1 and a partial summation argument we are able to show the following consequence.

Corollary 2. *For all numbers $A > 0$, $x \geq 2$, and for any positive integer $k \leq (\log x)/(2 \log \log x)$, we have*

$$\frac{1}{\pi(x)} \sum_{p \leq x} \alpha(p^k - 1) = K_k \frac{\text{li}(x^{k+1})}{\text{li}(x)} + O_A \left(\frac{x^k}{\log^A x} \right),$$

where K_k is the constant from Theorem 1 and $\text{li}(x) := \int_2^x dt / \log t$.

Since $\text{li}(x^{k+1})/\text{li}(x) \sim x^k/(k+1)$ as $x \rightarrow \infty$, Corollary 2 implies that

$$\frac{1}{\pi(x)} \sum_{p \leq x} \alpha(p^k - 1) \sim \frac{K_k}{k+1} x^k, \text{ as } x \rightarrow \infty.$$

We identify the constants K_k as follows. Let $N_k(n)$ denote the number of solutions to the congruence $s^k \equiv 1 \pmod{n}$.

Proposition 3. *For each prime p and positive integer k let*

$$S_k(p) = \sum_{j=1}^{\infty} \frac{N_k(p^j)}{p^{3j-1}}.$$

Then $S_k(p) < 1$ and

$$K_k := \prod_p (1 - S_k(p))$$

is a real number with $0 < K_k < 1$.

2. Preliminary results

In this section we prove Proposition 3 and we also prove a lemma concerning the function $N_k(n)$.

Proof of Proposition 3. We clearly have $N_k(n) \leq \varphi(n)$ for every n , since $N_k(n)$ counts the number of elements in the group $(\mathbb{Z}/n\mathbb{Z})^*$ with order dividing k and there are $\varphi(n)$ elements in all in this group. Thus, we have

$$S_k(p) \leq \sum_{j=1}^{\infty} \frac{\varphi(p^j)}{p^{3j-1}} = \left(1 - \frac{1}{p}\right) \sum_{j=1}^{\infty} \frac{p}{p^{2j}} = \left(1 - \frac{1}{p}\right) \frac{p}{p^2 - 1} = \frac{1}{p+1}.$$

This proves the first assertion, but it is not sufficient for the second assertion. For p an odd prime, the group $(\mathbb{Z}/p^j\mathbb{Z})^*$ is cyclic so that the number of elements in this group of order dividing k is

$$N_k(p^j) = \gcd(k, \varphi(p^j)). \tag{1}$$

The same holds for $p^j = 2$ or 4 , or if $p = 2$ and k is odd. Suppose now that $p = 2$, $j \geq 3$, and k is even. Since $(\mathbb{Z}/2^j\mathbb{Z})^*$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{j-2} , we have

$$N_k(2^j) = 2 \cdot \gcd(k, 2^{j-2}) = \gcd(2k, \varphi(2^j)). \tag{2}$$

Thus, we always have $N_k(p^j) \leq 2k$, and so

$$S_k(p) \leq \sum_{j=1}^{\infty} \frac{2k}{p^{3j-1}} = \frac{2kp}{p^3 - 1}.$$

In particular, we have $S_k(p) = O_k(1/p^2)$, which with our first assertion implies that the product for K_k converges to a positive real number that is less than 1. This completes the proof. \square

Lemma 4. *For every positive integer k and each real number $x \geq 1$ we have*

$$\sum_{n \leq x} \frac{N_k(n)}{n} \leq 2(1 + \log x)^k.$$

Proof. Let $\omega(n)$ denote the number of distinct primes that divide n and let $\tau_k(n)$ denote the number of ordered factorizations of n into k positive integral factors. Since $k^{\omega(n)}$ is the number of ordered factorizations of n into k pairwise coprime factors, we have $k^{\omega(n)} \leq \tau_k(n)$ for all n . Further, from (1), (2) and the fact that $N_k(n)$ is multiplicative in the variable n , we have $N_k(n) \leq 2k^{\omega(n)}$, so that $N_k(n) \leq 2\tau_k(n)$. Thus, it suffices to show that

$$\sum_{n \leq x} \frac{\tau_k(n)}{n} \leq (1 + \log x)^k. \tag{3}$$

We prove (3) by induction on k . It holds for $k = 1$ since $\tau_1(n) = 1$ for all n , so that

$$\sum_{n \leq x} \frac{N_1(n)}{n} = \sum_{n \leq x} \frac{1}{n} \leq 1 + \int_1^x \frac{dt}{t} = 1 + \log x.$$

Assume now that $k \geq 1$ and that (3) holds for k . Since

$$\tau_{k+1}(n) = \sum_{d|n} \tau_k(n/d),$$

we have

$$\begin{aligned} \sum_{n \leq x} \frac{\tau_{k+1}(n)}{n} &= \sum_{n \leq x} \frac{1}{n} \sum_{d|n} \tau_k(d) = \sum_{d \leq x} \frac{\tau_k(d)}{d} \sum_{m \leq x/d} \frac{1}{m} \\ &\leq \sum_{d \leq x} \frac{\tau_k(d)}{d} (1 + \log x) \leq (1 + \log x)^{k+1}, \end{aligned}$$

by the induction hypothesis. This completes the proof. □

Corollary 5. *For k a positive integer and y a positive real with $k \leq 1 + \log y$, we have*

$$\sum_{n > y} \frac{N_k(n)}{n^2} \leq 2(k + 1) \frac{(1 + \log y)^k}{y}.$$

Proof. By partial summation, Lemma 4, and integration by parts, we have

$$\begin{aligned} \sum_{n > y} \frac{N_k(n)}{n^2} &= \int_y^\infty \frac{1}{t^2} \sum_{y < n \leq t} \frac{N_k(n)}{n} dt \leq 2 \int_y^\infty \frac{(1 + \log t)^k}{t^2} dt \\ &= \frac{2}{y} ((1 + \log y)^k + k(1 + \log y)^{k-1} + k(k - 1)(1 + \log y)^{k-2} + \dots + k!) \\ &\leq 2(k + 1) \frac{(1 + \log y)^k}{y}, \end{aligned}$$

using $k \leq 1 + \log y$. This completes the proof. □

3. The main theorem

Proof of Theorem 1. The function

$$\frac{\alpha(m)}{m} = \frac{1}{m^2} \sum_{n|m} n\varphi(n)$$

is multiplicative and so by Möbius inversion, we may write

$$\frac{\alpha(m)}{m} = \sum_{n|m} \gamma(n),$$

where γ is a multiplicative function. It is easy to compute that

$$\gamma(p^j) = -\frac{p - 1}{p^{2j}} \tag{4}$$

for every prime p and positive integer j . If $\text{rad}(n)$ denotes the largest squarefree divisor of n , we thus have

$$\gamma(n) = (-1)^{\omega(n)} \frac{\varphi(\text{rad}(n))}{n^2} \tag{5}$$

for each positive integer n . Note that (4), (5) are also in [Luca 2005].

For n a positive integer, label the $N_k(n)$ roots to the congruence $s^k \equiv 1 \pmod{n}$ as $s_{k,1}, s_{k,2}, \dots, s_{k,N_k(n)}$. We have

$$\begin{aligned} \sum_{p \leq x} \frac{\alpha(p^k - 1)}{p^k - 1} &= \sum_{p \leq x} \sum_{n|p^k-1} \gamma(n) = \sum_{n \leq x^k-1} \gamma(n) \sum_{\substack{p \leq x \\ n|p^k-1}} 1 \\ &= \sum_{n \leq x^k-1} \gamma(n) \sum_{i=1}^{N_k(n)} \pi(x; n, s_{k,i}), \end{aligned}$$

where $\pi(x; q, a)$ denotes the number of primes $p \leq x$ with $p \equiv a \pmod{q}$.

If q is not too large in comparison to x and if a is coprime to q , we expect $\pi(x; q, a)$ to be approximately $\pi(x)/\varphi(q)$. With this thought in mind, let $E_{q,a}(x)$ be defined by the equation

$$\pi(x; q, a) = \frac{1}{\varphi(q)} \pi(x) + E_{q,a}(x).$$

Further, let $y = x^{1/2} / \log^{A+4} x$, where A is as in the statement of Theorem 1. From the above, we thus have

$$\begin{aligned} &\sum_{p \leq x} \frac{\alpha(p^k - 1)}{p^k - 1} \\ &= \sum_{n \leq x^k-1} \gamma(n) \sum_{i=1}^{N_k(n)} \pi(x; n, s_{k,i}) \\ &= \sum_{n \leq y} \frac{\gamma(n) N_k(n)}{\varphi(n)} \pi(x) + \sum_{n \leq y} \gamma(n) \sum_{i=1}^{N_k(n)} E_{n,s_{k,i}}(x) + \sum_{y < n \leq x^k-1} \gamma(n) \sum_{i=1}^{N_k(n)} \pi(x; n, s_{k,i}) \\ &=: T_1 + T_2 + T_3, \text{ say.} \end{aligned}$$

We further refine the main term T_1 as

$$T_1 = \pi(x) \sum_{n=1}^{\infty} \frac{\gamma(n) N_k(n)}{\varphi(n)} - \pi(x) \sum_{n > y} \frac{\gamma(n) N_k(n)}{\varphi(n)}.$$

The first sum here has an Euler product as

$$\sum_{n=1}^{\infty} \frac{\gamma(n) N_k(n)}{\varphi(n)} = \prod_p \left(1 + \sum_{j=1}^{\infty} \frac{\gamma(p^j) N_k(p^j)}{\varphi(p^j)} \right) = \prod_p \left(1 - \sum_{j=1}^{\infty} \frac{N_k(p^j)}{p^{3j-1}} \right) = K_k,$$

where we used (4). For the second sum in the expression for T_1 , we have by (5) and Corollary 5,

$$\left| \sum_{n>y} \frac{\gamma(n)N_k(n)}{\varphi(n)} \right| \leq \sum_{n>y} \frac{N_k(n)}{n^2} \leq 2(k+1) \frac{(1+\log y)^k}{y}.$$

Here we have used $k \leq (\log x)/(2 \log \log x)$ and $y = x^{1/2}/\log^{A+4} x$, so that $k \leq 1 + \log y$ for all sufficiently large x depending on the choice of A . Further, with these choices for k, y we have $(1 + \log y)^k < x^{1/2}$ for x sufficiently large, so that

$$\pi(x) \left| \sum_{n>y} \frac{\gamma(n)N_k(n)}{\varphi(n)} \right| \leq \pi(x) \frac{2(k+1)(1+\log y)^k}{y} \leq \frac{\pi(x)}{\exp \frac{\log x}{3 \log \log x}}$$

for all sufficiently large values of x depending on A . Thus,

$$T_1 = K_k \pi(x) + O_A(\pi(x)/\log^A x).$$

It remains to show that both T_2 and T_3 are $O_A(\pi(x)/\log^A x)$. Using the elementary estimate $\pi(x; q, a) \leq 1 + x/q$, we have

$$|T_3| \leq \sum_{y < n \leq x^k - 1} |\gamma(n)| N_k(n) \left(1 + \frac{x}{n}\right) \leq \sum_{y < n \leq x^k - 1} \frac{N_k(n)}{n} + x \sum_{y < n \leq x^k - 1} \frac{N_k(n)}{n^2},$$

by (5). We have seen that the second sum here is negligible, and the first sum is bounded by $2(1 + k \log x)^k$ using Lemma 4. This last expression is smaller than

$$\left(\frac{\log^2 x}{\log \log x}\right)^k \leq \frac{x}{\exp \frac{\log x \log \log \log x}{2 \log \log x}} = O_A\left(\frac{\pi(x)}{\log^A x}\right)$$

for any fixed choice of A .

To estimate T_2 , note that

$$\begin{aligned} |T_2| &\leq \sum_{n \leq y} |\gamma(n)| N_k(n) \max_{(a,n)=1} \left| \pi(x; n, a) - \frac{1}{\varphi(n)} \pi(x) \right| \\ &\leq \sum_{n \leq y} \max_{(a,n)=1} \left| \pi(x; n, a) - \frac{1}{\varphi(n)} \pi(x) \right|, \end{aligned}$$

since $|\gamma(n)| \leq \varphi(n)/n^2 \leq 1/n$ and $N_k(n) \leq \varphi(n) \leq n$. Thus, by the Bombieri–Vinogradov theorem (see [Davenport 2000, Chapter 28]) we have

$$|T_2| = O_A(\pi(x)/\log^A x),$$

by our choice of y . These estimates conclude our proof of Theorem 1. □

4. Proof of Corollary 2 and more on the constants K_k

Proof of Corollary 2. By partial summation, we have

$$\begin{aligned} \sum_{p \leq x} \alpha(p^k - 1) &= \sum_{p \leq x} \frac{\alpha(p^k - 1)}{p^k - 1} (p^k - 1) \\ &= (x^k - 1) \sum_{p \leq x} \frac{\alpha(p^k - 1)}{p^k - 1} - \int_2^x kt^{k-1} \sum_{p \leq t} \frac{\alpha(p^k - 1)}{p^k - 1} dt. \end{aligned}$$

Thus, by Theorem 1, the prime number theorem, and integration by parts, we have

$$\begin{aligned} \sum_{p \leq x} \alpha(p^k - 1) &= (x^k - 1)K_k\pi(x) - \int_2^x kt^{k-1}K_k\pi(t) dt + O\left(\frac{\pi(x)x^k}{\log^A x}\right) \\ &= (x^k - 1)K_k\text{li}(x) - \int_2^x kt^{k-1}K_k\text{li}(t) dt + O\left(\frac{\pi(x)x^k}{\log^A x}\right) \\ &= \int_2^x K_k \frac{t^k}{\log t} dt + O\left(\frac{\pi(x)x^k}{\log^A x}\right). \end{aligned}$$

This last integral is $K_k\text{li}(x^{k+1}) - K_k\text{li}(2^{k+1})$, so the corollary now follows via one additional call to the prime number theorem. □

We now examine the constants K_k for $k \leq 4$. Since $N_1(p^j) = 1$ for all p^j , we have

$$K_1 = \prod_p \left(1 - \sum_{j \geq 1} \frac{p}{p^{3j}}\right) = \prod_p \left(1 - \frac{p}{p^3 - 1}\right) = 0.5759599689 \dots$$

(This constant is also worked out in [Luca 2005].) For K_2 we note that $N_2(p^j) = 2$ for all prime powers p^j except that $N_2(2) = 1$ and $N_2(2^j) = 4$ for $j \geq 3$. Thus,

$$\sum_{j \geq 1} \frac{N_2(2^j)}{2^{3j-1}} = \frac{1}{4} + \frac{2}{32} + \frac{1}{56} = \frac{37}{112},$$

and so

$$K_2 = \frac{75}{112} \prod_{p > 2} \left(1 - \frac{2p}{p^3 - 1}\right) = 0.4269891575 \dots$$

For K_3 , we have $N_3(p^j) = 3$ for $p \equiv 1 \pmod{3}$ and for $p = 3$ and $j \geq 2$. Otherwise, $N_3(p^j) = 1$. Thus,

$$K_3 = \frac{205}{234} \prod_{p \equiv 1 \pmod{3}} \left(1 - \frac{3p}{p^3 - 1}\right) \prod_{p \equiv 2 \pmod{3}} \left(1 - \frac{p}{p^3 - 1}\right) = 0.6393087751 \dots$$

For K_4 , we have $N_4(p^j) = 4$ for $p \equiv 1 \pmod{4}$, $N_4(p^j) = 2$ for $p \equiv 3 \pmod{4}$, $N_4(2) = 1$, $N_4(2^2) = 2$, $N_4(2^3) = 4$, and $N_4(2^j) = 8$ for $j \geq 4$. Thus,

$$K_4 = \frac{299}{448} \prod_{p \equiv 1 \pmod{4}} \left(1 - \frac{4p}{p^3 - 1}\right) \prod_{p \equiv 3 \pmod{4}} \left(1 - \frac{2p}{p^3 - 1}\right) = 0.3775394971 \dots$$

These calculations were done with the aid of Mathematica. With a little effort other constants K_k may be computed, but if k has many divisors, the calculation gets more tedious.

We close with the observation that there is an infinite sequence of numbers k on which $K_k \rightarrow 0$. In particular, if $k = k_m$ is the least common multiple of all numbers up to m , then $N_k(p) = p - 1$ for every prime $p \leq m + 1$, so that

$$K_k < \prod_p \left(1 - \frac{N_k(p)}{p^2}\right) < \prod_{p \leq m+1} \left(1 - \frac{p-1}{p^2}\right).$$

Since $\sum (p-1)/p^2 = +\infty$, it follows that as $m \rightarrow \infty$, $K_{k_m} \rightarrow 0$. Using the theorem of Mertens, we in fact have $\liminf K_k \log \log k < +\infty$.

References

- [Davenport 2000] H. Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics **74**, Springer, New York, 2000. MR 2001f:11001 Zbl 1002.11001
- [Luca 2005] F. Luca, "Some mean values related to average multiplicative orders of elements in finite fields", *Ramanujan J.* **9**:1-2 (2005), 33–44. MR 2006i:11111 Zbl 1155.11344
- [von zur Gathen 2004] J. von zur Gathen, A. Knopfmacher, F. Luca, L. G. Lucht, and I. E. Shparlinski, "Average order in cyclic groups", *J. Théor. Nombres Bordeaux* **16**:1 (2004), 107–123. MR 2006d:11111 Zbl 1079.11003

Received: 2011-12-07 Revised: 2012-01-11 Accepted: 2012-01-13

yilan.hu.10@alum.dartmouth.org 55 Maple Hill Road, Thetford Center, VT 05075,
United States

carl.pomerance@dartmouth.edu Mathematics Department, Kemeny Hall,
Dartmouth College, Hanover, NH 03755, United States
www.math.dartmouth.edu/~carlp

involve

msp.berkeley.edu/involve

EDITORS

MANAGING EDITOR

Kenneth S. Berenhaut, Wake Forest University, USA, berenhks@wfu.edu

BOARD OF EDITORS

Colin Adams	Williams College, USA colin.c.adams@williams.edu	David Larson	Texas A&M University, USA larson@math.tamu.edu
John V. Baxley	Wake Forest University, NC, USA baxley@wfu.edu	Suzanne Lenhart	University of Tennessee, USA lenhart@math.utk.edu
Arthur T. Benjamin	Harvey Mudd College, USA benjamin@hmc.edu	Chi-Kwong Li	College of William and Mary, USA ckli@math.wm.edu
Martin Bohner	Missouri U of Science and Technology, USA bohner@mst.edu	Robert B. Lund	Clemson University, USA lund@clemson.edu
Nigel Boston	University of Wisconsin, USA boston@math.wisc.edu	Gaven J. Martin	Massey University, New Zealand g.j.martin@massey.ac.nz
Amarjit S. Budhiraja	U of North Carolina, Chapel Hill, USA budhiraj@email.unc.edu	Mary Meyer	Colorado State University, USA meyer@stat.colostate.edu
Pietro Cerone	Victoria University, Australia pietro.cerone@vu.edu.au	Emil Minchev	Ruse, Bulgaria eminchev@hotmail.com
Scott Chapman	Sam Houston State University, USA scott.chapman@shsu.edu	Frank Morgan	Williams College, USA frank.morgan@williams.edu
Jem N. Corcoran	University of Colorado, USA corcoran@colorado.edu	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran moslehian@ferdowsi.um.ac.ir
Toka Diagana	Howard University, USA tdiagana@howard.edu	Zuhair Nashed	University of Central Florida, USA znashed@mail.ucf.edu
Michael Dorff	Brigham Young University, USA mdorff@math.byu.edu	Ken Ono	Emory University, USA ono@mathcs.emory.edu
Sever S. Dragomir	Victoria University, Australia sever@matilda.vu.edu.au	Timothy E. O'Brien	Loyola University Chicago, USA tobrie1@luc.edu
Behrouz Emamizadeh	The Petroleum Institute, UAE bemamizadeh@pi.ac.ae	Joseph O'Rourke	Smith College, USA orourke@cs.smith.edu
Joel Foisy	SUNY Potsdam foisyjs@potsdam.edu	Yuval Peres	Microsoft Research, USA peres@microsoft.com
Errin W. Fulp	Wake Forest University, USA fulp@wfu.edu	Y.-F. S. Pétermann	Université de Genève, Switzerland petermann@math.unige.ch
Joseph Gallian	University of Minnesota Duluth, USA jgallian@d.umn.edu	Robert J. Plemmons	Wake Forest University, USA rplemmons@wfu.edu
Stephan R. Garcia	Pomona College, USA stephan.garcia@pomona.edu	Carl B. Pomerance	Dartmouth College, USA carl.pomerance@dartmouth.edu
Anant Godbole	East Tennessee State University, USA godbole@etsu.edu	Vadim Ponomarenko	San Diego State University, USA vadim@sciences.sdsu.edu
Ron Gould	Emory University, USA rg@mathcs.emory.edu	Bjorn Poonen	UC Berkeley, USA poonen@math.berkeley.edu
Andrew Granville	Université Montréal, Canada andrew@dms.umontreal.ca	James Propp	U Mass Lowell, USA jpropp@cs.uml.edu
Jerrold Griggs	University of South Carolina, USA griggs@math.sc.edu	József H. Przytycki	George Washington University, USA przytyck@gwu.edu
Ron Gould	Emory University, USA rg@mathcs.emory.edu	Richard Rebarber	University of Nebraska, USA rrebarbe@math.unl.edu
Sat Gupta	U of North Carolina, Greensboro, USA sngupta@uncg.edu	Robert W. Robinson	University of Georgia, USA rwr@cs.uga.edu
Jim Haglund	University of Pennsylvania, USA jhaglund@math.upenn.edu	Filip Saidak	U of North Carolina, Greensboro, USA f_saidak@uncg.edu
Johnny Henderson	Baylor University, USA johnny_henderson@baylor.edu	James A. Sellers	Penn State University, USA sellersj@math.psu.edu
Jim Hoste	Pitzer College jhoste@pitzer.edu	Andrew J. Sterge	Honorary Editor andy@ajsterge.com
Natalia Hritonenko	Prairie View A&M University, USA nahritonenko@pvamu.edu	Ann Trenk	Wellesley College, USA atrenk@wellesley.edu
Glenn H. Hurlbert	Arizona State University, USA hurlbert@asu.edu	Ravi Vakil	Stanford University, USA vakil@math.stanford.edu
Charles R. Johnson	College of William and Mary, USA crjohnso@math.wm.edu	Ram U. Verma	University of Toledo, USA verma99@msn.com
K. B. Kulasekera	Clemson University, USA kk@ces.clemson.edu	John C. Wierman	Johns Hopkins University, USA wierman@jhu.edu
Gerry Ladas	University of Rhode Island, USA gladas@math.uri.edu	Michael E. Zieve	University of Michigan, USA zieve@umich.edu

PRODUCTION

Silvio Levy, Scientific Editor

Sheila Newbery, Senior Production Editor

Cover design: © 2008 Alex Scorpan

See inside back cover or <http://msp.berkeley.edu/involve> for submission instructions.

The subscription price for 2012 is US \$105/year for the electronic version, and \$145/year (+\$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY



mathematical sciences publishers

<http://msp.org/>

A NON-PROFIT CORPORATION

Typeset in L^AT_EX

Copyright ©2012 by Mathematical Sciences Publishers

involve

2012

vol. 5

no. 2

A Giambelli formula for the S^1 -equivariant cohomology of type A Peterson varieties DARIUS BAYEGAN AND MEGUMI HARADA	115
Weak Allee effect, grazing, and S-shaped bifurcation curves EMILY POOLE, BONNIE ROBERSON AND BRITTANY STEPHENSON	133
A BMO theorem for ϵ -distorted diffeomorphisms on \mathbb{R}^D and an application to comparing manifolds of speech and sound CHARLES FEFFERMAN, STEVEN B. DAMELIN AND WILLIAM GLOVER	159
Modular magic sudoku JOHN LORCH AND ELLEN WELD	173
Distribution of the exponents of primitive circulant matrices in the first four boxes of \mathbb{Z}_n . MARIA ISABEL BUENO, KUAN-YING FANG, SAMANTHA FULLER AND SUSANA FURTADO	187
Commutation classes of double wiring diagrams PATRICK DUKES AND JOE RUSINKO	207
A two-step conditionally bounded numerical integrator to approximate some traveling-wave solutions of a diffusion-reaction equation SIEGFRIED MACÍAS AND JORGE E. MACÍAS-DÍAZ	219
The average order of elements in the multiplicative group of a finite field YILAN HU AND CARL POMERANCE	229



1944-4176(2012)5:2;1-B