PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 12, December 2013, Pages 4119–4124
S 0002-9939(2013)11801-0
Article electronically published on August 8, 2013

# THE SUM OF DIGITS FUNCTION IN FINITE FIELDS

CÉCILE DARTYGE AND ANDRÁS SÁRKÖZY

(Communicated by Matthew A. Papanikolas)

Abstract. We define and study certain sum of digits functions in the context of finite fields. We give the number of polynomial values of $\mathbb{F}_q$ with a fixed sum of digits. We also state a result for the sum of digits of polynomial values with generator arguments.

## 1. Introduction

Let $g \in \mathbb{N}$ be fixed with $g \geq 2$. If $n \in \mathbb{N}$, then representing $n$ in the number system to base $g$,

$$n = \sum_{j=0}^{r-1} c_j g^j, \qquad 0 \leq c_j \leq g-1,\ c_r \geq 1, \tag{1.1}$$

we write

$$S(n) = \sum_{j=0}^{r-1} c_j. \tag{1.2}$$

Many papers have been written on the connection between this sum of digits function $S(n)$ and the arithmetic properties of $n$ (for example [1], [3], [4], [5], [6], [7], [8], [13]). In particular, Mauduit and Sárközy [12] studied the arithmetic structure of the integers whose sum of digits is fixed, while Mauduit and Rivat [10], [11] obtained some asymptotic formulae for the number of squares and also for the number of primes whose sum of digits is even, resp. odd. In this paper our goal is to study the analogs of some of these problems in finite fields.

Indeed, let $p$ be a prime number, $q = p^r$ with $r \geq 2$, and consider the field $\mathbb{F}_q$. Let $\mathcal{B} = \{a_1, \ldots, a_r\}$ be a basis of the linear vector space formed by $\mathbb{F}_q$ over $\mathbb{F}_p$; i.e., let $a_1, a_2, \ldots, a_r$ be linearly independent over $\mathbb{F}_p$. Then every $x \in \mathbb{F}_q$ has a unique representation

$$x = \sum_{j=1}^{r} c_j a_j \tag{1.3}$$

Received by the editors February 2, 2012.
2010 *Mathematics Subject Classification.* Primary 11A63; Secondary 11L99.
*Key words and phrases.* Sum of digits function, finite fields, character sums, generators, primitive elements.
The research of the first author was partially supported by the Agence Nationale de la Recherche, grant ANR-10-BLAN 0103 MUNUM.
The research of the second author was partially supported by the Hungarian National Foundation for Scientific Research, grants K72731 and K100291.

with $c_j \in \mathbb{F}_p$. Write

$$s_{\mathcal{B}}(x) = \sum_{j=1}^{r} c_j. \tag{1.4}$$

An important special case is when the basis $\mathcal{B}$ consists of the first $r$ powers of a generator of $\mathbb{F}_q^*$ :

$$\mathcal{B} = \{a_1, a_2, \ldots, a_r\} = \{1, z, z^2, \ldots, z^{r-1}\}.$$

Then (1.3) becomes

$$x = \sum_{j=1}^{r} c_j z^{j-1}. \tag{1.5}$$

Equations (1.4) and (1.5) are of the same form as (1.1) and (1.2); thus we may consider (1.3) as the finite field analog of the representation (1.1), and we may call $c_1, \ldots, c_r$ in (1.3) "digits", and $s_{\mathcal{B}}(x)$ can be called the "sum of digits" function. If we consider the generators (or primitive elements) as finite field analogs of primitive roots of $\mathbb{F}_p$, we then end up with the finite field analogs of some problems mentioned above :

How many squares are there in $\mathbb{F}_q$ with a fixed sum of digits and, more generally, how many values $f(x)$ of a polynomial $f$ have a fixed sum of digits? How many generators of $\mathbb{F}_q^*$ are there whose sum of digits is a fixed value? In this paper our goal is to study these problems.

Let $c \in \mathbb{F}_p$. We define $Q_c$ as the set of the squares of $\mathbb{F}_q$ such that their sum of digits is equal to $c$:

$$Q_c = \Big\{x \in \mathbb{F}_q : s_{\mathcal{B}}(x) = c \text{ and } \exists y \in \mathbb{F}_q \text{ such that } y^2 = x\Big\}.$$

We prove the following result:

**Theorem 1.1.** *For all $c \in \mathbb{F}_p$, we have*

$$\left||Q_c| - \frac{p^{r-1}}{2}\right| \leq \sqrt{q}.$$

Let $f \in \mathbb{F}_q[X]$ be of degree $n$ with $(n, q) = 1$. We are now interested in the cardinality of the sets

$$D(f, c) = \{x \in \mathbb{F}_q : s_{\mathcal{B}}(f(x)) = c\}.$$

While Theorem 1.1 can be proved elementarily, we will need Weil's Theorem [14] to estimate $|D(f, c)|$:

**Theorem 1.2.** *Let $f \in \mathbb{F}_q[X]$ be of degree $n$ with $(n, q) = 1$. Then for all $c \in \mathbb{F}_p$, we have*

$$\left||D(f, c)| - p^{r-1}\right| \leq (n-1)\sqrt{q}.$$

The main term of this estimate is larger than the one of Theorem 1.1 because here the values $f(x)$ are taken with multiplicities. We denote by $\mathcal{G}$ the set of the generators (or primitive elements) of $\mathbb{F}_q^*$, and for $c \in \mathbb{F}_p$ we consider the sets

$$G(f, c) = \{g \in \mathcal{G} : s_{\mathcal{B}}(f(g)) = c\}.$$

**Theorem 1.3.** *Let $f \in \mathbb{F}_q[X]$ be of degree $n$ with $(n,q)=1$. Then for all $c \in \mathbb{F}_p$ we have*

$$\Big| |G(f,c)| - \frac{\varphi(q-1)}{p} \Big| \le (n-1)\tau(q-1)\sqrt{q}$$

*where $\tau(n)$ denotes the divisor function.*

## 2. The sum of digits of the squares

In this section we prove Theorem 1.1. First we suppose that $c \in \mathbb{F}_p^*$. We use the quadratic character to detect the elements of $Q_c$:

$$|Q_c| = \frac{1}{2} \sum_{\substack{(c_1,c_2,\dots,c_r)\in\mathbb{F}_p^r \\ c_1+c_2+\cdots+c_r=c}} \Big[1+\gamma\Big(\sum_{j=1}^{r} c_j a_j\Big)\Big],$$

where $\gamma$ is the quadratic character. We replace $c_r$ by $c-(c_1+\cdots+c_{r-1})$:

$$|Q_c| = \frac{p^{r-1}}{2} + \frac{1}{2} \sum_{(c_1,\dots,c_{r-1})\in\mathbb{F}_p^{r-1}} \gamma\Big(ca_r + \sum_{j=1}^{r-1} c_j(a_j-a_r)\Big).$$

To make the $c_j$ independent, it is convenient to switch to the additive characters *via* the Gaussian sums. We recall that if $\chi$ is a multiplicative character of $\mathbb{F}_q^*$ and $\psi$ is an additive character of $\mathbb{F}_q$, then the Gaussian sum of $\chi$ and $\psi$ is defined by

$$G(\chi,\psi) = \sum_{x\in\mathbb{F}_q^*} \chi(x)\psi(x) \tag{2.1}$$

(see [9]). Then we can switch to additive characters with the following formula for all $x \in \mathbb{F}_q^*$ :

$$\chi(x) = \frac{1}{q}\sum_{\psi} G(\chi,\overline{\psi})\psi(x).$$

Since $c \neq 0$, $ca_r + \sum_{j=1}^{r-1} c_j(a_j-a_r) \in \mathbb{F}_q^*$ for all $c_1,\dots,c_{r-1} \in \mathbb{F}_p$. Then we obtain for $|Q_c|$:

$$|Q_c| = \frac{p^{r-1}}{2} + \frac{1}{2q}\sum_{\psi} G(\gamma,\overline{\psi}) \sum_{(c_1,\dots,c_{r-1})\in\mathbb{F}_p^{r-1}} \psi(ca_r)\prod_{j=1}^{r-1}\psi(c_j(a_j-a_r)). \tag{2.2}$$

If $\psi(a_j) \neq \psi(a_r)$, then $\psi(a_j-a_r)$ is a $p$-th root of the unity. There exists $\lambda_j \in \{1,\dots,p-1\}$ such that $\psi(a_j-a_r) = \mathrm{e}(\lambda_j/p)$ with the standard notation $\mathrm{e}(t) = \exp(2i\pi t)$. In this case,

$$\sum_{c_j\in\mathbb{F}_p} \psi(c_j(a_j-a_r)) = \sum_{c_j\in\mathbb{F}_p} \mathrm{e}\Big(\frac{c_j\lambda_j}{p}\Big) = 0.$$

Thus, in the right hand side of (2.2), the summation over $(c_1,\dots,c_{r-1})$ is not 0 if and only if $\psi(a_j) = \psi(a_r)$ for all $1 \le j \le r-1$. This means that $\psi$ is a power of $\psi_1$ where $\psi_1$ is the additive character defined by $\psi_1(a_j) = \mathrm{e}(1/p)$ for all $0 \le j \le r-1$. Then we have

$$|Q_c| = \frac{p^{r-1}}{2} + \frac{1}{2p}\sum_{j=0}^{p-1} G(\gamma,\overline{\psi}_1^j)\psi_1^j(c).$$

Next we use the classical fact ([9] Theorem 5.1) that $|G(\chi,\psi)| \le \sqrt{q}$ if $(\chi,\psi) \ne (\chi_0,\psi_0)$, the couple of the trivial multiplicative, respectively additive, character. We obtain

$$\Big||Q_c| - \frac{p^{r-1}}{2}\Big| \le \frac{\sqrt{q}}{2}.$$

If $c = 0$, then we have to remove the term with $c_1 = c_2 = \cdots = c_{r-1} = 0$ in (2.2). This gives an extra error term $\sqrt{q}/2$, and we obtain

$$\Big||Q_0| - \frac{p^{r-1}}{2}\Big| \le \sqrt{q}.$$

## 3. The sum of digits of the polynomial values

Let $f \in \mathbb{F}_q[X]$ be of degree $n$ such that $(n,q) = 1$. We are now interested in the cardinality of the sets $D(f,c)$. The character $\psi_1$ defined in the previous section is connected with the sum of digits function $s_{\mathcal{B}}$ by the formula

$$\psi_1(x) = \mathrm{e}\Big(\frac{s_{\mathcal{B}}(x)}{p}\Big).$$

Thus we have

$$|D(f,c)| = \frac{1}{p}\sum_{h=0}^{p-1}\sum_{x\in\mathbb{F}_q}\psi_1^h(f(x))\mathrm{e}\Big(\frac{-hc}{p}\Big).$$

The main term is provided by $h = 0$:

$$|D(f,c)| = \frac{q}{p} + \frac{1}{p}\sum_{h=1}^{p-1}E(h),$$

with

$$E(h) = \sum_{x\in\mathbb{F}_q}\psi_1^h(f(x))\mathrm{e}\Big(\frac{-hc}{p}\Big).$$

We will use the following theorem of Weil ([14]; see also [9], Theorem 5.38, p. 223) to obtain an upper bound for the terms $E(h)$.

**Theorem 3.1** (Weil)**.** *Let $g \in \mathbb{F}_q[X]$ be of degree $n \ge 1$ with $(n,q) = 1$ and $\psi$ a nontrivial additive character of $\mathbb{F}_q$. Then*

$$\Big|\sum_{x\in\mathbb{F}_q}\psi(g(x))\Big| \le (n-1)\sqrt{q}.$$

By this theorem, we deduce that $|E(h)| \le (n-1)\sqrt{q}$ for all $1 \le h \le p-1$. Thus we obtain

$$\Big||D(f,c)| - \frac{q}{p}\Big| \le (n-1)\sqrt{q}.$$

## 4. The sum of digits of polynomial values with primitive element arguments

As in the previous section, we consider a polynomial $f \in \mathbb{F}_q[X]$ of degree $n$ with $(n,q) = 1$, but we now study the sets $G(f,c)$. By the same argument as in the previous section we have

$$|G(f,c)| = \frac{1}{p}\sum_{h=0}^{p-1}\sum_{g\in\mathcal{G}}\psi_1^h(f(g))\mathrm{e}\Big(\frac{-hc}{p}\Big). \tag{4.1}$$

By using Weil's Theorem 3.1 we will deduce the following bound for additive character sums with primitive element arguments.

**Lemma 4.1.** *Let $f \in \mathbb{F}_q[X]$ be of degree $n$ with $(n,q)=1$. Let $\psi$ be a nontrivial additive character of $\mathbb{F}_q$. Then*

$$\Big|\sum_{g\in\mathcal{G}} \psi(f(g))\Big| \le (n-1)\tau(q-1)\sqrt{q} + \frac{\varphi(q-1)}{q-1}.$$

*Proof.* The proof follows the argument of Lemma 2.3 of [2], which gives a similar upper bound for the sum with multiplicative characters over $\mathbb{F}_p$. Let $g_0$ be a primitive root of $\mathbb{F}_q^*$. Then we have

$$\sum_{g\in\mathcal{G}} \psi(f(g)) = \sum_{\substack{1\le k<q\\ (k,q-1)=1}} \psi(f(g_0^k)).$$

Then as in [2], we use the Möbius function to handle the coprimality condition, and next we remark that $g_0^{kd}$ is periodic in $k$ with period $(q-1)/d$:

$$\sum_{g\in\mathcal{G}} \psi(f(g)) = \sum_{d|q-1} \mu(d) \sum_{k=1}^{(q-1)/d} \psi(f(g_0^{kd})) = \sum_{d|q-1} \frac{\mu(d)}{d} \sum_{x\in\mathbb{F}_q^*} \psi(f(x^d)). \tag{4.2}$$

When $d|q-1$, the degree of $f(X^d)$ is coprime with $q$, and we can apply Theorem 3.1. This ends the proof of Lemma 4.1; the $\varphi(q-1)/(q-1)$ term is the contribution of $x=0$ excluded in (4.2). □

It remains to insert Lemma 4.1 into (4.1), which gives

$$\Big||G(f,c)| - \frac{\varphi(q-1)}{p}\Big| \le (n-1)\tau(q-1)\sqrt{q} + 1.$$

This ends the proof of Theorem 1.3.

## References


[1] William D. Banks, Alessandro Conflitti, and Igor E. Shparlinski, *Character sums over integers with restricted g-ary digits*, Illinois J. Math. **46** (2002), no. 3, 819–836. MR1951242 (2003k:11133)

[2] C. Dartyge and A. Sárközy, *On additive decompositions of the set of primitive roots modulo p*, Monatsh. Math. **169** (2013), no. 3-4, 317–328. MR3019286

[3] Cécile Dartyge and Gérald Tenenbaum, *Sommes des chiffres de multiples d'entiers*, Ann. Inst. Fourier (Grenoble) **55** (2005), no. 7, 2423–2474 (French, with English and French summaries). MR2207389 (2007b:11120)

[4] Cécile Dartyge and Gérald Tenenbaum, *Congruences de sommes de chiffres de valeurs polynomiales*, Bull. London Math. Soc. **38** (2006), no. 1, 61–69, DOI 10.1112/S0024609305017789 (French, with English summary). MR2201604 (2006k:11039)

[5] Michael Drmota, Christian Mauduit, and Joël Rivat, *The sum-of-digits function of polynomial sequences*, J. Lond. Math. Soc. (2) **84** (2011), no. 1, 81–102, DOI 10.1112/jlms/jdr003. MR2819691 (2012f:11193)

[6] E. Fouvry and C. Mauduit, *Méthodes de crible et fonctions sommes des chiffres*, Acta Arith. **77** (1996), no. 4, 339–351 (French). MR1414514 (97j:11046)

[7] E. Fouvry and C. Mauduit, *Sommes des chiffres et nombres presque premiers*, Math. Ann. **305** (1996), no. 3, 571–599, DOI 10.1007/BF01444238 (French). MR1397437 (97k:11029)

[8] A. O. Gel′fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/1968), 259–265 (French). MR0220693 (36 #3745)

[9] Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn. MR746963 (86c:11106)

[10] Christian Mauduit and Joël Rivat, *La somme des chiffres des carrés*, Acta Math. **203** (2009), no. 1, 107–148, DOI 10.1007/s11511-009-0040-0 (French). MR2545827 (2010j:11119)

[11] Christian Mauduit and Joël Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2) **171** (2010), no. 3, 1591–1646, DOI 10.4007/annals.2010.171.1591 (French, with English and French summaries). MR2680394 (2011j:11137)

[12] Christian Mauduit and András Sárközy, *On the arithmetic structure of the integers whose sum of digits is fixed*, Acta Arith. **81** (1997), no. 2, 145–173. MR1456239 (99a:11096)

[13] T. Stoll, The sum of digits of polynomial values in arithmetic progressions, Funct. Approx. Comment. Math. **47** (2012), part 2, 233–239. MR3051450

[14] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann, Paris (1948). MR0027151 (10, 262c)

Institut Élie Cartan, Université de Lorraine, BP 239, 54506 Vandœuvre Cedex, France

*E-mail address*: `Cecile.Dartyge@univ-lorraine.fr`

Department of Algebra and Number Theory, Eötvös Loránd University, 1117 Budapest, Pázmány Péter sétány 1/C, Hungary

*E-mail address*: `sarkozy@cs.elte.hu`