Functiones et Approximatio
52.1 (2015), 65–74
doi: 10.7169/facm/2015.52.1.5

POLYNOMIAL VALUES AND GENERATORS WITH MISSING DIGITS IN FINITE FIELDS

Cécile Dartyge, Christian Mauduit, András Sárközy

Abstract: We consider the linear vector space formed by the elements of the finite field $\mathbb{F}_q$ with $q = p^r$ over $\mathbb{F}_p$. Then the elements x of $\mathbb{F}_q$ have a unique representation in the form $x = \sum_{j=1}^{r} c_j a_j$ with $c_j \in \mathbb{F}_p$; the coefficients c_j will be called digits. Let $\mathcal{D}$ be a subset of $\mathbb{F}_p$ with $2 \leqslant |\mathcal{D}| < p$. We consider elements x of $\mathbb{F}_q$ such that for their every digit c_j we have $c_j \in \mathcal{D}$; then we say that the elements of $\mathbb{F}_p \setminus \mathcal{D}$ are "missing digits". We will show that if $\mathcal{D}$ is a large enough subset of $\mathbb{F}_p$, then there are squares with missing digits in $\mathbb{F}_q$; if the degree of the polynomial $f(x) \in \mathbb{F}_q[X]$ is at least 2 then it assumes values with missing digits; there are generators g in $\mathbb{F}_q$ such that $f(g)$ is of missing digits.

Keywords: digits properties, finite fields, character sums, squares, polynomials, generators, primitive roots.

1. Introduction

Let $b \in \mathbb{N}$ be fixed with $b \geqslant 2$. If $n \in \mathbb{N}$, then consider the representation of n in the number system to base b:

$$n = \sum_{j=0}^{r-1} c_j b^j, \qquad 0 \leqslant c_j \leqslant b-1,\ c_{r-1} \geqslant 1, \tag{1.1}$$

and write

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

Many papers have been written on the connection between the arithmetic properties of n and certain properties of its digits $c_0, c_1, \dots c_{r-1}$. In particular the sum of

Research partially supported by the Hungarian National Foundation for Scientific Research, Grant K72731 and K100291 and the Agence Nationale de la Recherche, grant ANR-10-BLAN 0103 MUNUM and French-Hungarian "Balaton" exchange program TÉT-09-1-2010-0056, and Ciência sem Fronteiras, projet PVE 407308/2013-0.

2010 Mathematics Subject Classification: primary: 11A63; secondary: 11L99

digits function $S(n)$ restricted to polynomial or prime numbers has been studied in [12], [13], [15]-[17], [20]-[22], [27], [28], [30], [31], [32]. In some other papers [1]-[9], [14], [18], [19], [24], [25], [29] the arithmetic properties of integers with missing digits have been studied.

In [11] Dartyge and Sárközy initiated the study of the analogs of some of these problems in finite fields. Indeed, let p be a prime number, $q = p^r$ with $r \geqslant 2$, and consider the field $\mathbb{F}_q$. Let $\mathcal{B} = \{a_1, a_2, \ldots, a_r\}$ 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 in form

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

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 z 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

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

(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 $c_1, c_2, \ldots, c_r$ in (1.3) as "digits", and $S_{\mathcal{B}}(x)$ can be called as "sum of digits " function. It was shown in [11] that if we fix an $s \in \mathbb{F}_p$ and $f(x) \in \mathbb{F}_q[x]$ satisfying certain assumptions then there are squares x^2, elements $y \in \mathbb{F}_q$ and generators $g \in \mathbb{F}_q$ with $S_{\mathcal{B}}(x^2) = s$, $S_{\mathcal{B}}(f(y)) = s$, $S_{\mathcal{B}}(f(g)) = s$ respectively.

In this paper our goal is to prove similar results for the elements $x \in \mathbb{F}_q$ with missing digits. More precisely, let us fix a set $\mathcal{D} \subset \{0, 1, 2, \ldots, p-1\}$ with $2 \leqslant |\mathcal{D}| \leqslant p-1$. We define the set $W_{\mathcal{D}}$ as the set of all elements $x \in \mathbb{F}_q$ such that all their digits belong to $\mathcal{D}$ in the basis $\mathcal{B} = \{a_1, a_2, \ldots, a_r\}$:

$$W_{\mathcal{D}} = \Big\{ x = \sum_{j=1}^{r} c_j a_j \text{ with } (c_1, \ldots, c_r) \in \mathcal{D}^r \Big\}.$$

Then we have $|\mathcal{W}_{\mathcal{D}}| = |\mathcal{D}|^r$, and the elements of $\{0, 1, \ldots, p-1\} \setminus \mathcal{D}$ are called missing digits. Let Q denote the set of the quadratic residues of $\mathbb{F}_q$ and for $f(x) \in \mathbb{F}_q[x]$, $W_{\mathcal{D}}(f)$ the set of the polynomial values of $f(x)$ with missing digits:

$$W_{\mathcal{D}}(f) = \{x \in \mathbb{F}_q : f(x) \in W_{\mathcal{D}}\}.$$

In order to formulate some of our results we will also use the notation

$$C(p,t)=\begin{cases}\frac{\log p}{t}+\frac{1}{t}\left(\frac{4}{3}-\frac{\log 3}{2}\right)+\frac{1}{p} & \text{if } \ 2\leqslant t<p-2,\\ \frac{2}{p}+\frac{2}{\pi(p-1)}(1-\log(2\sin\frac{\pi}{2p})) & \text{if } \ t=p-2.\end{cases} \tag{1.6}$$

We will show that if $\mathcal{D}$ is a large subset of $\mathbb{F}_p$, then there are many squares in Q with missing digits; if the degree of the polynomial $f(x)\in\mathbb{F}_q[x]$ is at least 2 then it assumes values with missing digits; there are generators g in $\mathbb{F}_q$ such that $f(g)$ is of missing digits. We remark that the analog problems in $\mathbb{N}$ (on squares, polynomial values and primes with missing digits) are open and seem to be very difficult.

2. Squares with missing digits

First we prove that if $|\mathcal{D}|$ is close to p, then half of the elements of $W_{\mathcal{D}}$ are quadratic residues.

Theorem 2.1. *Let $\mathcal{D}\subset\mathbb{F}_p$ with $2\leqslant|\mathcal{D}|\leqslant p-1$. Then we have*

$$\Big||W_{\mathcal{D}}\cap Q|-\frac{|W_{\mathcal{D}}|}{2}\Big|\leqslant\frac{1}{2\sqrt{q}}\Big(|\mathcal{D}|+p\sqrt{p-|\mathcal{D}|}\Big)^r. \tag{2.1}$$

Remark. Theorem Theorem 2.1 gives a non-trivial upper bound if

$$|\mathcal{D}|+p\sqrt{p-|\mathcal{D}|}<|\mathcal{D}|\sqrt{p},$$

that is

$$\begin{aligned}|\mathcal{D}|&>\frac{-p^2+\sqrt{p^4+4p^3(\sqrt{p}-1)^2}}{2(\sqrt{p}-1)^2}\\ &\sim\frac{(\sqrt{5}-1)p}{2}\qquad(p\to+\infty).\end{aligned} \tag{2.2}$$

Proof. The first step of the proof of Theorem 2.1 is to prove the following lemma. We will use the standard notation $\mathrm{e}(t)=\exp(2i\pi t)$.

Lemma 2.2. *We have*

$$\Big||W_{\mathcal{D}}\cap Q|-\frac{|W_{\mathcal{D}}|}{2}\Big|\leqslant\frac{1}{2\sqrt{q}}\Big(\sum_{h=0}^{p-1}\Big|\sum_{c\in\mathcal{D}}\mathrm{e}\Big(\frac{ch}{p}\Big)\Big|\Big)^r.$$

Let γ denote the quadratic character of $\mathbb{F}_q$. Then we have

$$|W_{\mathcal{D}}\cap Q|=\frac{1}{2}\sum_{x\in\mathcal{W}_{\mathcal{D}}}(1+\gamma(x))=\frac{|W_{\mathcal{D}}|}{2}+\frac{1}{2}\sum_{x\in\mathcal{W}_{\mathcal{D}}}\gamma(x). \tag{2.3}$$

Next following [11], we switch to additive characters by using Gaussian sums in order to separate the digits $c_1,\dots,c_r$. We recall that if χ is a multiplicative

character of $\mathbb{F}_q^*$ and ψ is an additive character of $\mathbb{F}_q$ then the Gaussian sum of χ and ψ is defined by

$$G(\chi,\psi)=\sum_{x\in\mathbb{F}_q^*}\chi(x)\psi(x) \tag{2.4}$$

(see [26]). Then we use the following formula for all $x\in\mathbb{F}_q^*$:

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

Inserting this in (2.3) we obtain:

$$|W_{\mathcal{D}}\cap Q|=\frac{|W_{\mathcal{D}}|}{2}+\frac{1}{2q}\sum_{\psi}G(\gamma,\overline{\psi})S(\psi)$$

with

$$S(\psi)=\sum_{c_1,\dots,c_r\in\mathcal{D}}\psi\Big(\sum_{i=1}^{r}c_ia_i\Big)=\prod_{i=1}^{r}\Big(\sum_{c\in\mathcal{D}}\psi(ca_i)\Big).$$

If ψ and χ are not both trivial, then $|G(\chi,\psi)|\leqslant\sqrt{q}$.

For all ψ and a_i, $\psi(a_i)\in\{\mathrm{e}\big(\frac{k}{p}\big),0\leqslant k<p-1\}$. There is a correspondence between the additive characters ψ and $\mathbb{F}_p^r$. This correspondence is given by $(\psi(a_1),\dots,\psi(a_r))=\Big(\mathrm{e}\big(\frac{k_1}{p}\big),\dots,\mathrm{e}\big(\frac{k_r}{p}\big)\Big)$. Thus we have

$$\Big||W_{\mathcal{D}}\cap Q|-\frac{|W_{\mathcal{D}}|}{2}\Big|\leqslant\frac{1}{2\sqrt{q}}\sum_{\substack{0\leqslant h_1,\dots,h_r<p\\(h_1,\dots,h_r)\neq(0,\dots0)}}\prod_{i=1}^{r}\Big|\sum_{c\in\mathcal{D}}\mathrm{e}\Big(\frac{h_ic}{p}\Big)\Big|. \tag{2.5}$$

This ends the proof of Lemma 2.2.

The second part of the proof of Theorem 2.1 is to obtain an upper bound for

$$\sum_{c\in\mathcal{D}}\mathrm{e}\Big(\frac{hc}{p}\Big).$$

When $\mathcal{D}$ is large we can use the following very simple fact for $h\neq0$:

$$\sum_{c\in\mathcal{D}}\mathrm{e}\Big(-\frac{hc}{p}\Big)=-\sum_{c\in\overline{\mathcal{D}}}\mathrm{e}\Big(-\frac{hc}{p}\Big),$$

with the notation $\overline{\mathcal{D}}=\mathbb{F}_p\backslash\mathcal{D}$. This remark gives something non-trivial if $|\overline{\mathcal{D}}|<|\mathcal{D}|$.

The main tool for the upper bound is the following result of Vinogradov (Lemma 14a in [33], Chapter VI page 128):

Lemma 2.3 (Vinogradov's Lemma). *If $\alpha(x)$ and $\beta(x)$ are complex valued functions on $\{0,\dots,m-1\}$ and $a\notin m\mathbb{Z}$ then we have*

$$\Big|\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\alpha(x)\beta(y)\mathrm{e}\Big(\frac{axy}{m}\Big)\Big|\leqslant(XYm)^{1/2},$$

with

$$X = \sum_{x=0}^{m-1} |\alpha(x)|^2 \qquad \textit{and} \qquad Y = \sum_{y=0}^{m-1} |\beta(y)|^2.$$

Recently Gyarmati and the third author [23] obtained a generalization of this lemma in finite fields.

For $0 < x < p$ we define

$$\alpha(x) = \frac{\sum_{d\in\overline{\mathcal{D}}} \mathrm{e}\Big(-\frac{xd}{p}\Big)}{\Big|\sum_{d\in\overline{\mathcal{D}}} \mathrm{e}\Big(-\frac{xd}{p}\Big)\Big|} \qquad \text{if} \quad \sum_{d\in\overline{\mathcal{D}}} \mathrm{e}\Big(-\frac{xd}{p}\Big) \neq 0,$$

and $\alpha(x) = 1$ otherwise. With this notation we have:

$$\sum_{x=1}^{p-1} \Big|\sum_{c\in\overline{\mathcal{D}}} \mathrm{e}\Big(\frac{xc}{p}\Big)\Big| = \sum_{x=1}^{p-1}\sum_{y=1}^{p} \alpha(x)\mathbf{1}_{\overline{\mathcal{D}}}(y)\mathrm{e}\Big(\frac{xy}{p}\Big).$$

We can now apply Lemma 2.3:

$$\sum_{h=0}^{p-1} \Big|\sum_{c\in\mathcal{D}} \mathrm{e}\Big(\frac{ch}{p}\Big)\Big| \leqslant |\mathcal{D}| + \sqrt{p(p-1)(p-|\mathcal{D}|)} \leqslant |\mathcal{D}| + p\sqrt{p-|\mathcal{D}|}. \tag{2.6}$$

Then we insert this bound in Lemma 2.2 and obtain the estimate (2.1) asserted in Theorem 2.1. ∎

3. Squares with missing digits when $\mathcal{D}$ consists of consecutive integers

Now we will prove that if $\mathcal{D}$ is a set of consecutive integers with at least $\gg \sqrt{p}\log p$ elements then a similar conclusion holds as in Theorem 2.1:

Theorem 3.1. *We suppose that $\mathcal{D} = \{0,\dots,t-1\}$ with $2 \leqslant t \leqslant p-1$. Then we have:*

$$\Big||W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2}\Big| \leqslant \frac{1}{2}(C(p,t)t\sqrt{p})^r. \tag{3.1}$$

Remark. Theorem Theorem 3.1 is non-trivial if $C(p,t)\sqrt{p} < 1$.

Proof. When $\mathcal{D}$ is a set of consecutive integers, we can apply some results of the two first authors.

Lemma 3.2 ([9, Lemma 3.1]).

(i) *If $\mathcal{D} = \{0,\dots,t-1\}$ then*

$$\frac{1}{pt}\sum_{h=0}^{p-1} \Big|\sum_{c\in\mathcal{D}} \mathrm{e}\Big(\frac{hc}{p}\Big)\Big| \leqslant \frac{\log p}{t} + \frac{1}{t}\Big(\frac{4}{3} - \frac{\log 3}{2}\Big) + \frac{1}{p}.$$

(ii) *If* $\mathcal{D} = \{0, \dots, p-2\}$ *(and* $p \geqslant 3$*) then*

$$\frac{1}{pt}\sum_{h=0}^{p-1}\Big|\sum_{c\in\mathcal{D}}\mathrm{e}\Big(\frac{hc}{p}\Big)\Big| \leqslant \frac{2}{p} + \frac{2}{\pi(p-1)}\Big(1 - \log\Big(2\sin\frac{\pi}{2p}\Big)\Big).$$

Then Theorem 3.1 can be proved by combining this lemma with Lemma 2.2. ∎

4. Polynomial values with missing digits

We obtain a similar result for $|W_{\mathcal{D}}(f)|$ as the estimates in Sections 2 and 3 (but now we will also need Weil's theorem to achieve this). We begin by stating the result for large $|\mathcal{D}|$.

Theorem 4.1. *Let* $\mathcal{D} \subset \mathbb{F}_p$ *with* $2 \leqslant |\mathcal{D}| \leqslant p-1$ *and* $f(x) \in \mathbb{Z}[x]$ *with degree* $n \geqslant 2$*. Then we have*

$$\Big||W_{\mathcal{D}}(f)| - |W_{\mathcal{D}}|\Big| \leqslant \frac{n-1}{\sqrt{q}}\Big(|\mathcal{D}| + p\sqrt{p-|\mathcal{D}|}\Big)^r. \tag{4.1}$$

When $\mathcal{D}$ is a set of consecutive integers we will prove:

Theorem 4.2. *We suppose that* $\mathcal{D} = \{0, \dots, t-1\}$ *with* $2 \leqslant t \leqslant p-1$*. Then we have:*

$$\Big||W_{\mathcal{D}}(f)| - |W_{\mathcal{D}}|\Big| \leqslant (n-1)(C(p,t)t\sqrt{p})^r.$$

Proofs of Theorems 4.1 and 4.2. First, we obtain in the following lemma, a similar result as Lemma 2.2 for the sets $W_{\mathcal{D}}(f)$.

Lemma 4.3. *We suppose that the degree of* f *is* $\geqslant 2$*. Then we have:*

$$\Big||W_{\mathcal{D}}(f)| - |\mathcal{D}|^r\Big| \leqslant \frac{(n-1)}{\sqrt{q}} \sum_{\substack{0\leqslant h_1,\dots,h_r<p\\(h_1,\dots,h_r)\neq(0,\dots,0)}} \prod_{i=1}^{r}\Big|\sum_{c\in\mathcal{D}}\mathrm{e}\Big(-\frac{hc}{p}\Big)\Big|.$$

For $1 \leqslant j \leqslant r$ we consider the additive character ψ_j defined by:

$$\psi_j(a_i) = \begin{cases}\exp\left(\frac{1}{p}\right) & \text{if } \ i = j\\ 1 & \text{otherwise } \ (1 \leqslant i \leqslant r).\end{cases}$$

Thus for $x = \sum_{i=1}^{r} x_i a_i \in \mathbb{F}_q$ we have

$$\psi_j(x) = \psi_j(x_1a_1)\cdots\psi_j(x_ra_r) = \psi_j^{x_1}(a_1)\cdots\psi_j^{x_r}(a_r) = \mathrm{e}\Big(\frac{x_j}{p}\Big).$$

We can use this to detect digit conditions since for $x = x_1a_1 + \cdots + x_ra_r$ we have

$$\frac{1}{p}\sum_{h=1}^{p}\psi_j^h(x)\mathrm{e}\Big(-\frac{hc}{p}\Big) = \begin{cases}1 & \text{if } \ x_j = c\\ 0 & \text{otherwise.}\end{cases}$$

If we sum this formula over all $c \in \mathcal{D}$, then we detect the x such that $x_j \in \mathcal{D}$. It remains then to take the product over all the digits to have an indicator of the elements of $W_{\mathcal{D}}$:

$$\prod_{j=1}^{r}\Big(\frac{1}{p}\sum_{c\in\mathcal{D}}\sum_{h=0}^{p-1}\psi_j^h(x)\mathrm{e}\Big(-\frac{hc}{p}\Big)\Big)=\begin{cases}1 & \text{if } x\in W_{\mathcal{D}}\\ 0 & \text{otherwise.}\end{cases}$$

We deduce that

$$|W_{\mathcal{D}}(f)|=\sum_{x\in\mathbb{F}_q}\prod_{j=1}^{r}\frac{1}{p}\sum_{c\in\mathcal{D}}\sum_{h=1}^{p}\psi_j^h(f(x))\mathrm{e}\Big(-\frac{hc}{p}\Big).$$

We develop this product and change the order of summation. The contribution of $h_1=\ldots=h_r=0$ provides the main term:

$$|W_{\mathcal{D}}(f)|=|\mathcal{D}|^r+\frac{1}{p^r}\sum_{\substack{0\leqslant h_1,\ldots,h_r<p\\(h_1,\ldots,h_r)\neq(0,\ldots,0)}}\sum_{x\in\mathbb{F}_q}\Big(\prod_{i=1}^{r}\psi_i^{h_i}(f(x))\Big)\prod_{i=1}^{r}\Big(\sum_{c\in\mathcal{D}}\mathrm{e}\Big(-\frac{hc}{p}\Big)\Big).$$

We can check easily that if $(h_1,\ldots,h_r)\neq(0,\ldots,0)$ then $\prod_{i=1}^{r}\psi_i^{h_i}\neq\psi_0$. Thus we can apply the following theorem ([34], see also [26, Theorem 5.38, p. 223]):

Lemma 4.4 (Weil). *Let $g\in\mathbb{F}_q[X]$ be of degree $n\geqslant 1$ with $(n,q)=1$ and ψ a nontrivial additive character of $\mathbb{F}_q$. Then*

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

It remains to apply this theorem to finish the proof of Lemma 4.3. (4.1) is obtained by combining Lemma 4.3 with (2.6). It is also sufficient to combine Lemma 4.3 with Lemma 3.2 to end the proof of Theorem 4.2. ∎

5. Polynomial values with generator argument and missing digits

Another variant of these problems is to study polynomial values with generator argument. According to the notations of [11] we will denote the set of the generators (or primitive elements) of $\mathbb{F}_q$ by $\mathcal{G}$. For $f(x)\in\mathbb{F}_q[x]$ we now consider

$$W_{\mathcal{D}}(f,\mathcal{G})=\{g\in\mathcal{G}: f(g)\in\mathcal{W}_{\mathcal{D}}\}.$$

Combining the method of the proof of the previous theorem with the estimates of character sums over generators and with polynomial arguments obtained in [11] we can prove:

Theorem 5.1. *Let $\mathcal{D}\subset\mathbb{F}_p$ with $2\leqslant|\mathcal{D}|\leqslant p-1$ and $f(x)\in\mathbb{Z}[x]$ with degree $n\geqslant 2$. Then we have*

$$\Big||W_{\mathcal{D}}(f)|-|\mathcal{D}|^r\frac{\varphi(q-1)}{q}\Big|\leqslant\Big(\frac{1}{q}+\frac{(n-1)\tau(q-1)}{\sqrt{q}}\Big)\Big(|\mathcal{D}|+p\sqrt{p-|\mathcal{D}|}\Big)^r.$$

When $\mathcal{D}$ is a set of consecutive integers, the corresponding result is

Theorem 5.2. *We suppose that* $\mathcal{D} = \{0, \dots, t-1\}$ *with* $2 \leqslant t \leqslant p-1$. *Then we have:*

$$\Big||W_{\mathcal{D}}(f)| - |\mathcal{D}|^r \frac{\varphi(q-1)}{q}\Big| \leqslant (1+(n-1)\tau(q-1))(C(p,t)t\sqrt{p})^r.$$

The proof of Lemma 4.3 can be adapted to detect the polynomial values with generator arguments and missing digits:

$$|W_{\mathcal{D}}(f,\mathcal{G})| = \sum_{g\in\mathcal{G}} \prod_{j=1}^{r} \frac{1}{p} \sum_{c\in\mathcal{D}} \sum_{h=1}^{p} \psi_j^h(f(g)) \mathrm{e}\Big(-\frac{hc}{p}\Big).$$

We argue in the same way as before. The only difference is that instead of applying Lemma 4.4 we use the following lemma proved in [11].

Lemma 5.3 ([11, Lemma 4.1]). *Under the notations and hypothesis of 4.4 we have:*

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

The analogue of Lemma 4.3 is then

$$\Big||W_{\mathcal{D}}(f,\mathcal{G})| - |\mathcal{D}|^r \frac{\varphi(q-1)}{q}\Big| \leqslant \Big(\frac{1}{q} + \frac{(n-1)\tau(q-1)}{\sqrt{q}}\Big)\Big(\sum_{h=1}^{p}\Big|\sum_{d\in\mathcal{D}} \mathrm{e}\Big(-\frac{hc}{p}\Big)\Big|\Big)^r. \tag{5.1}$$

Finally Theorem 5.1 is obtained by (5.1) and (2.6), Theorem 5.2 is proved by using (5.1) and Lemma 3.2.

References

[1] W.D. Banks, A. Conflitti and I.E. Shparlinski, *Character sums over integers with restricetd g-ary digits*, Illinois J. Math. **46**(3) (2002) 819–836.

[2] W.D. Banks and I.E. Shparlinski, *Arithmetic properties of numbers with restricted digits*, Acta Arith. **112** (2004), 313–332.

[3] S. Col, *Propriétés multiplicatives d'entiers soumis à des contraintes digitales*, Thèse de doctorat de mathématiques de l'Université Henri Poincaré-Nancy 1, (2006).

[4] S. Col, *Diviseurs des nombres ellipséphiques*, Periodica Mathematica Hungarica **58**(1) (2009), pp. 1–23.

[5] J. Coquet, *On the uniform distribution modulo one of some subsequences of polynomial sequences*, J. Number Theory **10**(3) (1978), 291–296.

[6] J. Coquet, *On the uniform distribution modulo one of some subsequences of polynomial sequences II*, J. Number Theory **12**(2) (1980), 244–250.

[7] J. Coquet, *Graphes connexes, représentation des entiers et équirépartition*, J. Number Theory **16**(3) (1983), 363–375.

[8] C. Dartyge and C. Mauduit, *Nombres presque premiers dont l'écriture en base r ne comporte pas certains chiffres*, *Journal of Number Theory* **81** (2000), 270–291.

[9] C. Dartyge and C. Mauduit, *Ensembles de densité nulle contenant des entiers possédant au plus deux facteurs premiers*, *Journal of Number Theory* **91** (2001), 230–255.

[10] C. Dartyge and A. Sárközy, *On additive decomposition of the set of primitive roots modulo p*, Monatsh. Math. to appear

[11] C. Dartyge and A. Sárközy, *The sum of digits function in finite fields*, Proc. Amer. Math. Soc. to appear.

[12] C. Dartyge and G. Tenenbaum, *Sommes des chiffres de multiples d'entiers*, Ann. Inst. Fourier (Grenoble) **55** (2005), 2423–2474.

[13] C. Dartyge and G. Tenenbaum, *Congruences de sommes de chiffres de valeurs polynomiales*, Bull. London Math. Soc. **38** (2006), no. 1, 61–69.

[14] M. Drmota and C. Mauduit, *Weyl sums over integers with affine digit restrictions*, Journal of Number Theory **130** (2010), 2404–2427.

[15] M. Drmota, C. Mauduit and J. Rivat, *Primes with and average sum for digits*, Compos. Math. **145** (2009), 271–292.

[16] M. Drmota, C. Mauduit and J. Rivat, *The sum of digits function of polynomial sequences*, J. London Math. Soc. **84** (2011), 81–102.

[17] M. Drmota and J. Rivat, *The sum-of-digits function of squares*, J. London Math. Soc. **72**(2) (2005), 273–292.

[18] P. Erdős, C. Mauduit and A. Sárközy, *On the arithmetic properties of integers with missing digits I: Distribution in residue classes*, Journal of Number Theory **70** (1998), no. 2, 99–120.

[19] P. Erdős, C. Mauduit and A. Sárközy, *On the arithmetic properties of integers with missing digits II: Prime factors*, Discrete Mathematics **200** (1999), 149–164.

[20] É. Fouvry and C. Mauduit, *Méthodes de crible et fonctions sommes des chiffres*, Acta Arith. **77** (1996), 339–351.

[21] É. Fouvry et C. Mauduit, *Sommes des chiffres et nombres presque premiers*, Math. Ann. **305** (1996), 571–599.

[22] A.O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/1968), 259–265.

[23] K. Gyarmati and A. Sárközy, *Equations in finite fields with restricted solutions sets, I. (Character sums.)*, Acta Math. Hungar. **118** (2008), 129–148.

[24] S. Konyagin, *Arithmetic properties of integers with missing digits: distribution in residue classes*, Periodica Mathematica Hungarica **42**(1-2) (2001), 145–162.

[25] S. Konyagin, C. Mauduit and A. Sárközy, *On the number of prime factors of integers characterized by digit properties*, Periodica Mathematica Hungarica **40**(1) (2000), 37–52.

[26] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications*, vol. 20, Addison-Wesley Publishing Company, (1983).

[27] B. Martin, C. Mauduit et J. Rivat, *Théorème des nombres premiers pour les fonctions digitales*, Acta Arithmetica **165** (2014), 11–45.

[28] C. Mauduit, *Multiplicative properties of the Thue-Morse sequence*, Period. Math. Hungar. **43** (2001), 137–153.
[29] C. Mauduit, *Propriétés arithmétiques des substitutions et automates infinis*, Ann. Inst. Fourier (Grenoble) **56** (2006), 2525–2549.
[30] C. Mauduit et J. Rivat, *La somme des chiffres des carrés*, Acta Math. **203** (2009), 107–148.
[31] C. Mauduit et J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Annals of Math. **171** (2010), no. 3, 1591–1646.
[32] T. Stoll, *The sum of digits of polynomial values in arithmetic progressions*, Functiones et Approximatio, to appear.
[33] I.M. Vinogradov, *Elements of Number Theory*, Dover 1954.
[34] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann, Paris, (1948).

Addresses: Cécile Dartyge: Institut Élie Cartan, CNRS, UMR 7502, Université de Lorraine, BP 239, 54506 Vandœuvre, Cedex, France;
Christian Mauduit: Université d'Aix-Marseille et Institut Universitaire de France, Institut de Mathématiques de Marseille CNRS, UMR 7373, 163 avenue de Luminy, 13288 Marseille cedex 9, France;
András Sárközy: Department of Algebra and Number Theory, Eötvös Loránd University, 1117 Budapest, Pázmány Péter sétány 1/C, Hungary.

E-mail: Cecile.Dartyge@univ-lorraine.fr, mauduit@iml.univ-mrs.fr, sarkozy@cs.elte.hu

Received: 18 June 2013; **revised:** 15 July 2013