NOTE ON THE HOPF-STIEFEL FUNCTION

Autor(en): **Eliahou, Shalom / Kervaire, Michel**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **49 (2003)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-66683

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'Enseignement Mathématique, t. 49 (2003), p. 117–122

A NOTE ON THE HOPF-STIEFEL FUNCTION

by Shalom ELIAHOU *) and Michel KERVAIRE

INTRODUCTION

In the preceding paper of this volume [P], Alain Plagne gives a formula for the (generalized) Hopf-Stiefel function β_p.

Given a prime number p, and two positive integers r, s, recall that $\beta_p(r,s)$ is defined as the smallest integer n such that $(x+y)^n \in (x^r, y^s)$, where (x^r, y^s) is the ideal generated by x^r and y^s in the polynomial ring $\mathbf{F}_p[x,y]$.

Plagne's theorem reads

THEOREM 1. *Let r, s be positive integers, then $\beta_p(r,s)$ is given by the formula*

$$\beta_p(r,s) = \min_{t \in \mathbf{N}} \left(\left\lceil \frac{r}{p^t} \right\rceil + \left\lceil \frac{s}{p^t} \right\rceil - 1 \right) p^t . \tag{1}$$

In [P], this formula is derived as a corollary of a theorem on Additive Number Theory, Theorem 4, which is the main result of the paper.

Here, we give another proof of Theorem 1 using a purely arithmetical argument.

Recall from [EK, p. 22], where $\beta_p(r,s)$ was introduced, that this function can be described in terms of the p-adic expansions of $r-1$ and $s-1$ as follows.

*) During the preparation of this paper, the first author has partially benefited from a research contract with the Fonds National Suisse pour la Recherche Scientifique.

THEOREM 2. *Let* $r-1=\sum_{i\geq 0} a_i p^i$ *and* $s-1=\sum_{i\geq 0} b_i p^i$ *be the respective* p*-adic expansions of* $r-1$ *and* $s-1$*, with* $0\leq a_i, b_i \leq p-1$ *for all* i*.*

Define the integer k *as the largest index for which* $a_k+b_k\geq p$*, if any exists. Otherwise, that is if* $a_i+b_i\leq p-1$ *for all* $i\geq 0$*, set* $k=-1$*.*

Then, $\beta_p(r,s)$ *is determined by*

$$\beta_p(r,s)=\left(\left\lfloor\frac{r-1}{p^{k+1}}\right\rfloor+\left\lfloor\frac{s-1}{p^{k+1}}\right\rfloor+1\right)p^{k+1}. \tag{2}$$

Although the point of Plagne's paper is to stress the relationship of his formula with Additive Number Theory, it is interesting to note that (1) also admits a direct proof using the above Theorem 2.

This is the content of the next section. In Section 2, we provide a simple proof of Theorem 2.

1. DERIVING THEOREM 1 FROM THEOREM 2

It is very easy to understand the relationship of the floor-function $\lfloor\xi\rfloor$, or integral part of ξ, appearing in Theorem 2, with the ceiling-function $\lceil\xi\rceil$, the smallest integer at least as big as ξ, used in formula (1).

The main object of this section will be to locate the minimum over $\ell\geq 0$ of the expression $\left(\left\lceil\frac{r}{p^\ell}\right\rceil+\left\lceil\frac{s}{p^\ell}\right\rceil-1\right)p^\ell$ and to show that this minimum is attained at $\ell=k+1$ with k as defined in Theorem 2.

For every index $\ell\geq 0$, we have

$$0<\frac{1+\sum_{i=0}^{\ell-1}a_ip^i}{p^\ell}\leq\frac{1+\sum_{i=0}^{\ell-1}(p-1)p^i}{p^\ell}=1.$$

Since $r=1+\sum_{i\geq 0}a_ip^i$, it follows that

$$\left\lceil\frac{r}{p^\ell}\right\rceil=\sum_{i\geq 0}a_{i+\ell}p^i+1.$$

Similarly, we have $0\leq\frac{\sum_{i=0}^{\ell-1}a_ip^i}{p^\ell}\leq\frac{\sum_{i=0}^{\ell-1}(p-1)p^i}{p^\ell}=\frac{p^\ell-1}{p^\ell}<1$, and

$$\left\lfloor\frac{r-1}{p^\ell}\right\rfloor=\sum_{i\geq 0}a_{i+\ell}p^i. \tag{3}$$

Hence, $\left\lceil \frac{r}{p^\ell} \right\rceil = \left\lfloor \frac{r-1}{p^\ell} \right\rfloor + 1$.

Applying the same formulas to s, we have $\left\lceil \frac{s}{p^\ell} \right\rceil = \left\lfloor \frac{s-1}{p^\ell} \right\rfloor + 1$. Hence,

$$\left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1\right) p^\ell = \left(\left\lfloor \frac{r-1}{p^\ell} \right\rfloor + \left\lfloor \frac{s-1}{p^\ell} \right\rfloor + 1\right) p^\ell$$

for every ℓ.

It remains to locate the minimum of the expression $\left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1\right) p^\ell$ as a function of ℓ.

If $a_i + b_i \leq p-1$ for every $i \geq 0$, then $\left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1\right) p^\ell$ is a weakly increasing function of $\ell \geq 0$. Indeed, the equation

$$\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1 = \sum_{i \geq 0} (a_{i+\ell} + b_{i+\ell}) p^i + 1$$

yields for $\ell < \ell'$

$$\begin{aligned}
&\left(\left\lceil \frac{r}{p^{\ell'}} \right\rceil + \left\lceil \frac{s}{p^{\ell'}} \right\rceil - 1\right) p^{\ell'} - \left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1\right) p^\ell \\
&\quad = (1 + \sum_{i \geq 0} (a_{i+\ell'} + b_{i+\ell'}) p^i) p^{\ell'} - (1 + \sum_{i \geq 0} (a_{i+\ell} + b_{i+\ell}) p^i) p^\ell \\
&\quad = p^{\ell'} - p^\ell - \sum_{\ell \leq i < \ell'} (a_i + b_i) p^i \geq p^{\ell'} - p^\ell - \sum_{\ell \leq i < \ell'} (p-1) p^i = 0 .
\end{aligned}$$

Thus, in the case where $k = -1$, the minimum of $\left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1\right) p^\ell$ is attained at $\ell = 0$ and $\min_{\ell \geq 0} \left\{ \left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1\right) p^\ell \right\} = r + s - 1$, as desired.

If there exists an index $k \geq 0$ such that $a_k + b_k \geq p$ and $0 \leq a_i + b_i \leq p-1$ for $k < i$, then the above calculation shows that $(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1) p^\ell$ is a weakly increasing function of ℓ for $k + 1 \leq \ell$.

On the other hand, for $\ell \leq k$, we have

$$\begin{aligned}
&\left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1\right) p^\ell - \left(\left\lceil \frac{r}{p^{k+1}} \right\rceil + \left\lceil \frac{s}{p^{k+1}} \right\rceil - 1\right) p^{k+1} \\
&\quad = p^\ell - p^{k+1} + \sum_{\ell \leq i \leq k} (a_i + b_i) p^i \geq p^\ell - p^{k+1} + p^{k+1} = p^\ell > 0 .
\end{aligned}$$

Therefore, even though the function $\left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1\right) p^\ell$ need not be monotonously decreasing in the interval $0 \leq \ell \leq k$, and it actually is not in general, it still does take its minimum at $\ell = k + 1$.

Consequently, in both cases $k=-1$ and $k \geq 0$, we have

$$\min_{\ell \geq 0}\left(\left\lceil\frac{r}{p^\ell}\right\rceil+\left\lceil\frac{r}{p^\ell}\right\rceil-1\right)p^\ell=\left(\left\lfloor\frac{r-1}{p^{k+1}}\right\rfloor+\left\lfloor\frac{s-1}{p^{k+1}}\right\rfloor+1\right)p^{k+1}.$$

Now, Theorem 2 tells us that

$$\left(\left\lfloor\frac{r-1}{p^{k+1}}\right\rfloor+\left\lfloor\frac{s-1}{p^{k+1}}\right\rfloor+1\right)p^{k+1}=\beta_p(r,s),$$

and Theorem 1 follows.

2. Proof of Theorem 2

As noted in equation (3) of Section 1, $\left\lfloor\frac{r-1}{p^{k+1}}\right\rfloor = \sum_{i \geq k+1} a_i p^{i-(k+1)}$. Similarly, $\left\lfloor\frac{s-1}{p^{k+1}}\right\rfloor = \sum_{i \geq k+1} b_i p^{i-(k+1)}$.

By definition of k, we have $a_i + b_i \leq p-1$ for $i \geq k+1$ and thus the right hand side of the equation

$$\left\lfloor\frac{r-1}{p^{k+1}}\right\rfloor+\left\lfloor\frac{s-1}{p^{k+1}}\right\rfloor=\sum_{i \geq k+1}(a_i+b_i)p^{i-(k+1)}$$

is the p-adic expansion of the left hand side.

For the purpose of the proof of Theorem 2, set

$$w=\left(\left\lfloor\frac{r-1}{p^{k+1}}\right\rfloor+\left\lfloor\frac{s-1}{p^{k+1}}\right\rfloor\right)p^{k+1}=\sum_{i \geq k+1}(a_i+b_i)p^i. \tag{4}$$

We proceed to show that $w+p^{k+1}$ is the smallest integer n such that $(x+y)^n$ belongs to the ideal $(x^r,y^s)=x^r\mathbf{F}_p[x,y]+y^s\mathbf{F}_p[x,y]$ in the polynomial ring $\mathbf{F}_p[x,y]$. That is $w+p^{k+1}=\beta_p(r,s)$.

We first calculate $(x+y)^w$ in the quotient algebra of $\mathbf{F}_p[x,y]$ modulo (x^r,y^s). We have from (4)

$$(x+y)^w=\prod_{i \geq k+1}\sum_{c_i=0}^{a_i+b_i}\binom{a_i+b_i}{c_i}x^{c_ip^i}y^{(a_i+b_i-c_i)p^i}.$$

We claim that

$$(x+y)^w \equiv \prod_{i \geq k+1}\binom{a_i+b_i}{a_i}x^{a_ip^i}y^{b_ip^i}=\prod_{i \geq k+1}\binom{a_i+b_i}{a_i}x^uy^v, \tag{5}$$

modulo (x^r,y^s), where $u=\sum_{i \geq k+1} a_ip^i$ and $v=\sum_{i \geq k+1} b_ip^i$.

Indeed, since $a_i + b_i \leq p - 1$ for $i \geq k+1$ by definition of k, the expressions $c = \sum_{i\geq k+1} c_i p^i$ and $d = \sum_{i\geq k+1}(a_i + b_i - c_i)p^i$ are the p-adic expansions of c and d respectively.

If for a given c, there is an index $i \geq k+1$ for which c_i is not equal to a_i, denote by ℓ the largest i such that $c_\ell \neq a_\ell$.

If $c_\ell < a_\ell$ and $c_i = a_i$ for $i \geq \ell + 1$, this implies $a_\ell + b_\ell - c_\ell > b_\ell$ and $a_i + b_i - c_i = b_i$ for $i \geq \ell + 1$. Therefore we have

$$d \geq \sum_{k+1\leq i\leq \ell-1} (a_i + b_i - c_i)p^i + p^\ell + \sum_{i\geq \ell} b_i p^i \geq p^\ell + \sum_{i\geq \ell} b_i p^i \geq s\,.$$

Thus in this case the monomial $x^c y^d$ belongs to the ideal (x^r, y^s).

If, on the contrary, $c_\ell > a_\ell$ and $c_i = a_i$ for $i \geq \ell + 1$, this implies

$$c = \sum_{i\geq k+1} c_i p^i \geq \sum_{k+1\leq i\leq \ell-1} c_i p^i + p^\ell + \sum_{i\geq \ell} a_i p^i \geq r\,.$$

Thus $(x+y)^w$ is indeed given by formula (5) modulo (x^r, y^s).

Now, observe that the product of binomial coefficients $\gamma = \prod_{i\geq k+1} \binom{a_i+b_i}{a_i}$ is non-zero in $\mathbf{F}_p$ and we can write $(x+y)^w \equiv \gamma \cdot x^u y^v$ modulo (x^r, y^s).

It is now easy to finish up the proof of the theorem:

- $$(x+y)^{p^{k+1}+w} = (x^{p^{k+1}} + y^{p^{k+1}})(x+y)^w \equiv \gamma \cdot (x^{p^{k+1}+u} y^v + x^u y^{p^{k+1}+v})\,.$$

However, $p^{k+1} + u = 1 + \sum_{i=0}^{k}(p-1)p^i + \sum_{i\geq k+1} a_i p^i \geq 1 + (r-1) = r$. Similarly, $p^{k+1} + v \geq s$.

Summarizing, $(x+y)^{p^{k+1}+w} \in (x^r, y^s)$ and thus

$$\left(\left\lfloor \frac{r-1}{p^{k+1}} \right\rfloor + \left\lfloor \frac{s-1}{p^{k+1}} \right\rfloor + 1\right) p^{k+1} \geq \beta_p(r,s)\,.$$

- $$(x+y)^{w+p^{k+1}-1} = \gamma \cdot \Big(\sum_{j=0}^{p^{k+1}-1} (-1)^j x^j y^{p^{k+1}-j-1} \Big) x^u y^v\,,$$

using $(x+y)^{p^{k+1}-1} = \frac{(x^{p^{k+1}} + y^{p^{k+1}})}{x+y} = \sum_{j=0}^{p^{k+1}-1} (-1)^j x^j y^{p^{k+1}-j-1}$ in $\mathbf{F}_p[x,y]$.

It is immediate to see that, calculating modulo (x^r, y^s), and with the notation $u_0 = \sum_{i=0}^{k} a_i$ and $v_0 = \sum_{i=0}^{k} b_i$, we can restrict the summation over j to the interval $p^{k+1} - 1 - v_0 \leq j \leq u_0$:

$$(x+y)^{w+p^{k+1}-1} \equiv \gamma \cdot \left(\sum_{j=p^{k+1}-1-v_0}^{j=u_0} (-1)^j x^j y^{p^{k+1}-j-1} \right) x^u y^v\,.$$

Moreover, the monomials appearing on the right hand side are distinct, have non-zero coefficient $\pm\gamma$ and form a non-empty subset of an $\mathbf{F}_p$-basis of $\mathbf{F}_p[x,y]/(x^r, y^s)$. Indeed, on the one hand, $p^{k+1} - 1 - v_0 \leq u_0$ in view of the inequalities

$$u_0 + v_0 = \sum_{i=0}^{k} (a_i + b_i)p^i \geq (a_k + b_k)p^k \text{ and } a_k + b_k \geq p\,,$$

and on the other hand $j+u \leq u_0+u = r-1$ and $p^{k+1}-j-1+v \leq v_0+v = s-1$. If $k = -1$, then $u_0 = v_0 = 0$ and the above conclusion still holds.

Summarizing:

$$\left(\left\lfloor \frac{r-1}{p^{k+1}} \right\rfloor + \left\lfloor \frac{s-1}{p^{k+1}} \right\rfloor + 1 \right) p^{k+1} = \beta_p(r,s)\,,$$

and this completes the proof of Theorem 2.

REFERENCES

[EK] ELIAHOU, S. and M. KERVAIRE. Sumsets in vector spaces over finite fields. *J. of Number Theory 71* (1998), 12–39.

[P] PLAGNE, A. Additive number theory sheds new light on the Hopf-Stiefel ∘ function. *L'Enseignement Math. (2) 49* (2003), 109–116.

(Reçu le 31 janvier 2003)

Shalom Eliahou

Département de Mathématiques
LMPA Joseph Liouville
Université du Littoral Côte d'Opale
Bâtiment Poincaré
50, rue Ferdinand Buisson, B.P. 699
F-62228 Calais
France
e-mail: eliahou@lmpa.univ-littoral.fr

Michel Kervaire

Département de Mathématiques
Université de Genève
2-4, rue du Lièvre
B.P. 240
CH-1211 Genève 24
Suisse
e-mail: Michel.Kervaire@math.unige.ch