Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 49 (2003)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: NOTE ON THE HOPF-STIEFEL FUNCTION
Autor: Eliahou, Shalom / Kervaire, Michel
Kapitel: 2. Proof of Theorem 2
DOI: https://doi.org/10.5169/seals-66683

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 01.04.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

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, $\left\lfloor\frac{r-1}{p^{k+1}}\right\rfloor=\sum_{i\geq k+1}a_ip^{i-(k+1)}$. Similarly, $\left\lfloor\frac{s-1}{p^{k+1}}\right\rfloor=\sum_{i\geq k+1}b_ip^{i-(k+1)}$.

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 o 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