

1. Deriving Theorem 1 from Theorem 2

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **29.04.2024**

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.

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

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

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

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

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

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

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

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

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 $\ell < \ell'$

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

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 $\left(\left\lceil \frac{r}{p^\ell} \right\rceil + \left\lceil \frac{s}{p^\ell} \right\rceil - 1 \right) p^\ell$ is a weakly increasing function of ℓ for $k+1 \leq \ell$.

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

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

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

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

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

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

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)

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

We claim that

$$(5) \quad (x+y)^w \equiv \prod_{i \geq k+1} \binom{a_i+b_i}{a_i} x^{a_i p^i} y^{b_i p^i} = \prod_{i \geq k+1} \binom{a_i+b_i}{a_i} x^u y^v,$$

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