ACTA ARITHMETICA
113.3 (2004)

Fermat's equation for matrices or quaternions over q-adic fields

by

Paulo Ribenboim (Kingston)

1. Introduction. We consider Fermat's equation

$$X^n + Y^n = Z^n \tag{1.1}$$

(with $n \geq 2$) and we investigate the existence of solutions which are square matrices or quaternions over the field $\mathbb{Q}_q$ of q-adic numbers.

We recall some known facts.

(a) Let p, q be prime numbers. Then the equation

$$X^p + Y^p = Z^p \tag{1.2}$$

has solutions in q-adic integers, all different from zero. This is obvious when $p = 2$. If $p \neq 2$, more precisely, there exists a q-adic integer $x \neq 0$ such that $x^p = 1 + q^p$. The proof is an application of Hensel's Lemma (when $p \neq q$) or of Hensel–Rychlik's Lemma (when $p = q$). See [4, Chapter X, (1A)].

It follows that Fermat's equation (1.2) has solutions in $n \times n$ diagonal matrices or in quaternions of the form $a(1+i+j+k)$ with a non-zero q-adic integer. So we are interested in solutions which are not of the forms just indicated.

(b) It is easy to give solutions of (1.1) which are non-zero singular matrices. Indeed, let

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

For each $k \geq 3$ let

$$\widetilde{A} = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}, \quad \widetilde{B} = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}, \quad \widetilde{C} = \begin{pmatrix} C & 0 \\ 0 & 0 \end{pmatrix}.$$

So $\widetilde{A} + \widetilde{B} = \widetilde{C}$, the matrices $\widetilde{A}$, $\widetilde{B}$, $\widetilde{C}$ are singular and idempotent, hence for each $n \geq 2$,

$$\widetilde{A}^n + \widetilde{B}^n = \widetilde{C}^n.$$

2000 *Mathematics Subject Classification*: 11D41, 11S80.

This was noted by Bolker in 1968 (see [3, p. 275]). So we are interested in solutions of (1.1) which are not singular matrices.

(c) Bolker also proved (see above reference) that for every $n \geq 2$ the equation (1.1) (with the same exponent n) has solutions in $n \times n$ matrices (which are non-diagonal and non-singular) with entries in any commutative ring R. Such solutions are explicitly given as follows. Let a, b, c be non-zero elements of R such that $a + b = c$. Let π be the circular permutation of $\{1, 2, \ldots, n\}$ given by $\pi(j) = j + 1$ for $j = 1, \ldots, n - 1$, and $\pi(n) = 1$. Let P be the $n \times n$ matrix whose (i, j) entry is $\delta_{\pi(i),j}$, where $\delta_{r,s}$ denotes the Kronecker symbol ($\delta_{r,r} = 1$, $\delta_{r,s} = 0$ when $r \neq s$). Let

$$\begin{aligned} A &= \operatorname{diag}(a, 1, \ldots, 1)P, \\ B &= \operatorname{diag}(b, 1, \ldots, 1)P, \\ C &= \operatorname{diag}(c, 1, \ldots, 1)P, \end{aligned}$$

where $\operatorname{diag}(x_1, \ldots, x_n)$ denotes the diagonal matrix with diagonal elements $x_1, \ldots, x_n$. Then A, B, C are non-singular and non-diagonal $n \times n$ matrices such that $A^n + B^n = C^n$.

(d) Not much is known about the solutions of (1.1) in matrices which are non-diagonal, non-singular but not of size $n \times n$.

Our purpose is to show that (1.2) has indeed many solutions in non-diagonal, non-singular square matrices of any size with entries which are q-adic numbers.

Due to the matrix representation of quaternions, we obtain a similar result about solutions in quaternions with coefficients which are q-adic numbers.

It is important to stress that when $n \geq 2$ the ring of $n \times n$ matrices is, as we know, not commutative, so it is no more possible to apply the lemmas of Hensel and of Hensel–Rychlik. Instead, the powerful Fixed Point Theorem is applied. This theorem holds in ultrametric spaces, even devoid of algebraic structure, provided the space is spherically complete. This is the case for space of square matrices with entries which are q-adic integers, as it will be seen later.

The result obtained in this paper illustrate a method to show the existence of solutions, applicable to a much wider class of diophantine equations —but we shall not develop this in the present paper.

2. Preliminaries. The method of proof requires facts about ultrametric spaces, which we indicate without proof.

Let Γ be a totally ordered set with smallest element denoted by 0. Let $\Gamma^{\cdot} = \Gamma \setminus \{0\}$ and let X be a non-empty set. A mapping $d : X \times X \rightarrow \Gamma$ is called an *ultrametric distance* (with values in Γ) when the following properties are satisfied:

- $d(x,y)=0$ if and only if $x=y$;
- $d(x,y)=d(y,x)$;
- $d(x,y)\le\max\{d(x,z),d(y,z)\}$ for all $x,y,z\in X$.

The triple (X,d,Γ) is called an *ultrametric space.*

Let (X,d,Γ) be an ultrametric space, let $\gamma\in\Gamma^{\cdot}$, $x_0\in X$. The set $B_\gamma(x_0)=\{x\in X\mid d(x,x_0)\le\gamma\}$ is called a *ball.* It is immediate to verify that:

(2.1) *If* $B_\gamma(x_0)\cap B_{\gamma'}(x_0')\ne\emptyset$ *and* $\gamma\le\gamma'$ *then* $B_\gamma(x_0)\subseteq B_{\gamma'}(x_0')$.

Any non-empty family of balls which is totally ordered by inclusion is called a *chain* of balls.

The ultrametric space is said to be *spherically complete* if any chain of balls has a non-empty intersection.

A mapping $\varphi:X\to X$ is said to be *strictly contracting* if $d(\varphi(x),\varphi(y))<d(x,y)$ whenever $x\ne y$.

The important Fixed Point Theorem is the following:

(2.2) *Let* (X,d,Γ) *be a spherically complete ultrametric space. If* $\varphi:X\to X$ *is a strictly contracting mapping, there exists a unique* $z\in X$ *such that* $\varphi(z)=z$. [z *is the fixed point of* φ.]

For the proof of the above theorem, see S. Priess-Crampe [1] or P. Ribenboim [2]. [We just stated the theorem in the particular case which will be needed in this paper.]

Let q be a prime number, let $\mathbb{Q}_q$ denote the field of q-adic numbers. Let $\Gamma=\{0\}\cup\{1/q^m\mid m\in\mathbb{Z}\}$, so Γ is totally ordered and $\Gamma^{\cdot}=\Gamma\setminus\{0\}$ is a multiplicative group. Each element $\alpha\in\mathbb{Q}_q$, $\alpha\ne0$, is written in unique way in the form $\alpha=a_mq^m+a_{m+1}q^{m+1}+\dots$, where $m\in\mathbb{Z}$, $a_m,a_{m+1},\dots\in\{0,1,\dots,q-1\}$.

We define

$$|\alpha|_q=\frac{1}{q^m}\quad\text{and}\quad|0|_q=0.$$

So $|\ |_q:\mathbb{Q}_q\to\Gamma$ is the normalized *q-adic absolute value.* In particular, $|q|_q=1/q$ and if p is a prime, $p\ne q$, then $|p|_q=1$.

Properties of the q-adic absolute value are very well known and may be found in many books; see for example [5].

If $\alpha,\beta\in\mathbb{Q}_q$, we have:

- $|\alpha|_q=0$ if and only if $\alpha=0$;
- $|\alpha+\beta|_q\le\max\{|\alpha|_q,|\beta|_q\}$; in particular, if $|\alpha|_q<|\beta|_q$, then
$$|\alpha+\beta|_q=|\beta|_q.$$

We have also

$$|\alpha\beta|_q = |\alpha|_q|\beta|_q.$$

Let $d(\alpha,\beta) = |\alpha-\beta|_q$. Then

$$d : \mathbb{Q}_q \times \mathbb{Q}_q \to \left\{ \frac{1}{q^m} \,\middle|\, m \in \mathbb{Z} \right\} \cup \{0\}$$

is an ultrametric distance.

Since $\mathbb{Q}_q$ is complete (with respect to its absolute value), the associated ultrametric space $(\mathbb{Q}_q, d, \mathit{\Gamma})$ is spherically complete.

Let $n \geq 2$ and let $R = R_n$ be the ring of $n \times n$ matrices with entries in $\mathbb{Q}_q$. The absolute value $|\ |_q$ on $\mathbb{Q}_q$ may be canonically extended to R as follows:

If $A = (\alpha_{ij})_{i,j=1,\dots,n}$ let $|A|_q = \max\{|\alpha_{ij}|_q \mid i,j = 1,\dots,n\}$. It is easy to verify the following properties. If $A = (\alpha_{ij})_{i,j}, B = (\beta_{ij})_{i,j} \in R$ then:

- $|A|_q = 0$ if and only if $A = 0$;
- $|A+B|_q \leq \max\{|A|_q, |B|_q\}$;
- $|AB|_q \leq |A|_q|B|_q$.

The mapping $|\cdot|_q : R \to \mathit{\Gamma}$ is an *ultrametric norm.*

We also have: if $|A|_q < |B|_q$ then $|A+B|_q = |B|_q$ and if I denotes the $n \times n$ identity matrix and $\alpha \in \mathbb{Q}_q$ then

$$|(\alpha I)A|_q = |\alpha|_q|A|_q.$$

Let $d : R \times R \to \mathit{\Gamma}$ be defined by $d(A,B) = |A-B|_q$. Then d is an ultrametric distance on R. It is also easy to show that $(R, d, \mathit{\Gamma})$ is spherically complete.

Let

$$\mathcal{A} = \{A \in R \mid |A|_q \leq 1\}, \quad \mathcal{M} = \left\{ A \in R \,\middle|\, |A|_q \leq \frac{1}{q} \right\},$$
$$\mathcal{M}' = \left\{ A \in R \,\middle|\, |A|_q \leq \frac{1}{q^2} \right\}.$$

It is clear that $\mathcal{A}$ is a subring of R and that $\mathcal{M}$ and $\mathcal{M}'$ are two-sided ideals of $\mathcal{A}$. We denote by $\mathcal{U}$ the multiplicative group of units of $\mathcal{A}$, that is, the elements $U \in \mathcal{A}$ such that there exists $V \in R$ such that $UV = VU = I$.

We also note that any chain of balls in $(R, d, \mathit{\Gamma})$ is countable. This follows from (2.1), because $\mathit{\Gamma}$ is countable.

3. Fermat's equation for matrices with q-adic entries. We keep the notations of Section 2. Moreover, if $A, B \in R$ let $[A,B] = AB - BA$. We note that if $A, B, C \in R$ then $[A, BC] = B[A,C] + [A,B]C$.

(3.1) Theorem. *Let $A, B \in R$ be such that*:

(1) $|A|_q \le 1/q$ *or if* $p = q = 2$ *then* $|A|_2 \le 1/2^2$;
(2) $B \in \mathcal{U}$;
(3) *for every* $Y \in \mathcal{M}'$,

$$|[B, Y]|_q \le \frac{1}{q^2}|Y|_q.$$

Then there exists $X \in \mathcal{A}$ such that $A^p + B^p = X^p$.

Proof. Since $B \in \mathcal{U}$ we have $|B|_q = 1$ and $B^{p-1} \in \mathcal{U}$, so there exists $U \in \mathcal{U}$ such that $UB^{p-1} = B^{p-1}U = I$. Thus $|U|_q = 1$.

The proof will be divided into several steps.

(1°) *For all* $Y \in \mathcal{M}'$,

$$|I - U(Y + B)^{p-1}|_q \le 1/q^2.$$

Indeed, for all $j \ge 1$ let $\mathcal{W}_j$ be the set of all words $W = T_1T_2 \dots T_{p-1}$ where $T_i \in \{Y, B\}$ and $\#\{i \mid T_i = Y\} = j$.

We write

$$(Y + B)^{p-1} = \sum_{j=1}^{p-1} S_j + B^{p-1} \quad \text{where} \quad S_j = \sum_{W \in \mathcal{W}_j} W.$$

Now, if $W \in \mathcal{W}_j$ then

$$|W|_q \le |Y|_q^j \le |Y|_q \le 1/q^2.$$

So

$$\Big|\sum_{j=1}^{p-1} S_j\Big|_q \le 1/q^2.$$

We deduce that

$$|I - U(Y + B)^{p-1}|_q = \Big|I - UB^{p-1} - U\Big(\sum_{j=1}^{p-1} S_j\Big)\Big|_q \le \Big|\sum_{j=1}^{p-1} S_j\Big|_q \le \frac{1}{q^2}.$$

(2°) *For all* $Y, Z \in \mathcal{M}'$, $Z \ne 0$, *and for all* $i \ge 1$,

$$\left|\frac{[Z, (Y + B)^i]}{pI}\right|_q < |Z|_q.$$

Let $C = Y + B$, so $|C|_q = 1$. The proof is by induction on i. Let $i = 1$. Then

$$\left|\frac{[Z, C]}{pI}\right|_q = \frac{|[Z, C]|_q}{|p|_q}.$$

But

$$|[Z, C]|_q = |[Z, Y] + [Z, B]|_q \le \max\{|[Z, Y]|_q, |[Z, B]|_q\};$$

next

$$|[Z,Y]|_q = |ZY - YZ|_q \leq |Z|_q|Y|_q \leq |Z|_q \cdot \frac{1}{q^2}$$

and

$$|[Z,B]|_q \leq |Z|_q \cdot \frac{1}{q^2}$$

by hypothesis, so

$$|[Z,C]|_q \leq |Z|_q \cdot \frac{1}{q^2}.$$

If $p \neq q$ then

$$\left|\frac{[Z,C]}{pI}\right|_q = \frac{|[Z,C]|_q}{|p|_q} \leq |Z|_q \cdot \frac{1}{q^2} < |Z|_q.$$

If $p = q$ also

$$\left|\frac{[Z,C]}{pI}\right|_q = \frac{|[Z,C]|_q}{1/q} \leq q|Z|_q \cdot \frac{1}{q^2} < |Z|_q.$$

Now let $i \geq 2$. Then

$$[Z,C^i] = C[Z,C^{i-1}] + [Z,C]C^{i-1}.$$

Since $|C|_q = 1$, by induction we deduce that

$$\left|\frac{[Z,C^i]}{pI}\right|_q \leq \max\left\{\left|\frac{C[Z,C^{i-1}]}{pI}\right|_q, \left|\frac{[Z,C]C^{i+1}}{pI}\right|_q\right\} < |Z|_q.$$

(3°) *For all* $Y, Z \in \mathcal{M}'$, $Z \neq 0$,

$$\left|Z - \frac{U}{pI}\left\{(Z+Y+B)^p - (Y+B)^p\right\}\right|_q < |Z|_q.$$

Let $C = Y + B$, so $|C|_q = 1$. For all $j \geq 1$ let $\mathcal{W}'_j$ be the set of all words $W' = T_1 \dots T_p$ where $T_i \in \{Z, C\}$ and $\#\{i \mid T_i = Z\} = j$. We write

$$(Z+C)^p - C^p = \sum_{j=1}^{p} S'_j \quad \text{where} \quad S'_j = \sum_{W \in \mathcal{W}'_j} W.$$

If $j \geq 2$ and $W \in \mathcal{W}'_j$ then

$$\left|\frac{W}{pI}\right|_q \leq \frac{|Z|_q^j}{|p|_q} \leq \frac{|Z|_q^2}{|p|_q}.$$

If $p \neq q$ then

$$\frac{|Z|_q^2}{|p|_q} = |Z|_q^2 < |Z|_q.$$

If $p = q$ then

$$\frac{|Z|_q^2}{|p|_q} \leq q|Z|_q \cdot \frac{1}{q^2} < |Z|_q.$$

So

$$\Big|\sum_{j=2}^{p} S'_j\Big|_q < |Z|_q.$$

On the other hand,

$$\begin{aligned} S'_1 &= C^{p-1}Z + C^{p-2}ZC + \ldots + ZC^{p-1} \\ &= pC^{p-1}Z + C^{p-2}[Z, C] + C^{p-3}[Z, C^2] + \ldots + [Z, C^{p-1}]. \end{aligned}$$

By (2°),

$$\left|\frac{\sum_{i=1}^{p-1} C^{p-1-i}[Z, C^i]}{pI}\right|_q \leq \max_{1\leq i\leq p-1}\left\{\left|\frac{[Z, C^i]}{pI}\right|_q\right\} < |Z|_q.$$

Next by (1°),

$$\left|Z - \frac{U}{pI}\, pC^{p-1}Z\right|_q = |\{I - U(Y+B)^{p-1}\}Z|_q \leq \frac{1}{q^2}\, |Z|_q < |Z|_q.$$

Finally,

$$\begin{aligned} &\left|Z - \frac{U}{pI}\,\{(Z+C)^p - C^p\}\right|_q \\ &\qquad = \left|Z - \frac{U}{pI}\Big\{pC^{p-1}Z + \sum_{i=1}^{p-1} C^{p-1-i}[Z, C^i] + \sum_{j=2}^{p} S'_j\Big\}\right|_q < |Z|_q. \end{aligned}$$

(4°) Let the mapping φ be defined by

$$\varphi(Z) = Z - \frac{U}{pI}\,\{(Z+B)^p - B^p - A^p\} \quad \text{for all } Z \in \mathcal{M}'.$$

If $p = q = 2$ then

$$\left|\frac{A^2}{2I}\right|_2 \leq \frac{|A|_2^2}{1/2} < \frac{1}{2^2}.$$

In the other cases, if $p \neq q$ then

$$\left|\frac{A^p}{pI}\right|_q \leq |A|_q^p \leq |A|_q^2 \leq \frac{1}{q^2}.$$

If $p = q \neq 2$ then

$$\left|\frac{A^p}{pI}\right|_q \leq \frac{|A|_q^p}{1/q} \leq \frac{|A|_q^3}{1/q} \leq \frac{1}{q^2}.$$

It follows from (3°) that $\varphi(Z) \in \mathcal{M}'$.

We show that φ is a strictly contracting mapping. Let $X, Y \in \mathcal{M}'$, $X \neq Y$, let $Z = X - Y \neq 0$ and let $C = Y + B$. Then

$$\varphi(X) - \varphi(Y) = Z - \frac{U}{pI}\,\{(Z+C)^p - C^p\}.$$

By (3°),

$$|\varphi(X)-\varphi(Y)|_q = \left| Z - \frac{U}{pI}\{(Z+C)^p - C^p\}\right|_q < |Z|_q = |X-Y|_q.$$

So φ is a strictly contracting mapping. Since $\mathcal{M}'$ is spherically complete, there exists $T \in \mathcal{M}'$ such that $\varphi(T) = T$, hence

$$\frac{U}{pI}\left((T+B)^p - B^p - A^p\right) = 0$$

and so

$$A^p + B^p = X^p \quad \text{with} \quad X = T + B \in \mathcal{A}. \ \blacksquare$$

(3.2) NOTE. It is easy to give examples of matrices B satisfying the conditions (2) and (3) of the theorem. Indeed, let $C \neq 0$ be such that $|C|_q \leq 1/q^2$, let $B = I - C$. Then $B \in \mathcal{U}$ because

$$I + C + C^2 + \ldots \in \mathcal{A}$$

and

$$(I-C)(I+C+C^2+\ldots) = (I+C+C^2+\ldots)(I-C) = I,$$

so $B \in \mathcal{U}$. Moreover, if $Y \in \mathcal{M}'$ then

$$[B,Y] = [I,Y] - [C,Y] = -[C,Y].$$

Hence

$$|[B,Y]|_q = |YC - CY|_q \leq |C|_q |Y|_q \leq \frac{1}{q^2}\,|Y|_q.$$

4. Fermat's equation for quaternions with q-adic coefficients. We shall establish a theorem about Fermat's equation for quaternions with q-adic coefficients. Using the representation of quaternions as 4×4 matrices, the theorem will follow from (3.1).

Let $n = 4$, $R = R_4$ and let H be the set of all matrices

$$A = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

with a, b, c, d q-adic numbers. Then H is a subfield of R, which is isomorphic to the field of quaternions.

Explicitly, the isomorphism is given by

$$1 \mapsto I, \qquad i \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$j \mapsto \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

If $X = (x_{ij}) \in R$ then $X \in H$ if and only if

$$(*) \qquad \begin{cases} x_{11} = x_{22} = x_{33} = x_{44}, \\ x_{12} = -x_{21} = x_{34} = -x_{43}, \\ x_{13} = -x_{24} = -x_{31} = x_{42}, \\ x_{14} = x_{23} = -x_{32} = -x_{41}. \end{cases}$$

Let

$$\mathcal{A}_H = \mathcal{A} \cap H, \quad \mathcal{M}_H = \mathcal{M} \cap H, \quad \mathcal{M}'_H = \mathcal{M}' \cap H, \quad \mathcal{U}_H = \mathcal{U} \cap H.$$

For each $A \in H$ and $m \geq 1$ we shall consider the balls

$$\mathcal{B}_{1/q^m}(A) = \{X \in R \mid |A - X|_q \leq 1/q^m\}$$

and

$$\mathcal{B}^H_{1/q^m}(A) = \mathcal{B}_{1/q^m}(A) \cap H.$$

(4.1) $\mathcal{M}'_H$ *is spherically complete.*

Proof. It suffices to show that every infinite chain of balls

$$\mathcal{C} : \mathcal{B}^H_{1/q^{m_1}}(A_1) \supset \mathcal{B}^H_{1/q^{m_2}}(A_2) \supset \ldots \quad \text{with} \quad m_1 < m_2 < \ldots,$$

has a non-empty intersection in $\mathcal{M}'_H$. Since $\mathcal{M}'$ is spherically complete, it follows that there exists $C \in \mathcal{M}'$ belonging to the intersection of the balls $\mathcal{B}_{1/q^{m_1}}(A_1), \mathcal{B}_{1/q^{m_2}}(A_2), \ldots$

We show that $C \in H$, hence $C \in \mathcal{M}'_H$.

Let $C = (c_{ij})$. We show that the entries c_{ij} satisfy the conditions in $(*)$. Say, for example, that $c_{11} \neq c_{22}$, and let $1/q^{m_k} < |c_{11} - c_{22}|_q$. Since $|C - A_{m_k}| \leq 1/q^{m_k}$, writing $A_{m_k} = (a_{ij})_{i,j}$, we have

$$|c_{11} - a_{11}|_q \leq \frac{1}{q^{m_k}}, \quad |c_{22} - a_{22}| \leq \frac{1}{q^{m_k}}.$$

From $a_{11} = a_{22}$ it follows that

$$|c_{11} - c_{22}| \leq \frac{1}{q^{m_k}},$$

which is a contradiction. With similar proofs, we deduce that $C \in H$, as required. ■

(4.2) Note. If $B \in \mathcal{U} \cap H$ let $C \in \mathcal{A}$ be such that $BC = CB = I$. Then $C \in H$, so B is an invertible element of $\mathcal{A}_H$.

Indeed, since H is a field, there exists $C' \in H$ such that $BC' = C'B = I$. Hence $B(C - C') = 0$, so $C - C' = CB(C - C') = 0$.

(4.3) Theorem. *Let $A, B \in H$ be such that*:

(1) $|A|_q \leq 1/q$ *or if* $p = q = 2$ *then* $|A|_2 \leq 1/2^2$;
(2) $B \in \mathcal{U}_H$;
(3) *for all* $Y \in \mathcal{M}'_H$,

$$|[B, Y]|_q \leq \frac{1}{q^2}\,|Y|_q.$$

Then there exists $X \in \mathcal{A}_H$ *such that* $A^p + B^p = X^p$.

Proof. Let $U \in \mathcal{U}$ be such that $UB^{p-1} = B^{p-1}U = I$. By (4.2), $U \in H$. Let φ_H be the restriction to $\mathcal{M}'_H$ of the mapping φ defined in step (4°) of the proof of (3.1). Since $\varphi_H(\mathcal{M}'_H) \subseteq \mathcal{M}'_H$, and φ_H is strictly contracting, and since $\mathcal{M}'_H$ is spherically complete by (4.1), there exists $T \in \mathcal{M}'_H$ such that $\varphi_H(T) = T$. Hence

$$\frac{U}{pI}\left((T + B)^p - B^p - A^p\right) = 0.$$

Thus if $X = T + B \in \mathcal{A}_H$ we have $A^p + B^p = X^p$. ∎

(4.4) Note. If $C \in H$, $C \neq 0$, $|C|_q \leq 1/q^2$ and $B = I - C$ then, as in (3.2), $B \in \mathcal{U}_H$ and

$$|[B, Y]|_q \leq \frac{1}{q^2}\,|Y|_q.$$

References

[1] S. Priess-Crampe, *Der Banachsche Fixpunktsatz für ultrametrische Räume*, Results Math. 18 (1990), 178–186.

[2] P. Ribenboim, *The new theory of ultrametric spaces*, Period. Math. Hungar. 32 (1996), 108–111.

[3] —, *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1979.

[4] —, *Fermat's Last Theorem for Amateurs*, Springer, New York, 1999.

[5] —, *The Theory of Classical Valuations*, Springer, New York, 1998.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario K7L 3N6, Canada

Received on 2.7.2002
and in revised form on 3.7.2003 (4319)