On the $p$-th root of a $p$-adic number

Alfonso Di Bartolo
Dipartimento di Matematica e Applicazioni
Via Archirafi 34, I-90123 Palermo (Italy)
alfonso@math.unipa.it

Giovanni Falcone
Dipartimento di Metodi e Modelli Matematici
Viale delle Scienze Ed. 8, I-90128 Palermo (Italy)
gfalcone@unipa.it

Abstract
We give a sufficient and necessary condition for a $p$–adic integer to have $p$–th root in the ring of $p$–adic integers. The same condition holds clearly for residues modulo $p^k$. We give a proof that Fermat’s last theorem is false for $p$–adic integers and for residues mod $p^k$.

Under the assumption that the prime $p$ does not divide the integer $k$, an immediate consequence of Hensel’s lemma is that a $p$–adic unit $a = l_0 + pl_1 + p^2l_2 + \cdots$ has a $k$–th root in the ring of $p$–adic integers if and only if $l_0$ has a $k$–th root in $Z_p = Z/pZ$. The same argument gives for the $p$–th root a sufficient but not necessary condition. In order to find the $p$–th root, we apply the exponential and logarithm maps to the Witt ring $\mathfrak{w}(Z_p)$, which is isomorphic to the ring of $p$–adic integers.

In his paper [4] of 1936, E. Witt found the algorithm which gives recursively the factor systems necessary to describe the ring of $p$–adic integers as the inverse limit of the rings of residues $Z_{p^k} = Z/p^kZ$. In this context this ring is denoted by

$$\mathfrak{w}(Z_p) = \{x = (x_0, x_1, \cdots, x_k, \cdots) | x_i \in Z_p\}$$

and its elements are called Witt vectors. For a detailed exposition, we refer to [2], Ch. V, no. 1.

The ground subring generated by the unitary element $1 = (1, 0, 0, \cdots)$ is isomorphic to $Z$ and in [3] we gave the representation of an arbitrary natural integer $n \in N$ as the element $n1$ of $\mathfrak{w}(Z_p)$.

One of the reasons to use the representation of integers as Witt vectors is that the quotient ring $\mathfrak{w}_k(Z_p) = \mathfrak{w}(Z_p)/p^k\mathfrak{w}(Z_p)$, which is isomorphic to the ring $Z/p^kZ$ of residues modulo $p^k$, can be represented as the ring of truncations of Witt vectors after the first $k$ entries, that is the set of elements of the shape

$$(x_0, x_1, \cdots, x_{k-1}).$$
This allows one to consider simultaneously integers, rationals, $p$–adics and residues modulo $p^k$ in many arguments.

1. Integers, residues and $p$–adics as Witt vectors.

For any $k = 0, 1, \ldots$, let $a_0, \ldots, a_k \in \mathbb{Q}$ be such that

$$\Phi_k(a_0, \ldots, a_k) = a_0^{p^k} + pa_1^{p^{k-1}} + \cdots + p^ka_k = n.$$  

Then we have (cf. [3]):

i) $a_0 = n$ and $a_{k+1} = \sum_{i=0}^{k} \frac{1}{p^{k-i}} (a_i^{p^{k-i}} - a_i^{p^{k-i+1}})$ are integers;

ii) $n \cdot 1 = (n_0, n_1, \cdots)$;

iii) if $p$ does not divide $n$, then $n$ divides each $a_k$.

We identify any integer $n$, not divisible by $p$, with $n \equiv \overline{n}$ modulo $p^k$ in many arguments.

According to a consolidated notation ([2], Ch. 5, §§ 1, 3, 4), the element $(\overline{a}, 0, 0, 0, \cdots) \in \mathbb{W}(\mathbb{Z}_p)$ is denoted by $a^T$ and is called the Teichmüller representative of $a$. Any Witt vector $x = (x_0, x_1, x_2, \cdots)$ such that $x_0 \not\equiv 0 \pmod{p}$ can be written as the product $x = x_0^T(1, x_1/x_0, x_2/x_0, \cdots)$. The invertible elements in $\mathbb{W}(\mathbb{Z}_p)$ are precisely those $x = (x_0, x_1, x_2, \cdots)$ having $x_0 \not\equiv 0 \pmod{p}$. Therefore any element of the quotient field of $\mathbb{W}(\mathbb{Z}_p)$, which is (isomorphic to) the field of $p$–adic numbers, can be written as $x = p^z x_0^T(1, x_1/x_0, x_2/x_0, \cdots)$, with $z \in \mathbb{Z}$ and $x_0 \not\equiv 0$. The
rational integer $p^{-z}$ is the $p$–adic valuation $|x|_p$ of $x$. With a slight abuse, we will call such elements Witt vectors, as well.

2. Logarithm and exponential map. De Moivre formula.

In this paragraph we assume $p > 2$. The formal power series

\[
\log(1 + px) = px - 1/2(px)^2 + 1/3(px)^3 - \cdots
\]

\[
e^{px} = 1 + px + 1/2!(px)^2 + 1/3!(px)^3 + \cdots
\]

are simply polynomials in the ring $\mathfrak{W}_k(Z_p)$ of truncated Witt vectors, isomorphic to the ring of residues $Z_{p^k} = Z/p^kZ$. For instance, for $p > 3$, we have

\[
\log(1 + a_1, a_2) = (0, a_1, a_2 - \frac{1}{2}a_1^2),
\]

\[
e^{(0, a_1, a_2)} = (1, a_1, a_2 + \frac{1}{2}a_1^2).
\]

Since the two maps can be defined for any $k > 0$, they are defined on the whole of

\[
1 + p\mathfrak{W}(Z_p) = \{x = (1, x_1, x_2, \cdots) : x_i \in Z_p\}
\]

and

\[
p\mathfrak{W}(Z_p) = \{x = (0, x_1, x_2, \cdots) : x_i \in Z_p\},
\]

respectively, and the two maps are mutually inverse.

Let $x = p^zx_0^z(1, x_1/x_0, x_2/x_0, \cdots)$, with $z \in \mathbb{Z}$ and $x_0 \not\equiv 0 (\text{mod } p)$, be an arbitrary Witt vector. If we define

the module $\rho_x := p^zx_0^z$,

the argument $\vartheta_x := \log(1, x_1/x_0, x_2/x_0, \cdots) \in \mathfrak{W}$,

then we can write

\[x = \rho_x e^{\vartheta_x}\]

and recover De Moivre formula

\[\rho_{xy} = \rho_x \rho_y,\]

\[\vartheta_{xy} = \vartheta_x + \vartheta_y,\]

holding for $p$–adics as well as for residues modulo $p^k$. We remark that, modulo $p^2$, De Moivre formula $\vartheta_{nm} = \vartheta_n + \vartheta_m$ coincides with the Eisenstein congruence $q_1(n \cdot m) \equiv q_1(n) + q_1(m) (\text{mod } p)$.

As an application we compute

\[x^{-1} = \rho_x^{-1} e^{-\vartheta_x}\]
for a natural integer \( n \equiv n^\tau(1, -q_1(n), -q_2(n), \ldots) \), not divisible by \( p \).

In fact,

\[
\left( n^\tau(1, -q_1(n), -q_2(n), \ldots) \right)^{-1} = (n^\tau)^{-1} e^{(0, -q_1(n), -q_2(n) - \frac{1}{2} q_1^2(n), \ldots)} =
\]

\[
(n^{-1})^\tau e^{(0, q_1(n), q_2(n) + \frac{1}{2} q_1^2(n), \ldots)} = (n^{-1})^\tau(1, q_1(n), q_2(n) + q_1^2(n), \ldots).
\]

Similarly, if \( m \) and \( n \) are two integers, not divisible by \( p \), we find

\[
\frac{m}{n} \equiv \left( \frac{m}{n}, -\frac{m}{n}(q_1(m) - q_1(n)), \ldots \right).
\]

It is standard to define, for \( x \in 1 + p \mathbb{W}(\mathbb{Z}_p) \) and \( y \in \mathbb{W}(\mathbb{Z}_p) \),

\[
x^y := e^{y \log x} \in \mathbb{W}(\mathbb{Z}_p),
\]

and the aim of this paper is to remark that \( x^y \) is still in \( \mathbb{W}(\mathbb{Z}_p) \) for a \( p \)-adic number \( y \) with positive \( p \)-adic valuation \( |y|_p = p^k \), if we assume \( x_i \equiv 0 \pmod{p} \) for \( i = 1, 2, \ldots, k \).

### 3. The \( p \)-th root.

Let \( p > 2 \) and let \( x = p^x x_0^\tau(1, x_1/x_0, \ldots, x_k/x_0, \ldots) \) be a Witt vector, with \( z \in \mathbb{Z} \) and \( x_0 \not\equiv 0 \pmod{p} \). As an immediate consequence of De Moivre formula, we have

\[
x^{p^k} = p^{x^p} x_0^\tau(1, 0, \ldots, 0, x_1/x_0, \ldots)
\]

(note that, from the \( k+2 \)-nd one on, the entries become more involved). Furthermore, if the Witt vector \( x = (x_0, x_1, \ldots) \) is such that \( x_0 \not\equiv 0 \) and \( x_i \equiv 0 \), for \( i = 1, \ldots, k \), then we find

\[
\frac{x - x^p}{p^{k+1}} \equiv \frac{(x_0, 0, \ldots, 0, x_{k+1}) - (x_0, 0, \ldots, 0, 0)}{p^{k+1}}
\]

\[
= \frac{(0, 0, \ldots, 0, x_{k+1})}{p^{k+1}} = (x_{k+1}, \ldots),
\]

(once again, we remark that, from the \( k+2 \)-nd one on, the entries become more involved). Thus we have in this case

\[
x_{k+1} \equiv -\frac{1}{p^k} \frac{x^p - x}{p} \pmod{p} = -\frac{1}{p^k} x q_1(x) \pmod{p},
\]

where, in analogy to the case of an integer, we define the Fermat quotient of the Witt vector \( x = (x_0, x_1, \ldots, x_k, \ldots) \), having \( x_0 \not\equiv 0 \pmod{p} \), as
q_1(x) = \frac{x^{p-1}}{p} \in \mathcal{W}(\mathbb{Z}_p). \text{ We note that, in accordance with the case of an integer, we have } x_1 \equiv -xq_1(x) \pmod{p} \text{ and again, De Moivre formula } \\
v_{xy} = v_x + v_y \text{ reduces in } \mathcal{W}_2(\mathbb{Z}_p) \text{ to Eisenstein congruence } q_1(x \cdot y) \equiv q_1(x) + q_1(y) \pmod{p}. \quad \Box

Having the entries \( x_i \equiv 0 \pmod{p} \) for \( i = 1, \ldots, k \) is not only a necessary condition for a Witt vector to be a \( p^k \)-th power, it is sufficient, as well. Our condition is based on the fact that

\[ p^{-k} \log(1, x_1/x_0, \ldots, x_k/x_0, \ldots) = p^{-k}(0, x_1/x_0, \ldots) \]

lies in \( p\mathcal{W}(\mathbb{Z}_p) \) if and only if \( x_i \equiv 0 \pmod{p} \), for \( i = 1, 2, \ldots k \). The Witt vector \( x = p^j x_0^j(1, x_1/x_0, \ldots, x_k/x_0, \ldots) \) has therefore a \( p^k \)-th root in \( \mathcal{W}(\mathbb{Z}_p) \) if and only if \( z \equiv 0 \pmod{p^k} \) and \( x_i \equiv 0 \pmod{p} \), for \( i = 1, 2, \ldots k \). In this case the root is unique and it is

\[ x^{\frac{1}{p^k}} = p^j x_0^{\frac{1}{p^k}} e^{\frac{1}{p^k} \log(1, 0, \ldots, 0, x_{k+1}/x_0, \ldots)}. \]

For instance, let \( x = x_0^j(1, 0, x_2/x_0, \ldots, x_k/x_0, \ldots) \in \mathcal{W}(\mathbb{Z}_p) \). Then we have

\[ x^{\frac{1}{p^k}} \equiv x_0^{\frac{1}{p^k}} e^{\frac{1}{p^k} \log(1, 0, x_2/x_0, x_3/x_0)} = x_0^{\frac{1}{p^k}} e^{(0, x_2/x_0, x_3/x_0)} \]

\[ = x_0^{\frac{1}{p^k}}(1, x_2/x_0, x_3/x_0 + 1/2(x_2/x_0)^2) \pmod{p^3}. \]

Therefore the integer \( n \), not divisible by \( p \), has the \( p \)-th root in the ring of \( p \)-adic integers if and only if \( q_1(n) \equiv 0 \pmod{p} \), that is if \( n^p \equiv n \pmod{p^2} \) and the \( p \)-adic unit \( a = l_0 + pl_1 + p^2 l_2 + \cdots \) has the \( p \)-th root in the ring of \( p \)-adic integers if and only if \( q_1(a) \equiv 0 \pmod{p} \), that is if \( a^p \equiv a \pmod{p^2} \). We remark that this condition is equivalent to say that

\[ l_1 \equiv \frac{l_0 - l_0}{p} \pmod{p}. \quad \Box \]

If \( p = 2 \), the two opposite square roots of a unit \( x \) exist if and only if \( x \equiv 1 \pmod{2} \). This follows directly from Hensel’s lemma. But we note that it is possible to compute these roots also as \( x^{\frac{1}{2}} = e^{\frac{1}{2} \log x} \). In fact, it is well–known that for \( p = 2 \) the exponential map is defined for \( x \in 4 \mathcal{W}(\mathbb{Z}_2) \). \quad \Box

Let \( x = (x_0, x_1, \ldots, x_k, \ldots) \) be a Witt vector, such that \( x_0 \neq 0 \) and \( x_i \equiv 0 \pmod{p} \), for \( i = 1, 2, \ldots, k \), and compute

\[ x^{\frac{1}{p^k}} \equiv (x_0, x_{k+1}] \pmod{p^2}. \]

Thus the above congruence \( x_{k+1} \equiv -\frac{1}{p^k} xq_1(x) \pmod{p} \) can be written meaningfully as

\[ q_1(x^{\frac{1}{p^k}}) \equiv \frac{1}{p^k} q_1(x) \pmod{p}, \]
in accordance with the Eisenstein congruence $q_1(x \cdot y) \equiv q_1(x) + q_1(y) \pmod{p}$.

□

**Example:** A non–trivial case where $q_1(n) \equiv 0 \pmod{p}$ is for $n = 3$ and $p = 11$. This means that $n = 3$ has 11–adic root in the 11–adic field or, equivalently, that the residue of $n = 3$ in $\mathbb{Z}_{11^k}$ has 11–th root in $\mathbb{Z}_{11^k}$, for any $k \geq 1$. In particular, we find

$$3^{11} = 3^\tau e^{(\frac{1}{11} \log(1,0,-q_2(3)))} = 3^\tau e^{(0,0,-q_2(3))} = 3^\tau (1, -q_2(3)).$$

As we mentioned above, a consequence of the congruence $q_1(3) \equiv 0 \pmod{11}$ is that $q_2(3) \equiv 5368 \equiv 4 \pmod{11}$. Therefore

$$3^{11} \equiv 3^\tau (1, -4) = (3, -1]$$

hence $3 - 11 = -8$ is the 11–th root of 3 modulo $11^2$.

□

Denote by $\varphi_1(x_0, y_0)$ the factor system defining the sum in the ring $\mathfrak{W}_2(\mathbb{Z}_p)$ of truncated Witt vectors, that is

$$(x_0, x_1) + (y_0, y_1) = (x_0 + y_0, x_1 + y_1 + \varphi_1(x_0, y_0)).$$

As remarked in [3], we have

$$\varphi_1(x_0, y_0) \equiv \sum_{i=1}^{p-1} \frac{(-1)^i}{i} x_0^i y_0^{p-i} \pmod{p}.$$

The smallest prime $p$ such that, for a suitable integer $0 < x < p - 1$,

$$\varphi_1(1, x) \equiv 0 \pmod{p}$$

is $p = 7$. In fact, $\varphi_1(1, 2) \equiv 0 \pmod{7}$. Since

$$129 = 7^2 + 2^7 \equiv (1, 0] + (2, 0] = (3, 0] \pmod{7^2},$$

it follows that 129 is the 7–th power of a 7–adic integer. This shows that the equality $x^7 + y^7 + z^7 = 0$ has a non–trivial 7–adic solution and the equality $x^7 + y^7 + z^7 \equiv 0 \pmod{7^k}$ has a non–trivial solution for any $k \geq 0$ (cfr. [1], Remark 1, p. 163).

□

It seems very rare that $n = 2$ has the $p$–th root in the field of $p$–adics. In fact 1093 and 3511 are the only known primes, up to $1.25 \cdot 10^{15}$, for which $q_1(2) \equiv 0 \pmod{p}$. These primes are called *Wieferich primes* since Wieferich proved in 1909 that, if $x^p + y^p + z^p = 0$ had a non trivial integer solution with $xyz$ not divisible by $p$, then $q_1(2) \equiv 0 \pmod{p}$. In 1910 Mirimanoff proved moreover that for such a prime $p$ it must hold that $q_1(3) \equiv 0 \pmod{p}$ and a still open question is whether it is possible that simultaneously $q_1(2) \equiv q_1(3) \equiv 0 \pmod{p}$. □
References

[1] A. I. Borevich, I. R. Shafarevich, *Number theory*, Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966.

[2] M. Demazure, P. Gabriel, *Groupes Algébriques*, Masson & Cie, Paris, North-Holland, Amsterdam 1991.

[3] A. Di Bartolo, G. Falcone, “Witt vectors and Fermat quotients”, submitted. http://www.unipa.it/~gfalcone/WF.pdf

[4] E. Witt, “Zyklische Körper und Algebren der Charakteristik $p$ vom Grad $p^n$. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik $p$”, J. Reine Angew. Math. 176, 126-140 (1936).