An Overview of Witt Vectors

Daniel Finkel

December 7, 2007

Abstract

This paper offers a brief overview of the basics of Witt vectors. As an application, we summarize work of Bartolo and Falcone to prove that Fermat's Last Theorem does not hold true over the p-adic integers.

1 Fundamentals of Witt vectors

The goal of this paper is to define Witt vectors and develop some of the structure surrounding them. In this section we describe how the Witt vectors generalize the p-adics, and how Witt vectors over any commutative ring themselves form a ring. In the second section we introduce the Teichmüller representative, show that the integers are a subring of the p-adics, and prove De Moivre's formula for Witt vectors. In the third and last section we give necessary and sufficient conditions for a p-adic integer to be a p^k-th power, and show that that Fermat's Last Theorem is false over the p-adic integers.

For the following, fix a prime number p.

Definition. A *Witt vector* over a commutative ring R is a sequence $(X_0, X_1, X_2 \ldots)$ of elements of R.

Remark. Witt vectors are a generalization of p-adic numbers; indeed, if $R = \mathbb{F}_p$ is the finite field with p elements, then any Witt vector over R is just a $p-$adic number. The original formulation of p-adics integers were power series $a_0 + a_1 p^1 + a_2 p^2 + \ldots$, with $a_i \in \{0, 1, 2, \ldots, p-1\}$. While the power series notation is suggestive of analytic inspiration, it proved unwieldy for actual calculation. Teichmüller suggested what has become the current notation, wherein each p-adic number is represented as an infinite sequence of elements of $\mathbb{F}_p$.

Witt Vectors have lots of nice properties, and their applications range through number theory and algebraic geometry. Ernst Witt (1911-1991) showed how to put a canonical ring structure on the collection of Witt vectors over any ring. To do this, he introduced Witt polynomials.

Definition. Let p be a prime number, and $(X_0 \ldots,\ X_n, \ldots)$ be an infinite sequence of indeterminates.For $n \geq 0$, we define the n-th *Witt polynomial* W_n as

$$W_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \ldots + p^n X_n.$$

Example. The first three Witt polynomials are

$$\begin{aligned} W_0 &= X_0, \\ W_1 &= X_0^p + pX_1, \\ W_2 &= X_0^{p^2} + px_1^p + p^2 x_2. \end{aligned}$$

The next theorem, which we cite without proof from [1], provides the key to adding and multiplying Witt vectors.

Theorem 1. Let $(X_0, X_1, X_2 \ldots)$ and $(Y_0, Y_1, Y_2 \ldots)$ be two sequences of indeterminates. For every polynomial function $\Phi \in \mathbb{Z}[X, Y]$ there exist a unique sequence $(\phi_0, \ldots, \phi_n, \ldots)$ of elements of $\mathbb{Z}[X_0, \ldots, X_n \ldots; Y_0, \ldots, Y_n, \ldots]$ such that

$$W_n(\phi_0, \ldots, \phi_n, \ldots) = \Phi(W_n(X_0, \ldots, X_n \ldots), W_n(Y_0, \ldots, Y_n, \ldots)), \qquad n = 0, 1, \ldots.$$

Applying Theorem 1, we denote by S_i (respectively P_i) the polynomials ϕ_i associated to

$$\Phi(X, Y) = X + Y \qquad \text{(respectively } \Phi(X, Y) = X.Y\text{)}.$$

Letting R be an arbitrary commutative ring, and letting $A = (a_0, a_1, \ldots)$, and $B = (b_0, b_1, \ldots)$ be Witt vectors over R, we have equations for adding and multiplying Witt vectors:

$$\begin{aligned} A + B &= (S_0(A, B), S_1(A, B), \ldots) \\ A.B &= (P_0(A, B), P_1(A, B), \ldots) \end{aligned}$$

Example. The first couple values of addition and multiplication of Witt vectors are:

$$\begin{aligned} S_0(A, B) &= a_0 + b_0, \quad S_1(A, B) = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p}, \\ P_0(A, B) &= a_0 b_0, \qquad P_1(A, B) = b_0^p a_1 + a_0^p b_1 + p a_1 b_1. \end{aligned}$$

Note that each term of the numerator of the quotient in $S_1(A, B)$ is divisible by p, so this makes sense even when we are in $\mathbb{F}_p$. We will deal more with this term in section 3.

In fact, one can check that these operations make the Witt vectors into a ring.

Corollary 2. The Witt vectors over any commutative ring R form a commutative ring, which we denote by $W(R)$.

Example.

(i) If p is invertible in R, then $W(R) = R^N$ (the product of countable number of copies of R). In fact, the Witt polynomials always give a homomorphism from the ring of Witt vectors to R^N, and if p is invertible this homomorphism is an isomorphism.

(ii) The Witt ring of the finite field of order p is the ring of p-adic integers.

(iii) The Witt ring of a finite field of order p^n is an unramified extension of the ring of p-adic integers.

The functions P_k and S_k are actually functions of the first k terms of A and B. In particular, if we truncate all the vectors at the k-th entry, we can still add and multiply them. This allows us to define the *truncated Witt ring* $W_k(R) := \{(a_0, a_1, \ldots, a_{k-1}) |\ a_i \in R\}$.

Example. The truncated Witt ring $W_k(\mathbb{F}_p) = \mathbb{Z}/p^k\mathbb{Z}$.

Definition. The "shift" map $V : W(R) \to W(R)$ is defined by

$$V(A) = (0, a_0, a_1, \ldots).$$

When R is a ring of characteristic p, the map $F : W(R) \to W(R)$ is defined by

$$F(A) = (a_0^p, a_1^p, \ldots).$$

Considering p to denote the map that is multiplication by p, we also have the identity $VF = p = FV$. This identity can easily be seen to be true when $R = \mathbb{F}_p$. In this case, $W(R)$ is the ring of p-adic integers, F is the identity map, and $p = V$.

Notice that $W_k(R) = W(R)/(V^k W(R))$. In particular, when $R = \mathbb{F}_p$ we have

$$W_k(\mathbb{F}_p) = W(\mathbb{F}_p)/(p^k W(\mathbb{F}_p)) = \mathbb{Z}/p^k\mathbb{Z}.$$

This allows us to speak of Witt vectors being equivalent modulo p^k when their k-th truncations agree.

2 De Moivre's Formula

Definition. The element $(\bar{a}, 0, 0, \ldots) \in W(\mathbb{F}_p)$ is denoted by a^τ and is called the *Teichmüller representative* of a, where $\bar{a}$ is the reduction of a modulo p. Notice that

$$(a^\tau)^p = (\bar{a}, 0, 0, \ldots)^p = (\bar{a}^p, 0, 0, \ldots) = (\bar{a}, 0, 0, \ldots) = a^\tau$$

since $\bar{a}^p = \bar{a}$ in $\mathbb{F}_p$.

There is a natural injection $\mathbb{Z} \to W(\mathbb{F}_p)$ defined by taking $1 \to 1^\tau$. Following [3] we can describe the representatives for $n \in \mathbb{N}$ in $W(\mathbb{F}_p)$ by the following proposition.

Proposition 3. Let $n \in \mathbb{N}$. For any $k = 0, 1, \ldots$, let $\mathfrak{a}_0, \ldots, a_k \in \mathbb{Q}$ be elements such that the k-th Witt polynomial $W_k(a_0, \ldots, a_k) = n$. Then

(i) $a_0 = n$ and $a_{k+1} = \sum_0^k \frac{1}{p^{k-i+1}}(a_{i^{p^{k-i}}} - a_i^{p^{k-i+1}}) \in \mathbb{Z}$;

(ii) $n \times 1^\tau = (\bar{a_0}, \bar{a_1}, \ldots)$; and

(iii) If p does not divide n, then n divides each a_k.

Proof: [3].

Any Witt vector $A = (a_0, a_1, \ldots)$ with $a_0 \neq 0 \pmod{p}$ can be written as the product $A = a_0^\tau(1, a_1/a_0, a_2/a_0, \ldots)$. The invertible elements in $W(\mathbb{F}_p)$ are precisely those A having $a_0 \neq 0 \pmod{p}$. Therefore any element of the quotient field of $W(\mathbb{F}_p)$, which is the field of p-adic numbers, can be written as $A = p^z a_0^\tau(1, a_1/a_0, a_2/a_0, \ldots)$.

This notation is suggestive (if you stare at it long enough) of the complex number notation $z = |z|e^{i\theta}$. In fact, we can formulate a similar module/argument notation for Witt vectors over $\mathbb{F}_p$, and prove that multiplication in this case also satisfies De Moivre's formula. In order to do this, we must first define the logarithmic and exponential maps for Witt vectors. Fortunately, we can simply extend the formal power series definition.

Definition. Assume $p > 2$, and let $A \in W_k(\mathbb{F}_p)$ be a truncated Witt vector. Then we define the functions

$$log(1 + pA) = pA - 1/2(pA)^2 + 1/3(pA)^3 - \ldots$$
$$e^{pA} = 1 + pA + 1/2!(pA)^2 + 1/3!(pA)^3 + \ldots$$

If A is a truncated Witt vectors over $\mathbb{F}_p$, then $log(1 + pA)$ and e^{pA} are just (finite) polynomials in $W_k(\mathbb{F}_p)$, since $p^k A = 0$ for all $A \in W_k(\mathbb{F}_p)$. However, since these two maps can be defined for any k, we can define them on the whole of

$$1 + pW(\mathbb{F}_p) = \{A = (1, a_1, a_2, \ldots) \quad a_i \in \mathbb{F}_p\} \quad \text{and}$$
$$pW(\mathbb{F}_p) = \{A = (0, a_1, a_2, \ldots) \quad a_i \in \mathbb{F}_p\}.$$

Since they are defined via their power series expansion, the two maps are mutually inverse.

Now writing an arbitrary Witt vector $A = p^z a_0^\tau(1, a_1/a_0.a_2/a_0, \ldots)$, we may define the *module* $\rho_A := p^z a_0^\tau$ and the *argument* $\theta_A := log(1, a_1/a_0, a_2, a_0, \ldots)$. This allows us to write, even more suggestively

$$A = \rho_A e^{\theta_A}$$

and recover De Moivre's formula

$$\rho_{AB} = \rho_A \rho_B, \qquad \theta_{AB} = \theta_A + \theta_B$$

for the p-adics.

3 An Application: Fermat's Last Theorem is false for p-adic Integers.

Armed with this structure, we can determine when p-adics have p^{th} roots. Letting $p > 2$ as above, take an arbitrary $A \in W(\mathbb{F}_p)$, with first term $x_0 \neq 0 \pmod{p}$. Using De Moivre, we have

$$A^{p^k} = (\rho_A e^{\theta_A})^{p^k} = (\rho_A)^{p^k}(e^{\theta_A})^{p^k} = (p^z a_0^\tau)^{p^k}(e^{p^k\theta_A}) = p^{zp^k} a_0^\tau(1, \underbrace{0, \ldots, 0}_{k}, a_1/a_0, \ldots)$$

where the entries to the right of a_1/a_0 get more complicated.

From this it is clear that having $x_i \equiv 0$ for $i = 1, \ldots, k$ is a necessary condition for a Witt vector to have a p^k-th power. It turns out that it is a sufficient condition as well. Let $A = (\rho_A e^{\theta_A}) = p^z a_0^\tau(1, a_1/a_0, a_2/a_0, \ldots)$ be a Witt vector such that p^k divides z and $a_i \equiv 0 \pmod{p}$ for $i = 1, 2, \ldots, k$. Then we can calculate explicitly that

$$A^{1/p^k} = p^{\frac{z}{p^k}} a_o^\tau \exp(\frac{1}{p^k}\log(1, 0, \ldots, 0, a_{k+1}/a_0, \ldots).$$

But

$$\frac{1}{p^k}\log(1, 0, \ldots, 0, a_{k+1}/a_0, \ldots) = \frac{1}{p^k}(0, \ldots, 0, a_{k+1}/a_0, \ldots) = (0, a_{k+1}/a_0, \ldots) \in pW(\mathbb{F}_p).$$

In other words, $(\frac{1}{p^k}\log(1, 0, \ldots, 0, a_{k+1}/a_0, \ldots)$ is in the domain of the exponential function, so A^{1/p^k} is well defined, and in fact, uniquely defined. Thus, we have proven

Theorem 4. A Witt vector $A = p^z a_0^\tau(1, a_1/a_0, a_2/a_0, \ldots)$ over $\mathbb{F}_p$ has a p^k-th root if and only if p^k divides z and $a_i = 0$ for $i = 1, 2, \ldots, k$. □

As an application of this theorem, we will exhibit an example of p-adics which solve a Fermat equation $a^n + b^n = c^n$. In particular, we will let $n = p$ prime, and we will restrict ourselves to Witt vectors with $z = 0$ in the language of Theorem 4. Now, to find such a solution, we need only concern ourselves with the truncated Witt vectors $W_2(\mathbb{F}_p)$, since a Witt vector A has a p-th root according to the theorem when the second term–a_1–is 0, and this term in a sum is determined only by the zero-th and first terms of the summands. So the problem of finding a solution to $a^p + b^p = c^p$ over the p-adics reduces to the

problem of finding three truncated Witt vectors $A, B, C \in W_2(\mathbb{F}_p)$ such that $A = (a_0, 0),\ B = (b_0, 0),\ C = (c_0, 0)$ and $A + B = C$. This is, of course, a much easier problem.

In particular, we need to choose $(a_0, 0),\ (b_0, 0)$, and p such that $(a_0, 0) + (b_0, 0) = (c_0, c_1)$ satisfies $c_1 = 0$. Looking back to our equations for sums (over $\mathbb{F}_p$, and hence modulo p, in this case) recall that

$$S_1(A, B) = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p} = \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p} \pmod{p}$$

because $a_1 = b_1 = 0$ in this case. Expanding $(a_0 + b_0)^p$ lets us rewrite this as

$$\frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p} = -\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} a_0^i b_0^{p-i}.$$

Now notice that

$$\frac{\binom{p}{i}}{p} = \frac{(p-1)(p-2)\dots(p-i+1)}{i(i-1)\dots(1)} \equiv \frac{(-1)(-2)\dots(-i+1)}{(1)(2)\dots(i)} \equiv \frac{(-1)^{i-1}}{i} \pmod{p}.$$

Which gives us the equivalence

$$S_1(A, B) = \sum_{i=1}^{p-1} \frac{(-1)^i}{i} a_0^i b_0^{p-i} \pmod{p}.$$

So to find our Fermat triple of p-adics is now a matter of finding a_0, b_0, and p such that $S_1(A, B) = 0 \pmod{p}$.

For example, we check that $S_1(1, 2) \equiv 0 \pmod{7}$.

$$S_1((1,0),(2,0)) = (-1)2^6 + \frac{1}{2}2^5 - \frac{1}{3}2^4 + \frac{1}{4}2^3 - \frac{1}{5}2^2 + \frac{1}{6}2^1 \equiv$$
$$-1 + 2 - 3 + 2 + 2 + 5 \equiv 0 \pmod{7}$$

This means that $(1, 0)+(2, 0) = (3, 0)$ gives a solution to the Fermat equation for $n = 7$ in $W_2(\mathbb{F}_p)$, since all three of the terms in the sum have 7-th roots. Furthermore, any Witt vectors $A, B \in W(\mathbb{F}_p)$ with

$$A = (1, 0, a_2, \dots), \qquad B = (2, 0, b_2, \dots)$$

are seventh powers that sum to a seventh power. Note also that since

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

using our association between truncated Witt vectors of length k and integers modulo p^k, we have that the image of 129 in $W(\mathbb{F}_p)$ has a seventh root.

References

[1] Serre, Jean-Pierre (1979), Local fields, vol. 67, Graduate Texts in Mathematics, Berlin, New York: Springer-Verlag, MR554237, ISBN 978-0-387-90424-5, section II.6

[2] A. Di Bartolo, G. Falcone, On the p-th root of a p-adic number, http://www.unipa.it/ gfalcone/MYPAPERS/

[3] A. Di Bartolo, G. Falcone, Witt vectors and Fermat quotients, http://www.unipa.it/ gfalcone/MYPAPERS/

[4] Wikipedia Entry for Witt Vectors, http://en.wikipedia.org/wiki/Witt_vectors