Using Witt Vectors to Disprove Fermat's Last Theorem

Benjamin Rosen

May 2026

Abstract

In this paper, we define the Witt vectors and provide (hopefully) good intuition for them. We will approach multiplication and addition, to show the Witt vectors form a commutative ring. We then apply the Witt vectors to disprove Fermat's Last Theorem over $\mathbb{Z}_p$.

1 Witt Vector Basics

For this paper, we'll work with some fixed prime number p, as we do with p-adic numbers.

Definition 1.1. A *Witt vector* over a commutative ring R is a sequence $(X_0, X_1, X_2 \ldots)$ of elements of R.

As a reminder, the definition of a ring is as follows:

Definition 1.2. A *ring* is a set R combined with two operations $+$ and $\cdot$, acting as addition and multiplication, with the following properties:

1. For all $a, b, c \in R$, $a + (b + c) = (a + b) + c$.
2. For all $a, b \in R$, $a + b = b + a$.
3. There exists an element 0 in R such that $a + 0 = 0 + a = a$ for all a in R.
4. For all a in R there exists an element $-a$ such that $(-a) + a = 0$.

5. For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

6. For all $a, b, c \in R$, $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$, and $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$.

7. There exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$.

If a ring also has the extra property that for all $a, b \in R$, $a \cdot b = b \cdot a$, then it is a *commutative ring*. An example of one such ring is $\mathbb{Z}/p\mathbb{Z}$.

As it turns out, Witt vectors are actually very close to the p-adic numbers, to the extent that they can even be seen as an generalization of them. If we let R be the finite field $\mathbb{F}_p$, then any Witt vector over R is just a p-adic number.

Next, to create a ring structure, we'll define the Witt polynomial.

Definition 1.3. Let p be a prime number, and let $(X_0, \ldots, X_n, \ldots)$ be an infinite sequence. Then the *n-th Witt polynomial* for $N \geq 0$ W_n is defined as the sum

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

As an example, the 2nd Witt polynomial is

$$W_2 = X_0^{p^2} + pX_1^p + p^2 X_2.$$

1.1 Addition and Multiplication

Next, to show the Witt vectors are a ring, we'll construct addition and multiplication. The W_n we constructed above are called the *ghost components* of the Witt vector $(X_0, X_1, X_2 \ldots)$. These are often denoted as $X^{(i)}$ rather than W_i. We make the addition and multiplication by the componentwise addition and multiplication of the ghost components. That is to say, we have

$$(X + Y)_i \text{ and } (X \cdot Y)_i$$

are given by polynomials, for which coefficients do not depend on p, and

$$X^{(i)} + Y^{(i)} = (X + Y)^{(i)}, X^{(i)} \cdot Y^{(i)} = (X \cdot Y)^{(i)},$$

again keeping in mind that $X^{(i)}$ is actually the ghost component W_i of $(X_0, X_1, \ldots, X_i, \ldots)$, and likewise for $Y^{(i)}$. With these operations, the Witt

vectors form a commutative ring, denoted $W(R)$.

As it turns out, if we truncate all of the vectors at the kth entry, we can still add and multiply them. This gives us what we'll call the *truncated Witt ring*, which is just $W_k(R) = \{(a_0, a_1, \ldots, a_k) : a_i \in R\}$. Two Witt vectors will then be equivalent modulo p^k if their kth truncations are the same.

2 Disproving Fermat's Last Theorem

Next, we'll apply Witt vectors to disprove Fermat's last theorem. In order to do this, we'll prove a result called De Moivre's formula first.

2.1 De Moivre's Formula

We first define the Teichmüller representative for Witt vectors.

Definition 2.1. A *Teichmüller representative* a^τ of an element $a \in \mathbb{F}_p$ is the Witt vector $(\overline{a}, 0, 0, 0, \ldots)$, where $\overline{a}$ is the reduction of a modulo p.

Any Witt vector $A = (a_0, a_1, a_2 \ldots)$ can be written as the product $A = a_0^\tau \cdot (1, a_1/a_0, a_2/a_0, \ldots)$. Then the invertible elements of $W(\mathbb{F}_p)$ are those such that $a_0 \neq 0 \pmod p$. Thus any element of the quotient field of $W(\mathbb{F}_p)$, the field of p-adic numbers, can be written as $A = p^z a_0^\tau (1, a_1/a_0, a_2/a_0, \ldots)$.

If you look at this hard enough, it is vaguely reminiscent of the complex number formula $z = |z|e^{i\theta}$. We can actually form a similar result do De Moivre's formula for complex numbers, with Witt vectors. In order to do this, we'll need to define exponential and logarithmic maps. Fortunately, we can simply extend the power series definitions of these.

Definition 2.2. Let $p > 2$, and then let $A \in W_k(\mathbb{F}_p)$ be a truncated Witt vector. Then

$$\log(1 + pA) = pA - \frac{(pA)^2}{2} + \frac{(pA)^3}{3} \cdots$$

and

$$e^{pA} = 1 + pA + \frac{(pA)^2}{2!} + \frac{(pA)^3}{3!} \cdots$$

Now, let us take a Witt vector $A = p^z a_0^\tau (1, a_1/a_0, a_2/a_0, \ldots)$. We can now define the *module* $\rho_A = p^z a_0^t$ and the *argument* $\theta_A = \log(1, a_1/a_0, a_2/a_0, \ldots)$. Thus we have the formula

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

and De Moivre's formulas $\rho_{AB} = \rho_A \rho_B$, $\theta_{AB} = \theta_A + \theta_B$.

2.2 Disproving Fermat

We'll now go through a proof that Fermat's Last Theorem is false, as described in [Fin07]. To do this, we'll first prove the following theorem. We'll continue assuming $p > 2$ as above, as Fermat's Last Theorem is specifically for powers greater than 2 amyways.

Theorem 2.3. *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^kth root if and only if p^k divides z and $a_i = 0$ for all $i \in 1, 2, \ldots, k$.*

Proof. Choose an arbitrary $A \in W(\mathbb{F}_p)$, with the first term $x_0 \neq 0 \mod p$. Then using De Moivre,

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

with exactly k zeroes between the first 1 and a_1/a_0, and the entries to the right of a_1/a_0 will get more complicated.

Thus having $x_i \equiv 0$ for $i = 1, 2, \ldots, k$ is a necessary condition for a Witt vector to have a p^kth power. It is a sufficient condition as well. To show this, 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 $a_i \equiv 0 \mod p$ for $i = 1, 2, \ldots, k$. Then we can calculate that

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

and

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

so that $\frac{1}{p^k} \log(1, 0, \ldots, 0, a_{k+1}/a_{0,\ldots})$ is in the domain of the exponential function. Thus $A^{\frac{1}{p^k}}$ is well defined, and uniquely defined. □

To disprove Fermat's Last Theorem over the p-adic numbers, we'll find an example of $a^n + b^n = c^n$, with $n = p$, and we'll restrict ourselves to Witt vectors with $z = 0$, so that p^k always divides z with the above theorem.

To find such a solution, we only need to consider the truncated Witt vectors $W_2(\mathbb{F}_\text{ı})$, since a Witt vector A has a pth root when the second term a_1 is 0, and this term in a sum is only determined by the 0th and 1st terms of the summands. In other words, finding $a^p + b^p = c^p$ over the p-adic numbers reduces to finding three trucated Witt vectors $A, B, C \in W_2(\mathbb{F}_p)$ such that

$A = (a_0, 0)$, $B = (b_0, 0)$, and $C = (c_0, 0)$, and $A + B = C$.

We need to choose specifically $(a_0, 0)$, $(b_0, 0)$, and p such that $(a_0, 0) + (b_0, 0) = (c_0, c_1)$ is such that $c_1 = 0$. Recalling our above definition for addition of Witt vectors, we have that $S_0(A, B) = a_0 + b_0$ and $S_1(A, B) = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0+b_0)^p}{p}$, where $A + B = (S_0(A, B), S_1(A, B), \ldots)$. We're more focused on the second equation, as we are concerned with c_1, and since our Witt vectors are truncated to length 2, we do not need any $S_i : i > 1$. Keep in mind that in this case,

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

because $a_1 = b_1 = 0$. Expanding $(a_0 + b_0)^p$ allows us to rewrite this as

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

Consider now that

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

This gives us

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

Then finding our counterexample is finding a_0, b_0, and p such that $S_1(A, B) = 0 \mod p$. One such example is $a_0 = 1, b_0 = 2, p = 7$. Checking the sum, we have that

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

$$\equiv 1 - 2 + 3 - 2 - 2 - 5 \equiv 0 \mod 7.$$

This means $(1, 0) + (2, 0) = (3, 0)$ gives a solution for $n = 7$ in $W_2(\mathbb{F}_{\text{ı}})$, since all three terms have 7th roots. Furthermore, since $129 = 1^7 + 2^7 \equiv (1, 0) + (2, 0) = (3, 0) \mod 7^2$, associating 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

[Con26] Wikipedia Contributors. Witt vector, May 2026.

[Fin07] Daniel Finkel. An overview of witt vectors, 2007.