WITT VECTORS

ABHISHEK RENGARAJAN

1. Introduction

When doing arithmetic in the p-adics, we are confronted with two major questions

- Can we remedy "holes" when doing arithmetic in the p-adics?
- Is it possible to generate a general formula for adding and multiplying p-adic numbers?

2. Some Definitions

Definition: A Witt vector is an infinite sequence of elements of a commutative ring. The reason why it relates to the p-adic integers is because one can put a ring structure on the set of Witt vectors, in such a way that the ring of Witt vectors over the finite field of order p is the ring of p-adic integers.

Definition: A Teichmüller representative is the solution to either of the following (they are both equivalent), where $\omega : \mathbb{Z}_p \to \mathbb{Z}_p$

- $\omega(x) = \lim_{n\to\infty} x^{p^n}$
- The unique solution of $\omega(x)^p = \omega(x)$ that is also congruent to $x \pmod p$.

Definition: A Teichmüller character is just the Teichmüller representative where the domain of ω is restricted to strictly $\mathbb{F}_p$.

Note: For most of our purposes, some Witt Vector will basically map to a Teichmüller representative

$$a = (a_0, a_1, a_2, \cdots) \leftrightarrow \omega(a_0) + \omega(a_1)p + \omega(a_2)p^2 + \cdots$$

3. Motivating Witt Vectors

Motivation: We know that any $\mathbb{Z}_p$ can be written as a power series $a_0 + a_1p + a_2p^2 + ...$ where $a_n \in \mathbb{F}_p$. However, the problem is that it's very difficult to add or subtract elements of $\mathbb{Z}_p$. If $a, b \in \mathbb{Z}_p$ we might think to define addition in the form

$$c_0 = a_0 + b_0 \pmod p$$

$$c_1 = a_0 + a_1p + b_0 + b_1p \pmod{p^2}$$

$$c_2 = a_0 + a_1p + a_2p^3 + b_0 + b_1p + b_2p^2 \pmod{p^3}$$

however, this formula doesn't work in every instance, for example, we can't find a $c_i = c_i^p$.

Date: June 11, 2018.

Teichmuller representatives provide a nice form to write out addition and multiplication in a closed form because of the property that

$$c_0^p \equiv (a_0 + b_0)^p \pmod{p^2}$$

After a decent amount of fairly trivial manipulations, we find that the new form of addition using Teichmuller representatives is actually of the form

$$c_0 \equiv a_0 + b_0 \pmod{p}$$
$$c_0^p + c_1 p \equiv a_0^p + a_1 p + b_0^p + b_1 p \pmod{p^2}$$
$$c_0^{p^2} + c_1^p p + c_2 p \equiv a_0^{p^2} + a_1^p p + a_2 p + b_0^{p^2} + b_1^p p + b_2 p \pmod{p^3}$$

4. Constructing a Witt Vector

Construction: We now move to the actual construction of the Witt vectors. In order to construct one over a ring R in a sequence: $(X_0, X_1, X_2, ...)$ with $X_n \in R$. We'll define a Witt polynomial by

$$W_i = \sum_i p^i X_i^{p^{n-i}}$$

This is also usually denoted as $X^{(i)}$. We can make the set of Witt Vectors themselves into a ring where two conditions need to hold:

- the sum and the product are given by polynomials with integral coefficients that do not depend on R.
- Every Witt polynomial is a homomorphism from the ring of Witt vectors over R to R.

Now we can define the addition and multiplication operations over the Witt Ring. If a Witt vector is $(X_0, X_1, X_2, ...)$ then,

- Addition between $(X_0, X_1, X_2, ...) + (Y_0, Y_1, Y_2, ...) = (X_0 + Y_0, X_1 + Y_1 + (X_0^p + Y_0^p - (X_0 + Y_0)^p), ...)$.
- $(X_0, X_1, ...) \times (Y_0, Y_1, ...) = (X_0 Y_0,\ X_0^p Y_1 + X_1 Y_0^p + p X_1 Y_1,\ \cdots)$.

To write this in closed form, we first need to introduce one piece of notation.

Definition: $\phi : (X_0, X_1, X_2, ..., Y_0, Y_1, Y_2, ...) \mapsto (X_0^p, X_1^p, X_2^p, ..., Y_0^p, Y_1^p, Y_2^p, ...)$

Now, in closed form, this means that at a given position Z_n in the tuple on the RHS, addition is defined by

$$Z_n = X_n + Y_n + \frac{\phi(X^{(n-1)} + Y^{(n-1)}) - (Z_0^{p^n} + p Z_1^{p^{n-1}} + \cdots + Z_{n-1} p^{n-1})}{p^n}$$

For multiplication,

$$Z_n = \phi(X^{(n-1)}) Y_n + \phi(Y^{(n-1)}) X_n + X_n Y_n p^n + \frac{\phi(X^{(n-1)} Y^{(n-1)}) - (Z_0^{p^n} + p Z_1^{p^{n-1}} + \cdots + Z_{n-1} p^{n-1})}{p^n}$$

5. Proving the Addition Equation

Proof: We will prove that this is the case for addition by induction, the proof for multiplication is very similar.

$$\begin{aligned} X^{(n)} &= (X_0^p)^{p^{n-1}} + (X_1^p)^{p^{n-2}}p + \cdots + (X_{n-1}^p)p^{n-1} + X_n p^n \\ &= \phi(X^{(n-1)}) + X_n p^n \end{aligned}$$

$$\phi(X^{(n-1)} + Y^{(n-1)}) = \phi(Z^{(n-1)}) = \sum_{k=0}^{n-1} \phi(Z_k)^{p^{n-1-k}} p^k$$

So now, if $Z^{(n)} = X^{(n)} + Y^{(n)}$ Because Z is a Teichmüller representative, we know that

$$\phi(X^{(n-1)} + Y^{(n-1)}) \equiv \sum_{k=0}^{n-1} \phi(Z_k)^{p^{n-k}} p^k \pmod{p^n}$$

$$Z_n \in \mathbb{Z}[X_0, X_1, X_2, \cdot, Y_0, Y_1, Y_2]$$

Euler Circle, Palo Alto, CA 94306
E-mail address: abhir518@gmail.com