ON FERMAT CURVES MODULO A FINITE NUMBER

YOCHAY JERBY

Abstract. We show that the existence of a non-trivial solution of $x^n + y^n = p^n$, with $p$ a prime number, is equivalent to the existence of a solution of a certain (over-determined) system of $(n - 1)$-recursion relations ("zipper" equations) in $\mathbb{Z}_{p-1}$.

1. Introduction

The famous Fermat’s last theorem states that the equation $x^n + y^n = z^n$ admits no positive integral solutions, if $n \geq 3$, see [1, 2] and references therein. But what happens if we ease the condition and require for points $(x, y) \in \mathbb{Z}^2$ for which $z^n$ just divides $x^n + y^n$, for some fixed $z \in \mathbb{Z}$? In general, this leads us to define the main subject of study in this work:

Definition: For $n \in \mathbb{N}$ and $j \geq 1$ let

$$T_n(z; j) := \{(x, y)|x^n + y^n \equiv 0 \pmod{z^j}\} \subset (\mathbb{Z}_{z^j})^2$$

be the $j$-th Fermat tile of radius $z$.

We think of elements of $T_n(z; n)$ as "mock solutions" of the equation $x^n + y^n = z^n$ (as clearly, a genuine solution, if exists, induces an element of $T_n(z; n)$ but not the other way around). Remarkably, not only do such "mock solutions" exist, they actually satisfy a neat algebraic structure which we describe, using Fermat’s little theorem, in section 2. From the elementary features of the plane geometry of Fermat curves, it follows that the tiles $T_n(z; n)$ satisfy the following property:

Proposition A: If $(x, y, z) \in \mathbb{Z}_+^3$ is a solution of $x^n + y^n = z^n$ then $(x, y) \in T_n(z; n) \cap [0, z]^2$.

In section 3 we study the properties of elements $(x, y) \in T_n(p; n) \cap [0, p]^2$, for $p$ a prime number, and show that such elements are subject to a substantial system of highly non-trivial restrictions. The description of these restrictions requires a study of the functions

$$Log_j : \mathbb{Z}_{p^j}^* \rightarrow \mathbb{Z}_{\phi(p^j)}^* ; \quad Exp_j : \mathbb{Z}_{\phi(p^j)} \rightarrow \mathbb{Z}_{p^j}^*$$
given by

\[ \text{Log}_j(g^s) = [s]_{\phi(p^j)} \in \mathbb{Z}_{\phi(p^j)} \quad \text{and} \quad \text{Exp}_j(s) := [g^s]_{p^j} \in \mathbb{Z}_{p^j}, \]

where \( \phi(p^j) = (p-1) \cdot p^{j-1} \) is the totient function and \( j \geq 1 \). The main feature is the definition of a natural class of functions of the form \( A^o_j : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^j-1} \to \mathbb{Z}_p \), for \( a \in \mathbb{Z}_{p-1} \).

In terms of these functions, the restrictions are given as follows:

**Theorem B** ("zipper" relations): If \((x, y) \in T_n(p; n) \cap [0, p]^2\) there exists an element \( s = s(x, y) \in \mathbb{Z}_{p-1} \) and \( a \in \mathbb{Z}_{p-1} \) which satisfy the following overdetermined double recursion ("zipper") relations

\[
\begin{align*}
    r_0 &= A_1^0(s) = A_1^1(s) \\
    r_1 &= A_2^0(s; r_0) = A_2^1(s; r_0) \\
    &\vdots \\
    r_{n-1} &= A_n^0(s; r_0, \ldots, r_{n-2}) = A_n^a(s; r_0, \ldots, r_{n-2})
\end{align*}
\]

As one can see the number of equations in the variable \( s \in \mathbb{Z}_{p-1} \) grows with \( n \) (in the Pythagorean case \( n = 2 \), there is one equation). In particular, Fermat’s last theorem would follow from showing that the zipper relations have no solutions for \( n \geq 3 \). We define and study various properties of the zipper relations in section 4.

The rest of the work is organized as follows: In section 2 we describe Fermat tiles, in section 3 we study \( \text{Log}_j \) and \( \text{Exp}_j \) and define \( A^o_j \). In section 4 we define the zipper relations.

**2. The geometric structure of Fermat tiles**

Before describing Fermat tiles in general, let us start with a few examples (which justify the term *tile*).

**Example 2.1** (\( n = 2 \)): Figure 4 shows the first Fermat tile \( T_2(5, 1) \) of radius 5.

![Figure 1. First Fermat tile \( T_2(5, 1) \) of radius 5.](image)
Figure 5 shows the second Fermat tile $T_2(5, 2)$ of radius 5.

![Figure 2. Second Fermat tile $T_2(5, 2)$ of radius 5.](image)

Note that, as expected, one has $(3, 4), (4, 3), (5, 0), (0, 5) \in T_2(5, 2) \cap [0, 5]^2$.

**Example 2.2** ($n \geq 3$): Figure 6 shows the first Fermat tile $T_4(7, 1)$ of radius 7:

![Figure 3. Second Fermat tile $T_3(7, 1)$ of radius 7.](image)

Figure 7 shows the first Fermat tile $T_4(17, 1)$ of radius 17:

![Figure 4. First Fermat tile $T_4(17, 1)$ of radius 17.](image)
We refer to
\[ C_n(z) := \{(x, y) | x^n + y^n = z^n\} \subset \mathbb{R}^2 \]
as the \(n\)-th Fermat curve of radius \(z \in \mathbb{R}\). Note that Fermat’s last theorem is equivalent to stating that \(C_n(z) \cap \mathbb{N}^2 = \{(z, 0), (0, z)\}\) for any \(n \geq 3\) and \(z \in \mathbb{N}\). Let us proceed with the following remark:

**Remark 2.3** (plane geometry of Fermat curves): Figure 5 shows \(C_2(5)\), the circle of radius \(z = 5\), with the integer lattice:

**Figure 5.** Graph of \(C_2(5)\) together with the integer lattice \(\mathbb{Z}^2\).

Recall that a solution \((x, y, z) \in \mathbb{N}^3\) of \(x^2 + y^2 = z^2\) is called a Pythagorean triple. Note that \(C_2(5) \cap \mathbb{N}^2 = \{(3, 4), (4, 3), (5, 0), (0, 5)\}\). Figure 6 shows \(C_8(5)\) with the integral lattice

**Figure 6.** Graph of \(C_8(5)\) together with the integer lattice \(\mathbb{Z}^2\).

Figure 7 shows \(C_9(10)\) with the integer lattice

**Figure 7.** Graph of \(C_9(10)\) together with the integer lattice \(\mathbb{Z}^2\).
In particular, it is easy to see that Fermat curves satisfy $C_n(z) \cap (\mathbb{R}^+)^2 \subset [0, z]^2$ for any $n \in \mathbb{N}$ and $z \in \mathbb{R}^+$.

Note that, in view the above remark, showing that $T_n(z; n) \cap [0, z]^2 = \{(0, 0), (z, 0), (0, z), (z, z)\}$ would imply Fermat’s last theorem. Let us now turn to describe the structure of the $j$-th Fermat tile, $T_n(p, j)$, for $p$ a prime number. Let us start with the following:

**Lemma 2.4:** Let $S_n(p) \subset \mathbb{Z}_p$ be the solution set of the equation $x^n + 1 \equiv 0 \pmod{p}$ and let $g \in \mathbb{Z}_p$ be a primitive generator.

(a) If $2^n | (p - 1)$ then $S_n(p) = \{g^{a_0 + im}\}_{i=0}^{n-1}$ where $a_0 := \frac{p-1}{2n}$ and $m := \frac{p-1}{n}$.

(b) If $2^n \nmid (p - 1)$ then $S_n(p) = \emptyset$.

**Proof:** As $g \in \mathbb{Z}_p$ is a primitive generator we have

$$\{g^s | s = 0, \ldots, p - 2\} \subset \mathbb{Z}_p^*$$

By Fermat’s little theorem $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Hence, we are looking for some $x = g^a$ such that

$$g^{na} \equiv g^{\frac{p-1}{2}} \pmod{p}.$$

Again, by Fermat’s little theorem, this is equivalent to solving

$$n \cdot a \equiv \frac{p-1}{2} \pmod{p - 1}.$$

The solutions are given by $a_i := a_0 + im$ for $i = 0, \ldots, n - 1$. □

Consider the following example:

**Example 2.5:** Let $n = 4$ and $p = 17$. One has $a_0 = 2, m = 4$ and $g = 3$. Hence

$$S_4(17) = \{3^2, 3^6, 3^{10}, 3^{14}\} = \{9, 15, 8, 2\} \subset \mathbb{Z}_{17},$$

which coincides with the first row of Fig. 4, as expected.

We have:

**Proposition 2.6** (reducibility): For any $1 \leq j \leq n$ the following holds:

(a) If $2n | (p - 1)$ then $T_n(p, j) = \left\{(a, ax^j) | x \in S_n(p), a \in \mathbb{Z}_p\right\} \cup (p\mathbb{Z}_{p^{j-1}})^2$. 
(b) If $2n \nmid (p - 1)$ then $T_n(p, j) = \left(p\mathbb{Z}_{p^j-1}\right)^2$.

For $x \in S_n(p), j \in \mathbb{N}$ consider the linear function $f^j_x : \mathbb{Z}_{p^j} \to \mathbb{Z}_{p^j}$ given by $a \mapsto ax^{p^j-1}$. Set

$$T(x; j) := \text{graph}(f^j_x) = \left\{(a, ax^{p^j-1}) \mid a \in \mathbb{Z}_{p^j}\right\}.$$ 

Consider the following example:

**Example 2.7:** Let $n = 4$ and $p = 17$. Figure 8 shows the graphs of $f^1_x : \mathbb{Z}_{17} \to \mathbb{Z}_{17}$ for $x = 9, 15, 8, 2$

![Figure 8](image)

**Figure 8.** Graphs of $f^1_x$ for $x = 9, 15, 8, 2$.

As one can see, Figure 8 coincides with the interior of the Fermat tile $T_4(17, 1)$, presented in Figure 7. Figure 9 presents the four linear components separately:

![Figure 9](image)

**Figure 9.** Separated graphs of $f^1_x$ for $x = 9, 15, 8, 2$.

Figure 10 shows the graphs of $f^2_x : \mathbb{Z}_{17^2} \to \mathbb{Z}_{17^2}$ for $x = 9, 15, 8, 2$

![Figure 10](image)

**Figure 10.** Graphs of $f^2_x$ for $x = 9, 15, 8, 2$. 
Figure 11 presents the four linear components separately:

Figure 11. Separated graphs of $f_x^2$ for $x = 9, 15, 8, 2$.

In view of the above, Fermat’s last theorem would thus follow from showing

$$T(x; n) \cap [0, p]^2 = \{(0, 0)\} \quad \text{for all} \quad x \in S_n(p).$$

That is, showing $f_x^n(a) > p$ for any $1 \leq a \leq p$. First, let us make the following remark:

**Remark 2.8** (empirics): $T(x; j)$, is the graph of a line of slope $x^{p^{j-1}}$ in $\mathbb{Z}_{p^j}^2$, for $x \in S_n(p)$. In practice, such a line actually traces a 2-dimensional lattice in $\mathbb{Z}_{p^j}^2$, due to the truncation caused by the quotient relation (see Fig. 11 and 13). Empirics show that, for various values of $j$ and $x$, typically, the values of $T(x; j)$ can be bounded by a line $a_2 = \frac{m_j(x) a_1}{n_j(x)} + \frac{p^j}{n_j(x)}$ with $m_j(x) < \sqrt{p^j}$. Figure 12 shows $(a, f_x^3(a))$ for $9 \in S_4(17)$ in $[0, p^2] \times [0, p^3]$ and $[0, p^2] \times [0, p^2]$, together with the bounding line $a_2 = -\frac{23}{47} a_1 + 17^3 a_1$.

Figure 12. $(a, f_x^3(a))$ in $[0, 17^2] \times [0, 17^3]$ and $[0, 17^2] \times [0, 17^2]$.

Note that, if such a line exists in general, for $j \geq 3$, it would need to go more than $p$ steps in the $a_1$-axis to go below $p$ in the $a_2$-axis and, in particular, $f_x^j(a) > p$ if $0 \leq a \leq p$. However, showing that such a line exists, in general, requires for a more solid understanding of $T(x; j) \subset \mathbb{Z}_{p^j}^2$ (the subject of the following section).

It is also interesting to note the following: set $x_i = g^{a_i} \in S_n(p)$ for $i = 0, ..., n - 1$ and denote $\theta_i^j(p, n)$ be the number of elements $0 \leq a \leq p - 1$ such that $f_x^j(a) < p$ (we want $\theta_i^j(p, n) = 0$ for all $i$). For $n = 4$ we actually have

$$
\begin{pmatrix}
\theta_1^2 & 17 & 41 & 73 & 89 & 97 & 113 & 137 & 193 & 233 & 241 & 257 & 281 & 313 & 337 & 353 & 401 \\
\theta_2^2 & 1 & 3 & 2 & 0 & 3 & 0 & 1 & 2 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
\theta_3^2 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 3 \\
\theta_4^2 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 3 \\
\theta^2 & 1 & 3 & 2 & 0 & 3 & 0 & 1 & 2 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
\sum \theta_i^j & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
$$
3. Some remarks on the arithmetics of the ring of invertibles $\mathbb{Z}_{p^j}^*$

Let $g \in \mathbb{Z}_p$ be a fixed primitive generator. It is easy to see that $g$ is a primitive generator for $\mathbb{Z}_{p^j}$ for all $j \geq 1$, as well. Recall that the ring of invertibles is given by

$$\mathbb{Z}_{p^j}^* = \{a | a \equiv 0 \pmod{p}\} \subset \mathbb{Z}_{p^j}.$$

Set $\phi(p^j) := (p-1) \cdot p^{j-1}$. Let us consider the following two functions

$$\text{Log}_j : \mathbb{Z}_{p^j}^* \to \mathbb{Z}_{\phi(p^j)}^* ; \quad \text{Exp}_j : \mathbb{Z}_{\phi(p^j)}^* \to \mathbb{Z}_{p^j}^*$$

given by $\text{Log}_j(g^s) = [s]_{\phi(p^j)} \in \mathbb{Z}_{\phi(p^j)}$ and $\text{Exp}_j(s) := [g^s]_{p^j} \in \mathbb{Z}_{p^j}$. By definition, the amobea corresponding to the linear tile $T(x; j)$ is simply given by the following affine line

$$\mathcal{A}(x; j) := \text{Log}_j(T(x; j) \cap (\mathbb{Z}_{p^j}^*)^2) = \{(s_1, s_2) | s_1 - s_2 = a_i \cdot p^{j-1}\} \subset \mathbb{Z}_{p^j}^2,$$

where $\text{Log}_1(x_i) = a_i = \frac{(1+2i)(p-1)}{2n}$, with $i = 0, \ldots, n-1$. In particular, we want to show

$$\max \{\text{Exp}_n(s), \text{Exp}_n(s + a_i \cdot p^{n-1})\} \geq p,$$

for any $s \in \mathbb{Z}_{\phi(p^n)}$ and $i = 0, \ldots, n-1$.

**Remark 3.1** (Transcendentaly of $\text{Log}_j$ and $\text{Exp}_j$): It should be noted that finding a general full explicit description of $\text{Log}_j$ and $\text{Exp}_j$ is considered a completely transcendental question. For instance, Fig. 13 is a graph of $\text{Log}_1(a) \in \mathbb{Z}_{96}$ for $a \in \mathbb{Z}_{97}$ with $g = 5$:

![Figure 13. $\text{Log}_1(a)$ for $p = 97$ and $g = 5$.](image)

Note that, by definition, $[\text{Exp}_{j+1}(s)]_{p^j} = \text{Exp}_j([s]_{\phi(p^j)})$. Hence, for any $j \geq 1$ we can define the function $g_j : \mathbb{Z}_{\phi(p^{j+1})} \to \mathbb{Z}_p$ given by

$$g_j(s) := \frac{\text{Exp}_{j+1}(s) - \text{Exp}_j([s]_{\phi(p^j)})}{p^j}.$$

Consider the formal series

$$\text{Exp}(s, T) := \text{Exp}_1([s]_{p-1}) + \sum_{i=1}^{\infty} g_j([s]_{\phi(p^{j+1})}) \cdot T^j.$$
The formal series satisfies $\text{Exp}_j(s) = [\text{Exp}(s, p)]_{p^j}$. In particular, note that
\[
\begin{align*}
\text{Exp}_j(s) & \leq p \iff g_1(s) = \ldots = g_{j-1}(s) = 0, \\
\text{Exp}_j(s + a \cdot p^{j-1}) & \leq p \iff g_1(s + a \cdot p) = \ldots = g_{j-1}(s + a \cdot p^{j-1}) = 0
\end{align*}
\]
Note that an element $r \in \mathbb{Z}_{p^j}$ can be uniquely expressed as
\[
r = r_0 + r_1 \cdot p + \ldots + r_{j-1} \cdot p^{j-1},
\]
such that $r_i \in \mathbb{Z}_p$ for any $1 \leq i \leq j - 1$. For $a \in \mathbb{Z}_{p-1}$, let $h^a_j : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^j} \to \mathbb{Z}_p$ be the function given by
\[
h^a_j(s; r_0, \ldots, r_{j-1}) := g_j(s, r_0 + r_1 \cdot p + \ldots + r_{j-1} \cdot p^{j-1} + a \cdot p^j).
\]
It is easy to see that:

**Lemma 3.2** (shift): For any $a \in \mathbb{Z}_{p-1}$ and $j \geq 1$ the following holds
\[
h^a_j(s; r_0, \ldots, r_{j-1}) = h^0_j(s + a; r_0 + a + r(s + a), \ldots, r_{j-1} + a + r(s + a)),
\]
where $r(m) = \frac{(m-[m]_{p-1})}{p-1}$.

For instance, consider the following example:

**Example 3.3** ($p = 5$ and $j = 1$): The following is a table of the values of $h^0_1(s, r)$ for $p = 5$
\[
(h^0_1(s, r))^{3,4}_{0,0} = \begin{pmatrix} 0 & 3 & 1 & 4 & 2 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 1 & 0 & 4 & 3 & 2 \end{pmatrix}.
\]
The values of $h^3_1(s_1, s_2)$ are given by
\[
(h^3_1(s, r))^{3,4}_{0,0} = \begin{pmatrix} 3 & 2 & 1 & 0 & 4 \\ 2 & 0 & 3 & 1 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 0 & 2 & 4 & 1 \end{pmatrix}
\]
Note that $(s^0, r^0) = (3, 1)$ is a point satisfying $h^0_1(s^0, r^0) = h^3_1(s^0, r^0) = 0$. Indeed,
\[
\text{Exp}_2(7) = \text{Exp}_2(3 + 1 \cdot 4) = 3 ; \quad \text{Exp}_2(2) = \text{Exp}_2([22]_{20}) = \text{Exp}_2(7 + 3 \cdot 5) = 4,
\]
which represents the Pythagorean point $(3, 4) \in C_2(5)$, as expected.

In general, for any $j \geq 1$, set
\[
Z_j(a) := \{(s, r) | h^a_k(s, r_0, \ldots, r_{k-1}) = 0 \text{ for any } k \leq j \} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^j}.
\]
Let $p$ be a prime and $2 \leq n \in \mathbb{N}$ an integer such that $2n/(p - 1)$. Set $a_i := \frac{(1 + 2i)(p-1)}{2n}$ for $i = 1, \ldots, n - 1$. Our main object of study now is $Z_{n-1}(0) \cap Z_{n-1}(a_i)$. In particular, note that according to the above, showing $Z_{n-1}(0) \cap Z_{n-1}(a_i) = \emptyset$ would imply Fermat’s last theorem. Consider, for instance, the following example:

**Example 3.4** ($p = 5$ and $j = 2$): Note from the previous example that, for $(s, r_0) = (3, 1)$, we have

$$h_1^0(3; 1) = h_1^3(3; 1) = h_1^0(6; 4) = h_1^0(1, 0) = 0.$$ 

Note also that

$$h_1^0(3, r) = [4 \cdot (r - 1)]_5; \quad h_1^0(2, r) = [2 \cdot r]_5.$$

For $j = 2$, we have

$$(h_2^0(3; r_0, r_1))^{4,4}_{0,0} = \begin{pmatrix}
0 & 4 & 3 & 2 & 1 \\
0 & 4 & 3 & 2 & 1 \\
1 & 0 & 4 & 3 & 2 \\
0 & 4 & 3 & 2 & 1 \\
1 & 0 & 4 & 3 & 2
\end{pmatrix},$$

and

$$(h_2^0(2; r_0, r_1))^{4,4}_{0,0} = \begin{pmatrix}
0 & 2 & 4 & 1 & 3 \\
2 & 4 & 1 & 3 & 0 \\
0 & 2 & 4 & 1 & 3 \\
0 & 2 & 4 & 1 & 3 \\
0 & 2 & 4 & 1 & 3
\end{pmatrix}.$$ 

As one can see, we can still express

$$h_2^0(3, r_0, r_1) = [4 \cdot (r_1 - A_2^0(3; r_0))]_5; \quad h_2^0(2, r_0, r_1) = [2 \cdot (r_1 - A_2^0(2; r_0))]_5,$$

where $A_2^0 : \mathbb{Z}_{p-1} \times \mathbb{Z}_p \to \mathbb{Z}_p$ is a non-linear function, determining the position of the zero in the $r_0$-row (see Lemma 3.5 below). In particular, note that the linear system

$$h_2^0(3; 1, r_1) = [4 \cdot r_1]_5 = 0; \quad h_2^0(2; 1, r_1) = [2 \cdot (r_1 - 4)]_5 = 0$$

has no solution. Hence $Z_1(0) \cap Z_1(3) = \{(3, 1)\}$ while $Z_2(0) \cap Z_2(3) = \emptyset$. Finally, it should be noted that the values of $Exp_1(s)$ for $s \in \mathbb{Z}_4$ are given by

$$\begin{pmatrix}
s \\
Exp_1(s)
\end{pmatrix} = \begin{pmatrix}
0 & 1 & 2 & 3 \\
1 & 2 & 4 & 3
\end{pmatrix}.$$
In particular, $h_2^0$ can be expressed in the following form

$$h_2^0(s; r_0, r_1) = \left[ \text{Exp}_1([s + 3]_4) \cdot (r_1 - A_2^0(s; r_0)) \right]_5.$$ 

In general, we have:

**Lemma 3.5:** For any $a \in \mathbb{Z}_{p-1}$ and $j \geq 1$ there exists $A_j^a : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{j-1}} \rightarrow \mathbb{Z}_p$ and $s_0 \in \mathbb{Z}_{p-1}$, such that

$$h_j^a(s; r_0, ..., r_{j-1}) = \left[ \text{Exp}_1(s + a + s_0) \cdot (r_{j-1} - A_j^a(s; r_0, ..., r_{j-2})) \right]_p.$$ 

First, note that, due to the shift property

$$A_{j}^{a}(s; r_0, ..., r_{j-2}) = A_{j}^{a}(s + a; r_0 + a + r(s + a); ...; r_{j-2} + a + r(s + a)) - (a + r(s + a)).$$

For instance, consider the following example:

**Example 3.6:** For $p = 5$ and $j = 1$ we have

$$\begin{pmatrix} s & 0 & 1 & 2 & 3 \\ A_1^0 & 0 & 0 & 0 & 1 \\ A_1^3 & 3 & 1 & 1 & 1 \end{pmatrix}.$$ 

Indeed, note that

$$A_1^3(0) = [A_1^0(3) - 3]_5 = [1 - 3]_5 = [-2]_5 = 3 ; \quad A_1^3(1) = [A_1^0(4) - (3 + r(1 + 3))]_5 = [-4]_5 = 1 .$$

The study of various properties of the functions $A_j^a$, defined in Lemma 3.5, is the subject of the next section.

4. **The double recursion (“zipper”) equations**

For any $1 \leq k \leq j$, set

$$Z_j^k(a) := \{(s, r) | h_k^a(s, r_0, ..., r_{k-1}) = 0\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^j}.$$ 

Note that

$$Z_j(a) = Z_j^1(a) \cap ... \cap Z_j^j(a).$$

By definition,

$$Z_j^k(a) = \{(s, r_0, ..., r_{k-2}, A_k^a(s; r_0, ..., r_{k-2}), r_k, ..., r_{j-1})\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^j}.$$ 

Hence, from the above description, we deduce that $(s; r_0, ..., r_{j-1}) \in Z_j(a)$ if and only if it is a solution of the following recursion relations

$$r_0 = A_1^a(s) ; \quad r_1 = A_2^a(s; r_0) ; \quad ... ; \quad r_{j-1} = A_j^a(s; r_0, ..., r_{j-2})$$
In conclusion, combining the above relations for $Z_j(0)$ and $Z_j(a)$, we get:

**Theorem 4.1** ("zipper" relations): Let $j \geq 1$. Then $(s; r_0, ..., r_{j-1}) \in Z_j(0) \cap Z_j(a)$ if and only if it is a solution of the following (overdetermined) double recursion relations

$$
\begin{cases}
    r_0 = A^0_1(s) = A^a_1(s) \\
    r_1 = A^0_2(s; r_0) = A^a_2(s; r_0) \\
    \vdots \\
    r_j = A^0_{j+1}(s; r_0, ..., r_{j-1}) = A^a_{j+1}(s; r_0, ..., r_{j-1})
\end{cases}
$$

As mentioned in section 3, showing that the zipper relations admit no solutions for $j = n-1$ would imply Fermat’s last theorem. Let us conclude this section with a few further remarks on the properties of the zipper relations.

**Remark 4.2** (the geometry of $A^a_j$): The zipper relations are given in terms of the functions $A^a_j(s; r_0, ..., r_{j-2})$ which, by definition, represent a parametrization of the zero set of the function $h^a_j(s; r_0, ..., r_{j-1})$. It is interesting to note that the dependency of $A^a_j$ on the $s$-parameter is essentially different than its dependency on the $r = (r_0, ..., r_{j-2})$ parameters. For instance, let $p = 97$, $n = 4$ and $a = (96/8) = 12$. Figure 14 shows a matrix-plot of the function $h^a_2(s_0; r_0, r_1)$ for $s_0 = \log_1(11)$ fixed.

![Figure 14. Matrix-plot for $h^a_2(s; r_0, r_1)$ for $(r_0, r_1) \in \mathbb{Z}_p^2$.](image)

In particular, it might seem that the zeros of $h^a_j(s; r_0, r_1)$ (white points) are randomly distributed in the $r$-coordinates. However, they are determined as the local minima of a one-parametric family of quadrics dominating the picture. Hopefully, we would give a more detailed description of this one parametric family of quadrics in a future work.
On the other hand, it seems that, in the $s$-coordinate, the function $A_j^q(s;r)$ inherits the chaotic behavior of $\text{Log}_i(s)$. For instance, Figure 15 is a graph of $A_i^q(s)$ for the same parameters as above:

![Graph of $A_i^q(s)$](image)

**Figure 15.** $A_i^q(s)$ for $s \in \mathbb{Z}_{96}$ with $a = 12$.

Furthermore, it is also interesting to note, for the above parameters, that the solutions of the first zipper equation are give by

$$\{s|A_i^0(s) = A_i^1(s)\} = \{\text{Log}_1(11), \text{Log}_1(22), \text{Log}_1(33)\} \subset \mathbb{Z}_{96}.$$

On the other hand, the second zipper equations for these elements are already non-zero

$$(A_2^0(\text{Log}_1(11), A_1^0(\text{Log}_1(11)) - A_2^0(\text{Log}_1(11), A_1^0(\text{Log}_1(11))) =$$

$$= (A_2^0(\text{Log}_1(22), A_1^0(\text{Log}_1(22)) - A_2^0(\text{Log}_1(22), A_1^0(\text{Log}_1(22))) =$$

$$= (A_2^0(\text{Log}_1(33), A_1^0(\text{Log}_1(33)) - A_2^0(\text{Log}_1(33), A_1^0(\text{Log}_1(33)))) = 3 \neq 0.$$

Moreover, note that the value of the second zipper equation is actually independent of the element of the solution set of $A_i^q(s) = A_i^1(s)$ chosen. This repeats itself in other cases as well.

The above remark shows that $A_j^q(s,r)$ seems to be chaotic in the $s$-parameter and non-linear in the $r$-parameter. In order to overcome this, let us note that if $(s; A_i^0(s), A_i^0(s; A_i^1(s)))$ is a solution, for instance, of the first two zipper equations it needs to satisfy

$$h_1^0 (s; A_i^0(s)) = 0 \quad ; \quad h_1^0 (s; A_i^1(s)) = 0$$

$$h_2^0 (s; A_i^0(s), A_i^0(s; A_i^1(s))) = 0 \quad ; \quad h_2^0 (s; A_i^1(s), A_i^0(s; A_i^1(s))) = 0.$$  

In view of this, let us define for $i = 1, 2$ the functions $H_i^0, H_i^1 : \mathbb{Z}_{p-1} \to \mathbb{Z}_p$ given by

$$H_i^0(s) := h_1^0 (s; A_i^0(s)) \quad ; \quad H_i^1(s) := h_1^0 (s; A_i^1(s))$$

$$H_2^0(s) := h_2^0 (s; A_i^0(s), A_i^0(s; A_i^1(s))) \quad ; \quad H_2^1(s) := h_2^0 (s; A_i^1(s), A_i^0(s; A_i^1(s))).$$

Further define $\tilde{H}_i^0, \tilde{H}_i^1 : \mathbb{Z}_p^* \to \mathbb{Z}_p$ by $\tilde{H}_i^0(t) = H_i^0(\text{Log}_1(t))$ and $\tilde{H}_i^1(t) = H_i^1(\text{Log}_1(t))$.

Remarkably, contrary to $A_i^0(s;r)$ which are chaotic as functions of $s$, the functions $\tilde{H}_i^0, \tilde{H}_i^1$
are actually quite patterned. In fact, Figure 16 shows the graphs of $\tilde{H}_1^0, \tilde{H}_1^a$ for $p = 97$ and $a = 12$:

![Figure 16. $\tilde{H}_1^0(t)$ (left) and $\tilde{H}_1^a(t)$ (right) for $t \in \mathbb{Z}_{97}^*$ with $a = 12$.](image)

Note that, as expected, $\tilde{H}_1^0(t) = \tilde{H}_1^a(t) = 0$ for $t = 11, 22, 33$. Figure 17 shows the graphs of $\tilde{H}_2^0(t), \tilde{H}_2^a(t)$:

![Figure 17. $\tilde{H}_2^0(t)$ (left) and $\tilde{H}_2^a(t)$ (right) for $t \in \mathbb{Z}_{97}^*$ with $a = 12$.](image)

As expected, one clearly sees that these four graphs have no common zero. In order to further describe $\tilde{H}_i^a$ let us introduce their derivatives. Let $F : \mathbb{Z}_p^* \to \mathbb{Z}_p$ be a function. We refer to the function $D(F) : \mathbb{Z}_p^* \to \mathbb{Z}_p$, given by $D(F)(t) := [f(t + 1) - f(t)]_p$, as the derivative of $F$. For instance, Fig. 18 shows the derivatives $D(\tilde{H}_1^0)$ and $D(\tilde{H}_1^a)$:

![Figure 18. $D(\tilde{H}_1^0(t))$ (left) and $D(\tilde{H}_1^a(t))$ (right) for $t \in \mathbb{Z}_{97}^*$ with $a = 12$.](image)

Figure 19 shows the graphs of the derivatives $D(\tilde{H}_2^0)$ and $D(\tilde{H}_2^a)$:
What we see is that the functions $\tilde{H}_i^0, \tilde{H}_i^a$ are semilinear, that is they have semi-constant first derivative. In particular, this derivative uniformly changes for $i = 1, 2$. It is now understandable to expect, that such a collection of four semi-linear curves in the plane $\mathbb{Z}_p^2$ cannot have a common solution. Showing this, in general, however, requires some further analysis.

REFERENCES

[1] I. Kleiner. From Fermat to Wiles: Fermat’s Last Theorem Becomes a Theorem. Elem. Math. 55: 19–37, 2010.

[2] A. Wiles. Modular elliptic curves and Fermat’s Last Theorem. Annals of Mathematics. 142 (3), 443–551, 1995.