Pseudorandomness of a Markoff Automorphism over $\mathbb{F}_p$

Alois Cerbu Elijah Gunther Luke Peilen

Yale University

4 August, 2016

The Markoff Equation

The Markoff Equation

Classical Markoff Equation: $x^2 + y^2 + z^2 = 3xyz$

§ 10. -

Disons encore quelques mots sur la résolution en nombres entiers et positifs de l'équation

(16a) $$x^2 + y^2 + z^2 = 3xyz$$

The Markoff Equation

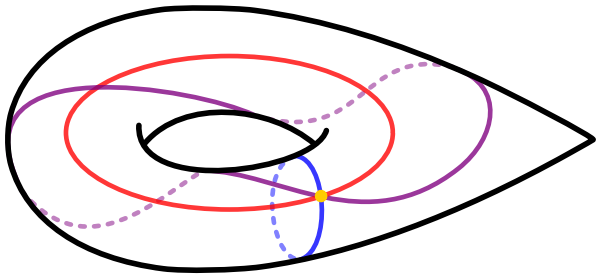
Classical Markoff Equation: $x^2 + y^2 + z^2 = 3xyz$

§ 10. -

Disons encore quelques mots sur la résolution en nombres entiers et positifs de l'équation

(16a) $$x^2 + y^2 + z^2 = 3xyz$$

Variant: $x^2 + y^2 + z^2 = xyz$



Solutions over a finite field

Solutions over a finite field

Definition

Define the *variety over* $\mathbb{F}_p$

$V(\mathbb{F}_p) = \{(x, y, z) \in (\mathbb{F}_p)^3 \mid x^2 + y^2 + z^2 = xyz\}.$

Solutions over a finite field

Definition

Define the *variety over* $\mathbb{F}_p$
$V(\mathbb{F}_p) = \{(x, y, z) \in (\mathbb{F}_p)^3 \mid x^2 + y^2 + z^2 = xyz\}$.

Remark

The size of this set is $|V(\mathbb{F}_p)| \simeq p^2$.

Solutions over a finite field

Definition

Define the *variety over* $\mathbb{F}_p$

$V(\mathbb{F}_p) = \{(x, y, z) \in (\mathbb{F}_p)^3 \mid x^2 + y^2 + z^2 = xyz\}$.

Remark

The size of this set is $|V(\mathbb{F}_p)| \simeq p^2$.

Note: We discard the "trivial" solution $(0, 0, 0)$.

Solutions over a finite field

Definition

Define the *variety over* $\mathbb{F}_p$
$V(\mathbb{F}_p) = \{(x, y, z) \in (\mathbb{F}_p)^3 \mid x^2 + y^2 + z^2 = xyz\}$.

Remark

The size of this set is $|V(\mathbb{F}_p)| \simeq p^2$.

Note: We discard the "trivial" solution $(0, 0, 0)$.

We will examine polynomial automorphisms of $V(\mathbb{F}_p)$.

Vieta Involutions

Vieta Involutions

$$(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta = 0$$

Vieta Involutions

$$(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta = 0$$

$$x^2 - (yz)x + (y^2+z^2) = 0$$

Vieta Involutions

$$(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta = 0$$

$$x^2 - (yz)x + (y^2+z^2) = 0$$

$$m_1 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} yz-x \\ y \\ z \end{pmatrix},$$

Vieta Involutions

$$(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta = 0$$

$$x^2 - (yz)x + (y^2+z^2) = 0$$

$$m_1 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} yz-x \\ y \\ z \end{pmatrix},$$

$$m_2 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x \\ xz-y \\ z \end{pmatrix}, \qquad m_3 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x \\ y \\ xy-z \end{pmatrix}$$

Even Sign Changes & S_3

Even Sign Changes & S_3

$$x^2 + y^2 + z^2 = xyz$$

$$n_1 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \\ -z \end{pmatrix}$$

Even Sign Changes & S_3

$$x^2 + y^2 + z^2 = xyz$$

$$n_1 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \\ -z \end{pmatrix}$$

$$n_2 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} -x \\ y \\ -z \end{pmatrix}$$

$$n_3 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} -x \\ -y \\ z \end{pmatrix}$$

Even Sign Changes & S_3

$$x^2 + y^2 + z^2 = xyz$$

$$n_1 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \\ -z \end{pmatrix}$$

$$n_2 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} -x \\ y \\ -z \end{pmatrix}$$

$$n_3 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} -x \\ -y \\ z \end{pmatrix}$$

$x_1 := x,\ x_2 := y,\ x_3 := z;$

$\sigma \in S_3$ acts by $x_i \mapsto x_{\sigma(i)}$.

Even Sign Changes & S_3

$$x^2 + y^2 + z^2 = xyz$$

$$n_1 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \\ -z \end{pmatrix}$$

$$n_2 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} -x \\ y \\ -z \end{pmatrix}$$

$$n_3 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} -x \\ -y \\ z \end{pmatrix}$$

$x_1 := x,\ x_2 := y,\ x_3 := z;$

$\sigma \in S_3$ acts by $x_i \mapsto x_{\sigma(i)}$.

Example

$$(1\ 3\ 2) : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \longmapsto \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix}$$

The Automorphism Group, Γ

The Automorphism Group, Γ

Theorem (Horowitz, 1975)

Vieta involutions, even sign changes, and permutations of the coordinates generate the full group Γ of polynomial automorphisms of the variety.

The Automorphism Group, Γ

Theorem (Horowitz, 1975)

Vieta involutions, even sign changes, and permutations of the coordinates generate the full group Γ of polynomial automorphisms of the variety.

Conjecture (McCullough, Wanderley, 2013)

Strong Approximation: The action of Γ on $V(\mathbb{F}_p) \setminus \{(0,0,0)\}$ is transitive for *all* primes.

The Automorphism Group, Γ

Theorem (Horowitz, 1975)

Vieta involutions, even sign changes, and permutations of the coordinates generate the full group Γ of polynomial automorphisms of the variety.

Conjecture (McCullough, Wanderley, 2013)

Strong Approximation: The action of Γ on $V(\mathbb{F}_p) \setminus \{(0,0,0)\}$ is transitive for *all* primes.

Theorem (Bourgain, Gamburd, Sarnak, 2016)

The action of Γ on $V(\mathbb{F}_p) \setminus \{(0,0,0)\}$ is transitive for **almost all** *primes (all but a small and slowly-growing exceptional set).*

Reduced Variety

Remark

$N = \langle n_1, n_2, n_3 \rangle \trianglelefteq \Gamma$

Reduced Variety

Remark

$N = \langle n_1, n_2, n_3 \rangle \trianglelefteq \Gamma$

Remark

Γ acts on $W(\mathbb{F}_p)$, the set of N-blocks.

Reduced Variety

Remark

$N = \langle n_1, n_2, n_3 \rangle \trianglelefteq \Gamma$

Remark

Γ acts on $W(\mathbb{F}_p)$, the set of N-blocks.

Definition

We denote by $H(p)$ the permutation representation of this action.

Reduced Variety

Remark

$N = \langle n_1, n_2, n_3 \rangle \trianglelefteq \Gamma$

Remark

Γ acts on $W(\mathbb{F}_p)$, the set of N-blocks.

Definition

We denote by $H(p)$ the permutation representation of this action.

The remainder of the talk concerns this series $\{H(p)\}$ of finite permutation groups.

Permutation Group, $H(p)$

Permutation Group, $H(p)$

Let $|W(\mathbb{F}_p)| = n$.

Lemma (CGP 2016)

$H(p) \leq A_n$ if and only $p \equiv 3 \pmod{16}$.

Permutation Group, $H(p)$

Let $|W(\mathbb{F}_p)| = n$.

Lemma (CGP 2016)

$H(p) \leq A_n$ *if and only* $p \equiv 3 \pmod{16}$.

Conjecture (CGP 2016)

- $H(p) \cong S_n$ for $p \not\equiv 3 \pmod{16}$
- $H(p) \cong A_n$ for $p \equiv 3 \pmod{16}$

We have checked this for primes up to 31.

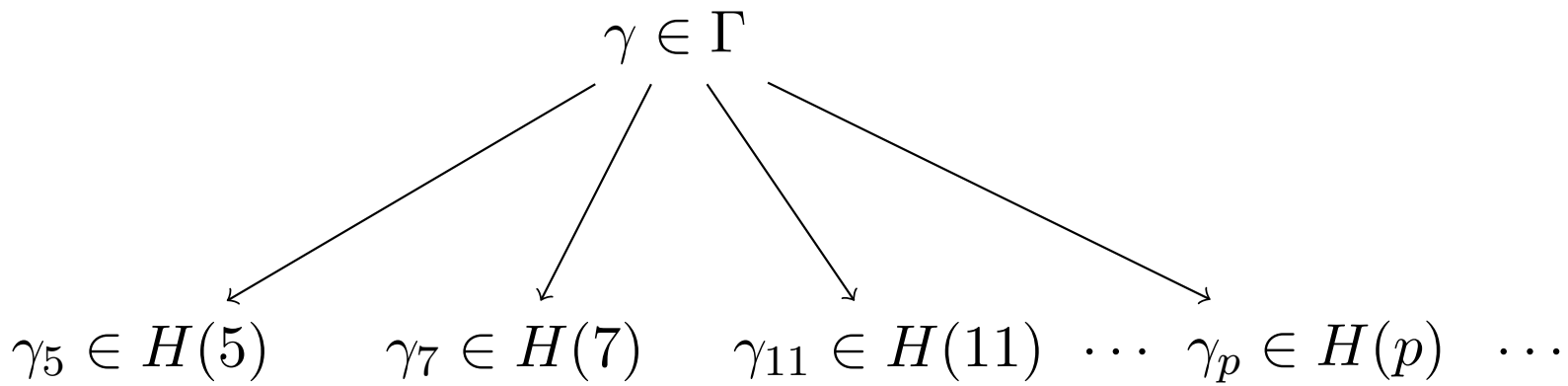
Pseudorandom Behavior

Pseudorandom Behavior

Question: Does a fixed automorphism behave pseudorandomly, modulo p?

Pseudorandom Behavior

Question: Does a fixed automorphism behave pseudorandomly, modulo p?



(Recall $H(p)$ is the permutation group generated by the action of Γ on $W(\mathbb{F}_p)$)

Nonexamples

Nonexamples

Automorphisms

m_1, n_1, $\sigma \in S_3$.

Don't change all the coordinates or entries; have low order.

Nonexamples

Automorphisms

m_1, n_1, $\sigma \in S_3$.

Don't change all the coordinates or entries; have low order.

This happens with probability zero.

Fixed Automorphism

Fixed Automorphism

We focus on one element of Γ acting on $W(\mathbb{F}_p)$:

$$\vartheta : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \overset{m_1}{\longmapsto} \begin{pmatrix} yz - x \\ y \\ z \end{pmatrix} \overset{(132)}{\longmapsto} \begin{pmatrix} y \\ z \\ yz - x \end{pmatrix}$$

Fixed Automorphism

We focus on one element of Γ acting on $W(\mathbb{F}_p)$:

$$\vartheta : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \overset{m_1}{\longmapsto} \begin{pmatrix} yz - x \\ y \\ z \end{pmatrix} \overset{(132)}{\longmapsto} \begin{pmatrix} y \\ z \\ yz - x \end{pmatrix}$$

This automorphism preserves no obvious structure.

Counting Cycles

Counting Cycles

Fact

For σ chosen uniformly at random from S_n or A_n, and $k < n$, the expected number of k-cycles in the decomposition for σ equals $1/k$.

Goal: Count the number of k-cycles in the decomposition of ϑ_p over all primes.

Counting Cycles

Fact

For σ chosen uniformly at random from S_n or A_n, and $k < n$, the expected number of k-cycles in the decomposition for σ equals $1/k$.

Goal: Count the number of k-cycles in the decomposition of ϑ_p over all primes. If $\{\vartheta_p\}$ behaves as a family of random permutations, we expect

$$\mathbb{E}_k := \lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} \#\{k\text{-cycles in } \vartheta_p\} = \frac{1}{k}$$

where $\pi(x)$ is the prime counting function.

Counting Cycles: Proven, $k \leq 5$

Counting Cycles: Proven, $k \leq 5$

Theorem (CGP 2016)

Let $\mathbb{E}_k$ be the expected number of k-cycles in the decomposition of $\vartheta_p \in W(\mathbb{F}_p)$. Then

k	1	2	3	4	5
$\mathbb{E}_k$	0	1/2	0	1/2	1/5

Counting Cycles: Proven, $k \leq 5$

Theorem (CGP 2016)

Let $\mathbb{E}_k$ be the expected number of k-cycles in the decomposition of $\vartheta_p \in W(\mathbb{F}_p)$. Then

k	1	2	3	4	5
$\mathbb{E}_k$	0	1/2	0	1/2	1/5

Proof.

Idea of proofs: For $k \leq 4$, quadratic reciprocity, polynomial manipulations, algebra. For $k = 5$, Galois Theory and Chebotarev Density Theorem. □

Long Orbits

Long Orbits

Fact

With positive probability, a random permutation $\sigma \in S_n$ has an orbit of length $\geq n/2$.

Long Orbits

Fact

With positive probability, a random permutation $\sigma \in S_n$ has an orbit of length $\geq n/2$.

If ϑ_p indeed behaves pseudorandomly, we expect its longest orbits to grow linearly with $|W(\mathbb{F}_p)| \simeq p^2$.

Lower Bound

Lower Bound

We prove a lower bound for the size of the largest orbit of the action of ϑ on $W(\mathbb{F}_p)$.

Theorem (CGP 2016)

$\forall$ primes p, $\exists$ an orbit of ϑ on $W(\mathbb{F}_p)$ of length greater than

$$N_0 = \frac{\log(p)}{\log(\varphi)} - \kappa,$$

where κ is a positive constant and $\varphi = \frac{1+\sqrt{5}}{2}$, the golden ratio.

Lower Bound

We prove a lower bound for the size of the largest orbit of the action of ϑ on $W(\mathbb{F}_p)$.

Theorem (CGP 2016)

$\forall$ primes p, $\exists$ an orbit of ϑ on $W(\mathbb{F}_p)$ of length greater than

$$N_0 = \frac{\log(p)}{\log(\varphi)} - \kappa,$$

where κ is a positive constant and $\varphi = \frac{1+\sqrt{5}}{2}$, the golden ratio.

Proof.

Idea: Combinatorial argument, and the fact that a polynomial of degree $n \geq 1$ has no more than n roots.

Acknowledgements

Acknowledgements

We'd like to thank the organizers of MathFest.

Acknowledgements

We'd like to thank the organizers of MathFest.

Special thanks to our mentor, Michael Magee, and to the other organizers of the SUMRY REU, José Gonzalez and Sam Payne.

Acknowledgements

We'd like to thank the organizers of MathFest.

Special thanks to our mentor, Michael Magee, and to the other organizers of the SUMRY REU, José Gonzalez and Sam Payne.

Thank you!

Questions