# Counting Points on Arbitrary Curves over Prime Power Rings

Caleb Robelle

Texas A&M University

July 23, 2019

# Overview

# Finite Fields, and Prime Power Rings

- Finite fields
  - $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle = \{0, 1, 2, 3, ..., p-1\}$

# Finite Fields, and Prime Power Rings

- Finite fields
  - $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle = \{0, 1, 2, 3, ..., p-1\}$
- Prime Power Rings
  - $\mathbb{Z}/\langle p^k \rangle = \{0, 1, 2, 3, ...p^k - 1\}$

# Finite Fields, and Prime Power Rings

- Finite fields
  - $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle = \{0, 1, 2, 3, ..., p-1\}$
- Prime Power Rings
  - $\mathbb{Z}/\langle p^k \rangle = \{0, 1, 2, 3, ...p^k - 1\}$

**$+$ and $\cdot$ over $\mathbb{Z}/\langle n \rangle$**

Let a and b $\in \mathbb{Z}/\langle n \rangle$

# Finite Fields, and Prime Power Rings

- Finite fields
  - $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle = \{0, 1, 2, 3, ..., p-1\}$
- Prime Power Rings
  - $\mathbb{Z}/\langle p^k \rangle = \{0, 1, 2, 3, ...p^k - 1\}$

**$+$ and $\cdot$ over $\mathbb{Z}/\langle n \rangle$**

Let a and b $\in \mathbb{Z}/\langle n \rangle$

- a $+$ b $:=$ a $+$ b mod n

# Finite Fields, and Prime Power Rings

- Finite fields
  - $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle = \{0, 1, 2, 3, ..., p-1\}$
- Prime Power Rings
  - $\mathbb{Z}/\langle p^k \rangle = \{0, 1, 2, 3, ...p^k - 1\}$

**$+$ and $\cdot$ over $\mathbb{Z}/\langle n \rangle$**

Let a and b $\in \mathbb{Z}/\langle n \rangle$

- a $+$ b $:=$ a $+$ b mod n
- a $\cdot$ b $:=$ a $\cdot$ b mod n

# Hensel's Lemma

For $f \in \mathbb{Z}[x]$ let $\tilde{f} := f \mod p$

- $\zeta \in \mathbb{F}_p$ is a degenerate root of $\tilde{f}$ if $\tilde{f}'(\zeta) = 0$

# Hensel's Lemma

For $f \in \mathbb{Z}[x]$ let $\tilde{f} := f \mod p$

- $\zeta \in \mathbb{F}_p$ is a degenerate root of $\tilde{f}$ if $\tilde{f}'(\zeta) = 0$

**Lemma**

*Suppose $k \in \mathbb{N}$, $f \in \mathbb{Z}[x]$ is not identically zero in $(\mathbb{Z}/\langle p \rangle)[x]$, and $\zeta_0 \in \mathbb{Z}/\langle p \rangle$ is a non-degenerate root of $\tilde{f} := f \bmod p$. Then there is a unique $\zeta \in \mathbb{Z}/\langle p^k \rangle$ with $\zeta_0 = \zeta \bmod p$, and $f(\zeta) = 0 \bmod p^k$.*

# Hensel's Lemma

For $f \in \mathbb{Z}[x]$ let $\tilde{f} := f \mod p$

- $\zeta \in \mathbb{F}_p$ is a degenerate root of $\tilde{f}$ if $\tilde{f}'(\zeta) = 0$

## Lemma

*Suppose $k \in \mathbb{N}$, $f \in \mathbb{Z}[x]$ is not identically zero in $(\mathbb{Z}/\langle p \rangle)[x]$, and $\zeta_0 \in \mathbb{Z}/\langle p \rangle$ is a non-degenerate root of $\tilde{f} := f \bmod p$. Then there is a unique $\zeta \in \mathbb{Z}/\langle p^k \rangle$ with $\zeta_0 = \zeta \bmod p$, and $f(\zeta) = 0 \bmod p^k$.*

## Example

Consider $f(x) = 7x^2 + 3x + 6$ over $\mathbb{Z}/\langle 2^{15} \rangle$

# Hensel's Lemma

For $f \in \mathbb{Z}[x]$ let $\tilde{f} := f$ mod p

- $\zeta \in \mathbb{F}_p$ is a degenerate root of $\tilde{f}$ if $\tilde{f}'(\zeta) = 0$

## Lemma

*Suppose $k \in \mathbb{N}$, $f \in \mathbb{Z}[x]$ is not identically zero in $(\mathbb{Z}/\langle p \rangle)[x]$, and $\zeta_0 \in \mathbb{Z}/\langle p \rangle$ is a non-degenerate root of $\tilde{f} := f$ mod p. Then there is a unique $\zeta \in \mathbb{Z}/\langle p^k \rangle$ with $\zeta_0 = \zeta$ mod p, and $f(\zeta) = 0$ mod $p^k$.*

## Example

Consider $f(x) = 7x^2 + 3x + 6$ over $\mathbb{Z}/\langle 2^{15} \rangle$

- $\tilde{f}(x) = x^2 + x$

# Hensel's Lemma

For $f \in \mathbb{Z}[x]$ let $\tilde{f} := f \mod p$

- $\zeta \in \mathbb{F}_p$ is a degenerate root of $\tilde{f}$ if $\tilde{f}'(\zeta) = 0$

**Lemma**

*Suppose $k \in \mathbb{N}$, $f \in \mathbb{Z}[x]$ is not identically zero in $(\mathbb{Z}/\langle p \rangle)[x]$, and $\zeta_0 \in \mathbb{Z}/\langle p \rangle$ is a non-degenerate root of $\tilde{f} := f \bmod p$. Then there is a unique $\zeta \in \mathbb{Z}/\langle p^k \rangle$ with $\zeta_0 = \zeta \bmod p$, and $f(\zeta) = 0 \bmod p^k$.*

**Example**

Consider $f(x) = 7x^2 + 3x + 6$ over $\mathbb{Z}/\langle 2^{15} \rangle$

- $\tilde{f}(x) = x^2 + x$
- $\tilde{f}(1) = \tilde{f}(0) = 0 \mod 2$

# Hensel's Lemma

For $f \in \mathbb{Z}[x]$ let $\tilde{f} := f \mod p$

- $\zeta \in \mathbb{F}_p$ is a degenerate root of $\tilde{f}$ if $\tilde{f}'(\zeta) = 0$

**Lemma**

*Suppose $k \in \mathbb{N}$, $f \in \mathbb{Z}[x]$ is not identically zero in $(\mathbb{Z}/\langle p \rangle)[x]$, and $\zeta_0 \in \mathbb{Z}/\langle p \rangle$ is a non-degenerate root of $\tilde{f} := f \mod p$. Then there is a unique $\zeta \in \mathbb{Z}/\langle p^k \rangle$ with $\zeta_0 = \zeta \mod p$, and $f(\zeta) = 0 \mod p^k$.*

**Example**

Consider $f(x) = 7x^2 + 3x + 6$ over $\mathbb{Z}/\langle 2^{15} \rangle$

- $\tilde{f}(x) = x^2 + x$
- $\tilde{f}(1) = \tilde{f}(0) = 0 \mod 2$
- $f(6641) = f(7402) = 0 \mod 2^{15}$

# Multivariate Hensel's Lemma

For $f \in \mathbb{Z}[x_1, ..., x_n]$ let $\tilde{f} := f$ mod p

- $\zeta \in (\mathbb{F}_p)^n$ is a degenerate root of $\tilde{f}$ iff $\frac{\partial \tilde{f}}{\partial x_i}(\zeta) = 0$ for all $i$

# Multivariate Hensel's Lemma

For $f \in \mathbb{Z}[x_1, ..., x_n]$ let $\tilde{f} := f \bmod p$

- $\zeta \in (\mathbb{F}_p)^n$ is a degenerate root of $\tilde{f}$ iff $\frac{\partial \tilde{f}}{\partial x_i}(\zeta) = 0$ for all $i$

**Hensel's Lemma**

Let $f(x) \in \mathbb{Z}\left[x_1, ..., x_n\right]$. If $f(\zeta_0) \equiv 0 \bmod p^j$ for $j \geq 1$, and ($\zeta_0$ mod p) is a non-degenerate root of $\tilde{f}$, then there are exactly $p^{n-1}$ many $t \in (\mathbb{Z}/\langle p \rangle)^n$ such that $f(\zeta_0 + tp^j) \equiv 0 \bmod p^{j+1}$.

# Multivariate Hensel's Lemma

For $f \in \mathbb{Z}[x_1, ..., x_n]$ let $\tilde{f} := f$ mod p

- $\zeta \in (\mathbb{F}_p)^n$ is a degenerate root of $\tilde{f}$ iff $\frac{\partial \tilde{f}}{\partial x_i}(\zeta) = 0$ for all $i$

## Hensel's Lemma

Let $f(x) \in \mathbb{Z}\left[x_1, ..., x_n\right]$. If $f(\zeta_0) \equiv 0 \bmod p^j$ for $j \geq 1$, and ($\zeta_0$ mod p) is a non-degenerate root of $\tilde{f}$, then there are exactly $p^{n-1}$ many $t \in (\mathbb{Z}/\langle p \rangle)^n$ such that $f(\zeta_0 + tp^j) \equiv 0 \bmod p^{j+1}$.

## Proposition

Let $f(x) \in \mathbb{Z}\left[x_1, ..., x_n\right]$. If $f(\zeta_0) \equiv 0 \bmod p^j$ for $j \geq 1$, and ($\zeta_0$ mod p) is a non-degenerate root of $\tilde{f}$, then $\zeta_0$ lifts to exactly $p^{(n-1)(k-j)}$ roots of f over $(\mathbb{Z}/\langle p^k \rangle)^n$.

# Hensel Lifting Example

- Consider $f = 13x + 10y + z$ over $(\mathbb{Z}/\langle 3^4 \rangle)^3$.

# Hensel Lifting Example

- Consider $f = 13x + 10y + z$ over $(\mathbb{Z}/\langle 3^4 \rangle)^3$.
- $\tilde{f} = x + y + z$ has 9 non-degenerate roots over $(\mathbb{Z}/\langle 3 \rangle)^3$
    - (0,0,0), (1,1,1), (2,2,2), and all permutations of (0,1,2)

# Hensel Lifting Example

- Consider $f = 13x + 10y + z$ over $(\mathbb{Z}/\langle 3^4 \rangle)^3$.
- $\tilde{f} = x + y + z$ has 9 non-degenerate roots over $(\mathbb{Z}/\langle 3 \rangle)^3$
  - (0,0,0), (1,1,1), (2,2,2), and all permutations of (0,1,2)
- Each lifts to $p^{(n-1)(k-j)}$ roots
  - p = 3, n = 3, k = 4, j = 1

# Hensel Lifting Example

- Consider $f = 13x + 10y + z$ over $(\mathbb{Z}/\langle 3^4 \rangle)^3$.
- $\tilde{f} = x + y + z$ has 9 non-degenerate roots over $(\mathbb{Z}/\langle 3 \rangle)^3$
  - (0,0,0), (1,1,1), (2,2,2), and all permutations of (0,1,2)
- Each lifts to $p^{(n-1)(k-j)}$ roots
  - p = 3, n = 3, k = 4, j = 1
- f has $9 \cdot 3^{(3-1)(4-1)} = 6561$ roots over $(\mathbb{Z}/\langle 3^4 \rangle)^3$

# Lifting Degenerate Roots

- Let $f \in \mathbb{Z}[x_1, ..., x_n]$

# Lifting Degenerate Roots

- Let $f \in \mathbb{Z}[x_1, ..., x_n]$
- For any degenerate root $\zeta_0 \in (\mathbb{F}_p)^n$ of $\tilde{f}$ define $s(f, \zeta_0) := ord_p(f(\zeta_0 + px))$

# Lifting Degenerate Roots

- Let $f \in \mathbb{Z}[x_1, ..., x_n]$
- For any degenerate root $\zeta_0 \in (\mathbb{F}_p)^n$ of $\tilde{f}$ define $s(f, \zeta_0) := ord_p(f(\zeta_0 + px))$
- Inductively define a set $T_{p,k}(f)$ of pairs $(f_{i,\zeta}, k_{i,\zeta})$ as follows:

# Lifting Degenerate Roots

- Let $f \in \mathbb{Z}[x_1, ..., x_n]$
- For any degenerate root $\zeta_0 \in (\mathbb{F}_p)^n$ of $\tilde{f}$ define $s(f, \zeta_0) := ord_p(f(\zeta_0 + px))$
- Inductively define a set $T_{p,k}(f)$ of pairs $(f_{i,\zeta}, k_{i,\zeta})$ as follows:
- Set $(f_{0,0}, k_{0,0}) := (f, k)$.

# Lifting Degenerate Roots

- Let $f \in \mathbb{Z}[x_1, ..., x_n]$
- For any degenerate root $\zeta_0 \in (\mathbb{F}_p)^n$ of $\tilde{f}$ define $s(f, \zeta_0) := ord_p(f(\zeta_0 + px))$
- Inductively define a set $T_{p,k}(f)$ of pairs $(f_{i,\zeta}, k_{i,\zeta})$ as follows:
- Set $(f_{0,0}, k_{0,0}) := (f, k)$.
- For $i \geq 1$ with $(f_{i-1,\mu}, k_{i-1,\mu}) \in T_{p,k}(f)$ and any degenerate root $\zeta_{i-1} \in (\mathbb{Z}/\langle p \rangle)^n$ of $\tilde{f}_{i-1,\mu}$ with $s_{i-1} := s(f_{i-1,\mu}, \zeta_{i-1}) \in \{2, ..., k_{i-1,\mu}\}$

# Lifting Degenerate Roots

- Let $f \in \mathbb{Z}[x_1, ..., x_n]$
- For any degenerate root $\zeta_0 \in (\mathbb{F}_p)^n$ of $\tilde{f}$ define $s(f, \zeta_0) := ord_p(f(\zeta_0 + px))$
- Inductively define a set $T_{p,k}(f)$ of pairs $(f_{i,\zeta}, k_{i,\zeta})$ as follows:
- Set $(f_{0,0}, k_{0,0}) := (f, k)$.
- For $i \geq 1$ with $(f_{i-1,\mu}, k_{i-1,\mu}) \in T_{p,k}(f)$ and any degenerate root $\zeta_{i-1} \in (\mathbb{Z}/\langle p \rangle)^n$ of $\tilde{f}_{i-1,\mu}$ with $s_{i-1} := s(f_{i-1,\mu}, \zeta_{i-1}) \in \{2, ..., k_{i-1,\mu}\}$
  - $\zeta = \mu + p^{i-1}\zeta_{i-1}$

# Lifting Degenerate Roots

- Let $f \in \mathbb{Z}[x_1, ..., x_n]$
- For any degenerate root $\zeta_0 \in (\mathbb{F}_p)^n$ of $\tilde{f}$ define $s(f, \zeta_0) := ord_p(f(\zeta_0 + px))$
- Inductively define a set $T_{p,k}(f)$ of pairs $(f_{i,\zeta}, k_{i,\zeta})$ as follows:
- Set $(f_{0,0}, k_{0,0}) := (f, k)$.
- For $i \geq 1$ with $(f_{i-1,\mu}, k_{i-1,\mu}) \in T_{p,k}(f)$ and any degenerate root $\zeta_{i-1} \in (\mathbb{Z}/\langle p \rangle)^n$ of $\tilde{f}_{i-1,\mu}$ with $s_{i-1} := s(f_{i-1,\mu}, \zeta_{i-1}) \in \{2, ..., k_{i-1,\mu}\}$
    - $\zeta = \mu + p^{i-1}\zeta_{i-1}$
    - $k_{i,\zeta} = k_{i-1,\mu} - s_{i-1}$

# Lifting Degenerate Roots

- Let $f \in \mathbb{Z}[x_1, ..., x_n]$
- For any degenerate root $\zeta_0 \in (\mathbb{F}_p)^n$ of $\tilde{f}$ define $s(f, \zeta_0) := ord_p(f(\zeta_0 + px))$
- Inductively define a set $T_{p,k}(f)$ of pairs $(f_{i,\zeta}, k_{i,\zeta})$ as follows:
- Set $(f_{0,0}, k_{0,0}) := (f, k)$.
- For $i \geq 1$ with $(f_{i-1,\mu}, k_{i-1,\mu}) \in T_{p,k}(f)$ and any degenerate root $\zeta_{i-1} \in (\mathbb{Z}/\langle p \rangle)^n$ of $\tilde{f}_{i-1,\mu}$ with $s_{i-1} := s(f_{i-1,\mu}, \zeta_{i-1}) \in \{2, ..., k_{i-1,\mu}\}$
  - $\zeta = \mu + p^{i-1}\zeta_{i-1}$
  - $k_{i,\zeta} = k_{i-1,\mu} - s_{i-1}$
  - $f_{i,\zeta}(x) := \left[\frac{1}{p^{s_{i-1}}} f_{i-1,\mu}(\zeta_{i-1} + px)\right] \bmod p^{k_{i,\zeta}}$

# Lifting Degenerate Roots

- We can associate the elements of $T_{p,k}(f)$ with a rooted directed tree

# Lifting Degenerate Roots

- We can associate the elements of $T_{p,k}(f)$ with a rooted directed tree
  - $(f_{0,0}, k_{0,0})$ is the root node

# Lifting Degenerate Roots

- We can associate the elements of $T_{p,k}(f)$ with a rooted directed tree
  - $(f_{0,0}, k_{0,0})$ is the root node
  - The non-root nodes of the tree are uniquely labeled by each $(f_{i,\zeta}, k_{i,\zeta}) \in T_{p,k}(f)$ with $i \geq 1$

# Lifting Degenerate Roots

- We can associate the elements of $T_{p,k}(f)$ with a rooted directed tree
  - $(f_{0,0}, k_{0,0})$ is the root node
  - The non-root nodes of the tree are uniquely labeled by each $(f_{i,\zeta}, k_{i,\zeta}) \in T_{p,k}(f)$ with $i \geq 1$
  - There is an edge from $(f_{j,\mu}, k_{j,\mu})$ to $(f_{i,\zeta}, k_{i,\zeta})$ if and only if $j = i - 1$, and there is degenerate root $\zeta_{i-1}$ of $\tilde{f}_{j,\mu}$ with $s(f_{j,\mu}, \zeta_{i-1}) \in \{2, ..., k_{i,\mu} - 1\}$, and $\zeta = \mu + p^{i-1}\zeta_{i-1}$

# Lifting Degenerate Roots

- Let $\zeta_0$ be a degenerate root of $\tilde{f}$

# Lifting Degenerate Roots

- Let $\zeta_0$ be a degenerate root of $\tilde{f}$
  - if $s(f, \zeta_0) = 1$ or $0$ then $\zeta_0$ does not lift

# Lifting Degenerate Roots

- Let $\zeta_0$ be a degenerate root of $\tilde{f}$
  - if $s(f, \zeta_0) = 1$ or 0 then $\zeta_0$ does not lift
  - if $s(f, \zeta_0) \geq k$ then $\zeta_0$ lifts to $p^{n(k-1)}$ roots

# Lifting Degenerate Roots

- Let $\zeta_0$ be a degenerate root of $\tilde{f}$
  - if $s(f, \zeta_0) = 1$ or 0 then $\zeta_0$ does not lift
  - if $s(f, \zeta_0) \geq k$ then $\zeta_0$ lifts to $p^{n(k-1)}$ roots
  - if $s(f, \zeta_0) \in \{2, ..., k-1\}$ then $\zeta_0$ lifts to $p^{s(f_{0,0},\zeta_0)} N_{p,k-s(f_{0,0},\zeta_0)}(f_{1,\zeta_0})$ roots

# Total Count

$$N_{p,k}(f) = p^{(k-1)(n-1)} n_{p,k}(f) + \left( \sum_{\substack{\zeta_0 \in (\mathbb{F}_p)^n \\ s(f,\zeta_0) \geq k}} p^{n(k-1)} \right) + \left( \sum_{\substack{\zeta_0 \in (\mathbb{F}_p)^n \\ s(f,\zeta_0) \in \{2,\dots,k-1\}}} p^{n(s(f,\zeta_0)-1)} N_{p,k-s(f,\zeta_0)}(f_{1,\zeta_0}) \right)$$

# Counting Example 1

How many points does $f(x, y) = 3x^2y^2 + 14xy^2 + y^2$ have over $(\mathbb{Z}/\langle 2^4 \rangle)^2$?

# Counting Example 1

How many points does $f(x, y) = 3x^2y^2 + 14xy^2 + y^2$ have over $(\mathbb{Z}/\langle 2^4 \rangle)^2$?

- $\tilde{f}(x, y) = (x-1)^2y^2$

# Counting Example 1

How many points does $f(x,y) = 3x^2y^2 + 14xy^2 + y^2$ have over $(\mathbb{Z}/\langle 2^4 \rangle)^2$?

- $\tilde{f}(x,y) = (x-1)^2y^2$
- Roots: $\{(0,0),(1,0),(1,1)\}$

# Counting Example 1

How many points does $f(x, y) = 3x^2y^2 + 14xy^2 + y^2$ have over $(\mathbb{Z}/\langle 2^4 \rangle)^2$?

- $\tilde{f}(x, y) = (x - 1)^2 y^2$
- Roots: $\{(0, 0), (1, 0), (1, 1)\}$
- $s(f, (0, 0)) = 2,\ s(f, (1, 0)) = 4,\ s(f, (1, 1)) = 2$

# Counting Example 1

How many points does $f(x,y) = 3x^2y^2 + 14xy^2 + y^2$ have over $(\mathbb{Z}/\langle 2^4 \rangle)^2$?

- $\tilde{f}(x,y) = (x-1)^2 y^2$
- Roots: $\{(0,0),(1,0),(1,1)\}$
- $s(f,(0,0)) = 2,\ s(f,(1,0)) = 4,\ s(f,(1,1)) = 2$
- (1,0) lifts to $2^{2(4-1)}$ roots over $(\mathbb{Z}/\langle 2^4 \rangle)^2$

# Counting Example 1

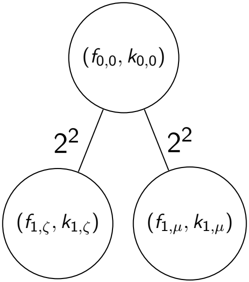
How many points does $f(x, y) = 3x^2y^2 + 14xy^2 + y^2$ have over $(\mathbb{Z}/\langle 2^4 \rangle)^2$?

- $\tilde{f}(x, y) = (x - 1)^2 y^2$
- Roots: $\{(0, 0), (1, 0), (1, 1)\}$
- $s(f, (0, 0)) = 2,\ s(f, (1, 0)) = 4,\ s(f, (1, 1)) = 2$
- (1,0) lifts to $2^{2(4-1)}$ roots over $(\mathbb{Z}/\langle 2^4 \rangle)^2$
- Construct nodes for $\zeta = \big(0, 0\big)$ and $\mu = \big(1, 1\big)$

# Counting Example 1

How many points does $f(x,y) = 3x^2y^2 + 14xy^2 + y^2$ have over $(\mathbb{Z}/\langle 2^4 \rangle)^2$?

- $\tilde{f}(x,y) = (x-1)^2y^2$
- Roots: $\{(0,0),(1,0),(1,1)\}$
- $s(f,(0,0)) = 2,\ s(f,(1,0)) = 4,\ s(f,(1,1)) = 2$
- (1,0) lifts to $2^{2(4-1)}$ roots over $(\mathbb{Z}/\langle 2^4 \rangle)^2$
- Construct nodes for $\zeta = (0,0)$ and $\mu = (1,1)$



# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

- $\tilde{f}_{1,\zeta} = x^2$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

- $\tilde{f}_{1,\zeta} = x^2$
- roots: $\{(0,0),(1,0)\}$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

- $\tilde{f}_{1,\zeta} = x^2$
- roots: $\{(0,0),(1,0)\}$
- $s(f_{1,\zeta},(0,0)) = 2$ and $s(f_{1,\zeta},(1,0)) = 2$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

- $\tilde{f}_{1,\zeta} = x^2$
- roots: $\{(0,0),(1,0)\}$
- $s(f_{1,\zeta},(0,0)) = 2$ and $s(f_{1,\zeta},(1,0)) = 2$
- Each root lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

- $\tilde{f}_{1,\zeta} = x^2$
- roots: $\{(0,0),(1,0)\}$
- $s(f_{1,\zeta},(0,0)) = 2$ and $s(f_{1,\zeta},(1,0)) = 2$
- Each root lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$

$(f_{1,\mu}, k_{1,\mu}) = (y^2, 2)$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

- $\tilde{f}_{1,\zeta} = x^2$
- roots: $\{(0,0),(1,0)\}$
- $s(f_{1,\zeta},(0,0)) = 2$ and $s(f_{1,\zeta},(1,0)) = 2$
- Each root lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$

$(f_{1,\mu}, k_{1,\mu}) = (y^2, 2)$

- $\tilde{f}_{1,\mu} = y^2$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

- $\tilde{f}_{1,\zeta} = x^2$
- roots: $\{(0,0),(1,0)\}$
- $s(f_{1,\zeta},(0,0)) = 2$ and $s(f_{1,\zeta},(1,0)) = 2$
- Each root lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$

$(f_{1,\mu}, k_{1,\mu}) = (y^2, 2)$

- $\tilde{f}_{1,\mu} = y^2$
- roots: $\{(0,0),(0,1)\}$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

- $\tilde{f}_{1,\zeta} = x^2$
- roots: $\{(0,0),(1,0)\}$
- $s(f_{1,\zeta},(0,0)) = 2$ and $s(f_{1,\zeta},(1,0)) = 2$
- Each root lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$

$(f_{1,\mu}, k_{1,\mu}) = (y^2, 2)$

- $\tilde{f}_{1,\mu} = y^2$
- roots: $\{(0,0),(0,1)\}$
- $s(f_{1,\mu},(0,0)) = 2$ and $s(f_{1,\mu},(0,1)) = 2$

# Counting Example 1 (cont)

$(f_{1,\zeta}, k_{1,\zeta}) = (x^2, 2)$

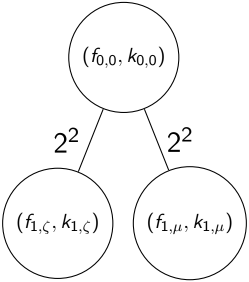
- $\tilde{f}_{1,\zeta} = x^2$
- roots: $\{(0,0),(1,0)\}$
- $s(f_{1,\zeta},(0,0)) = 2$ and $s(f_{1,\zeta},(1,0)) = 2$
- Each root lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$

$(f_{1,\mu}, k_{1,\mu}) = (y^2, 2)$

- $\tilde{f}_{1,\mu} = y^2$
- roots: $\{(0,0),(0,1)\}$
- $s(f_{1,\mu},(0,0)) = 2$ and $s(f_{1,\mu},(0,1)) = 2$
- Each root lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$

# Counting Example 1 (cont)

- Left node has 8 roots
- Right node has 8 roots
- Total count $= 64 + 2^2(8) + 2^2(8) = 128$ over $(\mathbb{Z}/\langle 2^4 \rangle)^2$



# Counting Example 2

How many points does $f(x, y) = 7x^2 + 13y^2$ have over $(\mathbb{Z}/\langle 2^2 \rangle)^2$?

# Counting Example 2

How many points does $f(x,y) = 7x^2 + 13y^2$ have over $(\mathbb{Z}/\langle 2^2 \rangle)^2$?

- $\tilde{f}(x,y) = x^2 + y^2$

# Counting Example 2

How many points does $f(x, y) = 7x^2 + 13y^2$ have over $(\mathbb{Z}/\langle 2^2 \rangle)^2$?

- $\tilde{f}(x, y) = x^2 + y^2$
- Roots: $\{(0,0),(1,1)\}$

# Counting Example 2

How many points does $f(x, y) = 7x^2 + 13y^2$ have over $(\mathbb{Z}/\langle 2^2 \rangle)^2$?

- $\tilde{f}(x, y) = x^2 + y^2$
- Roots: $\{(0,0),(1,1)\}$
- $s(f, (0, 0)) = 2$ and $s(f, (1, 1)) = 1$

# Counting Example 2

How many points does $f(x,y) = 7x^2 + 13y^2$ have over $(\mathbb{Z}/\langle 2^2 \rangle)^2$?

- $\tilde{f}(x,y) = x^2 + y^2$
- Roots: $\{(0,0),(1,1)\}$
- $s(f,(0,0)) = 2$ and $s(f,(1,1)) = 1$
- (0,0) lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$

# Counting Example 2

How many points does $f(x,y) = 7x^2 + 13y^2$ have over $(\mathbb{Z}/\langle 2^2 \rangle)^2$?

- $\tilde{f}(x,y) = x^2 + y^2$
- Roots: $\{(0,0),(1,1)\}$
- $s(f,(0,0)) = 2$ and $s(f,(1,1)) = 1$
- (0,0) lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$
- (1,1) lifts to none

# Counting Example 2

How many points does $f(x, y) = 7x^2 + 13y^2$ have over $(\mathbb{Z}/\langle 2^2 \rangle)^2$?

- $\tilde{f}(x, y) = x^2 + y^2$
- Roots: {(0,0),(1,1)}
- $s(f, (0, 0)) = 2$ and $s(f, (1, 1)) = 1$
- (0,0) lifts to $2^{2(2-1)}$ roots over $(\mathbb{Z}/\langle 2^2 \rangle)^2$
- (1,1) lifts to none

Roots of f over $(\mathbb{Z}/\langle 2^2 \rangle)^2$: {(0,0),(0,2),(2,0),(2,2)}

# Complexity

- The number of nodes in the tree is bounded by $\left\lfloor \frac{dp^{n-1}}{2} \right\rfloor \left\lfloor \frac{k-1}{2} \right\rfloor + 1$

# Complexity

- The number of nodes in the tree is bounded by $\left\lfloor \frac{dp^{n-1}}{2} \right\rfloor \left\lfloor \frac{k-1}{2} \right\rfloor + 1$
- At each node we need to count the number of points over $\mathbb{F}_p$

# Complexity

- The number of nodes in the tree is bounded by $\left\lfloor \frac{dp^{n-1}}{2} \right\rfloor \left\lfloor \frac{k-1}{2} \right\rfloor + 1$
- At each node we need to count the number of points over $\mathbb{F}_p$
- For curves (n = 2) one can attain complexity $dkp^{1+o(1)}$ if one has access to algorithms which count over $\mathbb{F}_p$ in time $(log\ p)^{O(1)}$

# Future Work

- Improve root finding for $\tilde{f}$ over $\mathbb{F}_p$

# Future Work

- Improve root finding for $\tilde{f}$ over $\mathbb{F}_p$
    - Currently using brute force

# Future Work

- Improve root finding for $\tilde{f}$ over $\mathbb{F}_p$
  - Currently using brute force
  - Should move to more recent algorithms with complexity $O(\sqrt{p})$.

# Future Work

- Improve root finding for $\tilde{f}$ over $\mathbb{F}_p$
    - Currently using brute force
    - Should move to more recent algorithms with complexity $O(\sqrt{p})$.
- Computing the intermediate $f_{i,\zeta}$ can be sped up with some interpolation tricks.

# Future Work

- Improve root finding for $\tilde{f}$ over $\mathbb{F}_p$
  - Currently using brute force
  - Should move to more recent algorithms with complexity $O(\sqrt{p})$.
- Computing the intermediate $f_{i,\zeta}$ can be sped up with some interpolation tricks.
- In one variable, [BLQ13] showed that $O(dk\ log\ p)$ is possible. Two variable case is open!

# The End