On Roots of Polynomials over Prime Fields and the Roots of Unity

Tyler Feemster

Princeton University

July 23, 2019

Definition and Directions

Beginning Goal

To determine when a non-trivial root exists over $\mathbb{F}_p$ of the polynomial

$$f(x) = \sum_{i=1}^{r} a_i x_i^{n_i},$$

where $a_i \in \mathbb{F}_p$, $x = (x_1, \ldots, x_r) \in \mathbb{F}_p^r$, and $n_i > 0$.

- The prime field $\mathbb{F}_p$ is the set of integers modulo p where addition, subtraction, multiplication, and division are well-defined via modular arithmetic.
- If $f(x) = 5 + 4x_1^2$ in $\mathbb{F}_7$, we have roots $x_1 = 2$ and $x_1 = 5$.

Definition and Directions

Beginning Goal

To determine when a non-trivial root exists over $\mathbb{F}_p$ of the polynomial

$$f(x) = \sum_{i=1}^{r} a_i x_i^{n_i},$$

where $a_i \in \mathbb{F}_p$, $x = (x_1, \ldots, x_r) \in \mathbb{F}_p^r$, and $n_i > 0$.

- The prime field $\mathbb{F}_p$ is the set of integers modulo p where addition, subtraction, multiplication, and division are well-defined via modular arithmetic.
- If $f(x) = 5 + 4x_1^2$ in $\mathbb{F}_7$, we have roots $x_1 = 2$ and $x_1 = 5$.

Definition and Directions

Beginning Goal

To determine when a non-trivial root exists over $\mathbb{F}_p$ of the polynomial

$$f(x) = \sum_{i=1}^{r} a_i x_i^{n_i},$$

where $a_i \in \mathbb{F}_p$, $x = (x_1, \ldots, x_r) \in \mathbb{F}_p^r$, and $n_i > 0$.

- The prime field $\mathbb{F}_p$ is the set of integers modulo p where addition, subtraction, multiplication, and division are well-defined via modular arithmetic.
- If $f(x) = 5 + 4x_1^2$ in $\mathbb{F}_7$, we have roots $x_1 = 2$ and $x_1 = 5$.

Chevalley-Warning Theorem and Ax's Extension

Chevalley-Warning Theorem 1935

Let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$, where $a_i \in \mathbb{F}_p$, $x = (x_1, \ldots, x_r) \in \mathbb{F}_p^r$, and $n_i > 0$. If $deg(f) < r$, then $f(x)$ has 0 (mod p) roots.

Consider $x_1^2 + x_2^2 + x_3^2 = 0$ over $\mathbb{F}_{11}$. Since $(0, 0, 0)$ is a root, there must be at least 10 more.

Ax 1964

Let b be the largest positive integer strictly less than $r/deg(f)$. Then, $f(x)$ has 0 (mod p^b) roots.

Chevalley-Warning Theorem and Ax's Extension

Chevalley-Warning Theorem 1935

Let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$, where $a_i \in \mathbb{F}_p$, $x = (x_1, \ldots, x_r) \in \mathbb{F}_p^r$, and $n_i > 0$. If $deg(f) < r$, then $f(x)$ has 0 (mod p) roots.

Consider $x_1^2 + x_2^2 + x_3^2 = 0$ over $\mathbb{F}_{11}$. Since $(0, 0, 0)$ is a root, there must be at least 10 more.

Ax 1964

Let b be the largest positive integer strictly less than $r/deg(f)$. Then, $f(x)$ has 0 (mod p^b) roots.

Chevalley-Warning Theorem and Ax's Extension

Chevalley-Warning Theorem 1935

Let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$, where $a_i \in \mathbb{F}_p$, $x = (x_1, \ldots, x_r) \in \mathbb{F}_p^r$, and $n_i > 0$. If $deg(f) < r$, then $f(x)$ has $0 \pmod{p}$ roots.

Consider $x_1^2 + x_2^2 + x_3^2 = 0$ over $\mathbb{F}_{11}$. Since $(0, 0, 0)$ is a root, there must be at least 10 more.

Ax 1964

Let b be the largest positive integer strictly less than $r/deg(f)$. Then, $f(x)$ has $0 \pmod{p^b}$ roots.

Chevalley-Warning Theorem and Ax's Extension

Chevalley-Warning Theorem 1935

Let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$, where $a_i \in \mathbb{F}_p$, $x = (x_1, \ldots, x_r) \in \mathbb{F}_p^r$, and $n_i > 0$. If $deg(f) < r$, then $f(x)$ has $0 \pmod{p}$ roots.

Consider $x_1^2 + x_2^2 + x_3^2 = 0$ over $\mathbb{F}_{11}$. Since $(0, 0, 0)$ is a root, there must be at least 10 more.

Ax 1964

Let b be the largest positive integer strictly less than $r/deg(f)$. Then, $f(x)$ has $0 \pmod{p^b}$ roots.

Condition for Guaranteed Root

Again, let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$ over $\mathbb{F}_p$.

- If there exists an n_i such that $gcd(n_i, p-1) = 1$, then there exists a non-trivial root automatically since $a_i x_i^{n_i}$ is a permutation of $\mathbb{F}_p$.
- If we consider the mapping $3x^5$ over $\mathbb{F}_7$, we obtain:

- Now, we see that $f(x) = 3x_1^5 + 4x_2^3$ has a root (7 actually).

Condition for Guaranteed Root

Again, let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$ over $\mathbb{F}_p$.

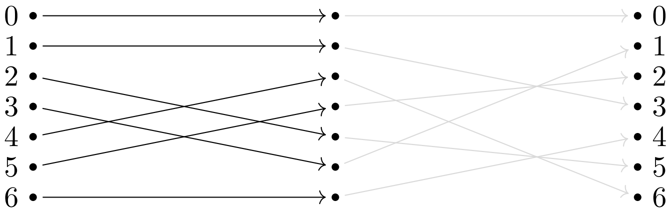
- If there exists an n_i such that $gcd(n_i, p-1) = 1$, then there exists a non-trivial root automatically since $a_i x_i^{n_i}$ is a permutation of $\mathbb{F}_p$.
- If we consider the mapping $3x^5$ over $\mathbb{F}_7$, we obtain:

- Now, we see that $f(x) = 3x_1^5 + 4x_2^3$ has a root (7 actually).

Condition for Guaranteed Root

Again, let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$ over $\mathbb{F}_p$.

- If there exists an n_i such that $gcd(n_i, p-1) = 1$, then there exists a non-trivial root automatically since $a_i x_i^{n_i}$ is a permutation of $\mathbb{F}_p$.
- If we consider the mapping $3x^5$ over $\mathbb{F}_7$, we obtain:

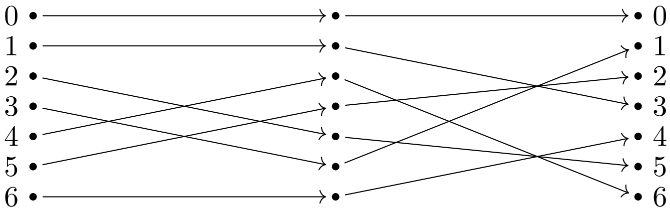


- Now, we see that $f(x) = 3x_1^5 + 4x_2^3$ has a root (7 actually).

Condition for Guaranteed Root

Again, let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$ over $\mathbb{F}_p$.

- If there exists an n_i such that $gcd(n_i, p-1) = 1$, then there exists a non-trivial root automatically since $a_i x_i^{n_i}$ is a permutation of $\mathbb{F}_p$.
- If we consider the mapping $3x^5$ over $\mathbb{F}_7$, we obtain:

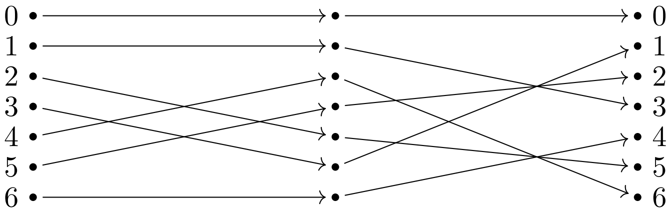


- Now, we see that $f(x) = 3x_1^5 + 4x_2^3$ has a root (7 actually).

Condition for Guaranteed Root

Again, let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$ over $\mathbb{F}_p$.

- If there exists an n_i such that $gcd(n_i, p-1) = 1$, then there exists a non-trivial root automatically since $a_i x_i^{n_i}$ is a permutation of $\mathbb{F}_p$.
- If we consider the mapping $3x^5$ over $\mathbb{F}_7$, we obtain:



- Now, we see that $f(x) = 3x_1^5 + 4x_2^3$ has a root (7 actually).

Extending the Condition for Guaranteed Root

If $gcd(n_i, p-1) = gcd(n_j, p-1) = 2$ for some n_i and n_j, then the image of $a_i x_i^{n_i} + a_j x_j^{n_j}$ is $\mathbb{F}_p$.

- The image of $a_i x_i^{n_i}$ has exactly $\frac{p-1}{2} + 1$ elements in $\mathbb{F}_p$.
  - Follows from $n_i = 2m$ where x^m permutes $\mathbb{F}_p$.
- Given $b \in \mathbb{F}_p$, the image of $b - a_j x_j^{n_j}$ has $\frac{p-1}{2} + 1$ elements.
- The images of $b - a_j x_j^{n_j}$ and $a_i x_i^{n_i}$ have union of at most p elements, but $(\frac{p-1}{2} + 1) + (\frac{p-1}{2} + 1) = p + 1$.
- So, for some x_i and x_j, $b - a_j x_j^{n_j} = a_i x_i^{n_i}$.

Extending the Condition for Guaranteed Root

If $gcd(n_i, p-1) = gcd(n_j, p-1) = 2$ for some n_i and n_j, then the image of $a_i x_i^{n_i} + a_j x_j^{n_j}$ is $\mathbb{F}_p$.

- The image of $a_i x_i^{n_i}$ has exactly $\frac{p-1}{2} + 1$ elements in $\mathbb{F}_p$.
  - Follows from $n_i = 2m$ where x^m permutes $\mathbb{F}_p$.
- Given $b \in \mathbb{F}_p$, the image of $b - a_j x_j^{n_j}$ has $\frac{p-1}{2} + 1$ elements.
- The images of $b - a_j x_j^{n_j}$ and $a_i x_i^{n_i}$ have union of at most p elements, but $(\frac{p-1}{2} + 1) + (\frac{p-1}{2} + 1) = p + 1$.
- So, for some x_i and x_j, $b - a_j x_j^{n_j} = a_i x_i^{n_i}$.

Extending the Condition for Guaranteed Root

If $gcd(n_i, p-1) = gcd(n_j, p-1) = 2$ for some n_i and n_j, then the image of $a_i x_i^{n_i} + a_j x_j^{n_j}$ is $\mathbb{F}_p$.

- The image of $a_i x_i^{n_i}$ has exactly $\frac{p-1}{2} + 1$ elements in $\mathbb{F}_p$.
  - Follows from $n_i = 2m$ where x^m permutes $\mathbb{F}_p$.
- Given $b \in \mathbb{F}_p$, the image of $b - a_j x_j^{n_j}$ has $\frac{p-1}{2} + 1$ elements.
- The images of $b - a_j x_j^{n_j}$ and $a_i x_i^{n_i}$ have union of at most p elements, but $(\frac{p-1}{2} + 1) + (\frac{p-1}{2} + 1) = p + 1$.
- So, for some x_i and x_j, $b - a_j x_j^{n_j} = a_i x_i^{n_i}$.

Extending the Condition for Guaranteed Root

If $gcd(n_i, p-1) = gcd(n_j, p-1) = 2$ for some n_i and n_j, then the image of $a_i x_i^{n_i} + a_j x_j^{n_j}$ is $\mathbb{F}_p$.

- The image of $a_i x_i^{n_i}$ has exactly $\frac{p-1}{2} + 1$ elements in $\mathbb{F}_p$.
  - Follows from $n_i = 2m$ where x^m permutes $\mathbb{F}_p$.
- Given $b \in \mathbb{F}_p$, the image of $b - a_j x_j^{n_j}$ has $\frac{p-1}{2} + 1$ elements.
- The images of $b - a_j x_j^{n_j}$ and $a_i x_i^{n_i}$ have union of at most p elements, but $(\frac{p-1}{2} + 1) + (\frac{p-1}{2} + 1) = p + 1$.
- So, for some x_i and x_j, $b - a_j x_j^{n_j} = a_i x_i^{n_i}$.

Extending the Condition for Guaranteed Root

If $gcd(n_i, p-1) = gcd(n_j, p-1) = 2$ for some n_i and n_j, then the image of $a_i x_i^{n_i} + a_j x_j^{n_j}$ is $\mathbb{F}_p$.

- The image of $a_i x_i^{n_i}$ has exactly $\frac{p-1}{2} + 1$ elements in $\mathbb{F}_p$.
  - Follows from $n_i = 2m$ where x^m permutes $\mathbb{F}_p$.
- Given $b \in \mathbb{F}_p$, the image of $b - a_j x_j^{n_j}$ has $\frac{p-1}{2} + 1$ elements.
- The images of $b - a_j x_j^{n_j}$ and $a_i x_i^{n_i}$ have union of at most p elements, but $(\frac{p-1}{2} + 1) + (\frac{p-1}{2} + 1) = p + 1$.
- So, for some x_i and x_j, $b - a_j x_j^{n_j} = a_i x_i^{n_i}$.

Extending the Condition for Guaranteed Root

If $gcd(n_i, p-1) = gcd(n_j, p-1) = 2$ for some n_i and n_j, then the image of $a_i x_i^{n_i} + a_j x_j^{n_j}$ is $\mathbb{F}_p$.

- The image of $a_i x_i^{n_i}$ has exactly $\frac{p-1}{2} + 1$ elements in $\mathbb{F}_p$.
  - Follows from $n_i = 2m$ where x^m permutes $\mathbb{F}_p$.
- Given $b \in \mathbb{F}_p$, the image of $b - a_j x_j^{n_j}$ has $\frac{p-1}{2} + 1$ elements.
- The images of $b - a_j x_j^{n_j}$ and $a_i x_i^{n_i}$ have union of at most p elements, but $(\frac{p-1}{2} + 1) + (\frac{p-1}{2} + 1) = p + 1$.
- So, for some x_i and x_j, $b - a_j x_j^{n_j} = a_i x_i^{n_i}$.

Pathological Polynomials

So, when are there no roots?

- Fermat's Little Theorem states that for any $x \in \mathbb{F}_p$, $x^{p-1} \in \{0, 1\}$, so $x^{\frac{p-1}{2}} \in \{-1, 0, 1\}$.
- Consider x^2 in $\mathbb{F}_5$:

$x_1^3 + x_2^3 - 3$ has no roots over $\mathbb{F}_7$,
$x_1^5 + x_2^5 + x_3^5 + x_4^5 - 5$ has no roots over $\mathbb{F}_{11}$, etc.

Pathological Polynomials

So, when are there no roots?

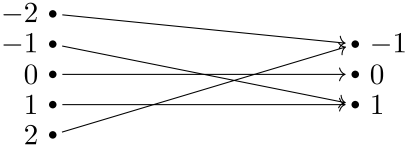
- Fermat's Little Theorem states that for any $x \in \mathbb{F}_p$, $x^{p-1} \in \{0, 1\}$, so $x^{\frac{p-1}{2}} \in \{-1, 0, 1\}$.
- Consider x^2 in $\mathbb{F}_5$:

$x_1^3 + x_2^3 - 3$ has no roots over $\mathbb{F}_7$,
$x_1^5 + x_2^5 + x_3^5 + x_4^5 - 5$ has no roots over $\mathbb{F}_{11}$, etc.

Pathological Polynomials

So, when are there no roots?

- Fermat's Little Theorem states that for any $x \in \mathbb{F}_p$, $x^{p-1} \in \{0, 1\}$, so $x^{\frac{p-1}{2}} \in \{-1, 0, 1\}$.
- Consider x^2 in $\mathbb{F}_5$:

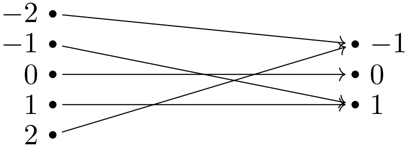


$x_1^3 + x_2^3 - 3$ has no roots over $\mathbb{F}_7$,
$x_1^5 + x_2^5 + x_3^5 + x_4^5 - 5$ has no roots over $\mathbb{F}_{11}$, etc.

Pathological Polynomials

So, when are there no roots?

- Fermat's Little Theorem states that for any $x \in \mathbb{F}_p$, $x^{p-1} \in \{0, 1\}$, so $x^{\frac{p-1}{2}} \in \{-1, 0, 1\}$.
- Consider x^2 in $\mathbb{F}_5$:

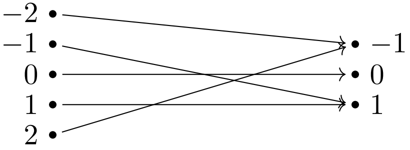


$x_1^3 + x_2^3 - 3$ has no roots over $\mathbb{F}_7$,
$x_1^5 + x_2^5 + x_3^5 + x_4^5 - 5$ has no roots over $\mathbb{F}_{11}$, etc.

Pathological Polynomials

So, when are there no roots?

- Fermat's Little Theorem states that for any $x \in \mathbb{F}_p$, $x^{p-1} \in \{0, 1\}$, so $x^{\frac{p-1}{2}} \in \{-1, 0, 1\}$.
- Consider x^2 in $\mathbb{F}_5$:



$x_1^3 + x_2^3 - 3$ has no roots over $\mathbb{F}_7$,
$x_1^5 + x_2^5 + x_3^5 + x_4^5 - 5$ has no roots over $\mathbb{F}_{11}$, etc.

Weil and his Bound

Weil 1949

Let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$, N be the number of roots of $f(x) + 1$, and $d_i = gcd(n_i, p-1)$. Then,

$$|N - p^{r-1}| \leq (d_1 - 1) \cdots (d_r - 1) p^{\frac{r-1}{2}}$$

- If $d_i = 1$ for any i, then $N = p^{r-1}$ exactly.
- If $d_i \geq 2$ for all i and $d_i = d_j = 2$ for some i and j, then since $a_i x_i^{n_i} + a_j x_j^{n_j}$ can be anything, the other $r-2$ variables are totally free and $N \simeq p^{r-1}$.

Weil and his Bound

Weil 1949

Let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$, N be the number of roots of $f(x)+1$, and $d_i = gcd(n_i, p-1)$. Then,

$$|N - p^{r-1}| \leq (d_1 - 1)\cdots(d_r - 1)p^{\frac{r-1}{2}}$$

- If $d_i = 1$ for any i, then $N = p^{r-1}$ exactly.
- If $d_i \geq 2$ for all i and $d_i = d_j = 2$ for some i and j, then since $a_i x_i^{n_i} + a_j x_j^{n_j}$ can be anything, the other $r-2$ variables are totally free and $N \simeq p^{r-1}$.

Weil and his Bound

Weil 1949

Let $f(x) = \sum_{i=1}^{r} a_i x_i^{n_i}$, N be the number of roots of $f(x)+1$, and $d_i = gcd(n_i, p-1)$. Then,

$$|N - p^{r-1}| \leq (d_1 - 1)\cdots(d_r - 1)p^{\frac{r-1}{2}}$$

- If $d_i = 1$ for any i, then $N = p^{r-1}$ exactly.
- If $d_i \geq 2$ for all i and $d_i = d_j = 2$ for some i and j, then since $a_i x_i^{n_i} + a_j x_j^{n_j}$ can be anything, the other $r-2$ variables are totally free and $N \simeq p^{r-1}$.

Univariate Polynomials and Roots of Unity

Multivariate polynomials over $\mathbb{F}_p$ are bad, but univariate polynomials over $\mathbb{F}_p$ are terrible!

- Consider $x^p - x$ over $\mathbb{F}_p$. By Fermat's Little Theorem, $x^p = x$, so every element of the field is a root.
- Also, $x^p - x + 1$ has no roots. These roots clearly do not behave well.

But, hope is not lost! Univariate Polynomials are very well-understood over the roots of unity.

Univariate Polynomials and Roots of Unity

Multivariate polynomials over $\mathbb{F}_p$ are bad, but univariate polynomials over $\mathbb{F}_p$ are terrible!

- Consider $x^p - x$ over $\mathbb{F}_p$. By Fermat's Little Theorem, $x^p = x$, so every element of the field is a root.
- Also, $x^p - x + 1$ has no roots. These roots clearly do not behave well.

But, hope is not lost! Univariate Polynomials are very well-understood over the roots of unity.

Univariate Polynomials and Roots of Unity

Multivariate polynomials over $\mathbb{F}_p$ are bad, but univariate polynomials over $\mathbb{F}_p$ are terrible!

- Consider $x^p - x$ over $\mathbb{F}_p$. By Fermat's Little Theorem, $x^p = x$, so every element of the field is a root.
- Also, $x^p - x + 1$ has no roots. These roots clearly do not behave well.

But, hope is not lost! Univariate Polynomials are very well-understood over the roots of unity.

Univariate Polynomials and Roots of Unity

Multivariate polynomials over $\mathbb{F}_p$ are bad, but univariate polynomials over $\mathbb{F}_p$ are terrible!

- Consider $x^p - x$ over $\mathbb{F}_p$. By Fermat's Little Theorem, $x^p = x$, so every element of the field is a root.
- Also, $x^p - x + 1$ has no roots. These roots clearly do not behave well.

But, hope is not lost! Univariate Polynomials are very well-understood over the roots of unity.

Univariate Polynomials and Roots of Unity

Multivariate polynomials over $\mathbb{F}_p$ are bad, but univariate polynomials over $\mathbb{F}_p$ are terrible!

- Consider $x^p - x$ over $\mathbb{F}_p$. By Fermat's Little Theorem, $x^p = x$, so every element of the field is a root.
- Also, $x^p - x + 1$ has no roots. These roots clearly do not behave well.

But, hope is not lost! Univariate Polynomials are very well-understood over the roots of unity.

Polynomials and Roots of Unity

Cheng 2007

We now have a deterministic (nonrandomized), polynomial time algorithm for deciding if the nth primitive root of unity ω_n satisfies $\sum_{i=1}^{k} c_i \omega_n^{e_i} = 0$, where $c_i \in \mathbb{Z}$.

- Previously, only randomized algorithms were known.
- He found a way to churn down lengthy polynomials with roots of unity having huge order into smaller ones and then using previously known techniques to do the rest.

Polynomials and Roots of Unity

Cheng 2007

We now have a deterministic (nonrandomized), polynomial time algorithm for deciding if the nth primitive root of unity ω_n satisfies $\sum_{i=1}^{k} c_i \omega_n^{e_i} = 0$, where $c_i \in \mathbb{Z}$.

- Previously, only randomized algorithms were known.
- He found a way to churn down lengthy polynomials with roots of unity having huge order into smaller ones and then using previously known techniques to do the rest.

Polynomials and Roots of Unity

Cheng 2007

We now have a deterministic (nonrandomized), polynomial time algorithm for deciding if the nth primitive root of unity ω_n satisfies $\sum_{i=1}^{k} c_i \omega_n^{e_i} = 0$, where $c_i \in \mathbb{Z}$.

- Previously, only randomized algorithms were known.
- He found a way to churn down lengthy polynomials with roots of unity having huge order into smaller ones and then using previously known techniques to do the rest.

The Possible Connection

Dvornicich and Zannier 2002

Essentially, roots of unity ζ_i satisfying $\sum_{i=0}^{k-1} a_i\zeta_i \equiv 0 \pmod{p}$ are no more complicated than those satisfying $\sum_{i=0}^{k-1} a_i\zeta_i = 0$, where $a_i \in \mathbb{Q}$.

- In fact, the independence of the roots of unity are bounded tightly below by essentially the same equation involving prime factors of the total order.
- Looking forward, we may be able to find and substitute portions of univariate polynomials with sums of roots of unity.

The Possible Connection

Dvornicich and Zannier 2002

Essentially, roots of unity ζ_i satisfying $\sum_{i=0}^{k-1} a_i\zeta_i \equiv 0 \pmod{p}$ are no more complicated than those satisfying $\sum_{i=0}^{k-1} a_i\zeta_i = 0$, where $a_i \in \mathbb{Q}$.

- In fact, the independence of the roots of unity are bounded tightly below by essentially the same equation involving prime factors of the total order.
- Looking forward, we may be able to find and substitute portions of univariate polynomials with sums of roots of unity.

Acknowledgements

I would like to thank Texas A&M, Dr. Maurice Rojas, Joann Coronado, Thomas Yahl, Nida Obatake, and the National Science Foundation.