- (Q1) Given a polynomial $f \in \mathbb{Z}[x]$, how many coefficients are nonzero?

- (Q1) Given a polynomial $f \in \mathbb{Z}[x]$, how many coefficients are nonzero?
- (Q2) What kind of information do they carry?

Example

Look at the polynomial $(1 + x + \cdots + x^{r-1})^n$, for $n > 0$.

- (A1) The number of nonzero coefficients is $(r-1)n + 1$ (not very interesting).

Example

Look at the polynomial $(1 + x + \cdots + x^{r-1})^n$, for $n > 0$.

- (A1) The number of nonzero coefficients is $(r-1)n+1$ (not very interesting).
- (A2)
  - The coefficient of x is the power of the polynomial.

Example

Look at the polynomial $(1 + x + \cdots + x^{r-1})^n$, for $n > 0$.

- (A1) The number of nonzero coefficients is $(r-1)n+1$ (not very interesting).
- (A2)
  - The coefficient of x is the power of the polynomial.
  - The coefficient of x^2 is the sum of the first n numbers for $r \geq 3$, and is $n(n-1)/2$ for $r = 2$.

Example

Look at the polynomial $(1 + x + \cdots + x^{r-1})^n$, for $n > 0$.

- (A1) The number of nonzero coefficients is $(r - 1)n + 1$ (not very interesting).
- (A2)
  - The coefficient of x is the power of the polynomial.
  - The coefficient of x^2 is the sum of the first n numbers for $r \geq 3$, and is $n(n - 1)/2$ for $r = 2$.
  - In general the coefficient of x^k corresponds to the number of ordered trees having $n + 1$ leaves, all at level r and $n + k + r$ edges.

What happens if we look at the same polynomial over a finite field $\mathbb{F}_p$, for p prime?

What happens if we look at the same polynomial over a finite field $\mathbb{F}_p$, for p prime?

- For $r = 2$, we have the polynomial $(1 + x)^n$. The coefficients of this polynomial mod p are well known.

What happens if we look at the same polynomial over a finite field $\mathbb{F}_p$, for p prime?

- For $r = 2$, we have the polynomial $(1 + x)^n$. The coefficients of this polynomial mod p are well known.

$$(1 + x)^n = \sum_{i=0}^{n} \binom{n}{k} x^k.$$

What happens if we look at the same polynomial over a finite field $\mathbb{F}_p$, for p prime?

- For $r = 2$, we have the polynomial $(1 + x)^n$. The coefficients of this polynomial mod p are well known.

$$(1 + x)^n = \sum_{i=0}^{n} \binom{n}{k} x^k.$$

Lucas Theorem tells us what $\binom{n}{k}$ is mod p. Caroline will discuss about it in more details.

What happens if we look at the same polynomial over a finite field $\mathbb{F}_p$, for p prime?

- For $r = 2$, we have the polynomial $(1+x)^n$. The coefficients of this polynomial mod p are well known.

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{k} x^k.$$

  Lucas Theorem tells us what $\binom{n}{k}$ is mod p. Caroline will discuss about it in more details.

- The case $r = 3$ is the one Caroline mostly dealt with.

The case $r = 3$.

For $r = 3$ we encode the coefficients of $(1 + x + x^2)^n$, for $n > 0$ in the following table:

$n = 1$	1	1	1								
$n = 2$	1	2	3	2	1						
$n = 3$	1	3	6	7	6	3	1				
$n = 4$	1	4	10	16	19	16	10	4	1		
$n = 5$	1	5	15	30	45	51	45	30	15	5	1
$\vdots$											

were the n-th row corresponds to the coefficients of $(1 + x + x^2)^n$.

If we look at the same polynomial over a finite field $\mathbb{F}_p$ our table looks completely different.

If we look at the same polynomial over a finite field $\mathbb{F}_p$ our table looks completely different.

- For example for $p = 3$ we have:

$n = 1$	1	1	1								
$n = 2$	1	-1	0	-1	1						
$n = 3$	1	0	0	1	0	0	1				
$n = 4$	1	1	1	1	1	1	1	1	1		
$n = 5$	1	-1	0	0	0	0	0	0	0	-1	1
$\vdots$											

If we look at the same polynomial over a finite field $\mathbb{F}_p$ our table looks completely different.

- For example for $p = 3$ we have:

$n = 1$	1	1	1								
$n = 2$	1	-1	0	-1	1						
$n = 3$	1	0	0	1	0	0	1				
$n = 4$	1	1	1	1	1	1	1	1	1		
$n = 5$	1	-1	0	0	0	0	0	0	0	-1	1
$\vdots$											

- The first question becomes more interesting.

Caroline will now tell us more about the number of nonzero coefficients for $r = 3$ for various p's although she will also give some results for larger r.

Polynomial Coefficients over Finite Fields

Caroline Ellison
MIT PRIMES

May 21, 2011

Problem Statement

Investigate the number of nonzero coefficients of the polynomial $(1 + x + x^2)^n$ over the finite field $\mathbb{F}_p$.

Problem Statement

Investigate the number of nonzero coefficients of the polynomial $(1 + x + x^2)^n$ over the finite field $\mathbb{F}_p$.

- The answer has already been found in the following cases:

Problem Statement

Investigate the number of nonzero coefficients of the polynomial $(1 + x + x^2)^n$ over the finite field $\mathbb{F}_p$.

- The answer has already been found in the following cases:
  - Case $p = 2$

Problem Statement

Investigate the number of nonzero coefficients of the polynomial $(1 + x + x^2)^n$ over the finite field $\mathbb{F}_p$.

- The answer has already been found in the following cases:
  - Case $p = 2$
  - Case $p = 3$, using *Lucas Theorem*.

Lucas Theorem

Theorem

Let $\sum_{i=1}^{r} a_i p^i$ *and* $\sum_{i=1}^{r} b_i p^i$ *be the base* p *expansions of* a *and* b *respectively. Then*

$$\binom{a}{b} \equiv \prod_{i=0}^{r} \binom{a_i}{b_i} \pmod{p}.$$

Notation

$$f_p(n) = \left\{ \begin{array}{c} \text{number of nonzero coefficients} \\ \text{of } (1+x+x^2)^n \pmod{p} \end{array} \right\}$$

$p = 3$

If $\sum_{i=0}^{r} a_i 3^i$ is the base 3 expansion of $2n$

$p = 3$

If $\sum_{i=0}^{r} a_i 3^i$ is the base 3 expansion of $2n$

then $f_3(n) = \prod_{i=0}^{r} (1 + a_i)$

$p = 3$

If $\sum_{i=0}^{r} a_i 3^i$ is the base 3 expansion of $2n$

then $f_3(n) = \prod_{i=0}^{r}(1 + a_i)$

Lucas Theorem applies because $(1 + x + x^2) \equiv (1 - x)^2 \pmod 3$. This result is due to R. Stanley and T. Amdeberhan.

$p = 2$

Write n as $n = \sum_{i=1}^{r} 2^{j_i}(2^{k_i} - 1)$, i.e. splits binary expansion of n into maximal strings of 1's.

$p = 2$

Write n as $n = \sum_{i=1}^{r} 2^{j_i}(2^{k_i} - 1)$, i.e. splits binary expansion of n into maximal strings of 1's. For instance

$$\begin{aligned} 54 &= 2 + 2^2 + 2^4 + 2^5 \\ &= \underline{11}0\underline{11}0_2 \\ &= 2(2^2 - 1) + 2^4(2^2 - 1) \end{aligned}$$

$p = 2$

Write n as $n = \sum_{i=1}^{r} 2^{j_i}(2^{k_i} - 1)$, i.e. splits binary expansion of n into maximal strings of 1's. For instance

$$\begin{aligned} 54 &= 2 + 2^2 + 2^4 + 2^5 \\ &= \underline{11}0\underline{11}0_2 \\ &= 2(2^2 - 1) + 2^4(2^2 - 1) \end{aligned}$$

$$f_2(2^k - 1) = \begin{cases} \frac{2^{k+2}+1}{3} & k \text{ odd} \\ \frac{2^{k+2}-1}{3} & k \text{ even} \end{cases}$$

and $f_2(n) = \prod_{i=1}^{r} f_2(2^{k_i} - 1)$
This result is due to R. Stanley.

Results

1. generalized the $p = 3$ case to all p with the polynomial $(1 + x + \ldots + x^{p-1})^n$

Results

1. generalized the $p = 3$ case to all p with the polynomial $(1 + x + \ldots + x^{p-1})^n$
2. found a formula that works for some particular digits in the expression of n in base p

Results

1. generalized the $p = 3$ case to all p with the polynomial $(1 + x + \ldots + x^{p-1})^n$
2. found a formula that works for some particular digits in the expression of n in base p
3. found answer for all p for selected values of n

Results

1. generalized the $p = 3$ case to all p with the polynomial $(1 + x + \ldots + x^{p-1})^n$
2. found a formula that works for some particular digits in the expression of n in base p
3. found answer for all p for selected values of n
4. found expressions for coefficients when $1 + x + x^2$ is reducible mod p

1. Generalization to $f(x) = (1 + x + \ldots + x^{p-1})^n$

The generalization of $p = 3$ to every p uses Lucas Theorem. We were able to use it because $(1 + x + \ldots + x^{p-1}) \equiv (1 - x)^{p-1} \pmod{p}$.

1. Generalization to $f(x) = (1 + x + \ldots + x^{p-1})^n$

The generalization of $p = 3$ to every p uses Lucas Theorem. We were able to use it because $(1 + x + \ldots + x^{p-1}) \equiv (1 - x)^{p-1} \pmod{p}$.

Proposition

If $\sum_{i=0}^{r} a_i p^i$ is the base p expansion of $np - n$ then $f_p(n) = \prod_{i=0}^{r} (1 + a_i)$.

2. $p = 5$

$n = \sum_{i=0}^{r} a_i 5^i$ is the base 5 expansion of n

2. $p = 5$

$n = \sum_{i=0}^{r} a_i 5^i$ is the base 5 expansion of n

$$\begin{aligned} (1+x+x^2)^n &= (1+x+x^2)^{\sum_{i=0}^{r} a_i 5^i} \\ &\equiv \prod_{i=0}^{r} (1+x^{5^i}+x^{2\cdot 5^i})^{a_i} \pmod 5 \end{aligned}$$

2. $p = 5$

$n = \sum_{i=0}^{r} a_i 5^i$ is the base 5 expansion of n

$$\begin{aligned} (1+x+x^2)^n &= (1+x+x^2)^{\sum_{i=0}^{r} a_i 5^i} \\ &\equiv \prod_{i=0}^{r} (1+x^{5^i}+x^{2 \cdot 5^i})^{a_i} \pmod 5 \end{aligned}$$

would be nice to have $f_5(n) = \prod_{i=0}^{r} f_5(a_i)$

2. $p = 5$

$n = \sum_{i=0}^{r} a_i 5^i$ is the base 5 expansion of n

$$\begin{aligned}(1+x+x^2)^n &= (1+x+x^2)^{\sum_{i=0}^{r} a_i 5^i} \\ &\equiv \prod_{i=0}^{r} (1+x^{5^i}+x^{2\cdot 5^i})^{a_i} \pmod{5}\end{aligned}$$

would be nice to have $f_5(n) = \prod_{i=0}^{r} f_5(a_i)$
NOT TRUE

2. $p = 5$

$n = \sum_{i=0}^{r} a_i 5^i$ is the base 5 expansion of n

$$\begin{aligned} (1+x+x^2)^n &= (1+x+x^2)^{\sum_{i=0}^{r} a_i 5^i} \\ &\equiv \prod_{i=0}^{r} (1+x^{5^i}+x^{2\cdot 5^i})^{a_i} \pmod 5 \end{aligned}$$

would be nice to have $f_5(n) = \prod_{i=0}^{r} f_5(a_i)$
NOT TRUE

It is true if $a_i \in \{0,1,2\}$. In general we have the following:

Proposition

If $n = \sum_{i=0}^{r} a_i p^i$ *is the base* p *expansion of* n, *and if* $a_i \in \{0, 1, \ldots, \frac{p-1}{2}\}$, *then*

$$f_p(n) = \prod_{i=0}^{r} f_p(a_i).$$

3. $n = p^k - 1$

coefficients of $(1 + x + x^2)^{p^k - 1}$ in $\mathbb{F}_p$ alternate in the following way:

3. $n = p^k - 1$

coefficients of $(1 + x + x^2)^{p^k - 1}$ in $\mathbb{F}_p$ alternate in the following way:

$$1, -1, 0, 1, -1, 0, 1, -1, 0, 1, -1, 0 \ldots$$

3. $n = p^k - 1$

coefficients of $(1 + x + x^2)^{p^k - 1}$ in $\mathbb{F}_p$ alternate in the following way:

$$1, -1, 0, 1, -1, 0, 1, -1, 0, 1, -1, 0 \ldots$$

$$f_p(p^k - 1) = \begin{cases} \frac{4p^k - 1}{3} & p^k \equiv 1 \pmod{3} \\ \frac{4p^k + 1}{3} & p^k \equiv 2 \pmod{3} \end{cases}$$

3. $n = p^k - 1$

coefficients of $(1 + x + x^2)^{p^k - 1}$ in $\mathbb{F}_p$ alternate in the following way:

$$1, -1, 0, 1, -1, 0, 1, -1, 0, 1, -1, 0 \dots$$

$$f_p(p^k - 1) = \begin{cases} \frac{4p^k - 1}{3} & p^k \equiv 1 \pmod 3 \\ \frac{4p^k + 1}{3} & p^k \equiv 2 \pmod 3 \end{cases}$$

We found the coefficients by starting at $n = p^k$ and working backwards by dividing.

3. More Special Cases

3. More Special Cases

- if $n = p^k - 2$, then $f(n) = 2p^k - 2p^{k-1} - 1$ ($p \equiv 1 \pmod 3$ or k odd) or $2p^k - 2p^{k-1} + 1$ ($p \equiv 2 \pmod 3$ and k even)

3. More Special Cases

- if $n = p^k - 2$, then $f(n) = 2p^k - 2p^{k-1} - 1$ ($p \equiv 1 \pmod 3$ or k odd) or $2p^k - 2p^{k-1} + 1$ ($p \equiv 2 \pmod 3$ and k even)
- if $n = p^k - 3$, then $f(n) = \frac{1}{3}(6p^k - 10p^{k-1} - 5)$ ($p \equiv 1 \pmod 3$ or k odd) or $\frac{1}{3}(6p^k - 10p^{k-1} + 5)$ ($p \equiv 2 \pmod 3$ and k even)

3. More Special Cases

- if $n = p^k - 2$, then $f(n) = 2p^k - 2p^{k-1} - 1$ ($p \equiv 1 \pmod 3$ or k odd) or $2p^k - 2p^{k-1} + 1$ ($p \equiv 2 \pmod 3$ and k even)
- if $n = p^k - 3$, then $f(n) = \frac{1}{3}(6p^k - 10p^{k-1} - 5)$ ($p \equiv 1 \pmod 3$ or k odd) or $\frac{1}{3}(6p^k - 10p^{k-1} + 5)$ ($p \equiv 2 \pmod 3$ and k even)
- if $n = p^k - 4$, then $f(n) = 2p^k - 6p^{k-1} - 2$ ($p \equiv 1 \pmod 3$), $2p^k - 6p^{k-1} + 1$ ($p \equiv 2 \pmod 3$ and k even), or $2p^k - 6p^{k-1} - 1$ ($p \equiv 2 \pmod 3$ and k odd)

4. $p \equiv 1 \pmod 3$

Fact: The polynomial $(1 + x + x^2)$ is reducible in $\mathbb{F}_p$ iff $p \equiv 1 \pmod 3$.

4. $p \equiv 1 \pmod 3$

Fact: The polynomial $(1 + x + x^2)$ is reducible in $\mathbb{F}_p$ iff $p \equiv 1 \pmod 3$. For example

$$(1 + x + x^2) \equiv (x - 2)(x - 4) \pmod 7$$

4. $p \equiv 1 \pmod 3$

Fact: The polynomial $(1 + x + x^2)$ is reducible in $\mathbb{F}_p$ iff $p \equiv 1 \pmod 3$. For example

$$(1 + x + x^2) \equiv (x - 2)(x - 4) \pmod 7$$

Proposition

Let a be a root of the polynomial $(1 + x + x^2)^n$, then for $d < n$,

$$a_d = (-1)^d \sum_{k=0}^{d} \binom{n}{k} \binom{n}{d-k} a^{2d-k},$$

where a_d is the coefficient of x^d.

Further Research

Further Research

- using findings for specific cases of n, solve $p = 5$ case

Further Research

- using findings for specific cases of n, solve $p = 5$ case
- investigate expressions for coefficients in reducible cases

Further Research

- using findings for specific cases of n, solve $p = 5$ case
- investigate expressions for coefficients in reducible cases

$$(-1)^{3d+1} \sum_{k=0}^{3d+1} \binom{n}{k} \binom{n}{3d+1-k} 2^{2-k} \equiv 1 \pmod{7}$$

Acknowledgments

My mentor, Giorgia Fortuna, for her insight, hard work, and patience.

Professor Richard P. Stanley for suggesting this problem.

The PRIMES program for providing me with this experience.

My family, for their love and support.