EE/Ma 127a
February 18, 2007
Copyright © 2007 by R. J. McEliece

Introduction to Finite Fields

Évariste Galois, 1811-1832
Outline

- What is a field?
- The rational numbers, $\mathbb{Q}$.
- The prime fields, $GF(p)$.
- Euclid’s algorithm for integers.
- Making $V_m(F)$ into a field.
- Euclid’s algorithm for polynomials.
What is an Abelian Group?

• A group is a triple \((G, +, 0)\):

  • \(a + (b + c) = (a + b) + c\).
  
  • \(a + b = b + a\).

  • \(a + 0 = 0 + a = a\).

  • \(a + x = b\) has a unique solution for all \(a, b\).
What is a Field?

- A set $F$ with two binary operations “+” and “×” such that
  - $(F, +, 0)$ is an Abelian group.
  - $(F \setminus \{0\}, \times, 1)$ is an Abelian group.
  - The Distributive Law: $ab + ac = a(b + c)$. 
Infinite Examples

- Real Numbers
- Rational numbers
- Complex Numbers
- $p$-adic field
- Algebraic number fields
Finite Examples

• $\mathbb{Z}_p$ for $p = 2, 3, 5, 7, 11, \ldots$

\[
GF(4) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}
\]

$GF(8) = ??$
Classical Euclidean Algorithm (Integers)

\[ r_{-1} := a; \quad r_0 := b; \]
\[ i := 0 \]
\[ \text{while } r_i \neq 0 \]
\[ r_{i+1} := r_{i-1} \mod r_i \]
\[ i := i + 1 \]
\[ n := i - 1 \]

**Theorem.** When the algorithm terminates, \( r_n \) is the gcd of \( a \) and \( b \), and \( n \) divisions were required.
The Division Algorithm for Polynomials

- Notation: $F[x]$: the polynomials in $x$ with coefficients from the field $F$

- Given $f(x)$ and $g(x) \neq 0$, both from $F[x]$, there exists a unique pair $q(x)$ and $r(x)$:

$$f(x) = q(x)g(x) + r(x)$$
$$\deg r(x) < \deg g(x) \quad \text{(or } r(x) \equiv 0).$$

- We summarize this by writing

$$f(x) \div g(x) = q(x) \; R \; r(x).$$
**Example**

- Example: $F = GF(2)$, $f(x) = x^t$, $g(x) = x^4 + x + 1$:

<table>
<thead>
<tr>
<th>$t$</th>
<th>$q(x)$</th>
<th>$r(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>$x$</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>$x^2$</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>$x^3$</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>$x + 1$</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>$x^2 + x$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Classical Euclidean Algorithm
(Polynomials over $F$)

$$r_{-1}(x) := a(x); \quad r_0 := b(x);$$

$i := 0$

while $r_i(x) \neq 0$

$$r_{i+1}(x) := r_{i-1}(x) \mod r_i(x)$$

$i := i + 1$

$n := i - 1$

**Theorem.** When the algorithm terminates, $r_n(x)$ is the gcd of $a(x)$ and $b(x)$, and $n$ divisions were executed.
Proof of Correctness (Integers)

Lemma. \( \gcd(m, n) = \gcd(n, m - kn) \).

Proof: (1) If \( d|m \) and \( d|n \), then \( d|m - kn \). (2) If \( d|n \) and \( d|m - kn \), then \( d|m = (m - kn) + kn \). Thus the set of common divisors of \( m \) and \( n \) is the same as the set of divisors of \( n \) and \( m - kn \).

Corollary. \( \gcd(r_{i-1}, r_i) = \gcd(r_i, r_{i+1}) \), for \( i = 0, 1, \ldots, n \).

Proof: \( r_{i-1} = q_{i+1}r_i + r_{i+1} \), or rather \( r_{i+1} = r_{i-1} - q_{i+1}r_i \).
Extended Euclidean Algorithm ( $F[x]$ )

\[ r_{-1}(x) := a(x); \quad r_0(x) := b(x); \]

\[ u_{-1}(x) := 1; \quad u_0(x) := -0 \]

\[ v_{-1}(x) := -0; \quad v_0(x) := 1 \]

\[ i := 0 \]

while \( r_i(x) \neq 0 \)

\[ q_{i+1}(x) R r_{i+1}(x) := r_{i-1}(x) \div r_i(x) \]

\[ u_{i+1}(x) := u_{i-1}(x) - q_{i+1}(x)u_i(x) \]

\[ v_{i+1}(x) := v_{i-1}(x) - q_{i+1}(x)v_i(x) \]

\[ i := i + 1 \]

\[ n := i - 1 \]
Example: $GF(2)[x]$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$u_i$</th>
<th>$v_i$</th>
<th>$r_i$</th>
<th>$q_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-1$</td>
<td>1</td>
<td>0</td>
<td>$x^4 + x + 1$</td>
<td>$-$</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$x^3 + x^2 + 1$</td>
<td>$-$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>$x + 1$</td>
<td>$x^2$</td>
<td>$x + 1$</td>
</tr>
<tr>
<td>2</td>
<td>$x + 1$</td>
<td>$x^2$</td>
<td>1</td>
<td>$x + 1$</td>
</tr>
</tbody>
</table>
What the EEA Accomplishes

**Theorem.** When the EEA terminates,

\[ u_n(x)a(x) + v_n(x)b(x) = r_n(x), \]

where \( d(x) = \gcd(a(x), b(x)) \).

**Corollary.** \( F[x] \mod p(x) \) is a field, if \( p(x) \) is irreducible.
**Example:** \( a = 222, \ b = 211 \)

<table>
<thead>
<tr>
<th>( u[I] )</th>
<th>( v[I] )</th>
<th>( r[I] )</th>
<th>( q[I] )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>223</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>-17</td>
<td>18</td>
<td>7</td>
<td>17</td>
</tr>
<tr>
<td>18</td>
<td>-19</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>-35</td>
<td>37</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>88</td>
<td>-93</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>-211</td>
<td>223</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>
**$GF(2)[x]$-Example:** \( a(x) = x^4 + x + 1, \)
\( b(x) = x^3 + x^2 + 1 \)

<table>
<thead>
<tr>
<th>(i)</th>
<th>(s_i)</th>
<th>(t_i)</th>
<th>(r_i)</th>
<th>(q_i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>(x^4 + x + 1)</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>(x^3 + x^2 + 1)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>(x + 1)</td>
<td>(x^2)</td>
<td>(x + 1)</td>
</tr>
<tr>
<td>2</td>
<td>(x + 1)</td>
<td>(x^2)</td>
<td>1</td>
<td>(x + 1)</td>
</tr>
</tbody>
</table>
Additional Properties of Euclid’s Algorithm: Integers

\[|u_i| = (-1)^{i+1}u_i\]
\[|v_i| = (-1)^i v_i\]
\[|u_{i+1}| = q_{i+1} |u_i| + |u_{i-1}|\]
\[|v_{i+1}| = q_{i+1} |v_i| + |v_{i-1}|\]

\[|v_i| r_{i-1} + |v_{i-1}| r_i = a\]
\[|u_i| r_{i-1} + |u_{i-1}| r_i = b\]

(1) \[|u_i| |v_{i-1}| - |u_{i-1}| |v_i| = (-1)^{i+1}\]

(2) \[u_ia + v_ib = r_i\]
Additional Properties of Euclid’s Algorithm — Polynomials

\[ v_i r_{i-1} + v_{i-1} r_i = a \]
\[ u_i r_{i-1} + u_{i-1} r_i = b \]
\[ u_i v_{i-1} - u_{i-1} v_i = (-1)^{i+1} \]
\[ u_i a - v_i b = (-1)^{i+1} r_i \]
\[ \text{deg } v_i + \text{deg } r_{i-1} = \text{deg } a \]
\[ \text{deg } u_i + \text{deg } r_{i-1} = \text{deg } b \]
Approximating Rationals with Rationals with Euclid’s Algorithm

\[
\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_n + \frac{1}{q_{n+1}}}}}}
\]
Approximating Rationals with Rationals with Euclid’s Algorithm

Let

\[ x = \frac{a}{b} \]

be a positive rational number, with \( \gcd(a, b) = 1 \). If we execute the EEA with inputs \( a \) and \( b \), the sequence of rational numbers

\[ x_i := \frac{|v_i|}{|u_i|}, \quad i = -1, \ldots, n + 1, \]

are called the convergents to \( x \).
Approximating Rationals with Rationals

Indeed, if we define the error term

\( E_i := x - x_i, \) for \( i = 1, \ldots, n + 1, \)

it can be shown that

\( E_i = \frac{r_i}{bu_i} \) for \( i = 1, \ldots, n + 1, \)

so that the errors \( E_i \) alternate in sign and decrease in absolute value, until \( E_{n+1} = 0. \) Also, by (1),

\[
|E_i| + |E_{i+1}| = |x_i - x_{i+1}| = \frac{1}{|u_i||u_{i+1}|} < \frac{1}{q_{i+1}|u_i|^2}
\]
Finally, if
\[ |x - x'| < |E_i|, \]
then \( x' \notin Q_{u_{i+1}} \).
**Inverses in** \( F[x] \mod p(x) \).

- **Assume** \( p(x) \) is irreducible, \( \deg p(x) = m \).

- **Problem:** Given \( a(x) \neq 0, \deg a(x) < m \), find \( b(x) \) so that

\[
a(x)b(x) \equiv 1 \pmod{p(x)}
\]

or what is the same thing, a \( b(x) \) and a \( q(x) \) so that

\[
a(x)b(x) + p(x)q(x) = 1.
\]

- But \( \gcd(a(x), p(x)) = 1 \) is guaranteed, if \( p(x) \) is irreducible. So the EEA will do the trick.
Example

- Example: What is $D^{-1}$? ($D = 1101 = x^3 + x^2 + 1$)

<table>
<thead>
<tr>
<th>$i$</th>
<th>$s_i$</th>
<th>$t_i$</th>
<th>$r_i$</th>
<th>$q_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-1$</td>
<td>1</td>
<td>0</td>
<td>$x^4 + x + 1$</td>
<td>---</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$x^3 + x^2 + 1$</td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>$x+1$</td>
<td>$x^2$</td>
<td>$x+1$</td>
</tr>
<tr>
<td>2</td>
<td>$x+1$</td>
<td>$x^2$</td>
<td>1</td>
<td>$x+1$</td>
</tr>
</tbody>
</table>

- Hence $(x + 1)(x^4 + x + 1) + (x^2)(x^3 + x^2 + 1) = 1,$ i.e., $D^{-1} = x^2 = 0100 = 4.$
Another way to compute inverses

- Example: $GF(8) = F_2[x] \mod (x^3 + x + 1)$. Let $\alpha = 010$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$\alpha^i$</th>
<th>$\gamma$</th>
<th>$\log_\alpha \gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\infty$</td>
<td>000</td>
<td>000</td>
<td>$\infty$</td>
</tr>
<tr>
<td>0 mod 7</td>
<td>001</td>
<td>001</td>
<td>0</td>
</tr>
<tr>
<td>1 mod 7</td>
<td>010</td>
<td>010</td>
<td>1</td>
</tr>
<tr>
<td>2 mod 7</td>
<td>100</td>
<td>011</td>
<td>3</td>
</tr>
<tr>
<td>3 mod 7</td>
<td>011</td>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>4 mod 7</td>
<td>110</td>
<td>101</td>
<td>6</td>
</tr>
<tr>
<td>5 mod 7</td>
<td>111</td>
<td>110</td>
<td>4</td>
</tr>
<tr>
<td>6 mod 7</td>
<td>101</td>
<td>111</td>
<td>5</td>
</tr>
</tbody>
</table>

- If $\text{ord } \alpha = 2^m - 1$, we call $\alpha$ a primitive root.
Example

• Example:

\[
[110]^{-1} =? \\
\log[110] = 4 \\
-\log[110] = -4 \mod 7 = 3 \\
\alpha^3 = [011] \\
[110]^{-1} = [011].
\]
The “Order” of A Nonzero Element of $GF(q)$

• For $x \neq 0$, define $\text{ord } x = \min\{t \geq 0 \mid x^t = 1\}$

• In the HexField,

<table>
<thead>
<tr>
<th>x</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>ord x</td>
<td>1</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>15</td>
<td>5</td>
<td>15</td>
<td>5</td>
<td>15</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
The Order of A Nonzero Element of $GF(q)$

**Theorem.** In general : $\text{ord } x | q - 1$.

**Proof:**

\[
\begin{array}{cccccc}
1 & x & x^2 & \cdots & x^{t-1} & G \\
y & yx & yx^2 & \cdots & yx^{t-1} & Gy \\
z & zx & zx^2 & \cdots & zx^{t-1} & Gz \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\end{array}
\]
Example: How Many Elements of order 12 are There?

- Suppose ord $\alpha = 12$ in some field $F$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gcd(12, i)$</td>
<td>12</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$\text{ord } \alpha^i$</td>
<td>1</td>
<td>12</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>2</td>
<td>12</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>12</td>
</tr>
</tbody>
</table>

**Theorem.** Given $\alpha$ with $\text{ord } a = t$. Then for $i \in \{0, 1, \ldots, t - 1\}$, $\text{ord } a^i = t / \gcd(t, i)$. 
An Important and Useful
number-theoretic
function: The Euler $\phi(n)$

Definition. For $n \geq 1$,

$$\phi(n) = |\{k : 1 \leq k \leq n : \gcd(k, n) = 1\}|.$$
Useful Facts About $\phi(n)$

$$n = \prod_{i} a_i^{e_i}$$

$$\phi(n) = \prod_{i} a_i^{e_i-1}(a_i - 1)$$

$$= n \prod_{p|n} (1 - \frac{1}{p}).$$
A Remarkable Fact

Corollary. \( F \) a field. The number of elements of order \( t \) is either 0 or \( \phi(t) \).

<table>
<thead>
<tr>
<th>( t )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \phi(t) )</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>10</td>
<td>4</td>
<td>12</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>
Example: $GF(61)$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>or</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>10</th>
<th>12</th>
<th>15</th>
<th>20</th>
<th>30</th>
<th>60</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>or</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>or</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>or</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>or</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>or</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>or</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>or</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>or</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>or</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td>or</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>0</td>
<td>or</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>0</td>
<td>or</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Therefore $GF(61)$ has 16 primitive roots. (What are they?)
A Theorem

Theorem.

\[ \sum_{d|n} \phi(d) = n. \]
\[
\begin{pmatrix}
\frac{1}{12} & \frac{1}{12} \\
\frac{2}{12} & \frac{1}{6} \\
\frac{3}{12} & \frac{1}{4} \\
\frac{4}{12} & \frac{1}{3} \\
\frac{5}{12} & \frac{5}{12} \\
\frac{6}{12} & \frac{1}{2} \\
\frac{7}{12} & \frac{7}{12} \\
\frac{8}{12} & \frac{2}{3} \\
\frac{9}{12} & \frac{3}{4} \\
\frac{10}{12} & \frac{5}{6} \\
\frac{11}{12} & \frac{11}{12} \\
\frac{12}{12} & \frac{1}{1}
\end{pmatrix}
\]
A Simple But Vital Fact

• Let \( f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \) be a polynomial of degree \( n \) with coefficients from a field \( F \).

Theorem. The number of solutions to the equation

\[
(1) \quad f(x) = 0
\]

is at most \( n \).

Proof: Induction on \( n \). If \( n = 1 \), there is exactly one solution to (1), viz., \( x = -a_1 \). Assuming the truth of the theorem for polynomials of degree \( n - 1 \), let us prove it for degree \( n \).
Proof Continues

If there are no solutions to (1), there is nothing to prove. Otherwise, if say $f(b) = 0$, use the division algorithm to divide $f(x)$ by $(x - b)$:

\[(2) \quad f(x) = q(x)(x - b) + r,\]

On substituting $x = b$ in (2) we see that $r = 0$ and so

\[f(x) = (x - b)q(x).\]

Thus every solution to (1) is either $x = b$ or $q(x) = 0$. But $q(x) = 0$, being of degree $n - 1$, has at most $n - 1$ solutions. ■
Counterexamples

• The equation \( x^2 = 1 \) has 4 solutions in \( \mathbb{Z}_8 \).

• The equation \( x^3 + x + 1 = 0 \) has 21 solutions in \( M_3(F_2) \).
<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>A</td>
<td>C</td>
<td>E</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>5</td>
<td>B</td>
<td>9</td>
<td>F</td>
<td>D</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>5</td>
<td>C</td>
<td>F</td>
<td>A</td>
<td>9</td>
<td>B</td>
<td>8</td>
<td>D</td>
<td>E</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>C</td>
<td>3</td>
<td>7</td>
<td>B</td>
<td>F</td>
<td>6</td>
<td>2</td>
<td>E</td>
<td>A</td>
<td>5</td>
<td>1</td>
<td>D</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>A</td>
<td>F</td>
<td>7</td>
<td>2</td>
<td>D</td>
<td>8</td>
<td>E</td>
<td>B</td>
<td>4</td>
<td>1</td>
<td>9</td>
<td>C</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>C</td>
<td>A</td>
<td>B</td>
<td>D</td>
<td>7</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>9</td>
<td>F</td>
<td>E</td>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>E</td>
<td>9</td>
<td>F</td>
<td>8</td>
<td>1</td>
<td>6</td>
<td>D</td>
<td>A</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>C</td>
<td>B</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>8</td>
<td>3</td>
<td>B</td>
<td>6</td>
<td>E</td>
<td>5</td>
<td>D</td>
<td>C</td>
<td>4</td>
<td>F</td>
<td>7</td>
<td>A</td>
<td>2</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>9</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>B</td>
<td>3</td>
<td>A</td>
<td>4</td>
<td>D</td>
<td>5</td>
<td>C</td>
<td>6</td>
<td>F</td>
<td>7</td>
<td>E</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
<td>A</td>
<td>7</td>
<td>D</td>
<td>E</td>
<td>4</td>
<td>9</td>
<td>3</td>
<td>F</td>
<td>5</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>B</td>
<td>6</td>
<td>C</td>
</tr>
<tr>
<td>B</td>
<td>0</td>
<td>B</td>
<td>5</td>
<td>E</td>
<td>A</td>
<td>1</td>
<td>F</td>
<td>4</td>
<td>7</td>
<td>C</td>
<td>2</td>
<td>9</td>
<td>D</td>
<td>6</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>C</td>
<td>B</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td>E</td>
<td>2</td>
<td>A</td>
<td>6</td>
<td>1</td>
<td>D</td>
<td>F</td>
<td>3</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>D</td>
<td>0</td>
<td>D</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td>C</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>F</td>
<td>B</td>
<td>6</td>
<td>3</td>
<td>E</td>
<td>A</td>
<td>7</td>
</tr>
<tr>
<td>E</td>
<td>0</td>
<td>E</td>
<td>F</td>
<td>1</td>
<td>D</td>
<td>3</td>
<td>2</td>
<td>C</td>
<td>9</td>
<td>7</td>
<td>6</td>
<td>8</td>
<td>4</td>
<td>A</td>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
<td>F</td>
<td>D</td>
<td>2</td>
<td>9</td>
<td>6</td>
<td>4</td>
<td>B</td>
<td>1</td>
<td>E</td>
<td>C</td>
<td>3</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>A</td>
</tr>
</tbody>
</table>
The Minimal Polynomial of “2”

\[ 2^0 = 1 = 0001 \leftarrow \]
\[ 2^1 = 2 = 0010 \leftarrow \]
\[ 2^2 = 4 = 0100 \]
\[ 2^3 = 8 = 1000 \]
\[ 2^4 = 3 = 0011 \leftarrow \]
Minimal Polynomials in $GF(16)$

\[
\begin{array}{ccc}
\{0\} & x & 1 \\
\{1\} & x + 1 & 1 \\
\{2, 3, 4, 5\} & x^4 + x + 1 & 15 \\
\{6, 7\} & x^2 + x + 1 & 3 \\
\{8, C, F, A\} & x^4 + x^3 + x^2 + x + 1 & 5 \\
\{9, D, E, B\} & x^4 + x^3 + 1 & 15 \\
\end{array}
\]
Discrete Logarithms

• Let $\alpha$ be a primitive root (an element of order $q - 1$) in $GF(q)$.

• Define the base-$\alpha$ discrete logarithm of $x \neq 0$:

$$x := \alpha^{L(x)}$$

• This simplifies multiplication:

$$L(xy) = L(x) + L(y)$$
Example: $\alpha^3 + \alpha + 1 = 0$ in $GF(8)$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$L(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>$NAN$</td>
</tr>
<tr>
<td>001</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>1</td>
</tr>
<tr>
<td>011</td>
<td>3</td>
</tr>
<tr>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>101</td>
<td>6</td>
</tr>
<tr>
<td>110</td>
<td>4</td>
</tr>
<tr>
<td>111</td>
<td>5</td>
</tr>
</tbody>
</table>
Zech’s Logarithms

\[ Z(m) = L(1 + \alpha^m) \]
\[ Z(L(y)) = L(1 + y) \]

\[ L(xy) = L(x) + L(y) \mod (q - 1) \]
\[ L(x + y) = L(x) + Z(L(y) - L(x)) \mod (q - 1) \]
## Conventional vs. Zech’s Logarithms

<table>
<thead>
<tr>
<th>$x$</th>
<th>$L(x)$</th>
<th>$m$</th>
<th>$Z(m)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>$\infty$</td>
<td>$\infty$</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>0</td>
<td>0</td>
<td>$\infty$</td>
</tr>
<tr>
<td>010</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>011</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>100</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>101</td>
<td>6</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>110</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>111</td>
<td>5</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>
Special Topic: Weight
Enumeration of \((n, k)\) MDS Codes

- Let \(C\) be an \((n, k)\) MDS code over \(GF(q)\). We regard each codeword \(c \in C\) as a function from \(\{1, \ldots, n\}\) to \(GF(q)\).

- Let \(V \subseteq \{1, 2, \ldots, n\}\), and define

\[
A(V) = |\{c \in C : c(i) = 0 \text{ if } i \in V\}|
\]
\[
B(V) = |\{c \in C : c(i) = 0 \text{ iff } i \in V\}|
\]

Then

\[
A(V) = a[v] = q^{\max\{v-k, 0\}}.
\]
and

\[ A(V) = \sum_{V' \supseteq V} B(V') \]

\[ a[v] = \sum_{j=0}^{n-v} \binom{n-v}{j} b[v+j] \]
Weight Enumeration of MDS Codes

\[ a[n] = b[n] \]
\[ a[n - 1] = b[n] + b[n - 1] \]
\[ a[n - 2] = b[n] + 2b[n - 1] + b[n - 2] \]
\[ \vdots \]

- The number of codewords of weight \( w \) is \( \binom{n}{n-w} b[n-w] \).