Outline

- The Period of a Polynomial.
- Irreducible v. Primitive Field Representations
- Testing for Primitivity
The Period of A Polynomial

• Let $F$ be a finite field with $q$ elements, e.g. $F = GF(2) = \{0, 1\}$.

• Let $F[x]$ denote the set of polynomials with coefficients in $F$.

• Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_0$, be a fixed polynomial with coefficients in $F$, and $a_0 \neq 0$.

• If $g(x) \in F[x]$, define

$$[g(x)] := g(x) \mod f(x).$$
The Period of A Polynomial

Consider the sequence

\[ [1], [x], [x^2], \ldots. \]

Since there are only \( q^n \) distinct equivalence classes modulo \( f(x) \), there must be repeats. Let the first repeat be \( [x^{j+e}] = [x^j] \), i.e.,

\[ f(x) \mid x^{j+e} - x^j. \]

Since \( \gcd(f(x), x) = 1 \), (here we use the \( a_0 \neq 0 \) assumption)

\[ f(x) \mid x^e - 1. \]

\( e \) is called the period of \( f(x) \), written \( \text{per } f(x) = e \).
Primitive Polynomials

Theorem. If $f(x)$ is irreducible of degree $n$,

$$\text{per } f(x) | q^n - 1.$$ 

If $\text{per } f = q^n - 1$, $f$ is said to be primitive.

Proof: Omitted.
And Now
Suppose we have an Irreducible Polynomial:

Let $f(x)$ be an irreducible (not necessarily primitive) polynomial of degree $n$ over the field $F = GF(q)$. Then the $q^n$ polynomials

$$[a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n] : a_i \in F$$

form a field under polynomial addition and multiplication modulo $f(x)$: the field $GF(q^n)$. 
Suppose we have Primitive Polynomial:

Let \( p(x) \) be a primitive polynomial of degree \( n \) over the field \( F = GF(q) \). Then the \( q^n \) monomials

\[
\{[0], [1], [x], [x^2], \ldots [x^{q-2}]\}
\]

form a field under polynomial addition and multiplication modulo \( p(x) \).
Example

- Let $q = 2$, $n = 3$, and $f(x) = x^3 + x + 1$. Then the eight polynomial equivalence classes

$[0], [1], [x], [x + 1], [x^2], [x^2 + 1], [x^2 + x], [x^2 + x + 1]$ form a field $GF(2^3)$ under polynomial addition and polynomial multiplication modulo $f(x)$. 
Example

• The eight monomial equivalence classes

\[ [0], [1], [x], [x^2], [x^3], [x^4], [x^5], [x^6] \]

also represent $GF(2^3)$, because $f(x)$ is in fact primitive.
In fact, modulo $x^3 + x + 1$,

\[
\begin{align*}
[0] &= [0] \\
[x] &= [x] \\
[x^2] &= [x^2] \\
[x^3] &= [x + 1] \\
[x^4] &= [x^2 + x] \\
[x^5] &= [x^2 + x + 1] \\
[x^6] &= [x^2 + 1]
\end{align*}
\]
Example

- Let $q = 3$, $n = 2$, and $f(x) = x^2 + 1$. Then the nine polynomial equivalence classes

  \[[0], [1], [2], [x], [x + 1], [x + 2], [2x], [2x + 1], [2x + 2]\]

form a field $GF(3^2)$ under polynomial addition and polynomial multiplication modulo $f(x)$. 
Example

- But the in this case the monomials

  \[0, [1], [x], [x^2], [x^3], [x^4], [x^5], [x^6], [x^7]\]

  do not form a field, because \( f(x) \), though irreducible, is not primitive. Indeed, \([x^4] = [1]\), i.e., \( \text{per } f(x) = 4 \).
A Matrix Representation of $GF(q^n)$

Let $C$ be the companion matrix of $f(x)$, an irreducible polynomial of degree $n$ over $GF(q)$. Then the $q^n$ matrices

$$\{g(C) : \deg g(x) \leq n - 1\}$$

form a field $GF(q^n)$ under ordinary matrix addition and multiplication.
Another Matrix Representation of $GF(q^n)$

Let $C$ be the companion matrix of $f(x)$, a primitive polynomial of degree $n$ over $GF(q)$. Then the $q^n$ matrices

$$\{O_n, I_n, C, C^2, \ldots C^{q^n-2}\}$$

form a field under ordinary matrix addition and multiplication.
Example: A Matrix Representation of $GF(8)$

- $C$ is the companion matrix for $x^3 + x + 1$

\[
\begin{align*}
O_3 &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} & I_3 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & C &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} & C^2 &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \\
C^3 &= C + I & C^4 &= C^2 + C & C^5 &= C^2 + C + I & C^6 &= C^2 + I \\
&= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} & & = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} & & = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} & & = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}
\end{align*}
\]
Example: A Matrix Representation of $GF(9)$

- $C$ is the companion matrix for $x^2 + 1$

<table>
<thead>
<tr>
<th></th>
<th>$O_2$</th>
<th>$I$</th>
<th>$2I$</th>
</tr>
</thead>
</table>
| $C$ | \[
\begin{pmatrix}
0 & 0 \\
0 & 0 \\
2 & 0
\end{pmatrix}
\] | \[
\begin{pmatrix}
1 & 0 \\
0 & 1 \\
2 & 1
\end{pmatrix}
\] | \[
\begin{pmatrix}
2 & 0 \\
0 & 2 \\
2 & 2
\end{pmatrix}
\] |
| $C + I$ | \[
\begin{pmatrix}
1 & 1 \\
1 & 1 \\
2 & 2
\end{pmatrix}
\] | \[
\begin{pmatrix}
2 & 1 \\
2 & 1 \\
2 & 2
\end{pmatrix}
\] |
| $C + 2I$ | \[
\begin{pmatrix}
2 & 1 \\
2 & 1 \\
2 & 2
\end{pmatrix}
\] | \[
\begin{pmatrix}
2 & 1 \\
2 & 1 \\
2 & 2
\end{pmatrix}
\] | \[
\begin{pmatrix}
2 & 1 \\
2 & 1 \\
2 & 2
\end{pmatrix}
\] |
And Now
How Can We Test For Primitivity?

• Suppose \( f(x) \) is irreducible of degree \( n \). The period of \( f(x) \) must be a divisor of \( q^n - 1 \).

**Theorem.** \( f(x) \) is primitive iff

\[
x^{(q^n - 1)/p} \neq 1 \mod f(x) \quad \text{for all primes } p \mid q^n - 1
\]

• Example. \( n = 16: \) \( p \mid 2^{16} - 1 \rightarrow p \in \{3, 5, 17, 257\} \)

• If per \( f \neq 2^{16} - 1 \), at least one of the following is true.

\[
x^t = 1 \mod f(x) \quad \text{for } t = 21845, 13107, 3855, 255
\]
A Problem

• How to raise $x$ to really big power mod $f(x)$?

• We adopt the "binary method" for evaluating $x^N$ in any monoid.

• Ref: Knuth II Sec. 4.6.3.
The Binary Method for Computing $x^N$

- Write out the binary expansion of $N$, suppressing 0’s on the left.

- Replace each “0” with “S” and each “1” with “SX.”

- Delete the initial “SX.”

- Example: 23 → 10111 → SSXSXSXSX.

- The resulting string is a rule for computing $x^N$: reading from left to right, “S” stands for squaring and “X’ stands for multiply by $x$. 
- Example:

\[ x \rightarrow S \rightarrow x^2 \rightarrow S \rightarrow x^4 \rightarrow X \rightarrow x^5 \rightarrow S \rightarrow x^{10} \rightarrow X \rightarrow x^{11} \rightarrow S \rightarrow x^{22} \rightarrow X \rightarrow x^{23} \]
Adapting the Binary Method to Our Problem.

- Define the $1 \times n$ vector $\mathbf{u}$ and the $n \times n$ matrices $Q_0$ and $Q_1$ as follows.

$$
\mathbf{u} = \left( \begin{array}{c}
x \mod f(x) \\
1 \mod f(x) \\
x^2 \mod f(x) \\
x^4 \mod f(x) \\
\vdots \\
x^{2n-2} \mod f(x)
\end{array}\right) = (0100000)
$$

$$
Q_0 = \left( \begin{array}{c}
1 \\
x \\
x^2 \\
x^4 \\
\vdots \\
x^{2n-2}
\end{array}\right) \\
Q_1 = \left( \begin{array}{c}
x \\
x^3 \\
x^5 \\
\vdots \\
x^{2n-1}
\end{array}\right)
$$
- Define the $1 \times n$ vector $\mathbf{u}$ and the $n \times n$ matrices $Q_0$ and $Q_1$ as follows.

\[
\mathbf{u} = \begin{pmatrix} x \mod f(x) \end{pmatrix} = (0100000)
\]

\[
Q_0 = \begin{pmatrix}
1 \mod f(x) \\
x^2 \mod f(x) \\
x^4 \mod f(x) \\
\vdots \\
x^{2n-2} \mod f(x)
\end{pmatrix}
\]

\[
Q_1 = \begin{pmatrix}
x \mod f(x) \\
x^3 \mod f(x) \\
x^5 \mod f(x) \\
\vdots \\
x^{2n-1} \mod f(x)
\end{pmatrix}
\]
Recall

• Recall: A row vector times a matrix is a linear combination of the rows of the matrix:

\[(a_1, \ldots, a_n) \cdot \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = a_1 \cdot r_1 + \cdots + a_n \cdot r_n\]
\( Q_0 \) and \( Q_1 \) are linear operators on \( F[x] \mod f(x) \)

- If \( g(x) = g_0 + \cdots + g_{n-1}x^{n-1} \), Then

\[
g(x)Q_0 = (g_0 + g_1x^2 + \cdots + g_{n-1}x^{2n-2}) \mod f(x)
\]

\[
= g(x)^2 \mod f(x)
\]

\[
g(x)Q_1 = (g_0x + g_1x^3 + \cdots + g_{n-1}x^{2n-1}) \mod f(x)
\]

\[
= xg(x)^2 \mod f(x)
\]
A Neat Trick

If \( N = N_mN_{m-1}\cdots N_0 \) is the binary expansion of \( N \), with \( N_m = 1 \), then

\[
x^N \mod f(x) \sim u(Q_{N_m-1} \cdots Q_{N_0})
\]

- Example:

\[
23 = 1 \quad 0 \quad 1 \quad 1 \quad 1 \\
x^{23} = u \quad Q_0 \quad Q_1 \quad Q_1 \quad Q_1
\]