Review/Outline

Review:
- Basic computations in finite fields
- Reed-Solomon codes
- Hamming codes
- Bose-Chaudhuri-Hocquengham (BCH) codes

Testing for irreducibility

Frobenius automorphisms
- Other roots of equations
  - Counting irreducibles
  - Counting primitive polynomials
  - New: Equation satisfied by field element
Counting irreducibles

**Theorem:** Let \( p \) be prime. Fix a degree \( d \).
The number of irreducible monic (=leading coefficient 1) polynomials of degree \( d \) in \( \mathbb{F}_p[x] \) is

\[
p^d - \sum_{q|d} p^{d/q} + \sum_{q_1,q_2|d} p^{d/q_1q_2} - \ldots \]

where \( q_1, q_2, \ldots \) are distinct primes dividing \( d \).
For example, in some simple cases:
degree \( d \) prime:

\[
p^d - p
\]

\( d = qr \) with \( q, r \) distinct primes:

\[
p^{qr} - p^q - p^r + p
\]

\( d = abc \) with \( a, b, c \) distinct primes:

\[
p^{abc} - p^{ab} - p^{ac} - p^{bc} + p^a + p^b + p^c - p
\]

**Remark:** The number of elements in the field, \( p \), did not have to be prime, but only prime-power.
In more succinct (but possibly less transparent) notation: the number of irreducible polynomials of degree \(d\) in \(\mathbb{F}_p[x]\) is

\[
\sum_{i \geq 0} (-1)^i \sum_{i\text{-tuples } q_1 < \ldots < q_i} p^{d/q_1 \ldots q_i} \frac{d}{p^{d/q_1 \ldots q_i}}
\]

where for each \(i\) the \(i\)-tuples \(q_1 < \ldots < q_i\) runs over (distinct) primes dividing \(d\).

Further examples:
for \(d = q^2\) with \(q\) prime:
\[
\frac{p^{q^2} - p^q}{q^2}
\]
for \(d = q^3\) with \(q\) prime:
\[
\frac{p^{q^3} - p^{q^2}}{q^3}
\]
for \(d = q^4\) with \(q\) prime:
\[
\frac{p^{q^4} - p^{q^3}}{q^3}
\]

**Remark:** It may not be entirely obvious that these are non-negative integer values.
**Example:** Find the number of irreducible degree 2 polynomials with coefficients in $\mathbb{F}_2$:

The formula above, in the case of prime degree $d$, says that the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is

$$\frac{p^d - p}{d}$$

Here $p = 2$ and $d = 2$, so the number of such is

$$\frac{2^2 - 2}{2} = 1$$

Indeed, by trial and error we know it’s $x^2 + x + 1$. 
**Example:** Number of irreducible degree 3 polynomials with coefficients in $\mathbb{F}_2$: The formula above, in the case of prime degree $d$, says that the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is

$$\frac{p^d - p}{d}$$

Here $p = 2$ and $d = 3$, so the number is

$$\frac{2^3 - 2}{3} = 2$$

Indeed, by trial and error we know they’re $x^3 + x + 1$ and $x^3 + x^2 + 1$. 
**Example:** Irreducible degree 4 polynomials with coefficients in $\mathbb{F}_2$: The formula above, in the case of degree $d$ the square of a prime $q$, says that the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is

$$\frac{p q^2 - p^q}{q^2}$$

Here $p = 2$ and $d = 4$, so $q = 2$, and the number of such is

$$\frac{2^4 - 2^2}{4} = 3$$

Again, by trial and error, we know they’re

$$x^4 + x + 1$$

$$x^4 + x^3 + 1$$

and

$$x^4 + x^3 + x^2 + x + 1$$
Example: Number of irreducible degree 5 polynomials with coefficients in $\mathbb{F}_2$: The formula above, in the case of prime degree $d$, says that the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is

$$\frac{p^d - p}{d}$$

Here $p = 2$ and $d = 5$, so the number is

$$\frac{2^5 - 2}{5} = 6$$

Example: Irreducible degree 6 polynomials with coefficients in $\mathbb{F}_2$: The formula says the number of irreducible degree $d = qr$ polynomials with coefficients in $\mathbb{F}_p$, with distinct primes $q, r$, is

$$\frac{p^{qr} - p^q - p^r + p}{qr}$$

Here $p = 2$, $q = 2$, $r = 3$ so the number is

$$\frac{2^6 - 2^2 - 2^3 + 2}{6} = 9$$
**Example:** Find the number of irreducible degree 2 polynomials with coefficients in $\mathbb{F}_3$: The formula above, in the case of prime degree $d$, says that the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is

$$\frac{p^d - p}{d}$$

Here $p = 3$ and $d = 2$, so the number of such is

$$\frac{3^2 - 3}{2} = 3$$

Indeed, by trial and error they’re

$$x^2 + 1$$

$$x^2 + x + 2$$

$$x^2 + 2$$
\textbf{Example:} Number of irreducible degree 3 polynomials with coefficients in $\mathbb{F}_3$: The formula above, in the case of prime degree $d$, says that the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is

\[ \frac{p^d - p}{d} \]

Here $p = 3$ and $d = 3$, so the number is

\[ \frac{3^3 - 3}{3} = 8 \]

\textbf{Example:} Irreducible degree 4 polynomials with coefficients in $\mathbb{F}_3$: in the case of degree $d$ the square of a prime $q$, the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is

\[ \frac{p^{q^2} - p^q}{q^2} \]

Here $p = 3$ and $d = 4$, so $q = 2$, and the number is

\[ \frac{3^4 - 3^2}{4} = 18 \]
Example: Find the number of irreducible degree 7 polynomials with coefficients in $\mathbb{F}_3$: The formula above, in the case of prime degree $d$, says that the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is
\[
\frac{p^d - p}{d}
\]
Here $p = 3$ and $d = 7$, so the number of such is
\[
\frac{3^7 - 3}{7} = 312
\]

Example: Find the number of irreducible degree 6 polynomials with coefficients in $\mathbb{F}_3$: The formula above, in the case of degree $d = qr$ with primes $q, r$, says that the number of irreducible degree $d$ polynomials with coefficients in $\mathbb{F}_p$ is
\[
\frac{p^{qr} - p^q - p^r + p}{qr}
\]
Here $p = 3$ and $d = qr$ with $q = 2$ and $r = 3$, so the number of such is
\[
\frac{3^6 - 3^3 - 3^2 + 3}{6} = 116
\]
Euler’s \( \varphi \)-function

A convenient counting function is Euler’s \( \varphi \)-function, or \textbf{totient} function

\[
\varphi(n) = \text{no. } t \text{ with } 1 \leq t \leq n \text{ and } \gcd(t,n) = 1
\]

For example

\[
\begin{align*}
\varphi(2) &= \text{no.}\{1\} = 1 \\
\varphi(3) &= \text{no.}\{1, 2\} = 2 \\
\varphi(4) &= \text{no.}\{1, 3\} = 2 \\
\varphi(5) &= \text{no.}\{1, 2, 3, 4\} = 4 \\
\varphi(6) &= \text{no.}\{1, 5\} = 2 \\
\varphi(7) &= \text{no.}\{1, 2, 3, 4, 5, 6\} = 6 \\
\varphi(8) &= \text{no.}\{1, 3, 5, 7\} = 4
\end{align*}
\]

\textbf{Remark:} Do \textit{not} compute \( \varphi(n) \) this way: do \textit{not} enumerate the set to be counted.
**Theorem:** Let

\[ n = p_1^{e_1} \cdots p_t^{e_t} \]

be the factorization of \( n \) into primes, with \( p_1 < \ldots < p_t \) and all \( e_i \geq 1 \). Then

\[ \varphi(n) = (p_1 - 1)p_1^{e_1-1} \cdots (p_t - 1)p_t^{e_t-1} \]

**Examples:**

\[ \varphi(10) = \varphi(2 \cdot 5) = (2 - 1) \cdot (5 - 1) = 4 \]
\[ \varphi(12) = \varphi(2^2 \cdot 3) = (2 - 1)2 \cdot (3 - 1) = 4 \]
\[ \varphi(15) = \varphi(3 \cdot 5) = (3 - 1) \cdot (5 - 1) = 8 \]
\[ \varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2 - 1) \cdot (3 - 1) \cdot (5 - 1) = 8 \]
\[ \varphi(100) = \varphi(2^2 \cdot 5^2) = (2 - 1)2 \cdot (5 - 1)5 = 40 \]

**Remark:** This formula fails if we cannot factor \( n \) (presumably due to \( n \) being very large and having no small prime factors).
Counting primitives

**Theorem:** Let $q$ be a prime power. Fix a degree $d$. The number of *primitive monic* degree $d$ polynomials in $\mathbf{F}_q[x]$ is

$$\frac{\varphi(q^d - 1)}{d}$$

**Remark:** It is completely unclear that the given expression is an integer.

**Remark:** We did not prove it, but it is true that *primitive* polynomials are necessarily *irreducible*: primitivity is a stronger condition than irreducibility.

**Example:** To count primitive monic degree 2 polynomials in $\mathbf{F}_2[x]$, in the theorem $d = 2$ and $q = 2$, giving

$$\text{no. prim. quadratics} = \frac{\varphi(2^2 - 1)}{2}$$

$$= \frac{\varphi(3)}{2} = \frac{(3 - 1)}{2} = 1$$

using also the formula for Euler’s $\varphi$-function.
Example: To count primitive monic degree 3 polynomials in $\mathbf{F}_2[x]$, in the theorem $d = 3$ and $q = 2$, giving

$$\text{no. prim. cubics} = \frac{\varphi(2^3 - 1)}{3}$$

$$= \frac{\varphi(7)}{3} = \frac{(7 - 1)}{3} = 2$$

using also the formula for Euler’s $\varphi$-function (factoring by trial division). There are only two irreducible cubics $x^3 + x + 1$ and $x^3 + x^2 + 1$ so they are necessarily primitive.

Example: To count primitive monic degree 4 polynomials in $\mathbf{F}_2[x]$, in the theorem $d = 4$ and $q = 2$, giving

$$\text{no. prim. quartics} = \frac{\varphi(2^4 - 1)}{4}$$

$$= \frac{\varphi(15)}{4} = \frac{(3 - 1)(5 - 1)}{4} = 2$$

using also the formula for Euler’s $\varphi$-function (factoring by trial division). Of the 3 irreducible quartics $x^4 + x + 1$ and $x^4 + x^3 + 1$ are primitive.
**Example:** To count primitive monic degree 5 polynomials in $\mathbf{F}_2[x]$, in the theorem $d = 5$ and $q = 2$, giving

$$\text{no. prim. quintics} = \frac{\varphi(2^5 - 1)}{5}$$

$$= \frac{\varphi(31)}{5} = \frac{(31 - 1)}{5} = 6$$

using also the formula for Euler’s $\varphi$-function (31 is prime, by trial division). There are $(2^5 - 2)/5 = 6$ irreducibles, to every irreducible is primitive. Indeed, generally,

**Corollary:** If $q^d - 1$ is prime, then every irreducible monic degree $d$ polynomial in $\mathbf{F}_q[x]$ is primitive (otherwise, there will be fewer primitives than irreducibles of a given degree).
**Example:** To count primitive monic degree 6 polynomials in $\mathbf{F}_2[x]$, in the theorem $d = 6$ and $q = 2$, giving

\[
\text{no. prim. sextics} = \frac{\varphi(2^6 - 1)}{6}
\]

\[
= \frac{\varphi(63)}{6} = \frac{(3 - 1)3 \cdot (7 - 1)}{6} = 6
\]

using the formula for Euler’s $\varphi$-function, factoring 63 by trial division.

**Example:** To count primitive monic degree 7 polynomials in $\mathbf{F}_2[x]$, in the theorem $d = 7$ and $q = 2$, giving

\[
\text{no. prim. sextics} = \frac{\varphi(2^7 - 1)}{6}
\]

\[
= \frac{\varphi(127)}{7} = \frac{(127 - 1)}{7} = 18
\]

using the formula for Euler’s $\varphi$-function (127 is prime by trial division).
**Example:** To count primitive monic degree 2 polynomials in $\mathbb{F}_3[x]$, in the theorem $d = 2$ and $q = 3$, giving

$$\text{no. prim. sextics} = \frac{\varphi(3^2 - 1)}{2}$$

$$= \frac{\varphi(8)}{2} = \frac{(2 - 1)2^{3-1}}{2} = 2$$

using the formula for Euler’s $\varphi$-function, factoring 8 by trial division.

Among the 3 irreducible quadratics $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2$ here, which is the non-primitive one? For $P(x) = x^2 + 2$, note that

$$x^2 = (x^2 + 2) + 1 = 1 \mod P(x)$$

so $x$ has order just 2 mod $P(x)$, not the maximal possible, namely $3^2 - 1 = 8$. So $x^2 + 2$ is the non-primitive one.
Example: To count primitive monic degree 3 polynomials in $\mathbb{F}_3[x]$, in the theorem $d = 3$ and $q = 3$, giving

$$\text{no. prim. cubics} = \frac{\varphi(3^3 - 1)}{3}$$

$$= \frac{\varphi(26)}{3} = \frac{(2 - 1) \cdot (13 - 1)}{3} = 4$$

using the formula for Euler’s $\varphi$-function (factoring by trial division).

Remark: If we believe the formula, then there really are primitive polynomials of all degrees.