Outline

• Math Warm-Up

• Order of Elements in (Finite) Fields

• Existence and Number of Primitive Roots

• Testing for Irreducibility
Important Notation

• \( d \mid n \) means “\( d \) divides \( n \).”

• Defined for positive integers only.

• Examples: \( 4 \mid 24 \), \( 4 \nmid 6 \).
The Möbius $\mu$-function.

Recursive Definition. 

$$\mu(1) = 1$$
$$\sum_{d|n} \mu(d) = 0 \quad \text{if } n > 1$$

Closed-Form Definition. If $p_1, \ldots, p_n$ are distinct primes, and $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then

$$\mu(n) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if any } e_i > 1 \\
(-1)^r & \text{if } e_1 = \cdots = e_r = 1.
\end{cases}$$
Homework Problem

- Show that the two definitions agree.
Theorem. If $f(n) = \sum_{d|n} g(d)$, then

$$g(n) = \sum_{d|n} \mu(d) f(n/d).$$
Proof

\[
\sum_{d|n} \mu(d) f \left( \frac{n}{d} \right) = \sum_{d|n} \mu(d) \left( \sum_{e|\frac{n}{d}} g(e) \right) \\
= \sum_{(d \cdot e)|n} \mu(d)g(e) \\
= \sum_{e|n} g(e) \left( \sum_{d|\frac{n}{e}} \mu(d) \right) \\
= g(n).
\]
Illustration for Proof \((n = 12)\)

\[
\begin{pmatrix}
  e = 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
  d = 1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\
  2 & -1 & -1 & -1 & -1 & -1 \\
  3 & -1 & -1 & -1 & -1 \\
  4 & 0 & 0 \\
  5 & 0 & 0 \\
  6 & +1 & +1 \\
  7 & 0 & 0 \\
  8 & 0 & 0 \\
  9 & 0 & 0 \\
  10 & 0 & 0 \\
  11 & 0 & 0 \\
  12 & 0 & 0 \\
\end{pmatrix}
\]
Some Unfinished Business

\[ q^n = \sum_{d|n} dI_d(q) \]
Some Unfinished Business

\[ q^n = \sum_{d|n} dI_d(q) \]

\[ I_n(q) = \frac{1}{n} \sum_{d|n} \mu(d)q^{n/d}. \]
The Euler $\phi$-function.

Definition.

$$\phi(n) := |\{i : 1 \leq i \leq n \text{ and } \gcd(i, n) = 1\}|.$$ 

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\phi(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 1 1</td>
</tr>
<tr>
<td>2</td>
<td>1 1 2</td>
</tr>
<tr>
<td>3</td>
<td>2 1 2 3</td>
</tr>
<tr>
<td>4</td>
<td>2 1 2 3 4</td>
</tr>
<tr>
<td>5</td>
<td>4 1 2 3 4 5</td>
</tr>
<tr>
<td>6</td>
<td>2 1 2 3 4 5 6</td>
</tr>
</tbody>
</table>
A Property of $\phi(n)$.

Theorem.

\[ \sum_{d|n} \phi(d) = n. \]
A Homework Problem

\[ \sum_{d \mid n} \frac{\mu(d)}{d} = ? \]
Six Solutions to $x^2 = x$

\[
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}
\]

\[
\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}
\]
Theorems About Polynomials.

Theorem. If $f(x)$ is a polynomial of degree $m$, with coefficients in a field, then the equation $f(x) = 0$ can have at most $m$ solutions.

Proof: Induction on $m$.

- $ax + b = 0$
Theorems About Polynomials.

Definition. A polynomial $f(x)$ is squarefree if there is no polynomial $p(x)$ of degree $\geq 1$ such that $p^2(x) \mid f(x)$.

Theorem. $f(x)$ is squarefree iff $\gcd(f(x), f(x)') = 1$. 
The Order of an Element

- Let $\alpha \in F$ where $\alpha \neq 0$, $F$ a field.

- Consider the sequence $1, \alpha, \alpha^2, \ldots$.

- If $F$ is finite, there will be a (first) repeat:

  $$a^k = \alpha^{k+t}.$$
The Order of an Element

• Let $\alpha \in F$ where $\alpha \neq 0$, $F$ a field.

• Consider the sequence $1, \alpha, \alpha^2, \ldots$.

• If $F$ is finite, there will be a (first) repeat:
  \[ \alpha^k = \alpha^{k+t}. \]

• But $\alpha^k \neq 0$: Thus \{1, $\alpha$, $\ldots$, $\alpha^{t-1}$\} are all distinct, and
  \[ 1 = \alpha^t. \]
The Order of an Element

- \( t \) is called the order of \( \alpha \), written

\[
t = \text{ord } \alpha.
\]

**Theorem.** \( t \) is a divisor of \( q - 1 \).

**Proof:** Example \( t = 5 \):

\[
\begin{array}{cccccc}
1 & a & a^2 & a^3 & a^4 \\
b & ab & a^2b & a^3b & a^4b \\
c & ac & a^2c & a^3c & a^4c \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\end{array}
\]
The Order of an Element

**Theorem.** If $\text{ord}(\alpha) = t$, and $1 \leq k \leq n$, then $\text{ord} \alpha^k = t / \gcd(k, t)$.

**Proof:** $\text{ord} \alpha^k$ is the least integer $s$ such that $(\alpha^k)^s = 1$, i.e., $k \cdot s$ is a multiple of $t$, i.e., $t \mid k \cdot s$.

\[
t \mid k \cdot s \iff \frac{t}{\gcd(k, t)} \mid \frac{k}{\gcd(k, t)} \cdot s \iff \frac{t}{\gcd(k, t)} \mid s
\]
The Order of an Element

Theorem. The number of elements of order $t$ is either 0 or $\phi(t)$.

Proof: If ord $\alpha = t$, then $\{1, \alpha, \ldots, \alpha^{t-1}\}$ is a set of $t$ solutions to the equation $x^t = 1$. Thus every element $\beta$ of order $t$ is a power of $\alpha$. But we have seen above that ord $\alpha^k = t$ iff $\gcd(k, t) = 1$. $\blacksquare$
**Primitive Roots Exist!**

**Definition.** A *primitive root* is an element of order $q - 1$.

**Corollary.** A field with $q$ elements has exactly $\phi(q - 1)$ primitive roots.