Bracelet Coloring

• How many ways are there to color a bracelet of \( n \) beads with \( k \) colors, where \( n \) is an odd prime?

• The bracelet can be rotated but not flipped over.

• The configurations are colorings.

• The permutation group consists of \( n \) clockwise rotations.

• The identity permutation \( g \) has \( |F(g)| = k^n \) because there are \( k^n \) colorings.\(^a\)

\(^a\)Now \( F'(g) = \{ z \in X : g(z) = z \} \), where \( X \) is the set of \( k^n \) colorings.
Bracelet Coloring (continued)
Bracelet Coloring (continued)

- All nonidentity permutations \( g \) have \( |F(g)| \geq k \).
  - If a coloring is monochromatic, then it looks the same under rotations.
  - So colorings with beads painted with the same color are in the same equivalence class (orbit).
  - There are \( k \) such colorings.
Bracelet Coloring (continued)

- In fact, all nonidentity permutations $g$ have $|F(g)| = k$.
  - Suppose coloring $C$ does not paint beads with the same color, say those at positions $a$ and $b$.
  - There exists an $i \in \mathbb{N}$ such that $g^i$ moves the bead at location $a$ to location $b$.
    * Solve $di \equiv (b - a) \mod n$ for $i$ if $g$ rotates the bracelet by $d > 0$ positions.\(^a\)
    - If coloring $C$ is a fixed point under $g$, then it is also a fixed point under $g^i$ by induction.
    - But this is impossible as positions $a$ and $b$ receive different colors.

\(^a\)Recall that $n$ is a prime hence $d^{-1} \mod n$ exists (p. 795).
Bracelet Coloring (concluded)

• The number of distinct colorings is

\[
\frac{k^n + k + k + \cdots + k}{n^{n-1}} = \frac{k^n}{n} + \frac{n-1}{n} \cdot k. \quad (106)
\]
Bracelet Coloring with $n = 5$ and $k = 2$

Equation (106) gives $\frac{2^5 + (5-1) \times 2}{5} = 8.$
Bracelet Coloring and Fermat’s “Little” Theorem

• On p. 948, the number of bracelet colorings is found to be
  \[ \frac{k^n}{n} + \frac{n - 1}{n} k \]
  when \( n \) is an odd prime.

• We next show that it is indeed an integer.

• If \( \gcd(k, n) \neq 1 \), then \( k \) is a multiple of \( n \) and the claim is trivially true.

• So assume \( \gcd(k, n) = 1 \).
Bracelet Coloring and Fermat’s “Little” Theorem (concluded)

• By Fermat’s “little” theorem (p. 856), $k^n = k \mod n$.

• Hence

\[
\frac{k^n}{n} + \frac{n-1}{n} k = \frac{nm + k}{n} + \frac{n-1}{n} k
\]

for some $m \in \mathbb{Z}$.

• Finally

\[
\frac{nm + k}{n} + \frac{n-1}{n} k = (m + k) \in \mathbb{Z}^+.
\]
Striped Flags

• Suppose we have a striped flag with 6 stripes.

• Each stripe can be colored in red (r), green (g), or blue (b).

• Here is an example:

\[
\begin{array}{cccc}
 r & g & b & r \\
 g & b & r & g \\
 b & r & g & b \\
\end{array}
\]

• Suppose two flags are considered equivalent if one looks the same as the other one when one stands in back of it.

• The following flag is considered equivalent to the one above:

\[
\begin{array}{cccc}
 b & g & r & b \\
 g & b & r & g \\
 b & r & g & r \\
\end{array}
\]
Striped Flags (continued)

• Let $X$ contain all possible (6-tuple) colorings $(c_1, c_2, \ldots, c_6)$, where $c_i \in \{r, g, b\}$.

• Let $\pi$ be the permutation that reverses the positions of the colors,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1 \ 6)(2 \ 5)(3 \ 4).$$

• It “turns over” the flag.
  – It makes $c_{\pi(i)}$ the next $i$th color $c_i$, $i = 1, 2, \ldots, 6$.

• Note that $\pi$ turns one coloring into another.

• The cyclic group $G = \langle \pi \rangle$ acts on $X$. 
Striped Flags (continued)

• It is clear that $|G| = 2$.
  - In fact, $G = \{ I, \pi \}$ as $\pi^2 = I$.

• By definition or the orbit-stabilizer theorem (p. 933), $|O_x| \leq |G|$.

• So each orbit contains either one coloring or two colorings.

• Here is the orbit we saw,

\[
\{ (r, g, b, r, g, b), (b, g, r, b, g, r) \}.
\]

• Note that

\[
\pi (r, g, b, r, g, b) = (b, g, r, b, g, r).
\]
Striped Flags (continued)

• Here is another orbit,

\[ \{ (r, g, b, b, g, r) \} , \]

and \( \pi \) fixes the coloring \((r, g, b, b, g, r)\), a palindrome!

• Palindromes form only a proper subset of all flags.
  – There are \( 3 \times 3 \times 3 = 27 \) palindromes as there are 3 choices for each of \( c_1, c_2, c_3 \).

• A distinct coloring of the flag corresponds to an orbit, and vice versa.
Striped Flags (continued)

• The number of distinct colorings of the flag is thus the number of orbits.

• Burnside’s lemma (p. 927) says the number of orbits is

\[
\frac{|F(I)| + |F(\pi)|}{2}.
\]

• The identity permutation \(I\) fixes every coloring \(x \in X\).

• So \(|F(I)| = 3^6\).
Striped Flags (concluded)

- On the other hand, $\pi$ fixes a coloring $x \in X$ if and only if $x$ is a palindrome.

- Hence $|F(\pi)| = 3^3$.

- Our desired count is hence

$$\frac{3^6 + 3^3}{2} = 378.$$  

- In general, if the flag has $2s$ stripes and $k$ colors, then the count equals

$$\frac{k^{2s} + k^s}{2}.$$
Coloring Defined

- Let us generalize the idea of coloring.
- Let $X = \{1, 2, \ldots, n\}$ and $\mathcal{C}$ be a set of $k$ colors.
- $\mathcal{C}^n$ consists of all $n$-tuples of colors, or colorings.
- The group $G$ acts on $\mathcal{C}^n$ by
  \[ \pi(c_1, c_2, \ldots, c_n) = (c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(n)}), \quad \pi \in G. \]
- An orbit of $(c_1, c_2, \ldots, c_n) \in \mathcal{C}^n$ is called a $(k, G)$-coloring of $X$. 
• Here we are double-loading the term $\pi$.

• Think of $G$ as a group of permutations $\pi$ on $X$.

• To be precise, the group action on $C^n$ is

$$\alpha_\pi(c_1, c_2, \ldots, c_n) = (c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(n)}), \quad \pi \in G.$$ 

• But our simplified notation should be clear enough.
2-Colorings of $4 \times 4$ Grid

• Color each square in a $4 \times 4$ grid black (b) or white (w).

• Let $X = \{1, 2, \ldots, 16\}$ consist of the 16 squares and $C = \{b, w\}$.

• Let $R$ denote the clockwise rotation by $90^\circ$.

\[
\begin{array}{cccc}
1 & 2 & 3 & 4 \\
5 & 6 & 7 & 8 \\
9 & 10 & 11 & 12 \\
13 & 14 & 15 & 16 \\
\end{array}
\quad 90^\circ \text{ rotation}
\]

\[
\begin{array}{cccc}
13 & 9 & 5 & 1 \\
14 & 10 & 6 & 2 \\
15 & 11 & 7 & 3 \\
16 & 12 & 8 & 4 \\
\end{array}
\]

• So $R$ is the following permutation:

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
4 & 8 & 12 & 16 & 3 & 7 & 11 & 15 & 2 & 6 & 10 & 14 & 1 & 5 & 9 & 13
\end{pmatrix}.
\]
2-Colorings of $4 \times 4$ Grid (continued)

• In terms of cycle decomposition,

$$R = (1 4 16 13)(2 8 15 9)(3 12 14 5)(6 7 11 10).$$

• $R$ “rotates” the $4 \times 4$ grid by $90^\circ$ clockwise.

• Note that $R$ turns one coloring into another.

• The cyclic group $G = \langle R \rangle$ acts on $C^{16}$.

• It is clear that $|G| = 4$.\(^{a}\)
  
  – In fact, $G = \{ I, R, R^2, R^3 \}$ as $R^4 = I$.

• A distinct coloring is now a $(2, G)$-coloring of $X$.

\(^{a}\)Or, one may quote Theorem 137 (p. 893).
2-Colorings of $4 \times 4$ Grid (continued)

- The number of distinct colorings is the number of orbits.
- By Burnside’s lemma (p. 927), it equals

$$\frac{|F(I)| + |F(R)| + |F(R^2)| + |F(R^3)|}{4}.$$ 

- The identity permutation $I$ fixes every coloring in $C^{16}$.
- So $|F(I)| = 2^{16}$.
- We proceed to calculate $|F(R)|$. 
2-Colorings of $4 \times 4$ Grid (continued)

- To be fixed by $R$, corner squares 1, 4, 16, 13 must have identical color.
- Similarly, squares 2, 8, 15, 9 must have identical color.
- Similarly, squares 3, 12, 14, 5 must have identical color.
- That covers all the border squares.
- Finally, the inner squares 6, 7, 11, 10 must have identical color.
- Note that each group corresponds to a cycle of $R$!
- Hence $|F(R)| = 2^4$ because there are 4 cycles.
2-Colorings of $4 \times 4$ Grid (continued)

- We move on to $R^2 = (1\ 16)(4\ 13)(2\ 15)(8\ 9)(3\ 14)(12\ 5)(6\ 11)(7\ 10)$.
- One can also show that $|F(R^2)| = 2^8$ because there are 8 cycles.
- Finally $|F(R^3)| = 2^4$ as $R^3$ has 4 cycles:

$$R^3 = (1\ 13\ 16\ 4)(2\ 9\ 15\ 8)(3\ 5\ 14\ 12)(6\ 10\ 11\ 7).$$
2-Colorings of $4 \times 4$ Grid (concluded)

- Our desired count is hence

$$\frac{2^{16} + 2^4 + 2^8 + 2^4}{2} = 16,456.$$ 

- Recall that the number of distinct colorings depends on the cycle structures$^a$ of group elements.

- This observation is in general true.

$^a$Roughly how many $i$-cycles are there for all $i$. 
Finite Fields and Combinatorial Designs
Fields Revisited

• A ring \((R, +, \cdot)\) is a field if \((R - \{0\}, \cdot)\) is an abelian group.
  - This means there is a multiplicative identity \(1 \neq 0\) and every nonzero element is a unit\(^a\) (review p. 761).

• Alternatively, \((R, +, \cdot)\) is a field if:
  - \((R, +)\) is an abelian group.
  - \((R - \{0\}, \cdot)\) is an abelian group.
  - The distributive law of \(\cdot\) over \(+\) holds.

\(^a\)That is, it has a multiplicative inverse.
Proper Divisors of Zero and Fields

**Theorem 149** If \((F, +, \cdot)\) is a field, then it has no proper divisors of zero.

- Let \(a, b \in F\) with \(a \cdot b = 0\).
- Suppose \(a \neq 0\) and \(b \neq 0\) instead.
- Then
  \[
  a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \implies (a^{-1} \cdot a) \cdot b = a^{-1} \cdot 0 \\
  \implies 1 \cdot b = a^{-1} \cdot 0 \\
  \implies b = 0,
  \]
  a contradiction.\(^a\)

\(^a\)See also Lemma 109 (p. 777).
Polynomials

- Let \((R, +, \cdot)\) be a ring.
- Let \(x\) denote an indeterminate—a formal symbol that is not an element of \(R\).
- Then

\[ f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \]

where \(a_i \in R\), is called a polynomial in the indeterminate \(x\) with coefficients from \(R\).
Polynomials (concluded)

- If $a_n \neq 0$, the $a_n$ is called the leading coefficient of $f(x)$, and the degree of $f(x)$ is $n$.

- A degree-0 polynomial is an element of $R$.

- $R[x]$ is the set of all polynomials in the indeterminate $x$ with coefficients from $R$. 
Polynomial Additions and Multiplications

• Let \( f(x) = \sum_{i=0}^{n} a_i x^i \) and \( g(x) = \sum_{i=0}^{m} b_i x^i \), with \( n \geq m \).

• \( f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i \), where \( b_i = 0 \) for \( i > m \).

• \( f(x) \cdot g(x) = \sum_{i=0}^{n+m} \left[ \sum_{j=0}^{i} (a_j \cdot b_{i-j}) \right] x^i \).

• Note that + and \( \cdot \) for polynomials are built on + and \( \cdot \) for elements of \( R \); they are not identical, however.

**Theorem 150** \( (R[x], +, \cdot) \) is a ring called the polynomial ring over \( R \).
The Ring Properties of $\mathbb{Z}_n$

- $(\mathbb{Z}_n, +, \cdot)$ is a ring, where both $+$ and $\cdot$ are modulo $n$.
- It is in fact abelian under $\cdot$ as well as $+$.
- Furthermore, it has a multiplicative identity, 1.
- From p. 795, we know each $a \in \mathbb{Z}_n$ has a multiplicative inverse $a^{-1}$ if and only if $\gcd(a, n) = 1$.
- Hence in $\mathbb{Z}_n$, $[a]$ is a unit\(^a\) if and only if $\gcd(a, n) = 1$.\(^b\)

\(^a\)I.e., $a \in \mathbb{Z}_n$ has a multiplicative inverse (p. 761).
\(^b\)Recall p. 789 for the notation $[a]$: All the integers congruent to $a$ modulo $n$. 
The Ring Properties of $\mathbb{Z}_n$ (concluded)

- For any positive integer $n > 1$, there are $\phi(n)$ units and $n - 1 - \phi(n)$ proper divisors of zero in $\mathbb{Z}_n$ (see p. 812).

- See p. 789 and p. 812 for more information.
When Is \( \mathbb{Z}_n \) a (Finite) Field?

**Theorem 151** \( \mathbb{Z}_n \) is a field if and only if \( n \) is a prime.

Proof (\( \Leftarrow \)):
- Verify each condition.

Proof (\( \Rightarrow \)):
- Suppose \( n = n_1 n_2 \) is not a prime, where \( 1 < n_1, n_2 < n \).
- Because \( n_1 n_2 \equiv 0 \, \text{mod} \, n \), we have \( n_1 \cdot n_2 = 0 \).
- As \( F \) has proper divisors of zero, it is not a field by Theorem 149 (p. 968).

\(^a\)Page 795 is helpful here.
A Finite Field with 4 Elements; Cannot Be $\mathbb{Z}_4$

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\cdot$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

\[\text{©2017 Prof. Yuh-Dauh Lyuu, National Taiwan University}\]
Application: Primality Testing Again

**Theorem 152** Let \( p > 2 \) be an odd integer. Then \( p \) is a prime if and only if

\[
a^{(p-1)/2} \equiv \pm 1 \mod p
\]

for all \( a \in \mathbb{Z}_p^* \).

Proof (\( \Rightarrow \)):

- Suppose \( p \) is a prime.
- By Fermat’s “little” theorem (p. 856), \( a^{p-1} \equiv 1 \mod p \) for all \( a \in \mathbb{Z}_p^* \).
The Proof (continued)

• Let \( p = 2p' + 1 \).

• Then \( a^{2p'} \equiv 1 \mod p \).

• Rearrange to obtain

\[
(a^{p'} - 1)(a^{p'} + 1) \equiv 0 \mod p.
\]

• As \( \mathbb{Z}_p \) is a field (p. 974), \( a^{p'} \equiv \pm 1 \mod p \).

• So

\[
a^{(p-1)/2} = a^{p'} \equiv \pm 1 \mod p.
\]
The Proof (continued)

Proof ($\iff$):

• By Theorem 151 (p. 974), it suffices to prove that $\mathbb{Z}_p$ is a field.

• $\mathbb{Z}_p$ is a ring (p. 972).

• Hence from p. 967, it remains to show:
  – A multiplicative inverse exists for every $a \in \mathbb{Z}_p^*$.
  – $\mathbb{Z}_p$ has a multiplicative identity not equal to 0.
The Proof (continued)

• Let \( a \in \mathbb{Z}_p^* \).

• Then

\[
a^{p-1} \equiv (\pm 1)^2 \equiv 1 \mod p
\]

by the assumption.

• Hence \( a \) has a nonzero multiplicative inverse \( a^{p-2} \mod p \) as

\[
aa^{p-2} = a^{p-1} \equiv 1 \mod p
\]

(see also p. 857).
The Proof (continued)

• Next let \( ab \equiv 0 \mod p \) for \( a, b \in \mathbb{Z}_p \) but \( b \not\equiv 0 \mod p \).

• Then \( b \) has a multiplicative inverse \( b^{-1} \) (p. 857).

• Now,

\[
 a \equiv a \left( bb^{-1} \right) \equiv \left( ab \right) b^{-1} \equiv 0b^{-1} \equiv 0 \mod p.
\]

• So \( \mathbb{Z}_p \) has no proper divisors of zero.

• Finally,

\[
 1 \equiv aa^{-1} \not\equiv 0 \mod p
\]

for any \( a \in \mathbb{Z}_p^* \) as a result.
The Proof (concluded)

• By the definition on p. 782, $\mathbb{Z}_p$ is a field.

• By Theorem 151 (p. 974), $p$ is a prime.
Polynomial Rings over $\mathbb{Z}_n$

- $\mathbb{Z}_n[x]$ is a polynomial ring because $\mathbb{Z}_n$ is a ring.
- The multiplication of two polynomials of degrees $n$ and $m$ may produce a polynomial of degree less than $n + m$.
- For example, in $\mathbb{Z}_8[x]$,

$$ (4x^2 + 1)(2x + 3) $$
$$ = 8x^3 + 12x^2 + 2x + 3 $$
$$ = 4x^2 + 2x + 3. $$
Polynomial Rings over a Field

- We shall limit polynomial rings $R[x]$ to cases where $R$ is a field from now on.

- The multiplication of two nonzero polynomials will produce a polynomial whose degree is the addition of the degrees of the original two polynomials.
  - Because a field has no proper divisors of zero, the product of two leading coefficients cannot be zero.
Number of Polynomials over $\mathbb{Z}_p$

**Lemma 153** There are $p^{n+1}$ polynomials of degree up to $n$ over $\mathbb{Z}_p$.\(^a\)

- A polynomial of degree $n$ over $\mathbb{Z}_p$ looks like
  \[\sum_{i=0}^{n} a_ix^i.\]
- There are $n + 1$ coefficients $a_i$.
- There are $p$ choices for each $a_i$.

\(^a\)Corrected by Mr. Chia-You Chen (B04611015) on June 16, 2016.
The Division Algorithm

- Let $f(x), g(x) \in F[x]$ with $f(x) \neq 0$.

- There exist unique polynomials $q(x), r(x) \in F[x]$ such that

\[ g(x) = q(x)f(x) + r(x), \]

where $r(x) = 0$ or $\deg r(x) < \deg f(x)$. 
Number of Roots

Theorem 154  If $f(x) \in F[x]$ has degree $n \geq 1$, then $f(x) = 0$ has at most $n$ roots in the field $F$.

- Use induction on the degree of $f(x)$.
- The theorem clearly holds when $\deg f(x) = 1$.
- In general, consider a polynomial $f(x)$ of degree $k + 1$.
- If $f(x) = 0$ has no roots in $F$, the theorem follows.
- Otherwise, assume $f(x) = 0$ has a root $r \in F$.
- Then $f(x) = (x - r)g(x)$, where $\deg g(x) = k$.
- By the induction hypothesis, $g(x) = 0$ has at most $k$ roots in $F$; thus $f(x) = 0$ has at most $k + 1$ roots in $F$. 
Irreducible Polynomials

• Let $f(x) \in F[x]$ with $F$ a field and $\deg f(x) \geq 2$.

• We call $f(x)$ reducible (over $F$) if:
  – There exist $g(x), h(x) \in F[x]$, where
    $$f(x) = g(x)h(x).$$
  – Each of $g(x), h(x)$ has degree at least one.

• If $f(x)$ is not reducible, it is called irreducible or prime.
Irreducible Polynomials (concluded)

- Every nonzero polynomial of degree at most one is irreducible.

- Testing irreducibility is not believed to be computationally easy unless factorization is easy.
Sieve Method to Enumerate Irreducible Polynomials over $\mathbb{Z}_p$

1: $P = \{ x, x + 1, \ldots, x + (p - 1) \}$;
2: {Find irreducible polynomials of degree $n$.}
3: for $n = 2, 3, \ldots$ do
4: for each polynomial $q(x)$ of degree $n$ over $\mathbb{Z}_p$ do
5: if $q_1(x) \not| q(x)$ for all $q_1(x) \in P$ with degree $< n$
     then
6:     $P := P \cup \{ q(x) \}$;
7: end if
8: end for
9: end for
Irreducible Polynomials over $\mathbb{Z}_2$

For polynomials over the binary field $\mathbb{Z}_2$, the irreducible polynomials are

\[
x, x + 1
\]
\[
x^2 + x + 1
\]
\[
x^3 + x + 1, x^3 + x^2 + 1
\]
\[
x^4 + x^3 + x^2 + x + 1, x^4 + x + 1, x^4 + x^3 + 1
\]
\[
:\vdots
\]
Greatest Common Divisors Again

• Let \( f(x), g(x) \in F[x] \).

• Then \( h(x) \in F[x] \) is a greatest common divisor of \( f(x) \) and \( g(x) \) if:
  
  – \( h(x) \) divides both \( f(x) \) and \( g(x) \).
  
  – \( k(x) \in F[x] \) and \( k(x) \) divides both \( f(x) \) and \( g(x) \), then \( k(x) \) divides \( h(x) \).
Greatest Common Divisors Again (concluded)

• A polynomial is **monic** if its leading coefficient is 1.

• A *monic* greatest common divisor, denoted by $\gcd(f(x), g(x))$, is unique.

• A greatest common divisor can be calculated by the Euclidean algorithm for polynomials.

• Two polynomials are **relatively prime** if their gcd is 1.
Congruence Modulo a Polynomial

- Let $f(x), g(x), s(x) \in F[x]$, and $s(x) \neq 0$.

- Write $f(x) \equiv g(x) \mod s(x)$ if $s(x)$ divides $f(x) - g(x)$.
  - We say $f(x)$ is congruent to $g(x)$ modulo $s(x)$.

- By the division algorithm, there exist polynomials $q(x), r(x) \in F[x]$ such that
  \[ f(x) = q(x)s(x) + r(x), \]
  where $r(x) = 0$ or $\deg r(x) < \deg s(x)$.

- Then $f(x) \equiv r(x) \mod s(x)$. 
Congruence Modulo a Polynomial Is an Equivalence Relation

Theorem 155 The relation $\mathcal{R}$ of congruence modulo a nonzero $s(x) \in F[x]$ is an equivalence relation.

- $p(x) \mathcal{R} p(x)$ because $s(x)$ divides $p(x) - p(x) = 0$.

- If $p(x) \mathcal{R} q(x)$ then $q(x) \mathcal{R} p(x)$ because $s(x)$ divides $p(x) - q(x)$ if and only if it divides $q(x) - p(x)$.

- If $p(x) \mathcal{R} q(x)$ and $q(x) \mathcal{R} r(x)$ then $p(x) \mathcal{R} r(x)$ because $s(x)$ divides

$$p(x) - r(x) = [p(x) - q(x)] + [q(x) - r(x)].$$
Application: A Lemma

Lemma 156 The weight of a polynomial over $\mathbb{Z}_2$ is the number of nonzero coefficients. For any polynomial $p(x)$ over $\mathbb{Z}_2$,

$$p(x)(x^{p-1} + x^{p-2} + \cdots + x + 1) \mod (x^p - 1) = \begin{cases} 
  x^{p-1} + x^{p-2} + \cdots + x + 1, & \text{if } p(x) \text{ has odd weight} \\
  0, & \text{if } p(x) \text{ has even weight}
\end{cases}$$

over $\mathbb{Z}_2$. 
The Proof

- Note that $x^i$ with integer $i$ has an odd weight.
- Use the division algorithm to verify the lemma when $p(x) = x^i$.
- As a result, in general, if $p(x)$ has $c$ nonzero terms, then the result is
  \[ c(x^{p-1} + x^{p-2} + \cdots + x + 1) \mod (x^p - 1). \]
  - If $c$ is even, the result is zero because $c \equiv 0 \mod 2$.
  - If $c$ is odd, the result is
    \[ x^{p-1} + x^{p-2} + \cdots + x + 1 \mod (x^p - 1) \]
    because $c \equiv 1 \mod 2$. 
Characteristic

• Let \( (R, +, \cdot) \) be a ring.

• Suppose there is a least positive integer \( n \) such \( nr = z \), the zero of \( R \), for all \( r \in R \).

  – Recall that \( nr \) means \( n \overbrace{r + r + \cdots + r}^{n} \), not \( n \cdot r \).

• Then we say \( R \) has characteristic \( n \).

• When no such integer exists, \( R \) is said to have characteristic 0.
Examples

- The ring \((\mathbb{Z}_n, +, \cdot)\) has characteristic \(n\).
  - Clearly, \(nr = 0 \mod n\) for all \(r \in \mathbb{Z}_n\).
  - Any other number \(m < n\) cannot cut it.

- The ring \((\mathbb{Z}, +, \cdot)\) has characteristic 0.

- The ring \(\mathbb{Z}_n[x]\) has characteristic \(n\).
  - Clearly, \(np(x) = 0\) for all polynomial \(p(x) \in \mathbb{Z}_n[x]\).
  - Any other number \(m < n\) cannot cut it.

  - Again, \(np(x)\) means \(\underbrace{p(x) + p(x) + \cdots + p(x)}_{n}\).
The Characteristic of a Field

**Theorem 157** The characteristic of a field must be zero or a prime.

- Let $n > 0$ be the characteristic.
- Write the unity of the field as $u$ to distinguish it from integer 1 for clarity.
- Suppose instead that $n = mk$, where $1 < m, k < n$.
- By definition, $nu = z$, the zero of the field.
- Hence,

  $$(mk)u = z.$$
The Proof (continued)

- But

\[(mk)u = \underbrace{mku + \cdots + mku}_{mk}\]

\[= \underbrace{u^2 + \cdots + u^2}_{mk}\]

\[= \underbrace{(mu + \cdots + mu)}_{m} \cdot \underbrace{(ku + \cdots + ku)}_{k}\]

\[= (mu) \cdot (ku).\]

- Note that \(u^2 = u\) (why?).
The Proof (concluded)

- As we are working with a field, \((mu) \cdot (ku) = z\) would imply \(mu = z\) or \(ku = z\).

- Assume \(ku = z\) (the case of \(mu = z\) is identical).

- Then for all \(r\) in the field,

\[
k r = k(u \cdot r) = u \cdot r + \cdots + u \cdot r
= (u + \cdots + u) \cdot r = (ku) \cdot r = z \cdot r = z.
\]

- This contradicts the assumption that \(n\) is the characteristic.
Order of a Finite Field

**Theorem 158** A finite field has order $p^t$ for some prime $p$ and some $t \in \mathbb{Z}^+$. ($p$ is the characteristic of the field.)

- Let $F$ be a finite field with characteristic $p$, a prime by Theorem 157 (p. 999).
- We will prove the theorem with this $p$.
- Let $u$ denote the unity and $z$ the zero of $F$. 
The Proof (continued)

• $S_0 \triangleq \{ u, 2u, \ldots, pu = z \}$ has size $p$.
  – Otherwise, $mu = nu$ for $1 \leq m < n \leq p$.
  – This implies that $(n - m)u = z$ with $0 < n - m < p$.
  – But then
    \[(n - m)x = (n - m)(u \cdot x) = [(n - m)u] \cdot x = z \cdot x = z\]
    for all $x \in F$ by Lemma 103 (p. 768).
    – This contradicts the choice of $p$ as the characteristic.

• If $S_0 = F$, then we are done.

• Otherwise, $S_0 \subset F$ and we can pick $a \in F - S_0$. 
The Proof (continued)

• $S_1 \triangleq \{ ma + nu \mid 1 \leq m, n \leq p \} \subseteq F$ has size $p^2$.
  
  – Suppose $|S_1| < p^2$.
  
  – Then
    
    $$m_1a + n_1u = m_2a + n_2u$$
    
    for $1 \leq m_1, m_2, n_1, n_2 \leq p$ with $m_1 - m_2 \neq 0$ or $n_1 - n_2 \neq 0$.
  
  – One can show that $m_1 - m_2 \neq 0$ and $n_1 - n_2 \neq 0$.
  
  – This implies $(m_1 - m_2)a = (n_2 - n_1)u \neq z$.
  
  – Pick $0 < k < p$ such that $k(m_1 - m_2) \equiv 1 \text{ mod } p$.
  
  – Then $a = k(m_1 - m_2)a = k(n_2 - n_1)u$.
  
  – So $a \in S_0$, a contradiction.
The Proof (concluded)

- If \( S_1 = F \), we are done.
- If not, simply continue this process with an element \( b \in F - S_1 \).
- We can prove that
  \[
  S_2 \overset{\Delta}{=} \{ \ell b + ma + nu \mid 1 \leq \ell, m, n \leq p \} \subseteq F
  \]
  has size \( p^3 \).
- Because \( F \) is finite, this procedure has to stop at some point with \( S_{t-1} = F \).
- Hence \( |F| = p^t \).
Algebra of Polynomials Modulo a Polynomial

- Let $s(x) \in F[x]$ be a nonzero polynomial.
- Consider the algebra of polynomials over $F$ where polynomial additions and multiplications are modulo $s(x)$.
- This algebra is a ring, denoted by $F[x]/(s(x))$.
  - Just go over each condition required of a ring.
Finite Field Representation

**Theorem 159** $F[x]/(s(x))$ is a field if and only if $s(x)$ is irreducible.

- We skip the proof.
- Let $p$ be a prime.
- If deg $s(x) = n$, then
  $$|\mathbb{Z}_p[x]/(s(x))| = p^n.$$  
- This is consistent with Theorem 158 (p. 1002).
The Galois Field

- Irreducible polynomial exists for any prime $p$ and $n \in \mathbb{Z}^+$.
- All finite fields of order $p^n$ are fundamentally identical.
- We call the finite field $\mathbb{Z}_p[x]/(s(x))$ when $s(x)$ is irreducible the **Galois field** of order $p^n$.
- It is denoted by $\text{GF}(p^n)$.
- By Theorem 159 (p. 1007), $\text{GF}(p^n)$ exists for any prime $p$ and any $n \in \mathbb{Z}^+$.

---

*A finite field is also called a Galois field.*
The Galois Field (concluded)

- $\text{GF}(p)$ is the field $\mathbb{Z}_p$ (also called a prime field).
- $\text{GF}(p^n)$, $n > 1$, is called an extension field.
- $\text{GF}(2^n)$ is called a binary field (see p. 975, e.g.).
Equations

- By Fermat-Euler’s theorem (p. 853), we know

\[ x^{p^n - 1} = 1 \]

for any \( x \in \text{GF}(p^n) \).

- Hence,

\[ x^{p^n} - x = \prod_{a \in \text{GF}(p^n)} (x - a). \]
Equations (concluded)

• In particular,

\[ x^{p-1} = 1 \mod p \]

for any \( 0 < x < p \) by Fermat’s “little” theorem (p. 856).

– Hence,

\[ x^p - x = \prod_{0 \leq a < p} (x - a). \]
An Example

• In $\mathbb{Z}_3[x],$

$$(x - 0)(x - 1)(x - 2)$$

$$= x^3 - 3x^2 + 2x$$

$$= x^3 + 2x$$

$$= x^3 - x.$$ 

• In $\mathbb{Z}_5[x],$

$$(x - 0)(x - 1)(x - 2)(x - 3)(x - 4)$$

$$= x^5 - 10x^4 + 35x^3 - 50x^2 + 24x$$

$$= x^5 + 24x$$

$$= x^5 - x.$$