Congruences and Residue Class Rings

(Chapter 2 of J. A. Buchmann, Introduction to Cryptography, 2nd Ed., 2004)

Shoichi Hirose

Faculty of Engineering, University of Fukui
Congruences

Definition (2.1.1)
a is congruent to \( b \) modulo \( m \) if \( m \mid b - a \).

\[ a \equiv b \pmod{m} . \]

Definition (Equivalence relation)
Let \( S \) be a non-empty set. A relation \( \sim \) is an equivalence relation on \( S \) if it satisfies

- **reflexivity** \( a \sim a \) for \( \forall a \in S \).
- **symmetry** \( a \sim b \Rightarrow b \sim a \) for \( \forall a, b \in S \).
- **transitivity** \( a \sim b \land b \sim c \Rightarrow a \sim c \) for \( \forall a, b, c \in S \).
Lemma (2.1.3)

The followings are equivalent

1. \( a \equiv b \pmod{m} \),
2. \( \exists k \in \mathbb{Z} \) s.t. \( b = a + km \),
3. \( a \mod m = b \mod m \).

Residue class of \( a \) modulo \( m \)

\[ \{ b \mid b \equiv a \pmod{m} \} = a + m\mathbb{Z} \]

It is an equivalence class.

\( \mathbb{Z}/m\mathbb{Z} \) is the set of residue classes mod \( m \). It has \( m \) elements.

\[ \mathbb{Z}/m\mathbb{Z} = \{ 0 + m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z} \} \]

A set of representatives for \( \mathbb{Z}/m\mathbb{Z} \) is a set of integers containing exactly one element of each residue class mod \( m \).
Example (2.1.5)

A set of representatives mod 3 contains an element of each of 0 + 3\(\mathbb{Z}\), 1 + 3\(\mathbb{Z}\), 2 + 3\(\mathbb{Z}\). Examples are \{0, 1, 2\}, \{3, −2, 5\}, \{9, 16, 14\}.

A set of representatives mod \(m\)

\[\mathbb{Z}_m \triangleq \{0, 1, \ldots, m - 1\}\]

is the set of least nonnegative residues mod \(m\).

Theorem (2.1.7)

\[a \equiv b \pmod{m} \land c \equiv d \pmod{m} \implies\]

- \(-a \equiv -b \pmod{m}\).
- \(a + c \equiv b + d \pmod{m}\).
- \(ac \equiv bd \pmod{m}\).
Definition (2.2.7)

\((H, \circ)\) is called a semigroup if

- \(\circ\) is closed: \(a \circ b \in H\) for every \(a, b \in H\),
- \(\circ\) is associative: \((a \circ b) \circ c = a \circ (b \circ c)\) for every \(a, b, c \in H\).

A semigroup is called **commutative** or **abelian** if \(a \circ b = b \circ a\) for \(\forall a, b \in H\).

Example (2.2.8)

\((\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Z}/m\mathbb{Z}, +), (\mathbb{Z}/m\mathbb{Z}, \cdot)\) are commutative semigroups.
Semigroups

Definition (2.2.9)

- A neutral element of a semigroup \((H, \circ)\) is \(e \in H\) s.t. 
  \[ e \circ a = a \circ e = a \quad \text{for } \forall a \in H. \]
- A semigroup \((H, \circ)\) is called a monoid if it has a neutral element.

Definition (2.2.10)

Let \(e\) be a neutral element of a monoid \((H, \circ)\). \(b \in H\) is called an inverse of \(a \in H\) if 
\[ a \circ b = b \circ a = e. \]
If \(a\) has an inverse, then it is called invertible.

Example (2.2.11)

- The neutral element of \((\mathbb{Z}, +)\) is 0. The inverse of \(a\) is \(-a\).
- The neutral element of \((\mathbb{Z}, \cdot)\) is 1. The invertible elements are \(1, -1\).
- The neutral element of \((\mathbb{Z}/m\mathbb{Z}, +)\) is the residue class \(m\mathbb{Z}\). The inverse of \(a + m\mathbb{Z}\) is \(-a + m\mathbb{Z}\).
A monoid is called a group if all of its elements are invertible.

- \((\mathbb{Z}, +)\) is an abelian group.
- \((\mathbb{Z}, \cdot)\) is not a group.
- \((\mathbb{Z}/m\mathbb{Z}, +)\) is an abelian group.

The order of a (semi)group is the number of its elements.

- The additive group \(\mathbb{Z}\) has infinite order.
- The additive group \(\mathbb{Z}/m\mathbb{Z}\) has order \(m\).
Definition (2.4.1)

A triplet \((R, +, \cdot)\) is called a ring if

- \((R, +)\) is an abelian group,
- \((R, \cdot)\) is a semigroup, and
- the distributivity law is satisfied: for every \(x, y, z \in R\),
  \[ x \cdot (y + z) = x \cdot y + x \cdot z \text{ and } (x + y) \cdot z = x \cdot z + y \cdot z. \]

The ring is called commutative if \((R, \cdot)\) is commutative. A unit element of the ring is a neutral element of \((R, \cdot)\).

Example (2.4.2)

- \((\mathbb{Z}, +, \cdot)\) is a commutative ring with unit element 1.
- \((\mathbb{Z}/m\mathbb{Z}, +, \cdot)\) is a commutative ring with unit element \(1 + m\mathbb{Z}\). It is called the residue class ring modulo \(m\).
Let \((R, +, \cdot)\) be a ring.

- \(a \in R\) is called invertible or unit if \(a\) is invertible in \((R, \cdot)\).
- \(a \in R\) is called zero divisor if \(a \neq 0\) and there exists some nonzero \(b \in R\) s.t. \(a \cdot b = 0\) or \(b \cdot a = 0\).

\((R, +, \cdot)\) is simply denoted by \(R\) if it is clear which operations are used.

The units of a commutative ring \(R\) form a group. It is called the unit group of \(R\) and is denoted by \(R^*\).
Fields

Definition (2.5.1)
A commutative ring is called a field if all of its nonzero elements are invertible.

Example (2.5.2)
- The set of integers is not a field.
- The set of rational numbers is a field.
- The set of real numbers is a field.
- The set of complex numbers is a field.
- The residue class ring modulo a prime is a field.
Definition (2.6.1)
Let \( R \) be a ring and \( a, n \in R \). \( a \) divides \( n \) if \( n = ab \) for \( \exists b \in R \).

Theorem (2.6.2)
- The residue class \( a + m\mathbb{Z} \) is invertible in \( \mathbb{Z}/m\mathbb{Z} \) iff \( \gcd(a, m) = 1 \).
- If \( \gcd(a, m) = 1 \), then the inverse of \( a + m\mathbb{Z} \) is unique.

Theorem (2.6.4)
The residue class ring \( \mathbb{Z}/m\mathbb{Z} \) is a field iff \( m \) is prime.
Theorem (2.7.1)

Suppose that the residue classes modulo $m$ are represented by their least non-negative representatives. Then, two residue classes modulo $m$ can be

- added or subtracted using time and space $O(\text{size}(m))$,
- multiplied or divided using time $O(\text{size}(m)^2)$ and space $O(\text{size}(m))$. 

Theorem (2.8.1)

The set of all invertible residue classes modulo $m$ is a finite abelian group with respect to multiplication. It is called the multiplicative group of residues modulo $m$ and is denoted by $(\mathbb{Z}/m\mathbb{Z})^*$. 

Example (2.8.2, The multiplicative group of residues modulo 12)

$$(\mathbb{Z}/12\mathbb{Z})^* = \{1 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 11 + 12\mathbb{Z}\}.$$ 

Definition (The Euler $\varphi$-function)

$\varphi : \mathbb{N} \to \mathbb{N}$ such that

$$\varphi(m) = \left| \{a \mid a \in \{1, 2, \ldots, m\} \land \gcd(a, m) = 1\} \right|.$$ 

The order of $(\mathbb{Z}/m\mathbb{Z})^*$ is $\varphi(m)$. 

S. Hirose (U. Fukui) Congruences and Residue Class Rings 13 / 44
Theorem (2.8.3)

\( p \text{ is prime} \Rightarrow \varphi(p) = p - 1. \)

Theorem (2.8.4)

\[
\sum_{d \mid m, d > 0} \varphi(d) = m.
\]

**Proof.** It is easy to see that \( \sum_{d \mid m, d > 0} \varphi(d) = \sum_{d \mid m, d > 0} \varphi(m/d). \)

\[
\varphi(m/d) = \left| \left\{ a \mid a \in \{1, 2, \ldots, m/d\} \land \gcd(a, m/d) = 1 \right\} \right|
\]
\[
= \left| \left\{ b \mid b \in \{1, 2, \ldots, m\} \land \gcd(b, m) = d \right\} \right|.
\]

On the other hand,

\[
\{1, 2, \ldots, m\} = \bigcup_{d \mid m, d > 0} \left\{ b \mid b \in \{1, 2, \ldots, m\} \land \gcd(b, m) = d \right\}.
\]
Example \( (m = 12) \)

\[
\sum_{\substack{d \mid 12, d > 0}} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12.
\]

\[
\sum_{\substack{d \mid 12, d > 0}} \varphi(12/d) = \varphi(12) + \varphi(6) + \varphi(4) + \varphi(3) + \varphi(2) + \varphi(1).
\]
Multiplicative Group of Residues mod $m$

\[ \varphi(1) = |\{a \mid a \in \{1\} \land \gcd(a, 1) = 1\}| = |\{12\}|. \]
\[ \varphi(2) = |\{a \mid a \in \{1, 2\} \land \gcd(a, 2) = 1\}| = |\{6\}|. \]
\[ \varphi(3) = |\{a \mid a \in \{1, 2, 3\} \land \gcd(a, 3) = 1\}| = |\{4, 8\}|. \]
\[ \varphi(4) = |\{a \mid a \in \{1, 2, 3, 4\} \land \gcd(a, 4) = 1\}| = |\{3, 9\}|. \]
\[ \varphi(6) = |\{a \mid a \in \{1, 2, 3, 4, 5, 6\} \land \gcd(a, 6) = 1\}| = |\{2, 10\}|. \]
\[ \varphi(12) = |\{a \mid a \in \{1, \ldots, 12\} \land \gcd(a, 12) = 1\}| = |\{1, 5, 7, 11\}|. \]
Order of Group Elements

Let $G$ be a group multiplicatively written with neutral element $1$.

**Definition (2.9.1)**

Let $g \in G$. If there exists a positive integer $e$ such that $g^e = 1$, then the smallest such integer is called the order of $g$. Otherwise, the order of $g$ is infinite.

The order of $g$ in $G$ is denoted by $\text{order}_G(g)$.

**Theorem (2.9.2)**

Let $g \in G$ and $e \in \mathbb{Z}$. Then, $g^e = 1$ iff $\text{order}_G(g) \mid e$.

**Example (2.9.4, $(\mathbb{Z}/13\mathbb{Z})^*$)**

<table>
<thead>
<tr>
<th>$k$</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>
</tr>
</thead>
<tbody>
<tr>
<td>$2^k \mod 13$</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>10</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>$4^k \mod 13$</td>
<td></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>
Theorem (2.9.5)

Suppose that $\text{order}_G(g) = e$ and $n$ is an integer. Then,

$$\text{order}_G(g^n) = e / \gcd(e, n).$$

Proof. Let $k = \text{order}_G(g^n)$. Since $$(g^n)^{e/\gcd(e, n)} = (g^e)^{n/\gcd(e, n)} = 1,$$

$k | e/\gcd(e, n)$.

Since $(g^n)^k = g^{nk} = 1$, $e | nk$. It implies $e/\gcd(e, n) | k$ since

$\gcd(e/\gcd(e, n), n) = 1$.

Thus, $k = e/\gcd(e, n)$. 

$\square$
Subgroups

Definition (2.10.1)

$U \subseteq G$ is called a subgroup of $G$ if $U$ is a group with respect to the group operation of $G$.

Example (2.10.2)

For $\forall g \in G$, the set $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ is a subgroup of $G$. It is called the subgroup generated by $g$.

Definition (2.10.4)

If $G = \langle g \rangle$ for $\exists g \in G$, then $G$ is called cyclic and $g$ is called a generator of $G$. 

Subgroups

Theorem (2.10.6)

If $G$ is finite and cyclic, then $G$ has exactly $\varphi(|G|)$ generators and they are all of order $|G|$.

Definition

A map $f : X \rightarrow Y$ is called

- **injective** if $f(x) = f(x') \Rightarrow x = x'$ for $\forall x, x' \in X$.
- **surjective** if for $\forall y \in Y$ there exists $x \in X$ s.t. $f(x) = y$.
- **bijective** if it is injective and surjective.

Theorem (2.10.9)

If $G$ is a finite group, then the order of each subgroup of $G$ divides the order $|G|$.
Let $H$ be a subgroup of $G$. Then, $|G|/|H|$ is called the index of $H$ in $G$. 
Fermat’s Little Theorem

Theorem (2.11.1, Fermat’s Little Theorem)

Let $a$ and $m$ be positive integers. Then,

$$\gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}.$$  

Theorem (2.11.2)

The order of every group element divides the group order.

Th. 2.11.2 follows from Th. 2.10.9.

Corollary (2.11.3)

$$g^{|G|} = 1 \text{ for } \forall g \in G.$$  

Th. 2.11.1 follows from Cor. 2.11.3.
Fast Exponentiation

The square-and-multiply method

Let \((e_{k-1}, e_{k-2}, \ldots, e_1, e_0)\) be the binary representation of \(e\), where \(e_i \in \{0, 1\}\) and \(e_0\) is the least significant bit.

**Example**

\[
e = e_0 + 2e_1 + 2^2e_2 + 2^3e_3 = e_0 + 2(e_1 + 2(e_2 + 2e_3))
\]

1. \(1^2 = 1\)
2. \(a^{e_3}1 = a^{e_3}\)
3. \((a^{e_3})^2 = a^{2e_3}\)
4. \(a^{e_2}a^{2e_3} = a^{e_2+2e_3}\)
5. \((a^{e_2+2e_3})^2 = a^{2(e_2+2e_3)}\)
6. \(a^{e_1}a^{2(e_2+2e_3)} = a^{e_1+2(e_2+2e_3)}\)
7. \((a^{e_1+2(e_2+2e_3)})^2 = a^{2(e_1+2(e_2+2e_3))}\)
8. \(a^{e_0}a^{2(e_1+2(e_2+2e_3))} = a^{e_0+2(e_1+2(e_2+2e_3))} = a^e\)
Fast Exponentiation

\[ a^e \mod n \] is computed with at most \( 2|e| \) modular multiplications (more precisely, \(|e| + \text{HW}(e)\)).

**Corollary (2.12.3)**

If \( e \) is an integer and \( a \in \{0, 1, \ldots, m - 1\} \), then \( a^e \mod m \) can be computed with time \( O(\text{size}(e)\text{size}(m)^2) \) and space \( O(\text{size}(e) + \text{size}(m)) \).
Let $b_{i,n-1}, b_{i,n-2}, \ldots, b_{i,0}$ be the binary expansion of $e_i$ for $1 \leq i \leq k$.

$$\prod_{i=1}^{k} g_i^{e_i} = \prod_{i=1}^{k} g_i^{b_{i,n-1}2^{n-1} + b_{i,n-2}2^{n-2} + \cdots + b_{i,0}2^0}$$

$$= \prod_{i=1}^{k} g_i^{b_{i,n-1}2^{n-1}} g_i^{b_{i,n-2}2^{n-2}} \cdots g_i^{b_{i,0}2^0}$$

$$= \left( \prod_{i=1}^{k} g_i^{b_{i,n-1}} \right)^{2^{n-1}} \left( \prod_{i=1}^{k} g_i^{b_{i,n-2}} \right)^{2^{n-2}} \cdots \left( \prod_{i=1}^{k} g_i^{b_{i,0}} \right)^{2^0}$$

Let $\prod_{i=1}^{k} g_i^{b_{i,j}} = G_j$ for $0 \leq j \leq n$. Then,
Fast Evaluation of Power Products

\[ \prod_{i=1}^{k} g_i^{e_i} = (G_{n-1})^{2^{n-1}} (G_{n-2})^{2^{n-2}} \cdots (G_0)^{2^0} \]

\[ = ((\cdots ((G_{n-1})^2 G_{n-2})^2 \cdots )G_1)^2 G_0 \]

Precomputation

\[ \prod_{i=1}^{k} g_i^{b_j} \quad \text{for all } (b_1, b_2, \ldots, b_k) \in \{0, 1\}^k \]
Computation of Element Orders

How to compute the order of \( g \in G \) when the prime factorization of \( |G| \) is known.

**Theorem (2.14.1)**

Let \( |G| = \prod_{p||G|} p^{e(p)} \). Let \( f(p) \) be the greatest integer s.t. \( g^{|G|/p^{f(p)}} = 1 \). Then,

\[
\text{order}(g) = \prod_{p||G|} p^{e(p) - f(p)}.
\]

**Proof.** Let \( |G| = p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k} \). Let \( \text{order}(g) = n \). Let \( f(p_i) = f_i \). Since \( n \mid |G| \),

\[
n = p_1^{e_1'}p_2^{e_2'} \cdots p_k^{e_k'}
\]

for \( e_i' \leq e_i \). Since \( n \mid |G|/p_i^{f_i} \), \( e_i' \leq e_i - f_i \). If \( e_j' \leq e_j - f_j \) for some \( j \), then, for \( f_j' = e_j - e_j' \geq f_j \), \( g^{|G|/p_j^{f_j'}} = 1 \). It contradicts the assumption that \( f_j \) is the greatest integer s.t. \( g^{|G|/p_j^{f_j}} = 1 \). Thus, \( e_j' = e_j - f_j \). \( \square \)
Corollary (2.14.3)

Let $n \in \mathbb{N}$. If $g^n = 1$ and $g^{n/p} \neq 1$ for every prime divisor $p$ of $n$, then $\text{order}(g) = n$. 
The Chinese Remainder Theorem

Let \( m_1, m_2, \ldots, m_n \) be pairwise co-prime positive integers. Then, for integers \( a_1, a_2, \ldots, a_n \),

\[
\begin{align*}
  x &\equiv a_1 \pmod{m_1} \\
  x &\equiv a_2 \pmod{m_2} \\
  &\vdots \\
  x &\equiv a_n \pmod{m_n}
\end{align*}
\]

has a unique solution in \( \{0, 1, \ldots, m - 1\} \), where \( m = \prod_{i=1}^{n} m_i \).
The solution is
\[
    x = \left( \sum_{i=1}^{n} a_i y_i M_i \right) \mod m,
\]
where, for \(1 \leq i \leq n,\)
\[
    M_i = \frac{m}{m_i},
\]
\[
    y_i = M_i^{-1} \mod n_i.
\]
Example

\begin{align*}
  x &\equiv 2 \pmod{7} \\
  x &\equiv 6 \pmod{8} \\
  x &\equiv 7 \pmod{11}
\end{align*}

\begin{align*}
  m &= 7 \times 8 \times 11 = 616 \\
  M_1 &= 88 \\
  M_2 &= 77 \\
  M_3 &= 56 \\
  y_1 &= 88^{-1} \pmod{7} = 4^{-1} \pmod{7} = 2 \\
  y_2 &= 77^{-1} \pmod{8} = 5^{-1} \pmod{8} = 5 \\
  y_3 &= 56^{-1} \pmod{11} = 1^{-1} \pmod{11} = 1
\end{align*}

\begin{align*}
  x &= 2 \times 88 \times 2 + 6 \times 77 \times 5 + 7 \times 56 \times 1 \pmod{616} = 590
\end{align*}
Decomposition of the Residue Class Ring

**Definition (2.16.1)**

Let $R_1, R_2, \ldots, R_n$ be rings. Their direct product $\prod_{i=1}^{n} R_i$ is the set of all $(r_1, r_2, \ldots, r_n) \in R_1 \times R_2 \times \cdots \times R_n$ with component-wise addition and multiplication.

- $\prod_{i=1}^{n} R_i$ is a ring.
- If $R_i$’s are commutative rings with unit elements $e_i$’s, then $\prod_{i=1}^{n} R_i$ is a commutative ring with unit element $(e_1, \ldots, e_n)$.

**Definition (2.16.3)**

Let $(X, \odot_1, \ldots, \odot_n)$ and $(Y, \diamond_1, \ldots, \diamond_n)$ be sets with $n$ operations. $f : X \to Y$ is called a homomorphism if $f(a \odot_i b) = f(a) \diamond_i f(b)$ for every $a, b \in X$ and $1 \leq i \leq n$. If $f$ is bijective, then it is called an isomorphism.
Decomposition of the Residue Class Ring

Example (2.16.4)

• If $m$ is a positive integer, then the map $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ s.t. $a \mapsto a + m\mathbb{Z}$ is a ring homomorphism.

• If $G$ is a cyclic group of order $n$ with generator $g$, then the map $\mathbb{Z}/n\mathbb{Z} \rightarrow G$ s.t. $e + n\mathbb{Z} \mapsto g^e$ is an isomorphism of groups.

Theorem (2.16.5)

Let $m_1, m_2, \ldots, m_n$ be pairwise coprime integers and let $m = \prod_{i=1}^{n} m_i$. Then, the map

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z} \quad \text{s.t.} \quad a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z})$$

is an isomorphism of rings.
Theorem (2.17.1)

Let \( m_1, \ldots, m_n \) be pairwise co-prime integers and \( m = \prod_{i=1}^{n} m_i \). Then,
\[
\varphi(m) = \prod_{i=1}^{n} \varphi(m_i).
\]

Proof. Th. 2.16.5 implies
\[
(\mathbb{Z}/m\mathbb{Z})^* \rightarrow \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z})^* \quad \text{s.t.} \quad a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z})
\]

is an isomorphism of groups. Actually, for \( x + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} \),
\[
\gcd(x, m) \neq 1 \iff \gcd(x, m_i) \neq 1 \text{ for some } i.
\]
Thus,
\[
x + m\mathbb{Z} \notin (\mathbb{Z}/m\mathbb{Z})^* \iff x + m_i\mathbb{Z} \notin (\mathbb{Z}/m_i\mathbb{Z})^* \text{ for } \exists i.
\]
Therefore,
\[
\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*| = \prod_{i=1}^{n} |(\mathbb{Z}/m_i\mathbb{Z})^*| = \prod_{i=1}^{n} \varphi(m_i).
\]
Theorem (2.17.2)

Let \( m > 0 \) be an integer and \( \prod_{p \mid m} p^{e(p)} \) be the prime factorization of \( m \). Then,

\[
\varphi(m) = \prod_{p \mid m} (p - 1)p^{e(p) - 1} = m \prod_{p \mid m} \frac{p - 1}{p}.
\]

Proof. From Th. 2.17.1,

\[
\varphi(m) = \prod_{p \mid m} \varphi(p^{e(p)}).
\]

Thus, the theorem follows from

\[
\varphi(p^{e(p)}) = |\{1, 2, \ldots, p^{e(p)} - 1\}| - (\# \ of \ p's \ multiples)
= p^{e(p)} - 1 - (p^{e(p)} - p)/p
= (p - 1)p^{e(p) - 1}.
\]
Polynomials

$R$ commutative ring with unit element $1 \neq 0$

polynomial in one variable over $R$

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

coefficients $a_0, \ldots, a_n \in R$

$R[X]$ the set of all polynomials in the variable $X$

$n$ degree of the polynomial $f$ if $a_n \neq 0$

monomial $a_nX^n$

If $f(r) = 0$, then $r$ is called zero of $f$.

sum of polynomials

product of polynomials
Let $K$ be a field.

**Lemma (2.19.1)**
The ring $K[X]$ has no zero divisors.

**Lemma (2.19.2)**
$f, g \in K[X] \land f, g \neq 0 \Rightarrow \deg(fg) = \deg(f) + \deg(g)$

**Theorem (2.19.3)**
Let $f, g \in K[X]$ and $g \neq 0$. Then, there exists unique $q, r \in K[X]$ s.t.
$f = qg + r$ and $r = 0$ or $\deg(r) < \deg(g)$.

**Example (2.19.4)**
Let $K = \mathbb{Z}/2\mathbb{Z}$.

$$x^3 + x + 1 = (x^2 + x)(x + 1) + 1$$
Corollary (2.19.6)

Let $f \in K[x]$ and $f \neq 0$. If $f(a) = 0$, then $f(x) = (x - a)q(x)$ for some $q \in K[x]$.

Corollary (2.19.8)

$f \in K[x] \wedge f \neq 0 \Rightarrow f$ has at most $\deg(f)$ zeros

Proof. Let $n = \deg(f)$. If $n = 0$, then $f \neq 0$ has no zero. Let $n \geq 1$. If $f(a) = 0$, then $f(x) = (x - a)q(x)$ and $\deg(q) = n - 1$. By the induction hypothesis, $q$ has at most $n - 1$ zeros. Thus, $f$ has at most $n$ zeros.

Example (2.19.9)

- $x^2 + x \in (\mathbb{Z}/2\mathbb{Z})[x]$ has zeros 0 and 1 in $\mathbb{Z}/2\mathbb{Z}$.
- $x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ has a zero 1 in $\mathbb{Z}/2\mathbb{Z}$.
- $x^2 + x + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ has no zero in $\mathbb{Z}/2\mathbb{Z}$.
GF($p^n$) for any prime $p$ and any integer $n \geq 1$
- GF stands for *Galois field*
- $p$ is called the *characteristic* of GF($p^n$)
- GF($p$) is called a *prime field*

Let $f$ be an *irreducible* polynomial of degree $n$ in $(\mathbb{Z}/p\mathbb{Z})[X]$.

The elements of GF($p^n$) are residue classes mod $f$.

Residue class of $g \in (\mathbb{Z}/p\mathbb{Z})[X]$ mod $f$

\[
g + f(\mathbb{Z}/p\mathbb{Z})[X] = \{g + fh | h \in (\mathbb{Z}/p\mathbb{Z})[X]\} = \{v | v \in (\mathbb{Z}/p\mathbb{Z})[X] \text{ and } v \equiv g \pmod{f}\}
\]

The number of different residue classes mod $f$ is $p^n$.
Example (2.20.2)

Residue classes in \((\mathbb{Z}/2\mathbb{Z})[X] \mod f(X) = X^2 + X + 1\) are

- \(0 + f(\mathbb{Z}/2\mathbb{Z})[X]\)
- \(1 + f(\mathbb{Z}/2\mathbb{Z})[X]\)
- \(X + f(\mathbb{Z}/2\mathbb{Z})[X]\)
- \(X + 1 + f(\mathbb{Z}/2\mathbb{Z})[X]\)

They are simply denoted by 0, 1, X, X + 1, respectively.

It can be shown that the fields with two distinct irreducible polynomials in \((\mathbb{Z}/p\mathbb{Z})[X]\) of degree \(n\) are isomorphic.
The Structure of the Unit Group of Finite Fields (1/2)

Theorem (2.21.1)

Let $K$ be a finite field with $q$ elements. Then, for $\forall d$ s.t. $d \mid q - 1$, there are exactly $\varphi(d)$ elements of order $d$ in the unit group $K^*$.

Proof. Let $\psi(d)$ be the number of elements of order $d$ in $K^*$. All the elements of order $d$ are zeros of $x^d - 1$.

Let $a \in K^*$ be an element of order $d$. Then, the zeros of $x^d - 1$ are $a^e$ ($e = 0, 1, \ldots, d - 1$). $a^e$ is of order $d$ iff $\gcd(e, d) = 1$ (Cor. 2.19.8). Thus, $\psi(d) > 0 \Rightarrow \psi(d) = \varphi(d)$.

If $\psi(d) = 0$ for $\exists d$ s.t. $d \mid q - 1$. Then,

$$ q - 1 = \sum_{d \mid q - 1} \psi(d) < \sum_{d \mid q - 1} \varphi(d) $$

which contradicts Th. 2.8.4.

$\square$
Corollary (2.21.3)

Let $K$ be a finite field with $q$ elements. Then, the unit group $K^*$ is cyclic of order $q - 1$. It has exactly $\varphi(q - 1)$ generators.
Structure of the Multiplicative Group of Residues Modulo a Prime Number

Corollary

For any prime $p$, the multiplicative group of residues mod $p$ is cyclic of order $p - 1$.

If the residue class $a + p\mathbb{Z}$ generates the multiplicative group of residues $(\mathbb{Z}/p\mathbb{Z})^*$, then $a$ is called a primitive root mod $p$. 
Example

For \((\mathbb{Z}/11\mathbb{Z})^*\), the number of the primitive elements is \(\varphi(10) = 4\).

\[
\begin{array}{cccccccccc}
\text{ord.} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 & 10 \\
3 & 3 & 9 & 5 & 4 & 1 & 3 & 9 & 5 & 4 & 1 \\
4 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 & 1 \\
5 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 & 1 \\
6 & 6 & 3 & 7 & 9 & 10 & 5 & 8 & 4 & 2 & 10 \\
7 & 7 & 5 & 2 & 3 & 10 & 4 & 6 & 9 & 8 & 10 \\
8 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 & 10 \\
9 & 9 & 4 & 3 & 5 & 1 & 9 & 4 & 3 & 5 & 1 \\
10 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\
\end{array}
\]