Rings and Modular Arithmetic
It you tackle a problem and seem to get stuck,
Just take it mod $p$ and you’ll have better luck.

— Tom M. Apostol (1955)
and Saunders MacLane (1973),
Where Are the Zeros of Zeta of $s$?
Rings\textsuperscript{a}

• Let $R$ be a nonempty set endowed with 2 \textit{closed} binary operations “+” and “·”.

• $(R, +, ·)$ is a \textbf{ring} if the following conditions hold for all $a, b, c \in R$.
  
  - $a + b = b + a$ (commutative law of $+$).
  
  - $a + (b + c) = (a + b) + c$ (associative law of $+$).
  
  - There exists $z \in R$ such that $a + z = z + a = a$ for every $a \in R$ (existence of identity for $+$).
  
  - For each $a \in R$, there is a $b \in R$ with $a + b = b + a = z$ (existence of inverse under $+$).

\textsuperscript{a}Named by David Hilbert (1862–1943).
Rings (concluded)

- (continued)
  - \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \) (associative law of \( \cdot \)).
  - \( a \cdot (b + c) = a \cdot b + a \cdot c \) and \((b + c) \cdot a = b \cdot a + c \cdot a\) for all \(a, b, c \in R\) (distributive laws of \( \cdot \) over \(+\)).

- The ring is said to be **commutative** if
  \[
  a \cdot b = b \cdot a
  \]
  for all \(a, b, \in R\).
Comments

- It is helpful but dangerous to think of "+" as addition and "." as multiplication.

- From the definitions,
  - A ring has an *additive* identity \( z \) (sometimes denoted by 0).
  - The *additive* inverse exists in a ring.
Comments (concluded)

• A ring may not have a *multiplicative* identity or **unity** denoted by 1 or $u$.\(^a\)
  
  – If it does, it is called a **ring with unity**.

• The *multiplicative* inverse is not guaranteed to exist in a ring.

• An element $b \in R$ is said to be $a$’s multiplicative inverse if $a \cdot b = b \cdot a = 1$.

• If $a \in R$ has a multiplicative inverse, then $a$ is called a **unit**.

\(^a\) $u \neq z$ and $a \cdot u = u \cdot a = a$ for all $a \in R$. 
Some Facts and Examples

- $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ are all rings.
  - The additive identity is 0.
  - The additive inverse of each number $x$ is $-x$.

- In any ring, the zero element $z$ (i.e., the additive identity) is unique.
  - If $z_1$ and $z_2$ are two additive identities, then
    \[ z_1 = z_1 + z_2 = z_2. \]
Some Facts and Examples (concluded)

- The additive inverse of each ring element is also unique.
  - For $a \in R$, suppose there are two elements $b, c \in R$ where
    
    $$a + b = b + a = z,$$
    $$a + c = c + a = z.$$

  - Then
    $$b = b + z = b + (a + c) = (b + a) + c = z + c = c.$$
A Useful Shorthand

• Let \((R, +, \cdot)\) be a ring.

• Consider \(kx\), where \(k \in \mathbb{Z}^+\) and \(x \in R\).

• This is clearly not an operation in \(R\) because \(k \notin R\).

• In fact, it is merely a shorthand for

\[
\underbrace{x + \cdots + x}_{k}.
\]
A Criterion for Commutativity

Lemma 95 Let \((R, +, \cdot)\) be a ring. It is commutative if and only if \((a + b)^2 = a^2 + 2(a \cdot b) + b^2\) for all \(a, b \in R\).

• Note that

\[(a + b)^2 = (a + b) \cdot (a + b) = a^2 + b \cdot a + a \cdot b + b^2.\]

• So if \((a + b)^2 = a^2 + 2(a \cdot b) + b^2\), then

\[2(a \cdot b) = a \cdot b + b \cdot a,\]

which implies \(a \cdot b = b \cdot a\).

• The other direction is trivial.
Rings with Sets

• Let \( U \) be a finite set.

• Consider \((2^U, \Delta, \cap)\).
  
  \(- A + B = A \Delta B\) (recall Eq. (23) on p. 186).
  
  \(- A \cdot B = A \cap B\), where \( A, B \subseteq U \).

• It is not hard to see that \((2^U, \Delta, \cap)\) is a ring with unity.

• The additive identity is \( \emptyset \).

• The multiplicative identity is \( U \).

• This example shows it is dangerous to think of “+” as addition and “·” as multiplication exclusively.
Generalized Distributive Laws

**Lemma 96** Let \((R, +, \cdot)\) be a ring. Then

\[
(a_1 + \cdots + a_m) \cdot (b_1 + \cdots + b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i \cdot b_j
\]

for \(m, n \in \mathbb{Z}^+\) and \(x, y \in R\).

Proof: It equals

\[
(a_1 + \cdots + a_m) \cdot b_1 + \cdots + (a_1 + \cdots + a_m) \cdot b_n
\]

\[
= a_1 \cdot b_1 + a_2 \cdot b_1 + \cdots + a_m \cdot b_n.
\]
Lemma 97  Let \((R, +, \cdot)\) be a ring. Then
\[(kx) \cdot (jy) = (kj)(x \cdot y)\] for \(k, j \in \mathbb{Z}^+\) and \(x, y \in R\).

Proof:
\[
(kx) \cdot (jy) = \underbrace{(x + \cdots + x)}_{k} \cdot \underbrace{(y + \cdots + y)}_{j}
= \underbrace{x \cdot y + \cdots + x \cdot y}_{kj}
= (kj)(x \cdot y),
\]
where the second equality is by Lemma 96 (p. 705).
Proper Divisor of Zero

- A ring may contain **proper divisors of zero**.
- \( a \) is a proper divisor of zero if \( a \neq 0 \) and there exists a \( b \neq 0 \) such that \( a \cdot b = 0 \) or \( b \cdot a = 0 \).
  - The set of \( 2 \times 2 \) integral matrices with matrix addition and multiplication is a ring.\(^a\)
  - But

\[
\begin{pmatrix}
1 & -1 \\
-1 & 1
\end{pmatrix}
\begin{pmatrix}
2 & 1 \\
2 & 1
\end{pmatrix}
= \begin{pmatrix}
0 & 0 \\
0 & 0
\end{pmatrix}.
\]

\(^a\)It is not commutative, however.
Units and Proper Divisors of Zero

Lemma 98  A unit in a ring $R$ cannot be a proper divisor of zero.

- Let $x \in R$ be a unit (recall p. 699).
- Hence there exists a $y \in R$ such that $x \cdot y = y \cdot x = 1$.
- Suppose $x \cdot w = 0$ for some $w \in R$.
- Then
  \[ y \cdot (x \cdot w) = y \cdot 0 = 0. \]
- On the other hand,
  \[ y \cdot (x \cdot w) = (y \cdot x) \cdot w = 1 \cdot w = w. \]
- As $w = 0$ and hence $x$ is not a proper divisor of zero.
Units and Proper Divisors of Zero in a Finite Commutative Ring

**Theorem 99** Let \((R, +, \cdot)\) be a finite commutative ring with unity 1. Then any nonzero element \(r \in R\) is either a unit or a proper divisor of zero.

- Assume \(r\) is not a proper divisor of zero and proceed to prove that it must be a unit.
- Consider the function \(f(a) = a \cdot r\) for all \(a \in R\).
The Proof (continued)

• $f$ is one-to-one (injective).
  – Otherwise, $a_1 \cdot r = a_2 \cdot r$ for some $a_1 \neq a_2$.
  – Let $b$ be the unique additive inverse of $a_2$.
  – But $a_1 + b \neq z$ because, otherwise,
    
    $a_2 = a_2 + z = a_2 + a_1 + b = a_2 + b + a_1 = z + a_1 = a_1$.
  
   – Now,
    
    $a_1 \cdot r + b \cdot r = a_2 \cdot r + b \cdot r = (a_2 + b) \cdot r = z \cdot r = z$.
  
  – But then $(a_1 + b) \cdot r = 0$.
  
  – As $r \neq 0$ and $a_1 + b \neq 0$, $r$ is a proper divisor of zero, a contradiction.
The Proof (concluded)

• Because \( f \) is from \( R \) to \( R \), it is also an onto function.

• As a result, there is an \( s \in R \) such that \( f(s) = 1 \).

• But \( f(s) = s \cdot r \).

• As \( R \) is commutative, \( s \cdot r = r \cdot s = 1 \).

• So \( r \) is a unit.
Remarks

- Theorem 99 (p. 709) is not valid when $R$ is infinite.
- For example, consider the ring $(\mathbb{Z}, +, \cdot)$.
- It is commutative and has unity 1.
- But any integer $n$ is neither a proper divisor of zero nor a unit as long as $n \not\in \{-1, 0, 1\}$.
Integral Domains and Fields

• Let \((R, +, \cdot)\) be a commutative ring with unity.

• \(R\) is called an integral domain if \(R\) has no proper divisors of zero.

• \(R\) is called a field\(^a\) if every nonzero element is a unit.

\(^a\)Evariste Galois (1811–1832).
Some Examples

• \((\mathbb{Z}, +, \cdot)\) is an integral domain but not a field.

• \((\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)\) are both integral domains and fields.
The Cancellation Laws of $+$

**Theorem 100** For all $a, b, c \in R$, (a) $a + b = a + c$ implies $b = c$, and (b) $b + a = c + a$ implies $b = c$.

- We focus on (a).
- As $a \in R$, it follows that $-a \in R$.
- Hence

$$a + b = a + c \Rightarrow (-a) + (a + b) = (-a) + (a + c)$$

$$\Rightarrow [(-a) + a] + b = [(-a) + a] + c$$

$$\Rightarrow z + b = z + c$$

$$\Rightarrow b = c.$$
A Corollary

Corollary 101  For any ring \((R, +, \cdot)\) and any \(a \in R\),

\[
a \cdot z = z \cdot a = z.
\]

- \(a \cdot z + a \cdot z = a \cdot (z + z) = a \cdot z\).

- By the left-cancellation property (p. 715), \(a \cdot z = z\).
Corollary 102  For any ring \((R, +, \cdot)\), for all \(a, b \in R\), \((a)\)
\(-(-a) = a\). \((b)\) \(a \cdot (-b) = (-a) \cdot b = -(a \cdot b)\). \((c)\)
\((-a) \cdot (-b) = a \cdot b\).

- \(-(-a)\) is the additive inverse of \(-a\).
- As \((-a) + a = z\), \(a\) is also the additive inverse of \(-a\).
- By the uniqueness of the additive inverse (p. 700),
\(-(-a) = a\), establishing \((a)\).
The Proof (concluded)

• \(-(a \cdot b)\) is the additive inverse of \(a \cdot b\).

• But

\[
a \cdot b + a \cdot (-b) = a \cdot [b + (-b)] = a \cdot z = z
\]

by Corollary 101 (p. 716).

• By the uniqueness of the additive inverse (p. 700),
\(a \cdot (-b) = -(a \cdot b)\), establishing part of (b).

• The other part of (b) can be proved similarly.

• From (b), \((-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)]\).

• Part (c) then follows from (a).
The Uniqueness of Unity

**Theorem 103** Let \((R, +, \cdot)\) be a ring with unity. (a) The unity is unique. (b) If \(x\) is a unit of \(R\), then the multiplicative inverse of \(x\) is unique.

- As a result, the unity of a ring with unity will be denoted by \(u\) or 1.
- Furthermore, the multiplicative inverse of each unit \(x\) will be denoted by \(x^{-1}\).
The Integers Modulo $n$

• Let $n \in \mathbb{Z}^+, \ n > 1$.

• For $a, b \in \mathbb{Z}$, we say $a$ is congruent\(^a\) to $b$ modulo $n$, written $a \equiv b \mod n$, if $n \mid (a - b)$.

• Congruence modulo $n$ is an equivalence relation on $\mathbb{Z}$ (prove it).

• Define $\mathbb{Z}_n$ to be the equivalence classes, or

$$\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}.$$  

\(^a\)Carl Friedrich Gauss.

\[\text{[This is more correct.]}\]
Elementary Facts about Arithmetics in $\mathbb{Z}_n$

- In $\mathbb{Z}_n$, all arithmetics are modulo $n$.
  - $5 + 6 \equiv 2 \text{ mod } 3$, and $5 \times 7 \equiv 2 \text{ mod } 3$.

- If $f(x_1, x_2, \ldots, x_n)$ is a polynomial with integer coefficients and $a_j \equiv b_j \text{ mod } m$ for $1 \leq j \leq n$, then
  $$f(a_1, a_2, \ldots, a_n) \equiv f(b_1, b_2, \ldots, b_n) \text{ mod } m.$$  
- $9^9 \text{ mod } 4 \equiv (9 \text{ mod } 4)^9 \equiv 1 \text{ mod } 4$. 
A Key Algorithm

- We are given two integers $m, n$.

- In many important applications, we need to find integers $m'$ and $n'$ such that

$$mm' + nn' = \gcd(m, n).$$

- This is called the extended Euclidean algorithm.
Extended Euclidean Algorithm

1: \((u_1, u_2, u_3) := (1, 0, m)\);
2: \((v_1, v_2, v_3) := (0, 1, n)\);
3: while \(v_3 \neq 0\) do
   4: \(q := \lfloor u_3/v_3 \rfloor\);
   5: \((t_1, t_2, t_3) := (u_1 - qv_1, u_2 - qv_2, u_3 - qv_3)\);
   6: \((u_1, u_2, u_3) := (v_1, v_2, v_3)\);
   7: \((v_1, v_2, v_3) := (t_1, t_2, t_3)\);
4: end while
6: \(m' := u_1\);
7: \(n' := u_2\);
8: \(gcd := u_3\);
9: return \((m', n', gcd)\);
An Example: $n = 100$ and $m = 17$

<table>
<thead>
<tr>
<th>$q$</th>
<th>$u_1$</th>
<th>$u_2$</th>
<th>$u_3$</th>
<th>$v_1$</th>
<th>$v_2$</th>
<th>$v_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>–</td>
<td>1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
<td>17</td>
<td>1</td>
<td>–5</td>
<td>15</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>–5</td>
<td>15</td>
<td>–1</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>–1</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>–47</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>–47</td>
<td>1</td>
<td>–17</td>
<td>100</td>
<td>0</td>
</tr>
</tbody>
</table>

We conclude that

$$100 \times 8 + 17 \times (–47) = 1,$$

which is true.
Inverses in \((\mathbb{Z}_n, \times)\)

- The \(x\) that solves \(ax \equiv 1 \mod m\) is \(a\)'s inverse denoted by \(a^{-1} \mod m\).

- \(\gcd(a, m) = 1\) is necessary to solve \(ax \equiv 1 \mod m\).
  - \(\gcd(a, m) > 1\) implies that \(\gcd(ax, m) > 1\).
  - That makes \(ax \equiv 1 \mod m\) unsolvable.
Inverses in \((\mathbb{Z}_n, \times)\) (continued)

- It is also sufficient to solve \(ax \equiv 1 \mod m\).
  - The extended Euclidean algorithm yields two integers \(a'\) and \(m'\) such that
    \[
    aa' + mm' = 1.
    \]
  - This implies \(aa' \equiv 1 \mod m\).
  - Thus \(x = a'\) is a solution.
Inverses in \((\mathbb{Z}_n, \times)\) (concluded)

- The solution to \(ax \equiv 1 \mod m\) is unique modulo \(m\).
  - Suppose there are two solutions \(0 \leq x', x'' < m\).
  - Then \(ax' \equiv 1 \mod m\) and \(ax'' \equiv 1 \mod m\).
  - This implies that \(a(x' - x'') \equiv 0 \mod m\).
  - Hence \(m | a(x' - x'')\).
  - Because \(\gcd(a, m) = 1\), we have \(m | (x' - x'')\).
  - It must be that \(x' = x''\).

- The inverse \(a^{-1} \mod m\) is hence unique.

- \(a^{-1} \mod m\) has nothing to do with \(1/a \in \mathbb{Q}\).
The Chinese Remainder Theorem

- Let $n = n_1 n_2 \cdots n_k$, where $n_i$ are pairwise relatively prime.

- Then for any integers $a_1, a_2, \ldots, a_k$, the set of simultaneous equations

  $\begin{align*}
  x &\equiv a_1 \mod n_1, \\
  x &\equiv a_2 \mod n_2, \\
  \vdots &
  \\
  x &\equiv a_k \mod n_k,
  \end{align*}$

  has a unique solution modulo $n$ for the unknown $x$. 
The Chinese Remainder Theorem (concluded)

• The solution can be written as a formula.
• Let \( m_i = n/n_i \) for \( i = 1, 2, \ldots, k \).\(^a\)
• The desired solution is

\[ x = a_1 c_1 + a_2 c_2 + \cdots + a_k c_k \mod n, \]

(remainder after division by \( n \)) where

\[ c_i = m_i (m_i^{-1} \mod n) \]

for \( i = 1, 2, \ldots, k \).

\(^a\)As \( m_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k \), we have \( m_i = 0 \mod n_j \) for \( j \neq i \).
An Example

• Let \( n = 5 \times 13 = 65 \).

• Consider the equations

\[
\begin{align*}
  x &\equiv 2 \mod 5, \\
  x &\equiv 3 \mod 13.
\end{align*}
\]

• Hence \( m_1 = 13 \) and \( m_2 = 5 \).

• Now verify that

\[
\begin{align*}
  13^{-1} &\equiv 2 \mod 5, \\
  5^{-1} &\equiv 8 \mod 13.
\end{align*}
\]
• Hence the solution is

\[ 2 \times [13 \times (13^{-1} \mod 5)] + 3 \times [5 \times (5^{-1} \mod 13)] \]
\[ = 2 \times (13 \times 2) + 3 \times (5 \times 8) \]
\[ = 2 \times 26 + 3 \times 40 \]
\[ = 172 \]
\[ \equiv 42 \mod 65. \]

• It is easy to confirm that, indeed,

\[ 42 \equiv 2 \mod 5 \]
\[ 42 \equiv 3 \mod 13 \]
Groups, Coding Theory, and Polya’s Method of Enumeration
The pursuit of mathematics is a divine madness of the human spirit.
— Alfred North Whitehead (1861–1947),
*Science and the Modern World*
Group Theory\textsuperscript{a}

- Let $G \neq \emptyset$ be a set and $\circ$ be a binary operation on $G$.

- $(G, \circ)$ is called a group if it satisfies the following.
  1. For all $a, b \in G$, $a \circ b \in G$ (closure).
  2. For all $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$ (associativity).
  3. There exists $e \in G$ with $a \circ e = e \circ a = a$ for all $a \in G$ (identity).
  4. For each $a \in G$, there is an element $b \in G$ such that $a \circ b = b \circ a = e$ (inverse).

- $G$ is commutative or abelian if $a \circ b = b \circ a$ for all $a, b \in G$.

\textsuperscript{a}Niels Henrik Abel (1802–1829) and Evariste Galois. This formal definition is by Cayley (1854).
A Loose End in Item 4?

- Can a “right” inverse be different from a “left” inverse?

- Suppose $a \circ b = e$ and $b' \circ a = e$.
  - $b$ is a right inverse of $a$.
  - $b'$ is a left inverse of $a$.

- Then $b' = b' \circ e = b' \circ (a \circ b) = (b' \circ a) \circ b = e \circ b = b$.

- Hence there is no point in distinguishing left and right inverses.

---

*aContributed by Mr. Bao (B90902039) on December 23, 2002.*
Examples of Groups

• Under ordinary $+$, $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are groups.
  – The inverse of $a$ is simply $-a$, which exists.

• Under ordinary $\times$, none of $(\mathbb{Z}, \times), (\mathbb{Q}, \times), (\mathbb{R}, \times), (\mathbb{C}, \times)$ are groups.
  – The number 0 has no inverses.

• Under ordinary $\times$, $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ are groups.
  – $A^*$ denotes the nonzero elements of $A$.

• Under ordinary $-$, $(\mathbb{Z}, -), (\mathbb{Q}, -), (\mathbb{R}, -)$ are not groups.
  – The associative axiom fails: $a - (b - c) \neq (a - b) - c$. 
Examples of Groups (concluded)

- \((Z_n, +)\) is an abelian group for \(n > 1\).
- But \((Z_n, \times)\) may not be a group for \(n > 1\).
- For all \(n \in \mathbb{Z}^+\), \(|(Z_n, +)| = n\).
The Group \((\mathbb{Z}_n^*, \times)\)

- Let \(\mathbb{Z}_n^*\) stand for the set of positive integers between 1 and \(n - 1\) that are relatively prime to \(n\).

- \((\mathbb{Z}_n^*, \times)\) is a group.
  - See pp. 725ff for the inverses modulo \(n\).

- By definition,
  \[
  \phi(n) \equiv |(\mathbb{Z}_n^*, \times)|. \tag{94}
  \]
  - \(\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}\).
  - Hence \(\phi(12) = 4\).
The Group \((\mathbb{Z}_n^*, \times)\) (concluded)

- In particular, \((\mathbb{Z}_p^*, \times)\) is an abelian group for prime \(p\).
- For all prime \(p\), \(|(\mathbb{Z}_p^*, \times)| = p - 1\).
  - Note that \(p - 1\) is not a prime.
Rings Revisited

• \((R, +, \cdot)\) is a ring if the following conditions hold.
  - \((R, +)\) is an abelian group.
  - \(a \cdot b \in R\) for all \(a, b \in R\) (closure).
  - \(a \cdot (b \cdot c) = (a \cdot b) \cdot c\) for all \(a, b, c \in R\) (associativity).
  - \(a \cdot (b + c) = a \cdot b + a \cdot c\) and \((b + c) \cdot a = b \cdot a + c \cdot a\) for all \(a, b, c \in R\) (distributive laws of \(\cdot\) over \(+\)).
Properties of Groups\textsuperscript{a}

• The identity of $G$ is unique.
  – If $e_1, e_2$ are both identities, then

$$e_1 = e_1 \circ e_2 = e_2$$

by the identity condition.

• The inverse of each element of $G$ is unique (it is $1/a$ under $\times$ and $-a$ under $+$, e.g.).
  – Suppose $b, c$ are both inverses of $a \in G$.
  – Then $b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c$.

\textsuperscript{a}Properties must be proved using only the four axioms or their logical corollaries.
The Cancellation Properties\(^a\)

The left-cancellation property: If \(a, b, c \in G\) and \(a \circ b = a \circ c\), then \(b = c\).

- \(b = (a^{-1} \circ a) \circ b = a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) = (a^{-1} \circ a) \circ c = c\).

The right-cancellation property: If \(a, b, c \in G\) and \(b \circ a = c \circ a\), then \(b = c\).

\(^a\)Recall Theorem 100 (p. 715).
Inverses

• \((a^{-1})^{-1} = a\).
  
  – Both are inverses of \(a^{-1}\) and inverses are unique.

• \((a \circ b)^{-1} = b^{-1} \circ a^{-1}\).
  
  – \((b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ b = e\).

• \((G, \circ)\) is abelian if and only if \((a \circ b)^{-1} = a^{-1} \circ b^{-1}\).
  
  – If \((G, \circ)\) is abelian, then
    
    \((a \circ b)^{-1} = (b \circ a)^{-1} = a^{-1} \circ b^{-1}\).
    
    – If \((a \circ b)^{-1} = a^{-1} \circ b^{-1}\), then \(a \circ b = ((a \circ b)^{-1})^{-1} = (a^{-1} \circ b^{-1})^{-1} = (b^{-1})^{-1} \circ (a^{-1})^{-1} = b \circ a\).
Powers

- The associative property implies that $a_1 \circ a_2 \circ \cdots \circ a_n$ is well-defined.

- For $n > 0$, define

\[
a^n = \underbrace{a \circ a \circ \cdots \circ a}_n.
\]

- For $n < 0$, define

\[
a^n = \underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{-n} = (a^{-1})^{-n}. \quad (95)
\]

  - Note that $a^{-n} = (a^{-1})^n$.

- Define $a^0 = e$. 
Powers (concluded)

• \((a^n)^{-1} = (a^{-1})^n\).
  
  - When \(n > 0\),
    \[
    a^n \circ (a^{-1})^n = a^{n-1} \circ a \circ a^{-1} \circ (a^{-1})^{n-1} \\
    = a^{n-1} \circ (a^{-1})^{n-1} \\
    = \cdots = e.
    \]

  - When \(n < 0\),
    \[
    a^n \circ (a^{-1})^n = (a^{-1})^{-n} \left( (a^{-1})^{-1} \right)^{-n} = e
    \]
    by Eq. (95) on p. 744.
Operations on Powers

Lemma 104 $a^n \circ a^m = a^{n+m}$ for $n, m \in \mathbb{Z}$.

- For $n, m \geq 0$,
  $$a^n \circ a^m = \underbrace{a \circ \cdots \circ a \circ a \circ \cdots \circ a}_{n+m} = a^{n+m}.$$

- For $n \geq 0, m < 0$, and $-m \leq n$,
  $$a^n \circ a^m = \underbrace{a \circ \cdots \circ a \circ a^{-1} \circ \cdots \circ a^{-1}}_{n+m} = \underbrace{a \circ \cdots \circ a}_{n-(-m)} = a^{n+m}.$$

- The other cases are similar.
Subgroups

- Let $(G, \circ)$ be a group.
- Let $\emptyset \neq H \subseteq G$.
- If $H$ is a group under $\circ$, we call it a **subgroup** of $G$.
- For example, the set of even integers is a subgroup of $(\mathbb{Z}, +)$.
- $H$ “inherits” $\circ$ from $G$ in that it is the same operation, producing the same result in both $G$ and $H$ wherever applicable.
Subgroups (concluded)

• Let \((G, \circ)\) be a group.

• Then \(\{ e \}\) and \(G\) are two trivial subgroups.
Criteria for Being a Subgroup

Only two axioms need to be checked.

**Theorem 105** Let $H$ be a nonempty subset of a group $(G, \circ)$. Then $H$ is a subgroup of $G$ if and only if (1) for all $a, b \in H$, $a \circ b \in H$ (closure), and (2) for all $a \in H$, $a^{-1} \in H$ (inverse).

Proof ($\Rightarrow$):

- Assume that $H$ is a subgroup of $G$.
- Then $H$ is a group.
- So $H$ satisfies, among other things, the closure axiom (1) and the inverse axiom (2).
The Proof (concluded)

Proof (⇐):

• Let $H \neq \emptyset$ satisfy (1) and (2).

• We need to verify the associative axiom and the existence of identity.
  
  – **Associativity:** For all $a, b, c \in H$,
    
    $$(a \circ b) \circ c = a \circ (b \circ c) \in G,$$
    
    hence in $H$ by (1).

  – **Identity:** For any arbitrary $a \in H$, $a^{-1} \circ a \in H$ by (2) and is an identity.
Simpler Criterion for Being a Subgroup

**Theorem 106** Let $H$ be a nonempty subset of a group $(G, \circ)$. Then $H$ is a subgroup of $G$ if and only if $a \circ b^{-1} \in H$ for all $a, b \in H$.

Proof ($\Rightarrow$):

- Obvious by the axioms of group theory.

Proof ($\Leftarrow$):

- First, $a \circ a^{-1} \in H$ for any $a \in H$.
- Hence $e = a \circ a^{-1} \in H$. 
The Proof (concluded)

• By Theorem 105 (p. 749), we only need to prove that if \( a \circ b^{-1} \in H \) for all \( a, b \in H \), then the closure and inverse axioms hold.

• **Inverse:** For any \( b \in H \), \( b^{-1} = e \circ b^{-1} \in H \).

• **Closure:** For any arbitrary \( a, b \in H \),
  \[ a \circ b = a \circ (b^{-1})^{-1} \in H. \]
Cyclic Groups

• A group $G$ is called **cyclic** if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in \mathbb{Z}$.

• In other words,

$$G = \{x^k : k \in \mathbb{Z}\}.$$ 

• $G$ is said to be **generated** by $x$, denoted by

$$G = \langle x \rangle.$$ 

• $x$ is called a **generator**, **primitive root**, or **primitive element**.\(^a\)

\(^a\)Paolo Ruffini (1765–1822).
Orders\(^a\) of Groups and Group Elements

- For every group \( G \), the number of elements in \( G \) is called the **order** of \( G \), denoted by \( |G| \).

- The **order** of \( a \in G \), written \( o(a) \), is the least *positive* integer \( n \) such that

\[
a^n = e.\]

- If a finite \( n \) does not exist, \( a \) has infinite order.

\(^a\)Paolo Ruffini.
Orders of Groups and Group Elements (concluded)

Lemma 107 *If* $n$ *is* $a$’s order and $a^k = e$, *then* $n | k$.

- Assume otherwise and $k = qn + r$, where $0 < r < n$.
- So
  \[ e = a^k = a^{qn+r} = a^{qn} a^r = a^r. \]
  - So $a$’s order is at most $r < n$, a contradiction.
Finiteness of Orders of Groups and Group Elements

**Lemma 108** If $G$ is a finite group, then the order of every element $a \in G$ must be finite.

- Consider the chain $a^1, a^2, a^3, \ldots$.
- Because $G$ is finite, the chain must eventually repeat itself.
- So there must be distinct $i < j$ such that $a^i = a^j$.
- By the cancellation property, $a^{j-i} = e$.
- As a result, $a$’s order is at most $j - i$.

---

*Contributed by Mr. Bao (B90902039) on December 23, 2002.*
Criterion for Being a Subgroup: The Finite Case

**Corollary 109** Let $H$ be a nonempty subset of a finite group $(G, \circ)$. Then $H$ is a subgroup of $G$ if and only if for all $a, b \in H$, $a \circ b \in H$ (closure).

- By Theorem 105 (p. 749), we only need to prove that if $a \circ b \in H$ for all $a, b \in H$, then $a^{-1} \in H$ for all $a \in H$ (inverse).
- Let $a \in H$.
- Then $a^m = e$ for some $m \in \mathbb{Z}$ by Lemma 108 (p. 756).
- Hence $a^{-1} = a^{m-1} \in H$. 

Finite Cyclic Groups

Lemma 110 Suppose $G$ is a finite group and $a \in G$. (1) $\langle a \rangle = \{a^k : k \in \mathbb{Z}^+\}$. (2) $|\langle a \rangle| = o(a)$.

- The set $\langle a \rangle \equiv \{a^k : k \in \mathbb{Z}\}$ contains at least
  
  $a, a^2, a^3, \ldots, a^{o(a)} = e$.

- But they are all distinct.
  - Otherwise, $a^i = a^j$ for $1 \leq i < j \leq o(a)$, and
    $a^{j-i} = e$, a contradiction because $j - i < o(a)$.

- As $a^m = a^{m \mod o(a)}$, there are no other elements.
Cyclic Subgroups

**Lemma 111** Let \((G, \circ)\) be a group and \(a \in G\). Then \(H = (\{a^k : k \in \mathbb{Z}\}, \circ)\) is a subgroup of \(G\).

- For \(a^i, a^j \in H\), we have
  \[ a^i \circ a^{-j} = a^{i-j} \in H \]
  by Lemma 104 (p. 746).

- Theorem 106 (p. 751) then implies the lemma.

**Corollary 112** Every finite group can be decomposed into disjoint cyclic subgroups.
Cosets\textsuperscript{a}

- If $H$ is a subgroup of $G$, the set $aH = \{a \circ h : h \in H\}$ is called a (left) coset of $H$ in $G$.

- $|aH| = |H|$ when $H$ is finite.\textsuperscript{b}
  - $|aH| \leq |H|$ by definition.
  - If $|aH| < |H|$, then $a \circ h_i = a \circ h_j$ for some distinct $h_i, h_j \in H$, which implies $h_i = h_j$ by the left-cancellation property, a contradiction.

- Similarly, we can also define a right coset of $H$ in $G$, denoted by $Ha$.

\textsuperscript{a}Augustin Louis Cauchy (1789–1857), who published more than 800 papers.

\textsuperscript{b}Contributed by Mr. Kai-Yuan Hou (B99201038) on June 7, 2012. Of course, if $G$ is finite, then $H$ must be, too.
Cosets as Partitions

- Let $G$ be a group.
- For $a, b \in G$, either $aH = bH$ or $aH \cap bH = \emptyset$.\(^a\)
  - Assume $aH \cap bH \neq \emptyset$.
  - Let $c = a \circ h_1 = b \circ h_2$ for some $h_1, h_2 \in H$.
  - If $x \in aH$, then $x = a \circ h$ for some $h \in H$ and
    
    $$x = (b \circ h_2 \circ h_1^{-1}) \circ h = b \circ (h_2 \circ h_1^{-1} \circ h) \in bH.$$  
  - So $aH \subseteq bH$.
  - Similarly, we can prove that $bH \subseteq aH$.

\(^a\)Do we need to require that $G$ be finite for this result as the textbook does? Contributed by Mr. Kai-Yuan Hou (B99201038) on June 7, 2012.
Cosets as Partitions (concluded)

- As

\[ a \in aH \quad \text{for any} \quad a \in G, \]

G can be partitioned by cosets.

1: print \( H \);
2: \( G := G - H \);
3: while \( G \neq \emptyset \) do
4: Pick \( a \in G \);
5: print \( aH \);
6: \( G := G - aH \);
7: end while
Constructing a Coset Partition of a Finite Group

\[ H \hspace{1cm} aH \hspace{1cm} bH \]

\[ e \hspace{1cm} a \hspace{1cm} b \hspace{1cm} \cdots \]
Lagrange’s\textsuperscript{a} Theorem

**Theorem 113** *If $G$ is a finite group with subgroup $H$, then $|H|$ divides $|G|$.*

- $G$ can be partitioned by cosets of $H$
- Each coset of $H$ has the same order, $|H|$.
- Hence $|H|$ divides $|G|$.

\textsuperscript{a}Joseph Louis Lagrange (1736–1813).
Applications of Lagrange’s Theorem

- Suppose $|G| = 16$, then the orders of its subgroups must be 1, 2, 4, 8, or 16.

- Suppose $|G| = 18$, then the orders of its subgroups must be 1, 2, 3, 6, 9, or 18.
First Corollary of Lagrange’s Theorem\textsuperscript{a}

Corollary 114 \textit{If} $G$ \textit{is a finite group and} $a \in G$, then $o(a)$ \textit{divides} $|G|$.

- The set generated by $a$, \{ $a^k : k \in \mathbb{Z}$ \}, has size $o(a)$ by Lemma 110 (p. 758).

- Set \{ $a^k : k \in \mathbb{Z}$ \} is a subgroup of $G$ by Lemma 111 (p. 759).

- Lagrange’s theorem then implies our claim.

\textsuperscript{a}See also Lemma 107 (p. 755).
The Fermat\textsuperscript{a}-Euler Theorem

**Theorem 115** If $G$ is a finite group, then every $a \in G$ satisfies

$$a^{|G|} = e.$$  

- By Corollary 114 (p. 766), $o(a)$ divides $|G|$.
- Let $|G| = o(a) \times k$, where $k \in \mathbb{Z}^+$.
- Now,
  $$a^{|G|} = a^{o(a) \times k} = (a^{o(a)})^k = e^k = e.$$  

\textsuperscript{a}Pierre de Fermat (1601–1665).
Euler’s Theorem

- Recall that $\mathbb{Z}_n^*$ is the set of positive integers between 1 and $n - 1$ that are relatively prime to $n$ (p. 738).
- Then $|\mathbb{Z}_n^*| = \phi(n)$ (p. 392).

**Theorem 116 (Euler’s theorem)** For all $a \in \mathbb{Z}_n^*$,

$$a^{\phi(n)} \equiv 1 \mod n.$$

- Prove that $(\mathbb{Z}_n^*, \times)$ is a group.
- Apply Theorem 115 (p. 767).
Fermat’s “Little” Theorem

Theorem 117 (Fermat’s “little” theorem) \( \text{Suppose } p \text{ is a prime. Then} \)

\[ a^{p-1} \equiv 1 \pmod{p} \]

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

\( \bullet \) By Euler’s theorem (p. 768).
Three Easy Applications

• The inverse of \( a \) in \( (\mathbb{Z}_p^*, \times) \) is \( a^{p-2} \mod p \).
  – \( a^{p-2}a = a^{p-1} \equiv 1 \mod p \) by Fermat’s “little” theorem.

• \( 3 \mid (n^2 - 1) \) when \( 3 \nmid n \).
  – The number 3 is a prime.
  – By Fermat’s “little” theorem, \( n^{3-1} \equiv 1 \mod 3 \).

• \( a^{p^n-p^{n-1}} \equiv 1 \mod p^n \) for odd prime \( p \) and \( \gcd(a, p) = 1 \).
  – By Euler’s theorem (p. 768) and Theorem 61 (p. 393),
    \[
    1 \equiv a^{\phi(p^n)} \equiv a^{p^n-p^{n-1}} \mod p^n.
    \]
Application: The RSA Function\textsuperscript{a}

- Let $n \equiv pq$, where $p$ and $q$ are distinct odd primes.
- Then $\phi(n) = (p - 1)(q - 1)$ by Theorem 61 (p. 393).
- Let $e$ be an odd integer relatively prime to $\phi(n)$.\textsuperscript{b}
- The RSA function is defined as

\[ E(x) = x^e \mod n, \]

where $\gcd(x, n) = 1$.

\textsuperscript{a}Rivest, Shamir, and Adleman (1978).
\textsuperscript{b}This $e$ should not be confused with the identity element.
Adi Shamir, Ron Rivest, and Leonard Adleman
Encryption Using the RSA Function

- The RSA function is a good candidate for the encryption of message $x$.
- The number $e$ is called the encryption key.
Decryption and Trapdoor Information

- To be useful, an efficient algorithm must exist for recovering $x$ from $E(x)$.
- But this is difficult (so far).
- The way out is the existence of the trapdoor information not available to the enemies.
- One possible piece of trapdoor information is the factorization of $n$.
  - Recall that factorization is believed to be hard.
Inversion of the RSA Function

• Let $d$ be the inverse of $e$ modulo $\phi(n)$, that is,

$$ed = 1 \mod \phi(n).$$

• Because $\gcd(e, \phi(n)) = 1$, such $d$ exists.
  - $d$ can be found by the extended Euclidean algorithm (p. 723).

• The encrypted message $y \equiv E(x)$ can be decrypted by

$$y^d \mod n.$$

  - By Euler’s theorem (p. 768),

$$y^d = (x^e)^d = x^{ed} = x^{1+k\phi(n)} = x x^{k\phi(n)} = x \mod n.$$
Security of the RSA Function (for Now)

- No one knows how to factor large numbers efficiently.
- No one knows how to calculate $d$ efficiently from $E(x)$ and $n$ without knowing $n$’s factors $p$ and $q$.
- No one knows how to calculate $\phi(n) = (p - 1)(q - 1)$ efficiently from $n$ without knowing $n$’s factors.
- Hence, $d$ cannot be found efficiently even if we know $n$ and $e$.
- Although it is conceivable that $d$ can be efficiently calculated without factoring $n$, no one has done it yet.
Sophie Germain Primes

- How many $e$’s are there such that $\gcd(e, \phi(n)) = 1$?
- The density of numbers between 1 and $\phi(n)$ that satisfy the above condition is

$$\frac{\phi(\phi(n))}{\phi(n)} = \frac{\phi((p - 1)(q - 1))}{(p - 1)(q - 1)}.$$ 

\(^a\)The 5th edition of Grimaldi’s *Discrete and Combinatorial Mathematics* errs with $\phi(n)/n$ on p. 760.
Sophie Germain Primes (concluded)

- Suppose $p = 2p' + 1$ and $q = 2q' + 1$, where $p', q'$ are also primes.
  - Such primes are called **Sophie Germain primes**.

- The density becomes

$$\frac{\phi(4p'q')}{(p - 1)(q - 1)} = \frac{2(p' - 1)(q' - 1)}{4p'q'} \approx \frac{1}{2}.$$
Sophie Germain (1776–1831)

- A French mathematician.

- Gauss on Germain: “But when a person of the sex which, according to our customs and prejudices, must encounter infinitely more difficulties than men to familiarize herself with these thorny researches, succeeds nevertheless in surmounting these obstacles and penetrating the most obscure parts of them, then without doubt she must have the noblest courage, quite extraordinary talents and superior genius.”