Introduction to Number Theory 1
Division

Definition: Let $a$ and $b$ be integers. We say that $a$ divides $b$, or $a|b$ if $\exists d$ s.t. $b = ad$. If $b \neq 0$ then $|a| \leq |b|$.

Division Theorem: For any integer $a$ and any positive integer $n$, there are unique integers $q$ and $r$ such that $0 \leq r < n$ and $a = qn + r$.

The value $r = a \mod n$ is called the remainder or the residue of the division.

Theorem: If $m|a$ and $m|b$ then $m|\alpha a + \beta b$ for any integers $\alpha, \beta$.

Proof: $a = rm; b = sm$ for some $r, s$. Therefore, $\alpha a + \beta b = \alpha rm + \beta sm = m(\alpha r + \beta s)$, i.e., $m$ divides this number. QED
**Division (cont.)**

If \( n | (a - b) \), i.e., \( a \) and \( b \) have the same residues modulo \( n \): \( (a \mod n) = (b \mod n) \), we write \( a \equiv b \pmod{n} \) and say that \( a \) is congruent to \( b \) modulo \( n \).

The integers can be divided into \( n \) equivalence classes according to their residue modulo \( n \):

\[
[a]_n = \{a + kn : k \in \mathbb{Z}\}
\]

\[
Z_n = \{[a]_n : 0 \leq a \leq n - 1\}
\]

or briefly

\[
Z_n = \{0, 1, \ldots, n - 1\}
\]
Greatest Common Divisor

Let $a$ and $b$ be integers.

1. $\text{gcd}(a, b)$ (the greatest common divisor of $a$ and $b$) is

   $$\text{gcd}(a, b) \triangleq \max\{d : d|a \text{ and } d|b\}$$

   (for $a \neq 0$ or $b \neq 0$).

   Note: This definition satisfies $\text{gcd}(0, 1) = 1$.

2. $\text{lcm}(a, b)$ (the least common multiplier of $a$ and $b$) is

   $$\text{lcm}(a, b) \triangleq \min\{d > 0 : a|d \text{ and } b|d\}$$

   (for $a \neq 0$ and $b \neq 0$).

3. $a$ and $b$ are coprimes (or relatively prime) iff $\text{gcd}(a, b) = 1$.  

© Eli Biham - October 18, 2015 242 Introduction to Number Theory 1 (10)
**Greatest Common Divisor (cont.)**

**Theorem:** Let $a, b$ be integers, not both zero, and let $d$ be the smallest positive element of $S = \{ax + by : x, y \in \mathbb{Z}\}$. Then, $\gcd(a, b) = d$.

**Proof:** $S$ contains a positive integer because $|a| \in S$.

By definition, there exist $x, y$ such that $d = ax + by$. $d \leq |a|$, thus there exist $q, r$ such that

$$a = qd + r, \quad 0 \leq r < d.$$ 

Thus,

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy) \in S.$$ 

$r < d$ implies $r = 0$, thus $d|a$.

By the same arguments we get $d|b$.

$d|a$ and $d|b$, thus $d \leq \gcd(a, b)$.

On the other hand $\gcd(a, b)|a$ and $\gcd(a, b)|b$, and thus $\gcd(a, b)$ divides any linear combination of $a, b$, i.e., $\gcd(a, b)$ divides all elements in $S$, including $d$, and thus $\gcd(a, b) \leq d$. We conclude that $d = \gcd(a, b)$. QED
Greatest Common Divisor (cont.)

**Corollary:** For any $a$, $b$, and $d$, if $d|a$ and $d|b$ then $d|\gcd(a, b)$.

**Proof:** $\gcd(a, b)$ is a linear combination of $a$ and $b$.

**Lemma:** For $m \neq 0$

$$\gcd(ma, mb) = |m| \gcd(a, b).$$

**Proof:** If $m \neq 0$ (WLOG $m > 0$) then $\gcd(ma, mb)$ is the smallest positive element in the set $\{amx + bmy\}$, which is $m$ times the smallest positive element in the set $\{ax + by\}$. 
**Greatest Common Divisor (cont.)**

**Corollary:** $a$ and $b$ are coprimes iff

$$\exists x, y \text{ such that } xa + yb = 1.$$  

**Proof:**

($\Leftarrow$) Let $d = \gcd(a, b)$, and $xa + yb = 1$. $d|a$ and $d|b$ and therefore, $d|1$, and thus $d = 1$.

($\Rightarrow$) $a$ and $b$ are coprimes, i.e., $\gcd(a, b) = 1$. Using the previous theorem, 1 is the smallest positive integer in $S = \{ ax + by : x, y \in \mathbb{Z} \}$, i.e., $\exists x, y$ such that $ax + by = 1$. QED
Euclid’s Lemma

Euclid’s Lemma: If $c|ab$ and $\gcd(b, c) = 1$ then $c|a$.

Proof: We know that $c|ab$. Clearly, $c|ac$.

Thus,

$$c| \gcd(ab, ac) = a \cdot \gcd(b, c) = a \cdot 1 = a.$$ 

QED
Prime Numbers and Unique Factorization

Definition: An integer $p \geq 2$ is called prime if it is divisible only by 1 and itself.

Theorem: Unique Factorization (Fundamental Theorem of Arithmetic): Every positive number can be represented as a product of primes in a unique way, up to a permutation of the order of primes.
Prime Numbers and Unique Factorization (cont.)

Proof: Every number can be represented as a product of primes, since if one element is not a prime, it can be further factored into smaller primes.

Assume that some number can be represented in two distinct ways as products of primes:

\[ p_1p_2p_3 \cdots p_s = q_1q_2q_3 \cdots q_r \]

where all the factors are prime, and no \( p_i \) is equal to some \( q_j \) (otherwise discard both from the product).

Then,

\[ p_1 | q_1q_2q_3 \cdots q_r. \]

But \( \gcd(p_1, q_1) = 1 \) and thus

\[ p_1 | q_2q_3 \cdots q_r. \]

Similarly we continue till

\[ p_1 | q_r. \]

Contradiction. QED
Euclid’s Algorithm

Let $a$ and $b$ be two positive integers, $a > b > 0$. Then the following algorithm computes $\gcd(a, b)$:

$r_{-1} = a$
$r_0 = b$

for $i$ from 1 until $r_i = 0$

$\exists q_i, r_i : r_{i-2} = q_i r_{i-1} + r_i$ and $0 \leq r_i < r_{i-1}$

$k = i-1$

Example: $a = 53$ and $b = 39$.

\[
\begin{align*}
53 &= 1 \cdot 39 + 14 \\
39 &= 2 \cdot 14 + 11 \\
14 &= 1 \cdot 11 + 3 \\
11 &= 3 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{align*}
\]

Thus, $\gcd(53, 39) = 1$. 
Extended Form of Euclid’s Algorithm

Example (cont.): \( a = 53 \) and \( b = 39 \).

\[
\begin{align*}
53 &= 1 \cdot 39 + 14 \quad \Rightarrow \quad 14 &= 53 - 39 \\
39 &= 2 \cdot 14 + 11 \quad \Rightarrow \quad 11 &= 39 - 2 \cdot 14 = -2 \cdot 53 + 3 \cdot 39 \\
14 &= 1 \cdot 11 + 3 \quad \Rightarrow \quad 3 &= 14 - 1 \cdot 11 = 3 \cdot 53 - 4 \cdot 39 \\
11 &= 3 \cdot 3 + 2 \quad \Rightarrow \quad 2 &= 11 - 3 \cdot 3 = -11 \cdot 53 + 15 \cdot 39 \\
3 &= 1 \cdot 2 + 1 \quad \Rightarrow \quad 1 &= 3 - 1 \cdot 2 = 14 \cdot 53 - 19 \cdot 39 \\
2 &= 2 \cdot 1 + 0
\end{align*}
\]

Therefore, \( 14 \cdot 53 - 19 \cdot 39 = 1 \).

We will use this algorithm later as a modular inversion algorithm, in this case we get that \((-19) \cdot 39 \equiv 34 \cdot 39 \equiv 1 \pmod{53}\).

Note that every \( r_i \) is written as a linear combination of \( r_{i-1} \) and \( r_{i-2} \), and ultimately, \( r_i \) is written as a linear combination of \( a \) and \( b \).
Proof of Euclid’s Algorithm

Claim: The algorithm stops after at most $O(\log a)$ steps.

Proof: It suffices to show that in each step $r_i < r_{i-2}/2$:

For $i = 1$: $r_1 < b < a$ and thus in $a = q_1 b + r_1$, $q_1 \geq 1$. Therefore, $a \geq 1b + r_1 > r_1 + r_1$, and thus $a/2 > r_1$.

For $i > 1$: $r_i < r_{i-1} < r_{i-2}$ and thus $r_{i-2} = q_i r_{i-1} + r_i$, $q_i \geq 1$. Therefore, $r_{i-2} \geq 1r_{i-1} + r_i > r_i + r_i$, and thus $r_{i-2}/2 > r_i$.

After at most $2 \log a$ steps, $r_i$ reduces to zero. QED
Proof of Euclid’s Algorithm (cont.)

Claim: \( r_k = \gcd(a, b) \).

Proof:

\( r_k \mid \gcd(a, b) \): \( r_k \mid r_{k-1} \) because of the stop condition. \( r_k \mid r_k \) and \( r_k \mid r_{k-1} \) and therefore \( r_k \) divides any linear combination of \( r_{k-1} \) and \( r_k \), including \( r_{k-2} \). Since \( r_k \mid r_{k-1} \) and \( r_k \mid r_{k-2} \), it follows that \( r_k \mid r_{k-3} \). Continuing this way, it follows that \( r_k \mid a \) and that \( r_k \mid b \), thus \( r_k \mid \gcd(a, b) \).

\( \gcd(a, b) \mid r_k \): \( r_k \) is a linear combination of \( a \) and \( b \); \( \gcd(a, b) \mid a \) and \( \gcd(a, b) \mid b \), therefore, \( \gcd(a, b) \mid r_k \).

We conclude that \( r_k = \gcd(a, b) \). QED
Groups

A group \((S, \oplus)\) is a set \(S\) with a binary operation \(\oplus\) defined on \(S\) for which the following properties hold:

1. **Closure**: \(a \oplus b \in S\) for all \(a, b \in S\).
2. **Identity**: There is an element \(e \in S\) such that \(e \oplus a = a \oplus e = a\) for all \(a \in S\).
3. **Associativity**: \((a \oplus b) \oplus c = a \oplus (b \oplus c)\) for all \(a, b, c \in S\).
4. **Inverses**: For each \(a \in S\) there exists an unique element \(b \in S\) such that \(a \oplus b = b \oplus a = e\).

If a group \((S, \oplus)\) satisfies the **commutative law** \(a \oplus b = b \oplus a\) for all \(a, b \in S\) then it is called an **Abelian group**.

**Definition**: The **order** of a group, denoted by \(|S|\), is the number of elements in \(S\). If a group satisfies \(|S| < \infty\) then it is called a **finite group**.

**Lemma**: \((Z_n, +_n)\) is a finite Abelian **additive group** modulo \(n\).
Groups (cont.)

Basic Properties:

Let:

\[ a^k = \bigoplus_{i=1}^{k} a = a \oplus a \oplus \ldots \oplus a. \]

\[ a^0 = e \]

1. The identity element \( e \) in the group is unique.

2. Every element \( a \) has a **single** inverse, denoted by \( a^{-1} \). We define \( a^{-k} = \bigoplus_{i=1}^{k} a^{-1} \).

3. \( a^m \oplus a^n = a^{m+n} \).

4. \( (a^m)^n = a^{nm} \).
Groups (cont.)

**Definition:** The order of $a$ in a group $S$ is the least $t > 0$ such that $a^t = e$, and it is denoted by $\text{order}(a, S)$.

For example, in the group $(\mathbb{Z}_3, +_3)$, the order of 2 is 3 since $2 + 2 \equiv 4 \equiv 1$, $2 + 2 + 2 \equiv 6 \equiv 0$ (and 0 is the identity in $\mathbb{Z}_3$).
Subgroups

**Definition:** If \((S, \oplus)\) is a group, \(S' \subseteq S\), and \((S', \oplus)\) is also a group, then \((S', \oplus)\) is called a **subgroup** of \((S, \oplus)\).

**Theorem:** If \((S, \oplus)\) is a finite group and \(S'\) is any subset of \(S\) such that \(a \oplus b \in S'\) for all \(a, b \in S'\), then \((S', \oplus)\) is a subgroup of \((S, \oplus)\).

**Example:** \(\{0, 2, 4, 6\}, +_8\) is a subgroup of \((\mathbb{Z}_8, +_8)\), since it is closed under the operation \(+_8\).

**Lagrange’s theorem:** If \((S, \oplus)\) is a finite group and \((S', \oplus)\) is a subgroup of \((S, \oplus)\) then \(|S'|\) is a divisor of \(|S|\).
Subgroups (cont.)

Let $a$ be an element of a finite group $S$, denote by $(\langle a \rangle, \oplus)$ the set:

$$\langle a \rangle = \{a^k : \text{order}(a, S) \geq k \geq 1\}$$

**Theorem:** $\langle a \rangle$ contains $\text{order}(a, S)$ distinct elements.

**Proof:** Assume by contradiction that there exists $1 \leq i < j \leq \text{order}(a, S)$, such that $a^i = a^j$. Therefore, $e = a^{j-i}$ – in contradiction to fact that $\text{order}(a, S) > j - i > 0$. QED

**Lemma:** $\langle a \rangle$ is a subgroup of $S$ with respect to $\oplus$.

We say that $a$ generates the subgroup $\langle a \rangle$ or that $a$ is a generator of $\langle a \rangle$. Clearly, the order of $\langle a \rangle$ equals the order of $a$ in the group. $\langle a \rangle$ is also called a cyclic group.

**Example:** $\{0, 2, 4, 6\} \subset \mathbb{Z}_8$ can be generated by 2 or 6.

Note that a cyclic group is always Abelian.
Corollary: The order of an element divides the order of group.

Corollary: Any group of prime order must be cyclic.

Corollary: Let $S$ be a finite group, and $a \in S$, then $a^{|S|} = e$.

Theorem: Let $a$ be an element in a group $S$, such that $a^s = e$, then $\text{order}(a, S) | s$.

Proof: Using the division theorem, $s = q \cdot \text{order}(a, S) + r$, where $0 \leq r < \text{order}(a, S)$. Therefore,

$$e = a^s = a^{q \cdot \text{order}(a, S) + r} = (a^{\text{order}(a, S)})^q \oplus a^r = a^r.$$ 

Due to the minimality of $\text{order}(a, S)$, we conclude that $r = 0$. QED
**Fields**

**Definition:** A Field \((S, \oplus, \odot)\) is a set \(S\) with two binary operations \(\oplus\) and \(\odot\) defined on \(S\) and with two special elements denoted by 0, 1 for which the following properties hold:

1. \((S, \oplus)\) is an Abelian group (0 is the identity with regards to \(\oplus\)).
2. \((S \setminus \{0\}, \odot)\) is an Abelian group (1 is the identity with regards to \(\odot\)).
3. **Distributivity:** \(a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)\).

**Corollary:** \(\forall a \in S, a \odot 0 = 0\).

**Proof:** \(a \odot 0 = a \odot (0 \oplus 0) = a \odot 0 \oplus a \odot 0\), thus, \(a \odot 0 = 0\).

**Examples:** \((\mathbb{Q}, +, \cdot)\), \((\mathbb{Z}_p, +_p, \cdot_p)\) where \(p\) is a prime.
**Inverses**

**Lemma**: Let $p$ be a prime. Then,

$$ab \equiv 0 \pmod{p}$$

iff

$$a \equiv 0 \pmod{p} \text{ or } b \equiv 0 \pmod{p}.$$

**Proof**:

($\Leftarrow$) From $p|a$ or $p|b$ it follows that $p|ab$.

($\Rightarrow$) $p|ab$. If $p|a$ we are done. Otherwise, $p \not| a$. Since $p$ a prime it follows that $\gcd(a, p) = 1$. Therefore, $p|b$ (by Euclid’s Lemma). QED
Inverses (cont.)

**Definition:** Let $a$ be a number. If there exists $b$ such that $ab \equiv 1 \pmod{m}$, then we call $b$ the **inverse** of $a$ modulo $m$, and write $b \triangleq a^{-1} \pmod{m}$.

**Theorem:** If $\gcd(a, m) = 1$ then there exists some $b$ such that $ab \equiv 1 \pmod{m}$.

**Proof:** There exist $x, y$ such that

$$xa + ym = 1.$$ 

Thus,

$$xa \equiv 1 \pmod{m}.$$ 

QED

**Conclusion:** $a$ has an inverse modulo $m$ iff $\gcd(a, m) = 1$. The inverse can be computed by Euclid’s algorithm.
Definition: $\mathbb{Z}_n^*$ is the set of all the invertible integers modulo $n$:

$$\mathbb{Z}_n^* = \{i \in \mathbb{Z}_n | \gcd(i, n) = 1\}.$$

Theorem: For any positive $n$, $\mathbb{Z}_n^*$ is an Abelian multiplicative group under multiplication modulo $n$.

Proof: Exercise.

$\mathbb{Z}_n^*$ is also called an Euler group.

Example: For a prime $p$, $\mathbb{Z}_p^* = \{1, 2, \ldots, p - 1\}$. 
Examples:

\[ Z_2 = \{0, 1\} \quad Z_2^* = \{1\} \]
\[ Z_3 = \{0, 1, 2\} \quad Z_3^* = \{1, 2\} \]
\[ Z_4 = \{0, 1, 2, 3\} \quad Z_4^* = \{1, 3\} \]
\[ Z_5 = \{0, 1, 2, 3, 4\} \quad Z_5^* = \{1, 2, 3, 4\} \]
\[ Z_1 = \{0\} \quad Z_1^* = \{0\} \]
Euler’s Function

Definition: Euler’s function $\varphi(n)$ represents the number of elements in $\mathbb{Z}_n^*$:

$$\varphi(n) \triangleq |\mathbb{Z}_n^*| = |\{i \in \mathbb{Z}_n | \gcd(i, n) = 1\}|$$

$\varphi(n)$ is the number of numbers in $\{0, \ldots, n - 1\}$ that are coprime to $n$.

Note that by this definition $\varphi(1) \triangleq 1$ (since $\mathbb{Z}_1^* = \{0\}$, which is because $\gcd(0, 1) = 1$).
Euler’s Function (cont.)

**Theorem:** Let \( n = p_1^{e_1}p_2^{e_2} \cdots p_l^{e_l} \) be the unique factorization of \( n \) to distinct primes. Then,

\[
\varphi(n) = \prod (p_i^{e_i-1}(p_i - 1)) = n \prod (1 - \frac{1}{p_i}).
\]

**Proof:** Exercise.

**Note:** If the factorization of \( n \) is not known, \( \varphi(n) \) is not known as well.

**Conclusions:** For prime numbers \( p \neq q \), and any integers \( a \) and \( b \)

1. \( \varphi(p) = p - 1. \)
2. \( \varphi(p^e) = (p - 1)p^{e-1} = p^e - p^{e-1}. \)
3. \( \varphi(pq) = (p - 1)(q - 1). \)
4. If \( \gcd(a, b) = 1 \) then \( \varphi(ab) = \varphi(a)\varphi(b). \).
Euler’s Function (cont.)

Theorem:

\[ \sum_{d|n} \varphi(d) = n. \]

Proof: In this proof, we count the numbers 1, \ldots, n in a different order. We divide the numbers into distinct groups according to their gcd \( d' \) with \( n \), thus the total number of elements in the groups is \( n \).

It remains to see what is the number of numbers out of 1, \ldots, n whose gcd with \( n \) is \( d' \).

Clearly, if \( d' \nmid n \), the number is zero.

Otherwise, let \( d'|n \) and \( 1 \leq a \leq n \) be a number such that gcd\((a, n) = d'\). Therefore, \( a = kd' \), for some \( k \in \{1, \ldots, n/d'\} \). Substitute \( a \) with \( kd' \), thus gcd\((kd', n) = d'\), i.e., gcd\((k, n/d') = 1\).
Euler’s Function (cont.)

It remains to see for how many $k$’s, $1 \leq k \leq n/d'$, it holds that

$$\gcd(k, n/d') = 1.$$  

But this is the definition of Euler’s function, thus there are $\varphi(n/d')$ such $k$’s.

Since we count each $a$ exactly once

$$\sum_{d' | n} \varphi(n/d') = n.$$  

If $d' | n$ then also $d = \frac{n}{d'}$ divides $n$, and thus we can substitute $n/d'$ with $d$ and get

$$\sum_{d | n} \varphi(d) = n.$$  

QED
Euler’s Theorem

Theorem: For any $a$ and $m$, if $\gcd(a, m) = 1$ then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Proof: $a$ is an element in the Euler group $\mathbb{Z}_m^*$. Therefore, as a corollary from Lagrange Theorem, $a^{\vert \mathbb{Z}_m^* \vert} = a^{\varphi(m)} = 1 \pmod{m}$. QED
Fermat’s Little Theorem

Fermat’s little theorem: \( \) Let \( p \) be a prime number. Then, any integer \( a \) satisfies

\[
a^p \equiv a \pmod{p}.
\]

Proof: If \( p \mid a \) the theorem is trivial, as \( a \equiv 0 \pmod{p} \). Otherwise \( p \) and \( a \) are coprimes, and thus by Euler’s theorem

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

and

\[
a^p \equiv a \pmod{p}.
\]

QED
Properties of Elements in the Group $\mathbb{Z}_m^*$

**Definition:** For $a, m$ such that $\gcd(a, m) = 1$, let $h$ be the smallest integer ($h > 0$) satisfying

$$a^h \equiv 1 \pmod{m}.$$  

(Such an integer exists by Euler’s theorem: $a^{\varphi(m)} \equiv 1 \pmod{m}$). We call $h$ the **order of $a$ modulo $m$** ($m$ של מודולו $a$), and write

$$h = \text{order}(a, \mathbb{Z}_m^*).$$

Obviously, it is equivalent to the order of $a$ in the Euler group $\mathbb{Z}_m^*$. 
**Properties of Elements in the Group $Z^*_m$ (cont.)**

**Conclusions:** For $a, m$ such that $\gcd(a, m) = 1$

1. If $a^s \equiv 1 \pmod{m}$, then $\text{order}(a, Z^*_m)|s$.

2. $\text{order}(a, Z^*_m)|\varphi(m)$

3. If $m$ is a prime, then $\text{order}(a, Z^*_m)|m - 1$.

4. The numbers
   \[1, a, a^2, a^3, \ldots, a^{\text{order}(a, Z^*_m) - 1}\]
   are all distinct modulo $m$.

**Proof:** Follows from the properties of groups.

QED
Modular Exponentiation

Given a prime $q$ and $a \in \mathbb{Z}_q^*$ we want to calculate $a^x \mod q$.

Denote $x$ in binary representation as

$$x = x_{n-1}x_{n-2} \ldots x_1x_0,$$

where $x = \sum_{i=0}^{n-1} x_i2^i$.

Therefore, $a^x \mod q$ can be written as:

$$a^x = a^{2^{(n-1)}x_{n-1}}a^{2^{(n-2)}x_{n-2}} \ldots a^{2^1x_1}a^{x_0}$$
An Algorithm for Modular Exponentiation

\[ a^x = a^{2^{(n-1)}x_{n-1}}a^{2^{(n-2)}x_{n-2}} \cdots a^{2x_1}a^{x_0} \]

**Algorithm:**

\[ r \leftarrow 1 \]
for \( i \leftarrow n - 1 \) down to 0 do
\[ r \leftarrow r^2a^{x_i} \mod q \quad (a^{x_i} \text{ is either 1 or } a) \]

At the end
\[ r = \prod_{i=0}^{n-1} a^{x_i2^i} = a^{(\sum_{i=0}^{n-1} x_i2^i)} = a^x \pmod{q}. \]

Complexity: \( O(\log x) \) modular multiplications. For a random \( x \) this complexity is \( O(\log q) \).
An important note:

\[(xy) \mod q = (((x \mod q)(y \mod q)) \mod q) \mod q,\]

i.e., the modular reduction can be performed every multiplication, or only at the end, and the results are the same.

The proof is given as an exercise.
The Chinese Remainder Theorem

Problem 1: Let $n = pq$ and let $x \in \mathbb{Z}_n$. Compute $x \mod p$ and $x \mod q$.
Both are easy to compute, given $p$ and $q$.

Problem 2: Let $n = pq$, let $x \in \mathbb{Z}_p$ and let $y \in \mathbb{Z}_q$. Compute $u \in \mathbb{Z}_n$ such that

\begin{align*}
u &\equiv x \pmod{p} \\
u &\equiv y \pmod{q}.
\end{align*}
The Chinese Remainder Theorem (cont.)

**Generalization:** Given moduli \( m_1, m_2, \ldots, m_k \) and values \( y_1, y_2, \ldots, y_k \). Compute \( u \) such that for any \( i \in \{1, \ldots, k\} \)

\[
u \equiv y_i \pmod{m_i}.
\]

We can assume (without loss of generality) that all the \( m_i \)'s are coprimes in pairs (\( \forall i \neq j \gcd(m_i, m_j) = 1 \)). (If they are not coprimes in pairs, either they can be reduced to an equivalent set in which they are coprimes in pairs, or else the system leads to a contradiction, such as \( u \equiv 1 \pmod{3} \) and \( u \equiv 2 \pmod{6} \)).

**Example:** Given the moduli \( m_1 = 11 \) and \( m_2 = 13 \) find a number \( u \pmod{11 \cdot 13} \) such that \( u \equiv 7 \pmod{11} \) and \( u \equiv 4 \pmod{13} \).

**Answer:** \( u \equiv 95 \pmod{11 \cdot 13} \). Check: \( 95 = 11 \cdot 8 + 7, 95 = 13 \cdot 7 + 4 \).
The Chinese Remainder Theorem (cont.)

The Chinese remainder theorem: (משופ הת хаָיִיתָה התיָניִית) Let \( m_1, m_2, \ldots, m_k \) be coprimes in pairs and let \( y_1, y_2, \ldots, y_k \). Then, there is an unique solution \( u \) modulo \( m = \prod m_i = m_1m_2 \cdots m_k \) of the equations:

\[
\begin{align*}
u & \equiv y_1 \pmod{m_1} \\
u & \equiv y_2 \pmod{m_2} \\
& \vdots \\
u & \equiv y_k \pmod{m_k},
\end{align*}
\]

and it can be efficiently computed.
The Chinese Remainder Theorem (cont.)

Example: Let

\[ u \equiv 7 \pmod{11} \quad u \equiv 4 \pmod{13} \]

then compute

\[ u \equiv ? \pmod{11 \cdot 13}. \]

Assume we found two numbers \( a \) and \( b \) such that

\[ a \equiv 1 \pmod{11} \quad a \equiv 0 \pmod{13} \]

and

\[ b \equiv 0 \pmod{11} \quad b \equiv 1 \pmod{13} \]

Then,

\[ u \equiv 7a + 4b \pmod{11 \cdot 13}. \]
The Chinese Remainder Theorem (cont.)

We remain with the problem of finding \( a \) and \( b \). Notice that \( a \) is divisible by 13, and \( a \equiv 1 \pmod{11} \).

Denote the inverse of 13 modulo 11 by \( c \equiv 13^{-1} \pmod{11} \). Then,

\[
13c \equiv 1 \pmod{11} \\
13c \equiv 0 \pmod{13}
\]

We conclude that

\[
a \equiv 13c \equiv 13(13^{-1} \pmod{11}) \pmod{11 \cdot 13}
\]

and similarly

\[
b \equiv 11(11^{-1} \pmod{13}) \pmod{11 \cdot 13}
\]

Thus,

\[
u \equiv 7 \cdot 13 \cdot 6 + 4 \cdot 11 \cdot 6 \equiv 810 \equiv 95 \pmod{11 \cdot 13}
\]
The Chinese Remainder Theorem (cont.)

Proof: \( m/m_i \) and \( m_i \) are coprimes, thus \( m/m_i \) has an inverse modulo \( m_i \).

Denote

\[ l_i \equiv (m/m_i)^{-1} \pmod{m_i} \]

and

\[ b_i = l_i(m/m_i). \]

\[ b_i \equiv 1 \pmod{m_i} \]
\[ b_i \equiv 0 \pmod{m_j}, \quad \forall j \neq i \text{ (since } m_j|m(m/m_i)). \]

The solution is

\[ u \equiv y_1b_1 + y_2b_2 + \cdots + y_kb_k \]
\[ \equiv \sum_{i=1}^{m} y_ib_i \pmod{m}. \]
The Chinese Remainder Theorem (cont.)

We still have to show that the solution is unique modulo $m$. By contradiction, we assume that there are two distinct solutions $u_1$ and $u_2$, $u_1 \neq u_2 \pmod{m}$. But any modulo $m_i$ satisfy $u_1 - u_2 \equiv 0 \pmod{m_i}$, and thus

$$m_i | u_1 - u_2.$$

Since $m_i$ are pairwise coprimes we conclude that

$$m = \prod m_i | u_1 - u_2$$

which means that

$$u_1 - u_2 \equiv 0 \pmod{m}.$$

Contradiction. QED
\[ Z_{ab}^* \equiv Z_a^* \times Z_b^* \text{ (for coprime } a, b) \]

Consider the homomorphism \( \Psi : Z_{ab}^* \rightarrow Z_a^* \times Z_b^* \),
\( \Psi(u) = (\alpha = u \mod a, \beta = u \mod b) \).

**Lemma:** \( u \in Z_{ab}^* \) iff \( \alpha \in Z_a^* \) and \( \beta \in Z_b^* \), i.e.,
gcd\(ab, u\) = 1 iff gcd\(a, u\) = 1 and gcd\(b, u\) = 1.

**Proof:**

(\(\Rightarrow\)) Trivial (\(k_1 ab + k_2 u = 1\) for some \(k_1\) and \(k_2\)).

(\(\Leftarrow\)) By the assumptions there exist some \(k_1, k_2, k_3, k_4\) such that

\[ k_1 a + k_2 u = 1 \text{ and } k_3 b + k_4 u = 1. \]

Thus,

\[ k_1 a(k_3 b + k_4 u) + k_2 u = 1 \]

from which we get

\[ k_1 k_3 ab + (k_1 k_4 a + k_2) u = 1. \]

QED
Lemma: $\Psi$ is onto.

Proof: Choose any $\alpha \in Z_a^*$ and any $\beta \in Z_b^*$, we can reconstruct $u$, using the Chinese remainder theorem, and $u \in Z_{ab}^*$ from previous lemma.

Lemma: $\Psi$ is one to one.

Proof: Assume to the contrary that for $\alpha \in Z_a^*$ and $\beta \in Z_b^*$ there are $u_1 \neq u_2$ (mod $ab$). This is a contradiction to the uniqueness of the solution of the Chinese remainder theorem.

QED

We conclude from the Chinese remainder theorem and these two Lemmas that $Z_{ab}^*$ is 1-1 related to $Z_a^* \times Z_b^*$.

For every $\alpha \in Z_a^*$ and $\beta \in Z_b^*$ there exists a unique $u \in Z_{ab}^*$ such that $u \equiv \alpha$ (mod $a$) and $u \equiv \beta$ (mod $b$), and vise versa.

Note: This can be used to construct an alternative proof for $\varphi(pq) = \varphi(p)\varphi(q)$, where $\gcd(p, q) = 1$. 

$Z_{ab}^* \equiv Z_a^* \times Z_b^*$ (for coprime $a$, $b$) (cont.)
Lagrange’s Theorem

**Theorem:** A polynomial of degree $n > 0$

$$f(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \ldots + c_{n-1}x + c_n$$

has at most $n$ distinct roots modulo a prime $p$.

**Proof:** It is trivial for $n = 1$.

By induction:

Assume that any polynomial of degree $n - 1$ has at most $n - 1$ roots. Let $a$ be a root of $f(x)$, i.e., $f(a) \equiv 0 \pmod{p}$.

We can write

$$f(x) = (x - a)f_1(x) + r \pmod{p}$$

for some polynomial $f_1(x)$ and constant $r$ (this is a division of $f(x)$ by $(x - a)$).

Since $f(a) \equiv 0 \pmod{p}$ then $r \equiv 0 \pmod{p}$ and we get

$$f(x) = (x - a)f_1(x) \pmod{p}.$$
Lagrange’s Theorem (cont.)

Thus, any root $b \neq a$ of $f(x)$ is also a root of $f_1(x)$:

$$0 \equiv f(b) \equiv (b - a)f_1(b) \pmod{p}$$

which causes

$$f_1(b) \equiv 0 \pmod{p}.$$  

$f_1$ is of degree $n - 1$, and thus has at most $n - 1$ roots. Together with $a$, $f$ has at most $n$ roots. QED

**Note:** Lagrange’s Theorem does not hold for composites, for example:

$$x^2 - 4 \equiv 0 \pmod{35}$$

has 4 roots: 2, 12, 23 and 33.
Generators

**Definition:** $a$ is called a **generator** (גנ"ר) of $\mathbb{Z}_n^*$ if $\text{order}(a, \mathbb{Z}_n^*) = \varphi(n)$.

Not all groups possess generators. If $\mathbb{Z}_n^*$ possesses a generator $g$, then $\mathbb{Z}_n^*$ is **cyclic**.

If $g$ is a generator of $\mathbb{Z}_n^*$ and $a$ is any element of $\mathbb{Z}_n^*$ then there exists a $z$ such that $g^z \equiv a \pmod{n}$. This $z$ is called the **discrete logarithm** or **index** of $a$ modulo $n$ to the base $g$. We denote this value as $\text{ind}_{n,g}(a)$ or $\text{DLOG}_{n,g}(a)$. 
The Number of Generators

**Theorem:** Let $h$ be the order of $a$ modulo $m$. Let $s$ be an integer such that $\gcd(h, s) = 1$, then the order of $a^s$ modulo $m$ is also $h$.

**Proof:** Denote the order of $a$ by $h$ and the order of $a^s$ by $h'$.

\[
(a^s)^h \equiv (a^h)^s \equiv 1 \pmod{m}.
\]

Thus, $h'|h$.

On the other hand,

\[
a^{sh'} \equiv (a^s)^{h'} \equiv 1 \pmod{m}
\]

and thus $h|sh'$. Since $\gcd(h, s) = 1$ then $h|h'$.

QED
The Number of Generators (cont.)

**Theorem:** Let $p$ be a prime and $d|p - 1$. The number of integers in $\mathbb{Z}_p^*$ of order $d$ is $\varphi(d)$.

**Proof:** Denote the number of integers in $\mathbb{Z}_p^*$ which are of order $d$ by $\psi(d)$. We should prove that $\psi(d) = \varphi(d)$.

Assume that $\psi(d) \neq 0$, and let $a \in \mathbb{Z}_p^*$ have an order $d$ ($a^d \equiv 1 \pmod{p}$).

The equation $x^d \equiv 1 \pmod{p}$ has the following solutions

$$1 \equiv a^d, a^1, a^2, a^3, \ldots, a^{d-1},$$

all of which are distinct.

We know that $x \equiv a^i \pmod{p}$ has an order of $d$ iff $\gcd(i, d) = 1$, and thus the number of solutions with order $d$ is $\psi(d) = \varphi(d)$. 
The Number of Generators (cont.)

We should show that the equality holds even if \( \psi(d) = 0 \). Each of the integers in \( \mathbb{Z}_p^* = \{1, 2, 3, \ldots, p - 1\} \) has some order \( d \mid p - 1 \). Thus, the sum of \( \psi(d) \) for all the orders \( d \mid p - 1 \) equals \( |\mathbb{Z}_p^*| \):

\[
\sum_{d \mid p-1} \psi(d) = p - 1.
\]

As we know that \( \sum_{d \mid p-1} \varphi(d) = p - 1 \), it follows that:

\[
0 = \sum_{d \mid p-1} (\varphi(d) - \psi(d)) =
\]

\[
= \sum_{d \mid p-1, \psi(d) = 0} (\varphi(d) - \psi(d)) + \sum_{d \mid p-1, \psi(d) \neq 0} (\varphi(d) - \psi(d)) =
\]

\[
= \sum_{d \mid p-1, \psi(d) = 0} \varphi(d) + \sum_{d \mid p-1, \psi(d) \neq 0} 0 = \sum_{d \mid p-1, \psi(d) = 0} \varphi(d)
\]

Since \( \varphi(d) \geq 0 \), then \( \psi(d) = 0 \Rightarrow \varphi(d) = 0 \). We conclude that for any \( d \):

\[
\psi(d) = \varphi(d).
\]

QED
Conclusion: Let $p$ be a prime. There are $\varphi(p - 1)$ elements in $\mathbb{Z}_p^*$ of order $p - 1$ (i.e., all of them are generators).

Therefore, $\mathbb{Z}_p^*$ is cyclic.

Theorem: The values of $n > 1$ for which $\mathbb{Z}_n^*$ is cyclic are $2, 4, p^e$ and $2p^e$ for all odd primes $p$ and all positive integers $e$.

Proof: Exercise.
Wilson’s Theorem

Wilson’s theorem: Let $p$ be a prime.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-1) \equiv -1 \pmod{p}.$$

Proof: Clearly it holds for $p = 2$. It suffices thus to prove it for $p \geq 3$.
Let $g$ be a generator of $Z_p^*$. Then,

$$Z_p^* = \{1, g, g^2, g^3, \ldots, g^{p-2}\}$$

and thus

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-1) \equiv 1 \cdot g \cdot g^2 \cdot g^3 \cdot \ldots \cdot g^{p-2}$$
$$\equiv g^{(p-2)(p-1)/2} \pmod{p}.$$
Wilson’s Theorem (cont.)

If $g^{(p-1)/2} \equiv -1 \pmod{p}$, then it follows that

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-1) \equiv g^{(p-2)(p-1)/2} \pmod{p}$$
$$\equiv (-1)^{p-2} \equiv -1 \pmod{p}.$$ 

It remains to show that $g^{(p-1)/2} \equiv -1 \pmod{p}$. From Euler theorem it follows that

$$g^{p-1} \equiv 1 \pmod{p}.$$ 

Thus,

$$0 \equiv g^{p-1} - 1 \equiv (g^{(p-1)/2} + 1)(g^{(p-1)/2} - 1) \pmod{p}.$$ 

$g^{(p-1)/2} \not\equiv 1 \pmod{p}$ since $\text{order}(g, Z_p^*) = p - 1$ (and $p$ is odd), and thus it must be that $g^{(p-1)/2} \equiv -1 \pmod{p}$.

QED