Lecture 2 Modular Arithmetic

Def. Let *m* be a positive integer (called the modulus). Integers *a*,*b* are said to be **congruent mod *m*** if $m \mid a-b$ and we write $a \equiv b \pmod{m}$. Note this is a true-false relationship.

If $a \equiv b \pmod{m}$ then $a = b + km$ for some integer *k*. Also, *a* and *b* will have the same remainder when divided by *m*.

Ex.
(1) $80 \equiv 4 \pmod{19}$ is true since $19 \mid 80 - 4 = 76$

(2) $135 \equiv 6 \pmod{22}$ is false because $22 \nmid 135 - 6 = 129$

(3) $105 \equiv 0 \pmod{7}$ is true because $7 \mid 105 - 0 = 105$

Proposition: (a) If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$ then $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$ and $a_1 b_1 \equiv a_2 b_2 \pmod{m}$
(b) Given an integer *a* there exists an integer *b* such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a,m) = 1$. Note: in this case we say that *b* is the multiplicative inverse of *a* (mod *m*).

Also, the multiplicative inverse is unique. If $ab_1 \equiv ab_2 \equiv 1 \pmod{m}$ then $b_1 \equiv b_2 \pmod{m}$

Pf of (b)
$(\Rightarrow)$ Assume $ab \equiv 1 \pmod{m}$. This means $ab = 1 + km$ for some integer *k*. Hence $ab - km = 1$.
Let $\gcd(a,m) = d \Rightarrow d \mid a,\ d \mid m \Rightarrow d \mid ab - km \Rightarrow d \mid 1 \Rightarrow d = 1$

$(\Leftarrow)$
Assume $\gcd(a,m) = 1$. By the Extended Euclidean Algorithm there exist integers *u*,*v* such that $au + mv = 1 \Rightarrow au - 1 = -mv \Rightarrow au \equiv 1 \pmod{m}$.

Suppose $ab_1 \equiv ab_2 \equiv 1 \pmod{m}$. Then $b_1 \equiv b_1(ab_2) \equiv (b_1 a)b_2 \equiv 1 \cdot b_2 \equiv b_2 \pmod{m}$

Note: If $ab \equiv 1 \pmod{m}$ then we write $b \equiv a^{-1} \pmod{m}$

Ex:
(1) Find $15^{-1} \pmod{23}$

By the Extended Euclidean Algorithm
23 = 15 + 8
15 = 8 + 7
8 = 7 + 1

1= 8 – 7 = 8 – (15 -8) = 2*8 – 15 = 2*(23-15) – 15 = 2*23 -3*15

$15^{-1} \equiv -3 \equiv 20 \pmod{23}$

(2) Compute $13/15 \pmod{23}$

$13/15 \equiv 13*15^{-1} \equiv 13*20 \equiv 7 \pmod{23}$

Def.
The **ring of integers mod *m*** is denoted $Z/mZ = Z_m = \{0,1,...,m-1\}$. In this set addition and multiplication are defined mod *m*.

Ex
(1) Consider the ring $Z_{11}$. Sample computations: $7+8=4,\ 7*8=1$ (these are valid mod 11).

Def. Group of units mod *m* is the set
$\{a \in Z_m \mid a \text{ has a multiplicative inverse mod } m\} = \{a \in Z_m \mid \gcd(a.m)=1\}$

Notation for the group of units: $(Z/mZ)^* = Z_m^* = U(m)$

Notes:
(1) U(*m*) is closed under multiplication
Pf: Let $a,b \in U(m)$ then $(ab)*(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$

(2) If *p* is a prime number then $(Z/pZ)^* = Z_p^* = U(p) = \{1,2,...,p-1\}$

Ex:
(1) Find U(8).

$\gcd(1,8)=1,\ \gcd(2,8)=2,\ \gcd(3,8)=1,\ \gcd(4,8)=4,\ \gcd(5,8)=5,\ \gcd(6,8)=2,\ \gcd(7,8)=7$
$U(8)=\{1,3,5,7\}$

(2) Find the multiplication table for U(8)

| | **1** | **3** | **5** | **7** |
|---|---|---|---|---|
| **1** | 1 | 3 | 5 | 7 |
| **3** | 3 | 1 | 7 | 5 |
| **5** | 5 | 7 | 1 | 3 |
| **7** | 7 | 5 | 3 | 1 |

Def. The Euler $\phi(n)$ function or Euler totient function is defined as $\phi(n) = \#U(n)$

Ex:

$\phi(2) = 1, \quad U(2) = \{1\}$

$\phi(3) = 2, \quad U(3) = \{1, 2\}$

$\phi(4) = 2, \quad U(4) = \{1, 3\}$

$\phi(5) = 4, \quad U(5) = \{1, 2, 3, 4\}$

$\phi(6) = 2, \quad U(6) = \{1, 5\}$

$\phi(15) = 8, \quad U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$