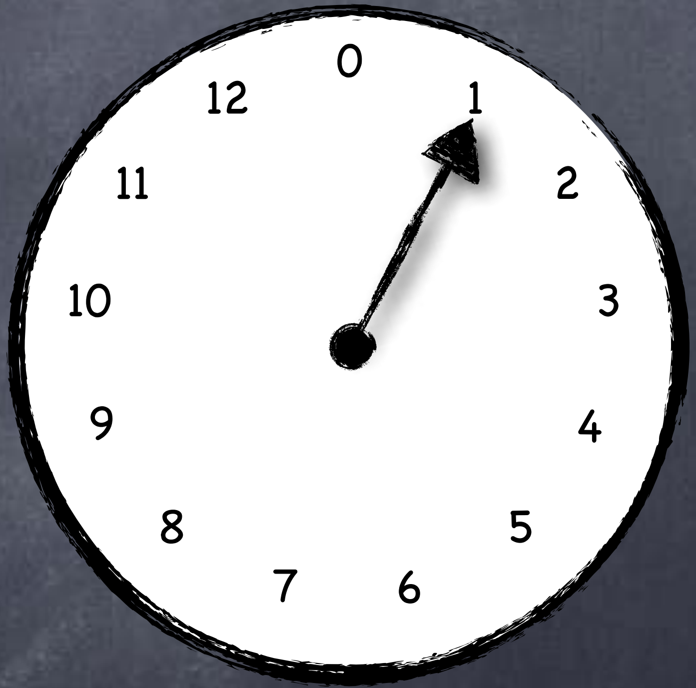
Numb3rs

Lecture 6
Modular Arithmetic
And More Intriguing Structures



Story So Far

- Quotient and Remainder
- GCD
  - Euclid's algorithm to compute gcd(a,b)
  - $L(a,b) \triangleq \{ au + bv \mid u,v \in \mathbb{Z} \}$
    $= \{ n \cdot gcd(a,b) \mid n \in \mathbb{Z} \}$

- Primes
  - Fundamental Theorem of Arithmetic
- **Modular Arithmetic ($\mathbb{Z}_m$)**
  - Addition and Multiplication
  - Multiplicative Inverse!
    - $gcd(a,m)=1 \leftrightarrow \exists u,v\ au+mv=1 \leftrightarrow \exists u\ [a]_m \times_m [u]_m = [1]_m$
    - For prime p, every element in $\mathbb{Z}_p \setminus \{0\}$ has mult. inverse

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Question

- Suppose $d|m$. Consider the two statements:

I. $\forall a,b \quad a \equiv b \pmod{m} \rightarrow a \equiv b \pmod{d}$

II. $\forall a,b \quad a \equiv b \pmod{d} \rightarrow a \equiv b \pmod{m}$

A. Both I & II are true
B. I is true, II is false
C. I is false, II is true
D. Both I & II are false

Chiming Clocks

- Two clocks, with a hours and b hours on their dials
- Say they both start at 0, and move one step every minute
  - e.g., a=13, b=9. After 3 minutes, both point to 3. After 10 minutes, the first clock points to 10, and the second to 1.
- Each clock has a position where it chimes, say r and s, respectively
  - e.g., r=11 and s=5
- Question: Will the two clocks ever chime together?

An Example

- Say, a=3 and b=5
- Note that after lcm(a,b) = 15 steps, both clocks will be back to 0
- So enough to check the first 15 steps
- Let's find out <u>all pairs</u> (r,s) that the two clocks will simultaneously reach
  - All 15 possible pairs occur, once each!

time	Clock 1	Clock 2
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

As Modular Arithmetic

- Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$
  - $x \mapsto (x \bmod 3, x \bmod 5)$
  - All 15 possible pairs occur, once each
- That is, for each $(r,s) \in \mathbb{Z}_3 \times \mathbb{Z}_5$, there is exactly one x such that
  $$x \equiv r \pmod 3 \text{ and } x \equiv s \pmod 5$$
- For which a,b are we guaranteed that there is a solution for this system (no matter what r,s is)?

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem

- If gcd(a,b) = 1, then for all (r,s) there is a unique solution (modulo ab) to the system
  $x \equiv r \pmod{a}$ and $x \equiv s \pmod{b}$
- Proof of existence:
  - Will solve for (r,s)=(1,0) and for (r,s)=(0,1)
    - i.e., $\alpha \equiv 1 \pmod{a}$, $\alpha \equiv 0 \pmod{b}$,
      $\beta \equiv 0 \pmod{a}$, $\beta \equiv 1 \pmod{b}$,
    - Then, can let $x = \alpha r + \beta s$.
  - $\exists$ u,v au+bv=1 (can compute using EEA)
  - Let $\alpha = 1 - au = bv$ and $\beta = 1 - bv = au$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem

- If gcd(a,b) = 1, then for all (r,s) there is a unique solution (modulo ab) to the system
  $x \equiv r \pmod{a}$ and $x \equiv s \pmod{b}$
- Existence: $x = bvr + aus$, where $au+bv=1$
- Uniqueness:
  - There are only ab possible values of x
  - There are ab pairs (r,s)
  - Each x is a solution for exactly one (r,s)
  - Every pair (r,s) has at least one solution
  - Hence, no pair (r,s) has two solutions

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Chinese Remainder Theorem

- If gcd(a,b) = 1, then for all (r,s) there is a unique solution (modulo ab) to the system

  $x \equiv r \pmod{a}$ and $x \equiv s \pmod{b}$

- Existence: $x = bvr + aus$, where $au+bv=1$
- Uniqueness: $|\mathbb{Z}_{ab}| = |\mathbb{Z}_a| \cdot |\mathbb{Z}_b|$
- CRT Representation:
  - Represent $x \in \mathbb{Z}_{ab}$ as the pair

    $(r,s) = (\text{ rem}(x,a), \text{rem}(x,b)) \in \mathbb{Z}_a \times \mathbb{Z}_b$
  - Can go back from (r,s) to x uniquely, using EEA

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

Arithmetic Using CRT

- Suppose $m = ab$, where $\gcd(a,b) = 1$
- Can use CRT representation to do arithmetic in $\mathbb{Z}_m$ using arithmetic in $\mathbb{Z}_a$ and $\mathbb{Z}_b$
- CRT representation of $\mathbb{Z}_m$: every element of $\mathbb{Z}_m$ can be written as a unique element of $\mathbb{Z}_a \times \mathbb{Z}_b$
- Addition and multiplication can be done coordinate-wise in CRT representation
    - If rem(x,a)=r and rem(x′,a)=r′, then rem(x+x′,a) $\equiv$ r + r′ (mod a). Similarly, mod b.
        - $(r, s) +_{(m)} (r', s') = (r +_{(a)} r', s +_{(b)} s')$
    - Similarly,
      $(r, s) \times_{(m)} (r', s') = (r \times_{(a)} r', s \times_{(b)} s')$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

$m = ab$, where $\gcd(a,b) = 1$

CRT and Inverses

- Addition and multiplication can be done coordinate-wise in CRT representation
  - Additive identity is (0,0) and multiplicative identity is (1,1)
- Additive and multiplicative inverses are coordinate-wise too
  - $(r,s) +_{(m)} (r',s') = (0,0) \longleftrightarrow r +_{(a)} r' = 0,\ s +_{(b)} s' = 0$
  - $(r,s) \times_{(m)} (r',s') = (1,1) \longleftrightarrow r \times_{(a)} r' = 1,\ s \times_{(b)} s' = 1$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

m = ab, where gcd(a,b) = 1

CRT and Inverses

- Addition and multiplication can be done coordinate-wise in CRT representation
  - Additive identity is (0,0) and multiplicative identity is (1,1)
- Additive and multiplicative inverses are coordinate-wise too
  - $(r,s) +_{(m)} (r',s') = (0,0) \longleftrightarrow r +_{(a)} r' = 0,\ s +_{(b)} s' = 0$
  - $(r,s) \times_{(m)} (r',s') = (1,1) \longleftrightarrow r \times_{(a)} r' = 1,\ s \times_{(b)} s' = 1$
  - x has multiplicative inverse modulo m iff it has multiplicative inverses modulo a and b
    - $\gcd(x,m)=1 \leftrightarrow \gcd(x,a)=1$ and $\gcd(x,b)=1$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

CRT Beyond 2 Factors

- Suppose $m = a_1 \cdot a_2 \cdot \ldots \cdot a_n$, where $\gcd(a_i,a_j)=1$ for all $i \neq j$. For any $(r_1,\ldots,r_n)$ with $r_i \in \mathbb{Z}_{a_i}$ for each i, there is a unique solution in $\mathbb{Z}_n$ for the system of congruences $\underline{x \equiv r_i \pmod{a_i} \text{ for } i=1,\ldots,n}$
- Proof by (weak) induction:
  - Base case: n=1 ✓
  - Induction step: We shall prove that for all $k \geq 1$,
    <u>(induction hypothesis)</u> if every system of k congruences with co-prime moduli has a unique solution,
    <u>(to prove)</u> then so does every such system of k+1 congruences
    - Given $(a_1,\ldots,a_{k+1},r_1,\ldots,r_{k+1})$, define a system for $(a_1,\ldots,a_k,r_1,\ldots,r_k)$, get its unique solution, say s. Define a system of 2 congruences, with co-prime moduli $a= a_1 \cdot \ldots \cdot a_k$, and $b=a_{k+1}$,
      $$x \equiv s \pmod{a} \text{ and } x \equiv r_{k+1} \pmod{a_{k+1}}.$$
      By CRT, this has a unique solution. This is the <u>unique</u> solution for the original system (why?).

Multiplicative Inverses, Again

- Recall: a has a multiplicative inverse in $\mathbb{Z}_m$ iff gcd(a,m) = 1
  - Such an element is called a unit of $\mathbb{Z}_m$
- **How many units are there in $\mathbb{Z}_m$?**
- When m is prime? m–1 (all except 0)
- When $m = p^2$, where p is prime?
  - A common factor with p^2 iff a multiple of p (in $\{0,p,2p,\ldots,(p-1)p\}$)
  - i.e., $p^2 - p$
- When $m = p^k$, where p is prime? $p^k - p^{k-1} = m(1-1/p)$
- When $m = p_1^{d_1} \cdot \ldots \cdot p_n^{d_n}$ where p_i are primes?
  - By CRT, elements of the form $(r_1,\ldots,r_n)$, where each r_i is invertible modulo $p_i^{d_i}$
  - $\prod_i \; p_i^{d_i} (1-1/p_i) = \mathbf{m(1-1/p_1) \cdot \ldots \cdot (1-1/p_n)}$

Multiplicative Inverses, Again

- **How many units are there in $\mathbb{Z}_m$?**
  - $\varphi(m) = m(1-1/p_1)\cdot \ldots \cdot(1-1/p_n)$ where $p_1,\ldots,p_n$ are the prime factors of m
- Euler's φ function (a.k.a. Euler's totient function)
- If $\gcd(a,b) = 1$, then $\varphi(ab) = \varphi(a)\cdot\varphi(b)$

Such a function is called a multiplicative function

Multiplicative Inverses, Again

- Examples
  - m=6
    - $\varphi(6) = (2-1)(3-1) = 2$
    - $\mathbb{Z}_6^* = \{1, 5\}$
  - m=10
    - $\varphi(10) = (2-1)(5-1) = 4$
    - $\mathbb{Z}_{10}^* = \{1,3,7,9\}$
- Note: The multiplication table restricted to units only has units!
- Why?

×	0	2	3	4	5	1
0	0	0	0	0	0	0
2	0	4	0	2	4	2
3	0	0	3	0	3	3
4	0	2	0	4	2	4
5	0	4	3	2	1	5
1	0	2	3	4	5	1

×	0	2	4	6	8	5	1	3	7	9
0	0	0	0	0	0	0	0	0	0	0
2	0	4	8	2	6	0	2	6	4	8
4	0	8	6	4	2	0	4	2	8	6
6	0	2	0	4	2	0	6	8	2	4
8	0	6	3	2	4	0	8	4	6	2
5	0	0	0	0	0	5	5	5	5	5
1	0	2	4	6	8	5	1	3	7	9
3	0	6	2	8	4	5	3	9	1	7
7	0	4	8	2	6	5	7	1	9	3
9	0	8	6	4	2	5	9	7	3	1

The Units, $\mathbb{Z}_m^*$

- If $a \in \mathbb{Z}_m \setminus \mathbb{Z}_m^*$ then $\exists u \neq 0$ s.t. $au=0$ in $\mathbb{Z}_m$
  - a not unit $\Rightarrow \gcd(a,m)>1 \Rightarrow m/\gcd(a,m) < m$

    $\Rightarrow \exists u$ (namely $m/\gcd(a,m)$) s.t. $0 < u < m$, $au = 0$ in $\mathbb{Z}_m$
- Converse also holds:
  - Suppose $\exists u \neq 0$, $au=0$ and $ba=1$. Then $0 = b0 = bau = 1u = u$!
- $a \in \mathbb{Z}_m^* \rightarrow a^{-1} \in \mathbb{Z}_m^*$
- $a,b \in \mathbb{Z}_m^* \rightarrow ab \in \mathbb{Z}_m^*$, because $(ab)(b^{-1}a^{-1}) = 1$
- For each $a \in \mathbb{Z}_m^*$, $a \cdot \mathbb{Z}_m^* \triangleq \{ ab \mid b \in \mathbb{Z}_m^* \} = \mathbb{Z}_m^*$
  - Since $a,b \in \mathbb{Z}_m^* \rightarrow ab \in \mathbb{Z}_m^*$, we have $a \cdot \mathbb{Z}_m^* \subseteq \mathbb{Z}_m^*$
  - $\forall x \in \mathbb{Z}_m^*$ we have $a^{-1}x \in \mathbb{Z}_m^*$ (why?) $\Rightarrow x \in a \cdot \mathbb{Z}_m^*$. Hence $\mathbb{Z}_m^* \subseteq a \cdot \mathbb{Z}_m^*$
  - So $a \cdot \mathbb{Z}_m^* = \mathbb{Z}_m^*$ (the row for a in the multiplication table restricted to $\mathbb{Z}_m^*$ has exactly all the elements in $\mathbb{Z}_m^*$)

Euler's Totient Theorem

- $\forall a \in \mathbb{Z}_m^*, \quad a^{\varphi(m)} \equiv 1 \pmod{m}$
- Proof: Fix any m and $a \in \mathbb{Z}_m^*$.

  Let $\mathbb{Z}_m^* = \{x_1,\ldots,x_n\}$ where $n = \varphi(m)$.

  Let $u = x_1 \ldots x_n$ and $w = (a \cdot x_1) \cdot \ldots \cdot (a \cdot x_n)$.

  $\Rightarrow w = a^n \cdot u$.

  But also, $w = \prod_{x \in a\mathbb{Z}_m^*} x = \prod_{x \in \mathbb{Z}_m^*} x = u$ (because $a \cdot \mathbb{Z}_m^* = \mathbb{Z}_m^*$)

  $\Rightarrow u = a^n \cdot u$, where $u \in \mathbb{Z}_m^*$

  $\Rightarrow 1 = a^n$ by multiplying both sides with u^{-1} $\square$

- Special case, when m is a prime
  - Fermat's Little Theorem:

    For prime p and a not a multiple of p, $a^{p-1} \equiv 1 \pmod{p}$