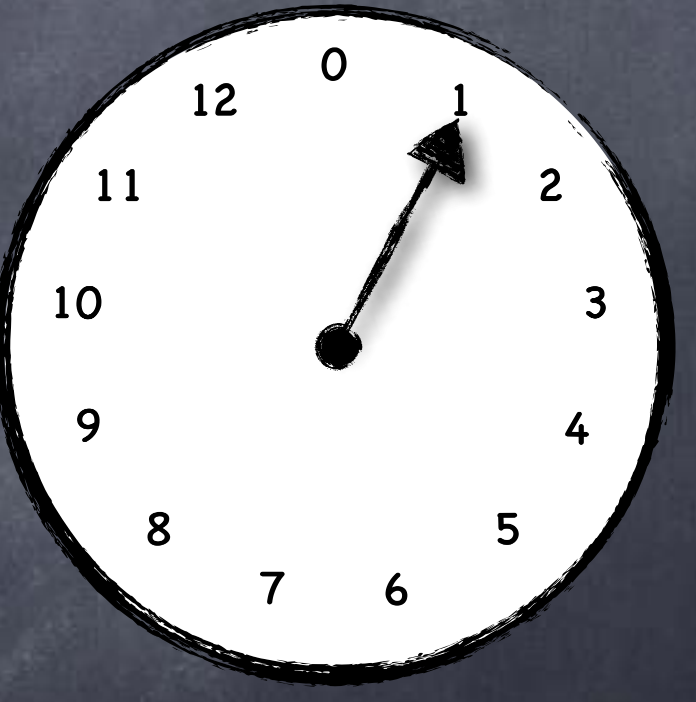
Numb3rs

The Chinese Remainder Theorem



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
- <u>Question</u>: 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

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

Any $(r,s) \in \mathbb{Z} \times \mathbb{Z}$ has exactly the same solutions as the pair $(\mathrm{rem}(r,a),\mathrm{rem}(s,b))$ has

So, w.l.o.g, $r \in [0,a)$ and $s \in [0,b)$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
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:
  - Take snapshots of the b-clock every time the needle of the a-clock reaches 0.
  - The snapshots correspond to the needle of the b-clock moving a hours at a time
  - Since gcd(a,b)=1, all positions in the b-clock will be reached in the snapshots
    - i.e., for all s, (0,s) has a solution
    - For any (r,s), let $s' \equiv s-r \pmod{b}$. Let x be a solution for (0,s'). x+r is one for (r,s).

0	4
1	0
2	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

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:
  - Recall, $r \in [0,a)$ and $s \in [0,b)$
  - There are ab such pairs (r,s). Every pair (r,s) has at least one solution.
  - There are only ab values of x (mod ab). Each x is a solution for (at most) one (r,s).
  - 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 $(r,s) = (\ \mathrm{rem}(x,a), \mathrm{rem}(x,b)\ ) \in \mathbb{Z}_a \times \mathbb{Z}_b$
  - Can go 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

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

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 $\mathrm{rem}(x,a)=r$ and $\mathrm{rem}(x',a)=r'$, then $\mathrm{rem}(x+x',a) \equiv r + r' \pmod a$. 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 <u>inverses</u> 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 $(r_1,\ldots,r_n)$, $r_i \in [0,a_i)$, there is a unique solution in $[0,m)$ for the system of congruences $x \equiv r_i \pmod{a_i}$ for $i=1,\ldots,n$
- Proof of existence, by (weak) induction:
  - Base case: $n=1$ ✓
  - Induction step: We shall prove that for all $k \geq 1$, (induction hypothesis) if every system of k congruences with co-prime moduli has a solution, (to prove) 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 a solution, say s. Define a system of 2 congruences, with co-prime moduli $a= a_1 \cdot \ldots \cdot a_k$, and $b=a_{k+1}$,

      $x \equiv s \pmod{a}$ and $x \equiv r_{k+1} \pmod{a_{k+1}}$.

    By CRT, this has a solution. This is a solution for the original system (**why?**).

Uniqueness as before:
$|\mathbb{Z}_m| = |\mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_n}|$

Exercise: $x \equiv s \pmod{a} \wedge a_1|a \Rightarrow x \equiv s \pmod{a_1}$