(SOLUTIONS)

CHINESE REMAINDER THEOREM

INTERMEDIATE GROUP - FEBRUARY 12, 2017

Warm Up

Theorem 1. Suppose m and n are two different prime numbers, and c is an integer. If $m|c$ and $n|c$, then $mn|c$.

Problem 1. Give values of m, n and c where Theorem 1 can be applied.

$m = 2$, $n = 5$, $c = 20$:

$2|20$, $5|20$ so $2 \times 5|20$

Note: $a|b \Leftrightarrow$ "a divides b" $\Leftrightarrow$ "b is divisible by a".

Note: Notice that this theorem doesn't work if m, n are not relatively prime:

$4|12$, $6|12$ but $4 \times 6 \nmid 12$.

Problem 2. Explain why Theorem 1 is true.

Fundamental theorem of arithmetic says that each integer has a unique prime factorization. If $m|c$ and $n|c$, m and n must both appear in the prime factorization of c, so $m \times n$ must also divide c.

Problem 3. Suppose we picked two prime numbers 3 and 5 and decided to make a table expressing the integers from 0 to 15 in $\mod 3$ and $\mod 5$.

For example, to find out where 7 belongs on the table, we would first find what 7 is in $\mod 3$ and $\mod 5$.

As $7 \equiv 1 \mod 3$ and $7 \equiv 2 \mod 5$, we would put 7 in the row corresponding to $1 \mod 3$ and the column corresponding to $2 \mod 5$. This is shown in the table below.

Fill out the rest of the table with integers from 0 to 15.

		mod 5				
		0	**1**	**2**	**3**	**4**
mod 3	**0**	0	6	12	3	9
	1	10	1	7	13	4
	2	5	11	2	8	14

Problem 4. Fill out the following tables. Can we make a table when we pick two integers that have a factor in common?

		mod 7						
		0	**1**	**2**	**3**	**4**	**5**	**6**
mod 3	**0**	0	15	9	3	18	12	6
	1	7	1	16	10	4	19	13
	2	14	8	2	17	11	5	20

		mod 6					
		0	**1**	**2**	**3**	**4**	**5**
mod 2	**0**	0, 6		2, 8		4, 10	
	1		1, 7		3, 9		5, 11

Problem 5. Notice that when we pick two prime numbers, m and n to create the table corresponding to $\mod m$ and $\mod n$, we can uniquely identify every number from 0 to $m \cdot n - 1$ by using the row and column they represent.

For example, there is only one number in the integers from 0 to 15 that is congruent to $2 \mod 3$ and $3 \mod 5$. Using the table you filled out in Problem 3, find this number.

$8 \equiv 2 \text{ mod } 3$
$\equiv 3 \text{ mod } 5$

Problem 6. Using the table from Problem 4, find a number between 0 and 20 that gives a remainder of 5 when we divide by 7 and a remainder of 2 when we divide by 3.

↳ $x \equiv 5 \text{ mod } 7$ ↳ $x \equiv 2 \text{ mod } 3$

$5 \equiv 5 \text{ mod } 7$
$\equiv 2 \text{ mod } 3$

Problem 7. Suppose Lev was trying to remember how many books he had brought to school with him. He knew that he had less than 12 books and that he would have 0 books remaining when he counted them by 2's and 4 books remaining when he counted them by 6's. Can we determine from the information above how many books he has?

↳ $x \equiv 4 \text{ mod } 6$ ↳ $x \equiv 0 \text{ mod } 2$

No. He could have 4 or 10 books, but we don't have enough info to determine which.

Chinese Remainder Theorem

Problem 8. Suppose we pick two prime numbers, n_1 and n_2. Prove that the system of equations

$$\begin{cases} x & \equiv r_1 \mod n_1 \\ x & \equiv r_2 \mod n_2 \end{cases}$$

has a unique solution for values of $x \mod n_1 \cdot n_2$.

To prove the above, we must show that if we have two numbers x_1 and x_2 that both satisfy the system of equations, then $x_1 \equiv x_2 \mod n_1 \cdot n_2$.

(1) Suppose that x_1 and x_2 both satisfy the system of equations. This would mean that

$$\begin{cases} x_1 & \equiv \underline{\ r_1\ } \mod n_1 \\ x_1 & \equiv \underline{\ r_2\ } \mod n_2 \end{cases}$$

and

$$\begin{cases} x_2 & \equiv \underline{\ r_1\ } \mod n_1 \\ x_2 & \equiv \underline{\ r_2\ } \mod n_2 \end{cases}.$$

(2) This implies that

$$\begin{cases} x_1 & \equiv x_2 \mod n_1 \\ x_1 & \equiv x_2 \mod n_2 \end{cases}$$

because

$$x_1 \equiv \underline{\ r_1\ } \mod n_1 \equiv x_2 \mod n_1$$

and

$$x_1 \equiv \underline{\ r_2\ } \mod n_2 \equiv x_2 \mod n_2.$$

(3) Thus

$$\begin{cases} x_1 - x_2 & \equiv \underline{\ 0\ } \mod n_1 \\ x_1 - x_2 & \equiv \underline{\ 0\ } \mod n_2 \end{cases},$$

which means that $n_1|(x_1 - x_2)$ and $n_2|(x_1 - x_2)$.

(4) From Theorem 1, we know that this implies that

$$\underline{n_1 \cdot n_2}|(x_1 - x_2),$$

so

$$x_1 - x_2 \equiv \underline{\ 0\ } \mod n_1 \cdot n_2.$$

(5) Finally, by adding x_2 to both sides of the equation, we obtain

$$x_1 \equiv \underline{x_2} \mod n_1 \cdot n_2.$$

Theorem 2. Chinese Remainder Theorem

Suppose we pick k prime numbers, $n_1, n_2, ..., n_k$. The system of equations

$$\begin{cases} x & \equiv r_1 \mod n_1 \\ x & \equiv r_2 \mod n_2 \\ & \dots \\ x & \equiv r_k \mod n_k \end{cases}$$

has a unique solution for values of $x \mod n_1 \cdot n_2 \cdot ... \cdot n_k$.

Problem 9. Consider the system of equations

$$\begin{cases} x & \equiv 2 \mod 11 \\ x & \equiv 3 \mod 13 \\ x & \equiv 3 \mod 17 \end{cases}.$$

How many solutions between 0 and 2430 does the system of equations have?

By the chinese remainder theorem, there is only 1 solution.

Problem 10. True/False: The system of equations has exactly one solution.

$$\begin{cases} x & \equiv 1 \mod 2 \\ x & \equiv 1 \mod 3 \\ x & \equiv 2 \mod 7 \end{cases}.$$

Justify your answer.

False. There is one solution between 0 and $(2\cdot3\cdot7-1)$ but there are infinitely many solutions:

$x = 37$, $37 + (2\cdot3\cdot7) = 79$, $37 + 2\cdot(2\cdot3\cdot7) = 121$, $37 + 3\cdot(2\cdot3\cdot7) = 163$, ...

Problem 11. True/False: The system of equations has exactly one solution between 0 and $n_1 \cdot n_2 \cdot n_3 - 1$.

$$\begin{cases} x & \equiv 1 \mod n_1 \\ x & \equiv 1 \mod n_2 \\ x & \equiv 2 \mod n_3 \end{cases}.$$

Justify your answer.

False. We can only apply the chinese remainder theorem if we know that n_1, n_2, n_3 are (relatively) prime.

Finding Solutions for the Chinese Remainder Theorem

So far, we have shown that there is a unique solution to a Chinese Remainder Theorem problem, but we have not discussed how to obtain the solution.

Suppose we're given the following system of equations:

$$\begin{cases} x & \equiv r_1 \mod n_1 \\ x & \equiv r_2 \mod n_2 \\ & \dots \\ x & \equiv r_k \mod n_k \end{cases}.$$

Then the solution x has the form

$$x = c_1 r_1 + c_2 r_2 + \dots + c_k r_k \mod n_1 \cdot n_2 \cdot \dots \cdot n_k$$

where

$$c_i \equiv 1 \mod n_i$$
$$c_i \equiv 0 \mod n_j \quad (i \neq j)$$

Problem 12. Find the least positive integer x where

$$\begin{cases} x & \equiv 1 \mod 7 \\ x & \equiv 7 \mod 11 \end{cases}.$$

(1) x must have the form:

$$x = c_1 \cdot 1 + c_2 \cdot \underline{\ 7\ } \mod 7 \cdot 11.$$

(2) To find c_1, we must find a number so that

$$c_1 \equiv 1 \mod 7$$
$$c_1 \equiv 0 \mod 11.$$
$$c_1 = \underline{\ 22\ }$$

(3) To find c_2, we must find a number so that

$c_2 \equiv 0 \mod 7$
$\equiv 1 \mod 11$

$$c_2 = \underline{\ 56\ }$$

(4) This gives $x = \underline{\ 29\ }$.

$x = 22 \cdot 1 + 56 \cdot 7 \mod 77 = 29 \mod 77$

Problem 13. A band of 7 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 2 coins remained. In the ensuing brawl over who should get the extra coins, two pirates were killed. The wealth was redistributed, but this time, and equal division left 3 coins. Again an argument developed in which two more pirates were killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

Write a system of equations to represent the question above and solve it using the algorithm we learned.

$$\begin{cases} x \equiv 2 \mod 7 \\ x \equiv 3 \mod 5 \\ x \equiv 0 \mod 3 \end{cases}$$

$x = c_1 \cdot 2 + c_2 \cdot 3 + c_3 \cdot 0 \mod (7 \cdot 5 \cdot 3)$

where

$c_1 \equiv 1 \mod 7$
$\equiv 0 \mod 5$
$\equiv 0 \mod 3$
$= 15$

$c_2 \equiv 0 \mod 7$
$\equiv 1 \mod 5$
$\equiv 0 \mod 3$
$= 21$

$c_3 \equiv 0 \mod 7$
$\equiv 0 \mod 5$
$\equiv 1 \mod 3$
$= 175$

so $x = 15 \cdot 2 + 21 \cdot 3 + 175 \cdot 0 \mod 105 \equiv 93 \mod 105 \Rightarrow 93$

Problem 14. Solve the system

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5\,. \\ x \equiv 2 \mod 7 \end{cases}$$

$x = c_1 \cdot 2 + c_2 \cdot 3 + c_3 \cdot 2 \mod (3 \cdot 5 \cdot 7)$

where

$c_1 \equiv 1 \mod 3$
$\equiv 0 \mod 5$
$\equiv 0 \mod 7$
$= 175$

$c_2 \equiv 0 \mod 3$
$\equiv 1 \mod 5$
$\equiv 0 \mod 7$
$= 21$

$c_3 \equiv 0 \mod 3$
$\equiv 0 \mod 5$
$\equiv 1 \mod 7$
$= 15$

so $x = 175 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 \mod 105 \equiv 443 \mod 105$
$\equiv 23 \mod 105 \Rightarrow 23$

(Any solution of the form $23 + 105k$ where k is an integer is correct as we did not ask for the least positive solution)

Problem 15. Explain why our algorithm for finding solutions to the Chinese Remainder Theorem works. If x has the form

$$x = c_1 r_1 + c_2 r_2 + \ldots + c_k r_k \mod n_1 \cdot n_2 \cdot \ldots \cdot n_k$$

why must

$$c_i \equiv 1 \mod n_i$$

and

$$c_i \equiv 0 \mod n_j \quad (i \neq j)?$$

We are looking for a solution to

$$\begin{cases} x \equiv r_1 \mod n_1 \\ x \equiv r_2 \mod n_2 \\ \quad\vdots \\ x \equiv r_k \mod n_k \end{cases}$$

To check if $x \equiv r_i \mod n_i$ for any i,

$$x \bmod n_i \equiv (c_1 r_1 + c_2 r_2 + \overset{+c_i r_i}{\cdot_\wedge\cdot} + c_k r_k) \bmod n_i$$

$$\begin{aligned} &\equiv c_1 (\mathrm{mod}\ n_i) \cdot r_1 (\mathrm{mod}\ n_i) \\ &\quad + c_2 (\mathrm{mod}\ n_i) \cdot r_2 (\mathrm{mod}\ n_i) \\ &\quad + \ldots \\ &\quad + c_i (\mathrm{mod}\ n_i) \cdot r_i (\mathrm{mod}\ n_i) \\ &\quad + \ldots \\ &\quad + c_k (\mathrm{mod}\ n_i) \cdot r_k \mathrm{mod}\ n_i) \end{aligned}$$

However each $c_j \equiv 0 \bmod n_i$ except for c_i, where $c_i \equiv 1 \bmod n_i$,

so the equation above gives

$$\begin{aligned} &\equiv 0 \cdot r_1 (\mathrm{mod}\ n_i) \\ &\quad + \ldots \\ &\quad + 1 \cdot r_i (\mathrm{mod}\ n_i) \\ &\quad + \ldots \\ &\quad + 0 \cdot r_k (\mathrm{mod}\ n_i) \end{aligned}$$

$$\equiv 1 \cdot r_i (\mathrm{mod}\ n_i) \equiv r_i \bmod n_i$$

which is what we wanted to show.

Two numbers are coprime if their greatest common denominator is 1.

So far, we have shown that the Chinese Remainder Theorem applies to system of equations moduli prime numbers. However, it can be extended to moduli which are coprime to each other.

Problem 16. Solve the system

$$\begin{cases} x & \equiv 1 \mod 4 \\ x & \equiv 3 \mod 5 \, . \\ x & \equiv 2 \mod 7 \end{cases}$$

gcd (4, 5, 7) = 1 , so we can use the chinese remainder theorem :

$x = c_1 \cdot 1 + c_2 \cdot 3 + c_2 \cdot 7 \mod 4 \cdot 5 \cdot 7$

where

$$\begin{array}{lll} c_1 \equiv 1 \bmod 4 & c_2 \equiv 0 \bmod 4 & c_3 \equiv 0 \bmod 4 \\ \equiv 0 \bmod 5 & \equiv 1 \bmod 5 & \equiv 0 \bmod 5 \\ \equiv 0 \bmod 7 & \equiv 0 \bmod 7 & \equiv 1 \bmod 7 \\ = 245 & = 196 & = 400 \end{array}$$

$x = 245 \cdot 1 + 196 \cdot 3 + 400 \cdot 2 \mod 140 \equiv 93 \mod 140$

$\Rightarrow$ any solution ~~where~~ of the form $93 + 140k$ where $k \in \mathbb{Z}$.

Problem 17. Based on your understanding of the Chinese Remainder Theorem, explain why the Chinese Remainder Theorem can be extended to moduli which are coprime to each other.

The only time we use the fact that the moduli is prime is when we apply Theorem 1 in the proof. However, theorem 1 is true for co-prime numbers as well, so the chinese remainder theorem is true when the moduli are coprime as well.

Problem 18. Comets 2P/Encke, 4P/Faye and 8P/Tuttle have orbital periods of 3 years, 8 years and 13 years respectively. The last perihelions (the point in the orbit which is closest to the sun) of each of these comets were in 2017, 2014 and 2008 respectively. What is the next year in which all three of these comets will achieve perihelions in the same year?

We want to solve

$$\begin{cases} x \equiv 2017 \mod 3 \\ x \equiv 2014 \mod 8 \\ x \equiv 2008 \mod 13 \end{cases}$$

So $x = c_1 \cdot 2017 + c_2 \cdot 2014 + c_3 \cdot 2008 \mod (3 \cdot 8 \cdot 13)$

$$\begin{array}{lll} \text{where } c_1 \equiv 1 \mod 3 & c_2 \equiv 0 \mod 3 & c_3 \equiv 0 \mod 3 \\ \equiv 0 \mod 8 & \equiv 1 \mod 8 & \equiv 0 \mod 8 \\ \equiv 0 \mod 13 & \equiv 0 \mod 13 & \equiv 1 \mod 13 \\ = 832 & = 1521 & = 110592 \end{array}$$

$x = 832 \cdot 2017 + 1521 \cdot 2014 + 110592 \cdot 2008 \mod 312 \equiv 2086 \mod 312$

$\Rightarrow 2086$

Problem 19. What are the last two digits of 49^{19}?

Hint: We are looking for x such that $x \equiv 49^{19} \mod 100$.

Furthermore, $100 = 25 \cdot 4$ and $\gcd(25, 4) = 1$.

We want to solve $x \equiv 49^{19} \mod 100$, which means

$$\begin{cases} x \equiv 49^{19} \mod 25 \equiv (49 \mod 25)^{19} \equiv -1 \mod 25 \\ x \equiv 49^{19} \mod 4 \equiv (49 \mod 4)^{19} \equiv 1^{19} \mod 4 \equiv 1 \mod 4 \end{cases}$$

by Theorem 1

$x = c_1 \cdot (-1) + c_2 \cdot (1) \mod 100$

$$\begin{array}{ll} \text{where } c_1 \equiv 1 \mod 25 & c_2 \equiv 0 \mod 25 \\ \equiv 0 \mod 4 & \equiv 1 \mod 4 \\ = 76 & = 25 \end{array}$$

$$\begin{aligned} x &= 76 \cdot (-1) + 25 \cdot (1) \mod 100 \\ &\equiv -51 \mod 100 \\ &\equiv 49 \mod 100 \end{aligned}$$

$\Rightarrow$ last two digits are 49.