5 The Chinese Remainder Theorem (CRT)

Q 5.0.1: $\varphi(72) =?$

Q 5.0.2: $[3^{-1}]_{72} =?$

Q 5.0.3: For any $x \in \mathbb{Z}_{105}$, $[x^s]_{105} = 1$ for what value of s?
-For the same s and any $x \in \mathbb{Z}_7$, $[x^s]_7 =?$
-For the same s and any $x \in \mathbb{Z}_{15}$, $[x^s]_{15} =?$
-Are the last two answers surprising? Why or why not?

Q 5.0.4: Alice and Bob are painting a picket fence. For no real reason, Alice paints every 7th board and Bob paints every 11th. What boards will they both paint?

Q 5.0.5: This time, Alice paints every 9th board and Bob paints every 15th. What boards will they both paint?

Q 5.0.6: Now, Alice paints every 7th board starting at with the 3rd and Bob paints every 11th starting at the 3rd. What boards will they both paint?

Q 5.0.7: Find a number, x, between 0 and 44 such that $[x]_5 = 2$ and $[x]_9 = 6$.

This last question is slightly analogous to the solution of simultaneous (linear) equations in our usual algebra. But instead of two conditions on two numbers, we have two conditions on the same number

The Chinese remainder theorem is a statement about handling two (or more) modular systems at the same time. It says that if you want to find z such that $[z]_A = [x]_A$ and also $[z]_B = [y]_B$, you can do that by solving $[z]_{AB} = [c]_{AB}$ for some value of c, provided A and B are relatively prime.

Example: "Find $x \in \mathbb{Z}_7$ and $y \in \mathbb{Z}_{25}$ such that $[x]_7 = [123]_7$ and $[y]_{25} = [123]_{25}$."
Going from one number in $\mathbb{Z}_{AB}$ to two numbers in $\mathbb{Z}_A$ and $\mathbb{Z}_B$ is very easy. Just take the mods:
$[x]_7 = [123]_7 = 4$
$[y]_{25} = [123]_{25} = 23$
So, $x = 4$ and $y = 23$.

What we've just done is taken a number, $123 \in \mathbb{Z}_{175}$ and found two numbers, $4 \in \mathbb{Z}_7$ and $23 \in \mathbb{Z}_{25}$, such that $[123]_7 = 4$ and $[123]_{25} = 23$.

We'll use the following notation to illustrate the relationship: $[123]_{175} \sim ([4]_7, [23]_{25})$. This is not the standard notation used in the math literature, but it is much clearer, so

we'll use it here.

Example: Find a number $z \in \mathbb{Z}_{15}$ such that $[z]_5 = 3$ and $[z]_3 = 1$.

(That is, we can find a number satisfying both $[z]_5 = 3$ and $[z]_3 = 1$ by looking at certain numbers in $\mathbb{Z}_{15}$.)

The two given conditions are the same as saying $z = 5k + 3$ and $z = 3j + 1$, for some integers j, k. Therefore:

$5k + 3 = 3j + 1$

$\Rightarrow 3 = 3j - 5k + 1$

$\Rightarrow 2 = 3j - 5k$

So we've reduced the problem to one in linear Diophantine equations, which we can solve using Euclid's algorithm. But in fact for this Diophantine equation we can easily guess a solution: $k = 2$, $j = 4$. Using either k or j, $z = 2 \cdot 5 + 3 = 4 \cdot 3 + 1 = 13$. So $z = 13$.

Q 5.0.8: When would you expect for $[z]_A = r$, $[z]_B = s$ to have a solution?

Hint: Use the ideas in the example above to turn the question into a Diophantine equation.

Example: Find a number $z \in \mathbb{Z}_{713}$ such that $[z]_{31} = 25$ and $[z]_{23} = 14$.

The two conditions are the same as saying $z = 31k + 25$ and $z = 23j + 14$. Therefore:

$31k + 25 = 23j + 14$

$\Rightarrow 25 = 23j - 31k + 14$

$\Rightarrow 11 = 23j - 31k$

So, we're looking to solve a Diophantine equation with $A = 31$ and $B = 23$.

$r_1 = 31$		$r_1 = 1A + 0B$
$r_2 = 23$		$r_2 = 0A + 1B$
$r_3 = 8$	$r_3 = r_1 - 1 \cdot r_2$	$r_3 = 1A - 1B$
$r_4 = 7$	$r_4 = r_2 - 2 \cdot r_3$	$r_4 = -2A + 3B$
$r_5 = 1$	$r_5 = r_3 - 1 \cdot r_4$	$r_5 = 3A - 4B$

We now know that $1 = 3 \cdot 31 - 4 \cdot 23$. Multiplying both sides by 11 yields $11 = 33 \cdot 31 - 44 \cdot 23$. So, $j = -44$ and $k = -33$. Plugging in either one we find that $[z]_{713} = [-998]_{713}$, and $[-998]_{713} = [-285]_{713} = [428]_{713}$.

So, $z = 428$.

Let's check. If $z = 428$, we have (just by dividing and taking remainders):

$[428]_{31} = 25$

$[428]_{23} = 14$. Done.

Q 5.0.9: Find $z \in \mathbb{Z}_{15}$ such that $[z]_3 = 2$ and $[z]_5 = 1$.

Q 5.0.10: Find $z \in \mathbb{Z}_{143}$ such that $[z]_{13} = 5$ and $[z]_{11} = 5$.

Q 5.0.11: Find $z \in \mathbb{Z}_{120}$ such that $[z]_8 = 3$ and $[z]_{15} = 9$.

So, if you've got a number $z \in \mathbb{Z}_{AB}$ you can find $x \in \mathbb{Z}_A$ and $y \in \mathbb{Z}_B$ by taking the appropriate mods. That is, $[x]_A = [z]_A$ and $[y]_B = [z]_B$. You can talk about this as going from $\mathbb{Z}_{AB} \to (\mathbb{Z}_A, \mathbb{Z}_B)$.

The Chinese Remainder Theorem is the statement that you can go backwards, $(\mathbb{Z}_A, \mathbb{Z}_B) \to \mathbb{Z}_{AB}$. That is, given $x \in \mathbb{Z}_A$ and $y \in \mathbb{Z}_B$, which can be written more succinctly as $(x, y) \in (\mathbb{Z}_A, \mathbb{Z}_B)$, you can find a $z \in \mathbb{Z}_{AB}$ such that $[z]_A = x$ and $[z]_B = y$.

Q 5.0.12: $z \in \mathbb{Z}_{35}$ and $(x, y) \in (\mathbb{Z}_5, \mathbb{Z}_7)$.
-If $y = 0$ and $z = ax$ (for every x), then what is a?
-If $x = 0$ and $z = by$ (for every y), then what is b?
-If $z = ax + by$ (for every x, y), then what are a and b?

What this last question is demonstrating is that you don't have to run through the process of the Chinese remainder theorem for every value of x and y, every single time you want to go from $\mathbb{Z}_{AB} \to (\mathbb{Z}_A, \mathbb{Z}_B)$. For any $(\mathbb{Z}_A, \mathbb{Z}_B)$ you can find a and b such that $[z]_{AB} = [ax + by]_{AB}$, for any $x \in \mathbb{Z}_A$ and $y \in \mathbb{Z}_A$.

Example: For $x \in \mathbb{Z}_5$ and $y \in \mathbb{Z}_7$, $[z]_{35} = [21x + 15y]_{35}$.
The reason this works is that

$$\left\{ \begin{array}{l} [z]_5 \\ = [21x + 15y]_5 \\ = [1x + 0y]_5 \\ = [x]_5 \end{array} \right\} \text{ and } \left\{ \begin{array}{l} [z]_7 \\ = [21x + 15y]_7 \\ = [0x + 1y]_7 \\ = [y]_7 \end{array} \right\}$$

Q 5.0.13: For $(x, y) \in (\mathbb{Z}_{10}, \mathbb{Z}_{19})$, find a and b so that when $z = ax + by$, you have $[x]_{10} = [z]_{10}$ and $[y]_{19} = [z]_{19}$

Q 5.0.14: $x \in \mathbb{Z}_{11}$, $y \in \mathbb{Z}_{13}$, $z \in \mathbb{Z}_{143}$, $[z]_{11} = x$, and $[z]_{13} = y$
Find a and b such that $[z]_{143} = [ax + by]_{143}$

Q 5.0.15: $[z]_{AB} = [ax + by]_{AB}$, with $[z]_A = x$, and $[z]_B = y$. What are a and b in the form $([\cdot]_A, [\cdot]_B)$?

Q 5.0.16: $[z]_{ABC} = [ax + by + cw]_{ABC}$, with $[z]_A = x$, $[z]_B = y$, and $[z]_C = w$. What are a, b, and c in the form $([\cdot]_A, [\cdot]_B, [\cdot]_C)$?

So, in order to have $[z]_{AB} = [ax+by]_{AB}$ with $[z]_A = x$, and $[z]_B = y$ as in the examples and problems above, we find that:

$[z]_A = x$ implies that $[a]_A = 1$ and $[b]_A = 0$
$[z]_B = y$ implies that $[a]_B = 0$ and $[b]_B = 1$
Since, $[a]_B = 0$ we know that $a = kB$. Since $[a]_A = 1$, we know that $[kB]_A = 1$, and therefore $[k]_A = [B^{-1}]_A$

Q 5.0.17: Using Euler's theorem, $[B^{-1}]_A =?$ and $[A^{-1}]_B =?$
-Based on the comment above this problem and using Euler's theorem, what are a and b in general, given A and B, for $[z]_{AB} = [ax + by]_{AB}$ with $[z]_A = x$, and $[z]_B = y$?

5.1 Algebra of the CRT

The reason that the CRT is useful is that it allows you to do arithmetic on large moduli using several smaller moduli. When $gcd(A, B) = 1$:

$$[r + s]_{AB} \sim ([r]_A, [r]_B) + ([s]A, [s]_B) = ([r + s]_A, [r + s]_B)$$
$$[r \cdot s]_{AB} \sim ([r]_A, [r]_B) \cdot ([s]_A, [s]_B) = ([r \cdot s]_A, [r \cdot s]_B)$$

That is, you can do addition and multiplication in $\mathbb{Z}_{AB}$ or in $(\mathbb{Z}_A, \mathbb{Z}_B)$ and (as long as you translate from one to the other properly) you'll get the same answer.

Example: "What is $[43^{50}]_{77}$?"
We can go from $\mathbb{Z}_{77} \to (\mathbb{Z}_7, \mathbb{Z}_{11})$ by taking mods, and to get back from $(\mathbb{Z}_7, \mathbb{Z}_{11}) \to \mathbb{Z}_{77}$ we need to use the CRT.
For $[z]_{77} = [ax + by]_{77}$, we need $[a]_{77} = [B^{\varphi(A)}]_{77}$ and $[b]_{77} = [A^{\varphi(B)}]_{77}$. So, $[a]_{77} = [11^{\varphi(7)}]_{77} = [11^6]_{77} = 22$ and $[b]_{77} = [7^{\varphi(11)}]_{77} = [7^{10}]_{77} = 56$.
$[z]_{77} = [22x+56y]_{77}$. Again, this equation allows us to rapidly go from $(\mathbb{Z}_7, \mathbb{Z}_{11}) \to \mathbb{Z}_{77}$. Now to calculate:

$[43^{50}]_{77}$
$\sim ([43^{50}]_7, [43^{50}]_{11})$
$= ([1^{50}]_7, [10^{50}]_{11})$ "multiply then mod" = "mod then multiply"
$= ([1^{50}]_7, [(-1)^{50}]_{11})$
$= ([1]_7, [1]_{11})$
$\sim [22 \cdot 1 + 56 \cdot 1]_{77}$
$= [78]_{77}$
$= 1$

Alternatively, you could notice that $(1, 1) \sim 1$ in general.

Q 5.1.1: Why is it that $[1]_{AB} \sim ([1]_A, [1]_B)$ in general?

Q 5.1.2: Demonstrate that doing addition and multiplication in $\mathbb{Z}_{15}$ is the same as doing them in $(\mathbb{Z}_3, \mathbb{Z}_5)$ for $[8]_{15} \sim ([2]_3, [3]_5)$ and $[6]_{15} \sim ([0]_3, [1]_5)$.

Q 5.1.3: Show that doing addition and multiplication in either $\mathbb{Z}_{AB}$ or $(\mathbb{Z}_A, \mathbb{Z}_B)$ works

in general, using the fact that $z = ax + by$.

Q 5.1.4: $[26^{100}]_{65} =?$

Q 5.1.5: Write $[26]_{3131}$ as $([\cdot]_{31}, [\cdot]_{101})$. What is the equation that takes you back from $(\mathbb{Z}_{31}, \mathbb{Z}_{101}) \to \mathbb{Z}_{3131}$?

Q 5.1.6: If $[z]_{AB} \sim ([x]_A, [y]_B)$, then $[z^{-1}]_{AB} \sim ([?]_A, [?]_B)$. Prove it.

Q 5.1.7: By using the decomposition in $(\mathbb{Z}_P, \mathbb{Z}_Q)$, show that $[z^{\varphi(PQ)+1}]_{PQ} = [z]_{PQ}$, when P and Q are different primes, for *all* values of z, even when $gcd(z, PQ) \neq 1$.