Chinese Remainder Theorem Exercise Solutions

1. In the example Evo problem on the previous page, we discussed how Evo would guess the number 23. Try this out on Evo. Does he get the correct result?
   Yes.

2. Consider the following set of simultaneous modular equations. Do they meet the requirements of the Chinese remainder theorem? Why or why not?

   $x \equiv 2 \pmod 3$
   $x \equiv 3 \pmod 5$
   $x \equiv 5 \pmod 6$

   They do not meet the requirements of the Chinese remainder theorem. The GCD(3,6) = 3. The GCD must be 1 to meet the requirements.

3. Suppose that a set of three simultaneous modular equations involves finding the remainders when a number *x* is divided by by 7, 11, and 13. What is the range for x?
   The product of the divisors 7•11•13 = 1001. Therefore, the range is 0 to 1000.

4. In exercise 3, could we design an OzoBlockly program with the stated divisors that makes use of the Chinese remainder theorem? Why or why not?
   No. OzoBlockly only allows integers up to 127.

5. Solve the following set of simultaneous modular equations for *x* using the three steps discussed earlier in this document. Show your work, so it is clear how you solved this modular system of equations. Can an OzoBlockly program be designed for this system using the Chinese remainder theorem? Why or why not?

   $x \equiv 1 \pmod 3$
   $x \equiv 3 \pmod 5$
   $x \equiv 6 \pmod 7$

   Step 1: The three divisors 3, 5, and 7 are all pairwise prime.
   Step 2: The modulus is 3•5•7 = 105.
   Step 3:

	mod 3	mod 5	mod 7
	5•7	3•7	3•5
	35•2	21•1	15•1
	70	21	15

   $x \equiv 70 \cdot 1 + 21 \cdot 3 + 15 \cdot 6 \pmod{105}$
   $x \equiv 223 \pmod{105} \rightarrow x = 13$

6. Solve the following set of *four* simultaneous modular equations for *x* using the three steps discussed earlier in this document. Show your work, so it is clear how you solved this modular system of equations. Check your final answer for x and make sure it satisfies all four congruences. If it doesn't, go back and find where you errored.

$x \equiv 1 \pmod 2$
$x \equiv 2 \pmod 3$
$x \equiv 4 \pmod 5$
$x \equiv 6 \pmod 7$

Step 1: The four divisors 2, 3, 5, and 7 are all pairwise prime.

Step 2: The modulus is $2 \cdot 3 \cdot 5 \cdot 7 = 210$.

Step 3:

	mod 2	mod 3	mod 5	mod 7
	$3 \cdot 5 \cdot 7$	$2 \cdot 5 \cdot 7$	$2 \cdot 3 \cdot 7$	$2 \cdot 3 \cdot 5$
	$105 \cdot 1$	$70 \cdot 1$	$42 \cdot 3$	$30 \cdot 4$
	105	70	126	120

$x \equiv 105 \cdot 1 + 70 \cdot 2 + 126 \cdot 4 + 120 \cdot 6 \pmod{210}$
$x \equiv 105 + 140 + 504 + 720 \pmod{210}$
$x \equiv 1469 \pmod{210} \rightarrow x = 209$

Check: $209 \equiv 1 \pmod 2$
$209 \equiv 2 \pmod 3$
$209 \equiv 4 \pmod 5$
$209 \equiv 6 \pmod 7$