CLARK UNIVERSITY

Exercises
Math 225 Modern Algebra
Fall 2017

34. Solve the following system of simultaneous linear congruences. You can use either Brahmagupta's algorithm, Qin Jiushao's algorithm, or something of your own devising.

$$\begin{aligned} x &\equiv 4 \pmod{33} \\ x &\equiv 22 \pmod{35} \\ x &\equiv 41 \pmod{53} \end{aligned}$$

Be sure to show how you derived the solution.

Here's Qin Jiushao's algorithm.

Step 1. For each modulus, find a reciprocal of the product of the remaining moduli modulo the given modulus.

For the first modulus, 33, that means we need the reciprocal of the products of the other two moduli, $35 * 53 = 1855$, modulo 33, that is, we need to solve $1855 \equiv 1 \pmod{33}$, which is equivalent to $7y \equiv 1 \pmod{33}$. Next, use the extended Euclidean algorithm to find a solution. Write that congruence as the equation $7y = 1 + 33z$. Since $33 = 4 \cdot 7 + 5$, that equation is $7(y - 4z) = 1 + 5z$, or $7w = 1 + 5z$ where $w = y - 4z$. Since $7 = 2 + 5$, the last equation is $2w = 1 + 5(z - w)$, or $2w = 1 + 5v$ where $v = z - w$. A solution to $2w + 1 + 5v$ is $w = 3, v = 1$. Then, since $v = z - w$, $1 = z - 3$, therefore $z = 4$. And since $w = y - 4z$, $3 = y - 4 \cdot 4$, therefore $y = 19$. Thus, $y \equiv 19 \pmod{33}$ is the reciprocal of 1855 modulo 33.

For the second modulus, 35, the solution to $1149y \equiv 1 \pmod{35}$, that is, $34y \equiv 1 \pmod{35}$, turns out to be $y = 34 \pmod{35}$.

For the third modulus, 53, the solution to $1155y \equiv 42y \equiv 1 \pmod{53}$ is $y \equiv 24 \pmod{53}$.

Step 2. To get x sum three products abc, one for each congruence, where a is the constant in the congruence, b is the product of the other moduli, and c is the reciprocal found in the previous step. That gives us

$$4 \cdot 1855 \cdot 19 + 22 \cdot 1749 \cdot 34 + 41 \cdot 1144 \cdot 22 = 2585752.$$

We can reduce that modulo the product $33 \cdot 35 \cdot 53 = 61215$ to get a smaller number, 14722.

37. Determine the initial object and the final object in the category $\mathcal{S}$ of sets.

Of these two objects, it's easier to find the final object in the category of sets. We need a set T such that for any set S there exists a unique function $S \to T$. The set T can't have more than one element, because if it has more, then there were be choices to make and the function won't be unique. But if T has exactly one element, then all the elements of S will have to be sent to that element. And, when T has exactly one element there is a function $S \to T$. Thus, any singleton set is a final object in the category of sets.

Finding the initial object is harder, at least conceptually. We need a set S such that for any set T there exists a unique function $S \to T$. If S has any element, then there will be choices to make as to where to send that element. So the initial object can't have any elements. All that's left is the emptyset $\emptyset$. Does there exist a unique function $\emptyset \to T$? Yes, there is exactly one such function. It's usually called the empty function. A function $f : S \to T$ can be identified with its graph, a subset of $S \times T$:

$$f = \{(x, y) \in S \times T \mid f(x) = y\}.$$

So a function $\emptyset \to T$ can be identified with a subset of $\emptyset \times T$. But $\emptyset \times T = \emptyset$ has exactly one subset, namely itself, $\emptyset$, which represents the empty function $\emptyset \to T$.

Math 225 Home Page at
`http://aleph0.clarku.edu/~djoyce/ma225/`