Math 25 — Assignment 2

Due Thursday, October 13th, *beginning of class*.

1. Write down the addition and multiplication tables for $\mathbb{Z}/4\mathbb{Z}$. Is the following statment true:

   If $6x \equiv 2 \pmod 4$, then $3x \equiv 1 \pmod 4$.

   Solution:

   The addition and multiplication tables are, respectively,

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

   We can see from the table the statement is false. If $x = 1$, then $6x \equiv 2 \pmod 4$, but $3x \not\equiv 1 \pmod 4$. The problem comes from the fact that 2 has no multiplicative inverse.

2. Solve the linear congruence equation

$$56x \equiv 29 \pmod{101}.$$

   Solution: Using the XGCD algorithm we find that $56(-9) + 101(5) = 1$. Thus, $\gcd(56, 101) = 1$ and $56 \cdot (-9) \equiv 1 \pmod{101}$. In particular,

$$56(-9 \cdot 29) \equiv 29 \pmod{101}.$$

   In other words, $x \equiv 42 \pmod{101}$ is the unique congruence class of solutions. (See Corollary 3.8 of the book.)

3. Find all integers x satisfying the simultaneous linear congruences:

$$\begin{aligned} 2x &\equiv 2 \pmod{11} \\ 5x &\equiv 3 \pmod{12} \\ 31x &\equiv 4 \pmod{13} \\ x &\equiv 5 \pmod{17} \\ x &\equiv 6 \pmod{19} \end{aligned}$$

   (You may want a calculator on hand for this one.)

   Solution: Because $\gcd(2, 11) = \gcd(5, 12) = \gcd(31, 13) = 1$, the solution to each individual congruence is unique. The numbers are small, so we see by inspection that:

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 3 \pmod{12} \\ x &\equiv 6 \pmod{13} \\ x &\equiv 5 \pmod{17} \\ x &\equiv 6 \pmod{19} \end{aligned}$$

(You can also use XGCD, but this is overkill.)

We next want to compute the lifting map from the Chinese Remainder Theorem. This requires solving

$$\hat{N}_i \cdot c_i \equiv 1 \pmod{n_i}$$

where $n_i = 11, 12, 13, 17, 19$ and $\hat{N}_i$ are as in Question 4. In particular

$$\begin{aligned} \hat{N}_1 c_1 &\equiv 1 \pmod{n}_1 \\ \hat{N}_2 c_2 &\equiv 1 \pmod{n}_2 \\ \hat{N}_3 c_3 &\equiv 1 \pmod{n}_3 \\ \hat{N}_4 c_4 &\equiv 1 \pmod{n}_4 \\ \hat{N}_5 c_5 &\equiv 1 \pmod{n}_5 \end{aligned} \implies \begin{aligned} 8c_1 &\equiv 1 \pmod{11} \\ c_2 &\equiv 1 \pmod{12} \\ 9c_3 &\equiv 1 \pmod{13} \\ 15c_4 &\equiv 1 \pmod{17} \\ 7c_5 &\equiv 1 \pmod{19} \end{aligned} \implies \begin{aligned} c_1 &\equiv 7 \pmod{11} \\ c_2 &\equiv 1 \pmod{12} \\ c_3 &\equiv 3 \pmod{13} \\ c_4 &\equiv 8 \pmod{17} \\ c_5 &\equiv 11 \pmod{19} \end{aligned}.$$

The CRT lifting map is then

$$\psi(x_1, x_2, x_3, x_4, x_5) = 50388 \cdot 7x_1 + 46189 \cdot x_2 + 42636 \cdot 3x_3 + 32604 \cdot 8x_4 + 29172 \cdot 11x_5 \pmod{554268}.$$

This gives that

$$x = \psi(1, 3, 6, 5, 6) \equiv 54099 \pmod{554268}.$$

Of course, we want all integers satisfying these congruences. Because the CRT guarantees that this is the unique lift satisfying the simultaneous system of congruences, which itself had unique solutions, we have that the set of all integer solutions is given by

$$\{54099 + 554268q : q \in \mathbb{Z}\}. \quad \square$$

Remark: Nothing this computationally intensive will be on the midterm. This is the type of exercise everyone has to do at least once in their life to really "get" the CRT.

Remark: Most computer algebra systems have a built-in CRT method. In sage, this is

```
crt([1,3,6,5,6], [11,12,13,17,19]) # Output 54099.
```

4. Recall the CRT-lift function f from the lectures, defined by:

$$f(x_1, \ldots, x_k) := \hat{N}_1 c_1 x_1 + \hat{N}_2 c_2 x_2 + \ldots + \hat{N}_k c_k x_k \pmod{N}$$

where $n_1, \ldots, n_k$ are coprime integers, $N := n_1 \ldots n_k$, $\hat{N}_i := N/n_i$, and the c_i are chosen so that $c_i \hat{N}_i \equiv 1 \pmod{n_i}$.

Prove the following assertions:

(a) f is well-defined. That is, if y_i are integers such that $y_i \equiv x_i \pmod{n_i}$, then

$$f(y_1, \ldots, y_k) \equiv f(x_1, \ldots, x_k) \pmod{N}$$

(b) f is invertible.

(c) $f(0, \ldots, 0) \equiv 0 \pmod{N}$.

(d) $f(1, \ldots, 1) \equiv 1 \pmod{N}$.

(e)

$$f(x_1, \ldots, x_k) + f(y_1, \ldots, y_k) \equiv f(x_1 + y_1, \ldots, x_k + y_k) \pmod{N}.$$

(f) (Advanced topics) That:

$$f(x_1, \ldots, x_k) \cdot f(y_1, \ldots, y_k) \equiv f(x_1 \cdot y_1, \ldots, x_k \cdot y_k) \pmod{N}.$$

The jargon for this is to say that $f \colon \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ is an *isomorphism of rings (with unity)*.

Solution:

(a) Let us write $y_i = n_i q_i + x_i$ for some integers q_i. Then

$$\begin{aligned} f(y_1, \ldots, y_k) &= \sum_{i=1}^{k} \hat{N}_i c_i (n_i q_i + x_i) \\ &= \sum_{i=1}^{k} \hat{N}_i c_i n_i q_i + \sum_{i=1}^{k} \hat{N}_i c_i x_i \\ &= \sum_{i=1}^{k} N c_i q_i + f(x_1, \ldots, x_k) \\ &\equiv f(x_1, \ldots, x_k) \pmod{N}. \end{aligned}$$

The second last equality is from the definition of the $\hat{N}_i$. In particular we see that f is well-defined on residue classes.

(b) We claim that the inverse to f is given by the map

$$g(y) := (y \bmod n_1, \ldots, y \bmod n_k).$$

Observe

$$g(f(x_1, \ldots, x_k)) = \left(\sum_{i=1}^{k} \hat{N}_i c_i x_i \bmod n_1, \ldots, \sum_{i=1}^{k} \hat{N}_i c_i x_i \bmod n_k \right).$$

Let us examine each coordinate. We have

$$\sum_{i=1}^{k} \hat{N}_i c_i x_i \equiv \hat{N}_j c_j x_j \equiv x_j \pmod{n_j}$$

because $n_j \mid \hat{N}_i$ if $i \neq j$, and furthermore, $\hat{N}_j c_j \equiv 1 \pmod{n_j}$ by definition. In other words,

$$g(f(x_1, \ldots, x_k)) = (x_1, \ldots, x_k)$$

that is, g is an inverse to f. Therefore f is a bijection.

(c) $f(0, \ldots, 0) = \sum_{i=1}^{k} c_i \hat{N}_i \cdot 0 \equiv 0 \pmod{N}$.

(d) Let use use the inverse g to f constructed before. We have

$$g(1) = (1, \ldots, 1).$$

Because $g(f(1, \ldots, 1)) = (1, \ldots, 1)$, we have $f(1, \ldots, 1) = 1$, since inverses are injective.

(e) Note

$$f(x_1, \ldots, x_k) \equiv \sum_{i=1}^{k} c_i \hat{N}_i \cdot x_i, \quad f(y_1, \ldots, y_k) \equiv \sum_{i=1}^{k} c_i \hat{N}_i \cdot y_i,$$

and

$$f(x_1 + y_1, \ldots, x_k + y_k) \equiv \sum_{i=1}^{k} c_i \hat{N}_i \cdot (x_i + y_i) \equiv \sum_{i=1}^{k} c_i \hat{N}_i \cdot x_i + \sum_{i=1}^{k} c_i \hat{N}_i \cdot y_i \pmod{N}$$

from which the claim follows.

5. Let p be a prime and let $f(x), g(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ be nonzero polynomials modulo p. The *degree* of a non-zero polynomial $a_n x^n + \ldots + a_0 \in \mathbb{Z}/p\mathbb{Z}[x]$ is the largest i such that $a_i \not\equiv 0 \pmod{p}$. For example, if $p = 7$, then
$$\deg(7x^3 + 5x^2 + 1) = 2.$$

(There are different conventions for what $\deg(0)$ should be.)

Prove that

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

Is the statement still true if we do not assume p is prime?

Solution: Let $f = a_n x^n + \ldots + a_0$ and $g = b_m x^m + \ldots + b_0$ with a_n, b_n non-zero modulo p. Then

$$fg = a_n b_m x^{n+m} + \cdots + a_0 b_0.$$

Observe that $a_n b_m \not\equiv 0 \pmod{p}$ because p is prime. By definition of the degree, $\deg(fg) = n+m = \deg(f) + \deg(g)$. □

The claim is not true if the modulus is not prime. Observe

$$(2x+1)(3x) \equiv 6x^2 + 3x \equiv 3x \pmod{6},$$

and $\deg(2x+1) = \deg(3x) = 1$.

6. A 3×3 grid of distinct numbers

$$\begin{matrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{matrix}$$

is called *magic* if the sum of the triples of entries in the rows, columns, and two main diagonals are all equal to the same number. For example, the following is the *Lo Shu* magic square

$$\begin{matrix} 2 & 7 & 6 \\ 9 & 5 & 1 \\ 4 & 3 & 8 \end{matrix}$$

A *magic square of squares* is a magic square, where all of the entries are squares.

The notion of a magic square makes sense if we say that the entries are elements of $\mathbb{Z}/n\mathbb{Z}$. We let $n > 1$ be an integer and let

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

be its prime factorization.

(a) (Advanced topics) Prove that each entry is a square modulo n if and only if it is a square modulo each $p_i^{e_i}$.

(b) Let a, b, c be three integers. Prove that $a + b + c \equiv 0 \pmod{n}$ if and only if $a + b + c \equiv 0 \pmod{p^{e_i}}$ for each prime power.

Conclude the following result:

Proposition 0.1. *Prove that if there exists a magic square of squares modulo $p_i^{e_i}$ for each i, then there exists a magic square of squares modulo n.*

Remark 0.2. For very silly reasons, the converse is false. Consider the following magic square modulo 10. Reducing modulo 2 gives the following grid

$$\begin{matrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{matrix}$$

Because the entries of a magic square are *distinct*, this grid is not a magic square modulo 2. In fact, it is impossible to have a magic square modulo 2.

Solution:

(b) By the Chinese Remainder Theorem, we have that $x \equiv 0 \pmod{p^{e_i}}$ if and only if $x \equiv 0 \pmod{n}$. Because $a+b+c$ is just a number, the result follows immediately.

Let us now address the conclusion about magic squares of squares. Denote by

$$M_\ell := \begin{matrix} x_{11}^{(\ell)} & x_{12}^{(\ell)} & x_{13}^{(\ell)} \\ x_{21}^{(\ell)} & x_{22}^{(\ell)} & x_{23}^{(\ell)} \\ x_{31}^{(\ell)} & x_{32}^{(\ell)} & x_{33}^{(\ell)} \end{matrix}$$

a given magic square of squares modulo $p_\ell^{e_\ell}$, for each $1 \le \ell \le k$. Let $x_{ij} \in \mathbb{Z}/n\mathbb{Z}$ be the unique element such that $x_{ij} \equiv x_{ij}^{(\ell)} \pmod{p_\ell^{e_\ell}}$ given by the CRT. We claim that

$$M := \begin{matrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{matrix}$$

is a magic square of squares modulo n. From part (a), each x_{ij} is a square because it is a square modulo each $p_\ell^{e_\ell}$. The entries of M are distinct, since they are distinct modulo some $p_\ell^{e_\ell}$. Finally, we claim that M is magic.

Because each M_ℓ is magic, we let s_ℓ be the sum of any row/column/diagonal of M_ℓ modulo $p_\ell^{e_\ell}$. We then set s to be the CRT lift of $(s_1, \dots, s_k)$. Note that for any ℓ, we have

$$x_{11} + x_{22} + x_{33} \equiv x_{11}^{(\ell)} + x_{22}^{(\ell)} + x_{33}^{(\ell)} \equiv s_\ell \pmod{p_\ell^{e_\ell}}$$

thus, by the CRT, we have that

$$x_{11} + x_{22} + x_{33} \equiv s \pmod{n}.$$

Similarly, the sum of any row/column/diagonal of M is congruent to $s \pmod{n}$. Thus M is magic modulo n.

Remark 0.3. It is presently unknown whether a 3×3 magic square of squares with integer entries exists. It is also "unknown" [1] whether a 3×3 magic square of squares with entries in $\mathbb{Z}/n\mathbb{Z}$ exists for all sufficiently large n. See `https://www.youtube.com/watch?v=FCczHiXPVcA`.

[1] Prof. Voight and I have ideas about how to solve this.