## SOLUTION OF ASSESSED COURSEWORK 1

**Q1**. Find the solutions for the following simultaneous congruences:

$$x \equiv 2 \bmod 3,$$
$$5x \equiv 1 \bmod 4,$$
$$3x \equiv 4 \bmod 5.$$

**A1**. We would like to use CRT (Theorem 9).

Proposition 8 in the notes shows that the congruence equation

$$ax \equiv b \bmod n$$

is soluble if and only if $\gcd(a, n) = 1$. The proof of Proposition 8 is indeed constructive: if $\gcd(a, n) = 1$, there exist $r, s$ in $\mathbb{Z}$ such that $ar + ns = \gcd(a, n) = 1$ by Euclid's algorithm. It therefore follows that

$$ar \equiv 1$$

mod $n$. Hence

$$x \equiv rax \equiv rb.$$

Applying the argument for $(a, b, n) = (5, 1, 4)$ and $(3, 4, 5)$, we are reduced to solving the simultaneous congruences

$$x \equiv 2 \bmod 3,$$
$$x \equiv 1 \bmod 4,$$
$$x \equiv 3 \bmod 5.$$

Of course, there are much simpler ways of doing this sort of thing. For example, one can simply subtract $4x \equiv 0 \bmod 4$ from $5x \equiv 1 \bmod 4$ to get $x \equiv 1 \bmod 4$.

The CRT twice then proves that $x \equiv 53 \bmod 60$. How to solve a system of 'monic' congruence equations was indeed explained in the lectures/in the notes (Example immediately after Theorem 10).

**Q2**. Let $(\mathbb{Z}/18\mathbb{Z})^\times$ be the subgroup of units in $\mathbb{Z}/18\mathbb{Z}$. Determine the least positive integer $N$ such that $[g]^N = [1]$ holds for any element $[g]$ in $(\mathbb{Z}/18\mathbb{Z})^\times$.

**A2**. If $[z]$ is an element of $\mathbb{Z}/18\mathbb{Z}$, then it lies in $(\mathbb{Z}/18\mathbb{Z})^\times$ if and only if $\mathrm{GCD}(z, 18) = 1$. Hence $(\mathbb{Z}/18\mathbb{Z})^\times = \{[1], [5], [7], [11], [13], [17]\}$. Proposition 14 asserts that $|(\mathbb{Z}/18\mathbb{Z})^\times| = \phi(18) = \phi(2 \cdot 3^2) = \phi(2)\phi(3^2) = (2 - 1)3(3 - 1) = 6$. We simply compute their orders mod 18:

*Date*: November 6, 2023.

| | order mod 18 |
|---|---|
| 1 | 1 |
| 5 | 6 |
| 7 | 3 |
| 11 | 6 |
| 13 | 3 |
| 17 | 2 |

In computing the order, we may use Proposition 20 to deduce that it has to be a divisor of $\phi(18) = 6$, i.e., it is either $1, 2, 3$ or 6. From the table, we conclude that $N = 6$.

**Q3**. Is 20964 a quadratic residue mod 1987?

An exercise in quadratic reciprocity. For example,

$$\begin{aligned}
& \left(\frac{20964}{1987}\right) \\
= & \left(\frac{1094}{1987}\right) \\
= & \left(\frac{547}{1987}\right)\left(\frac{2}{1987}\right) \\
= & -\left(\frac{547}{1987}\right) \\
= & \left(\frac{1987}{547}\right) \\
= & \left(\frac{346}{547}\right) \\
= & \left(\frac{173}{547}\right)\left(\frac{2}{547}\right) \\
= & -\left(\frac{173}{547}\right) \\
= & -\left(\frac{547}{173}\right) \\
= & -\left(\frac{28}{173}\right) \\
= & -\left(\frac{2}{173}\right)^2\left(\frac{7}{173}\right) \\
= & -\left(\frac{7}{173}\right) \\
= & -\left(\frac{173}{7}\right) \\
= & -\left(\frac{5}{7}\right) \\
= & -\left(\frac{7}{5}\right) \\
= & -\left(\frac{2}{5}\right) \\
= & (-1)(-1) \\
= & 1
\end{aligned}$$