Math 115A Final Exam

Ethan Martirosyan

March 20, 2024

Problem 1

Part (i)

We note that

$$\left(\frac{105}{191}\right) = \left(\frac{3}{191}\right)\left(\frac{5}{191}\right)\left(\frac{7}{191}\right)$$

First, we will compute

$$\left(\frac{3}{191}\right)$$

Notice that $3 \equiv 3 \pmod 4$ and $191 \equiv 3 \pmod 4$. Appealing to the quadratic reciprocity law, we have

$$\left(\frac{3}{191}\right) = -\left(\frac{191}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{(3^2-1)/8} = -(-1) = 1$$

Next, we compute

$$\left(\frac{5}{191}\right)$$

Notice that $5 \equiv 1 \pmod 4$. By the quadratic reciprocity law, we have

$$\left(\frac{5}{191}\right) = \left(\frac{191}{5}\right) = \left(\frac{1}{5}\right) = 1$$

Finally, we compute

$$\left(\frac{7}{191}\right)$$

Notice that $7 \equiv 3 \pmod 4$ and $191 \equiv 3 \pmod 4$. By the quadratic reciprocity law, we have

$$\left(\frac{7}{191}\right) = -\left(\frac{191}{7}\right) = -\left(\frac{2}{7}\right) = -(-1)^{(7^2-1)/8} = -(-1)^6 = -1$$

Substitution then yields

$$\left(\frac{105}{191}\right) = \left(\frac{3}{191}\right)\left(\frac{5}{191}\right)\left(\frac{7}{191}\right) = 1 \cdot 1 \cdot -1 = -1$$

Part (ii)

Notice that

$$\left(\frac{56}{101}\right) = \left(\frac{7}{101}\right)\left(\frac{8}{101}\right) = \left(\frac{7}{101}\right)\left(\frac{2^3}{101}\right) = \left(\frac{7}{101}\right)\left(\frac{2}{101}\right)^3 = \left(\frac{7}{101}\right)\left(\frac{2}{101}\right)$$

First, we will compute

$$\left(\frac{7}{101}\right)$$

Since $101 \equiv 1 \pmod 4$, we may appeal to the quadratic reciprocity law to deduce that

$$\left(\frac{7}{101}\right) = \left(\frac{101}{7}\right) = \left(\frac{3}{7}\right)$$

Since $3 \equiv 3 \pmod 4$ and $7 \equiv 3 \pmod 4$, we may appeal to the quadratic reciprocity law to find

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

Next, we will compute

$$\left(\frac{2}{101}\right)$$

Notice that $101 \equiv 5 \pmod 8$ so that

$$\left(\frac{2}{101}\right) = -1$$

Substitution then yields

$$\left(\frac{56}{101}\right) = \left(\frac{7}{101}\right)\left(\frac{2}{101}\right) = (-1)\cdot(-1) = 1$$

Part (iii)

Notice that

$$\left(\frac{106}{89}\right) = \left(\frac{17}{89}\right)$$

since $106 \equiv 17 \pmod{89}$. Because $17 \equiv 1 \pmod 4$, the quadratic reciprocity law informs us that

$$\left(\frac{17}{89}\right) = \left(\frac{89}{17}\right)$$

Because $89 \equiv 4 \pmod{17}$, we have

$$\left(\frac{89}{17}\right) = \left(\frac{4}{17}\right) = \left(\frac{2^2}{17}\right) = \left(\frac{2}{17}\right)^2 = 1$$

Problem 2

Part (i)

First, we compute $(14, 31)$ as follows:

$$
\begin{aligned}
31 &= 14 \cdot 2 + 3 \\
14 &= 3 \cdot 4 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 2 \cdot 1
\end{aligned}
$$

This shows that $(14, 31) = 1$. Thus, we know that this congruence has exactly one solution. Now, we have

$$1 = 3 - 2 = 3 - (14 - 3 \cdot 4) = 5 \cdot 3 - 14 = 5 \cdot (31 - 14 \cdot 2) - 14 = 5 \cdot 31 - 11 \cdot 14$$

From this, we find that

$$-11 \cdot 14 \equiv 1 \pmod{31}$$

so that

$$-33 \cdot 14 \equiv 3 \pmod{31}$$

Notice that $-33 \equiv 29 \pmod{31}$, so the solution of $14x \equiv 3 \pmod{31}$ is $29 \pmod{31}$.

Part (ii)

First, we will compute $(35, 15)$ as follows:

$$35 = 15 \cdot 2 + 5$$
$$15 = 5 \cdot 3$$

so that $(35, 15) = 5$. However, we note that $5 \nmid 9$, so the congruence $15x \equiv 9 \pmod{35}$ has no solution.

Part (iii)

First, we may compute $(35, 56)$ as follows:

$$
\begin{aligned}
56 &= 35 \cdot 1 + 21 \\
35 &= 21 \cdot 1 + 14 \\
21 &= 14 \cdot 1 + 7 \\
14 &= 7 \cdot 2
\end{aligned}
$$

so that $(35, 56) = 7$. Since $7 \mid 14$, we know that there are 7 solutions. Dividing the congruence $35x \equiv 14 \pmod{56}$ by 7 yields $5x \equiv 2 \pmod{8}$. Performing the Euclidean Algorithm, we obtain

$$
\begin{aligned}
8 &= 5 \cdot 1 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 2 \cdot 1
\end{aligned}
$$

Then, we have

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2 \cdot (8 - 5) - 5 = -3 \cdot 5 + 2 \cdot 8$$

so that $5 \cdot -3 \equiv 1 \pmod{8}$. This informs us that $5 \cdot -6 \equiv 2 \pmod{8}$. Since $-6 \equiv 2 \pmod{8}$, we find that $5 \cdot 2 \equiv 2 \pmod{8}$ so that $x = 2$ is a solution of the congruence $5x \equiv 2 \pmod{8}$. Thus it is also a solution of the congruence $35x \equiv 14 \pmod{56}$. The other solutions can be found by adding multiples of 8. That is, the solutions of $35x \equiv 14 \pmod{56}$ are $x \equiv 2, 10, 18, 26, 34, 42, 50 \pmod{56}$.

Problem 3

Part (i)

First, we note that

$$\left[\frac{x}{n}\right] = \sum_{m \le x/n} 1$$

because $[x/n]$ counts the number of positive integers less than or equal to x/n. Using this, we find that

$$\sum_{n \le x} \left[\frac{x}{n}\right] = \sum_{n \le x} \sum_{m \le x/n} 1 = \sum_{n \le x} \sum_{nm \le x} 1$$

Notice that we are summing over all pairs (n, m) of positive integers such that $nm \le x$. Letting $l = mn$ and interchanging the order of summation, we obtain

$$\sum_{n \le x} \sum_{nm \le x} 1 = \sum_{l \le x} \sum_{n \mid l} 1 = \sum_{l \le x} \tau(l)$$

Part (ii)

We may use the following facts:

$$\left[\frac{x}{n}\right] = \frac{x}{n} + O(1)$$

and

$$\sum_{n \le x} \frac{1}{n} = \log x + O(1)$$

Now, we note that

$$\begin{aligned}
&\sum_{n \le x} \tau(n) = \sum_{n \le x} \left[\frac{x}{n}\right] = \sum_{n \le x} \left(\frac{x}{n} + O(1)\right) = \sum_{n \le x} \frac{x}{n} + O(x) = x \sum_{n \le x} \frac{1}{n} + O(x) \\
&= x(\log x + O(1)) + O(x) = x \log x + O(x) + O(x) = x \log x + O(2x) \\
&= x \log x + O(x)
\end{aligned}$$

by the properties of O-notation.

Problem 4

First, we claim that the set

$$A = \{an + b \mid 1 \leq n \leq m\}$$

is a complete system of residues modulo m. To prove this, we will show that $|A| = m$ and that A is incongruent modulo m. It is evident that $|A| = m$ because there are m numbers between 1 and m. Next, we claim that A is incongruent modulo m. Suppose that

$$an_1 + b \equiv an_2 + b \pmod{m}$$

for some n_1 and n_2 satisfying $1 \leq n_1, n_2 \leq m$. Subtracting b yields

$$an_1 \equiv an_2 \pmod{m}$$

Since $(a, m) = 1$, we may divide by a to obtain

$$n_1 \equiv n_2 \pmod{m}$$

This implies that $n_1 - n_2$ is divisible by m. Since $|n_1 - n_2| < m$, we find that $n_1 = n_2$ so that $an_1 + b = an_2 + b$, thus proving that the set A is incongruent modulo m. This shows that A is a complete system of residues modulo m. Notice that the set $B = \{0, 1, \ldots, m-1\}$ is also a complete system of residues modulo m. Finally, we note that the function $\{x\}$ is of period 1. By a theorem we proved in class, we know that

$$\sum_{x \in A} \left\{ \frac{x}{m} \right\} = \sum_{y \in B} \left\{ \frac{y}{m} \right\}$$

so that

$$\sum_{n=1}^{m} \left\{ \frac{an+b}{m} \right\} = \sum_{n=0}^{m-1} \left\{ \frac{n}{m} \right\} = \sum_{n=0}^{m-1} \frac{n}{m} = \frac{1}{m} \sum_{n=0}^{m-1} n = \frac{1}{m} \cdot \frac{(m-1)m}{2} = \frac{m-1}{2}$$

Problem 5

Part (i)

The set S is a reduced system of residues modulo p. In class, we proved that S contains $(p-1)/2$ quadratic residues modulo p and $(p-1)/2$ quadratic non-residues modulo p. By definition, we know that

$$\left(\frac{s}{p}\right) = 1$$

if s is a quadratic residue modulo p and

$$\left(\frac{s}{p}\right) = -1$$

if s is a non-quadratic residue modulo p. Thus, we find that

$$\sum_{s \in S} \left(\frac{s}{p}\right) = \frac{p-1}{2} - \frac{p-1}{2} = 0$$

Part (ii)

Let $R = \{1, 2, \ldots, p-1\}$ be a reduced system of residues modulo p. First, we claim that

$$\sum_{s \in S} \left(\frac{1+s}{p}\right) = \sum_{r \in R} \left(\frac{1+r}{p}\right)$$

To show this, we note that S and R are both reduced systems of residues modulo p. Thus, we know that for every $s \in S$, there is exactly one $r \in R$ such that $s \equiv r \pmod{p}$. Then, we have $s + 1 \equiv r + 1 \pmod{p}$ so that

$$\left(\frac{s+1}{p}\right) = \left(\frac{r+1}{p}\right)$$

Summing over $s \in S$ and $r \in R$ then yields

$$\sum_{s \in S} \left(\frac{1+s}{p}\right) = \sum_{r \in R} \left(\frac{1+r}{p}\right)$$

Notice that

$$\sum_{r \in R} \left(\frac{1+r}{p}\right) = \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) + \left(\frac{p}{p}\right)$$

By assumption, we know that

$$\left(\frac{p}{p}\right) = 0$$

so that

$$\left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) + \left(\frac{p}{p}\right) = \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right)$$

Since

$$\left(\frac{1}{p}\right) = 1$$

we may write

$$\left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) - 1$$

Since $R = \{1, \ldots, p-1\}$, we have

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) - 1 = \sum_{r \in R} \left(\frac{r}{p}\right) - 1 = 0 - 1 = -1$$

by part (i).

Problem 6

Let $R = \{1, \ldots, p-1\}$ and let $r \in R$. We may consider the congruence

$$xr \equiv 1 \pmod{p}$$

We claim that this congruence has a unique solution x modulo p. Since $(r, p) = 1$, there must exist integers a and b such that

$$ar + bp = 1$$

so that $ar \equiv 1 \pmod{p}$. Thus $x = a$ is a solution to this congruence. Next, we claim that this solution is unique. Suppose that $x_1 r \equiv x_2 r \equiv 1 \pmod{p}$. Then, we have

$$(x_1 - x_2)r \equiv 0 \pmod{p}$$

Thus $(x_1 - x_2)r$ is divisible by p. Since r is not divisible by p, we find that $x_1 - x_2$ is divisible by p so that $x_1 \equiv x_2 \pmod{p}$. This shows that the solution is unique. Now, we may define $f : R \to R$ as follows: $f(r) \cdot r \equiv 1 \pmod{p}$. We claim that f is bijective. First, we will show that f is injective. Suppose that $f(x_1) = f(x_2)$ for $x_1, x_2 \in R$. Then, we have

$$f(x_1)x_1 \equiv 1 \equiv f(x_2)x_2 \pmod{p}$$

By substituting $f(x_1) = f(x_2)$ into the previous congruence, we have

$$f(x_1)x_1 \equiv f(x_1)x_2 \pmod{p}$$

Since $(f(x_1), p) = 1$, we deduce that

$$x_1 \equiv x_2 \pmod{p}$$

Thus $x_1 - x_2$ is divisible by p. Since $|x_1 - x_2| < p$, we must have $x_1 = x_2$, so f is injective. Next, we claim that f is surjective. Let $a \in R$. Above, we proved that there exists some $x \in R$ such that $ax \equiv 1 \pmod{p}$. By definition, $x = f(a)$. Thus f is surjective. This means that f is bijective. Now, we note that

$$\left(\frac{f(r)}{p}\right)^2 = 1$$

so that

$$\left(\frac{r(r+k)}{p}\right) = \left(\frac{f(r)}{p}\right)^2 \left(\frac{r(r+k)}{p}\right) = \left(\frac{f(r)}{p}\right)\left(\frac{f(r)}{p}\right)\left(\frac{r}{p}\right)\left(\frac{r+k}{p}\right) = \left(\frac{f(r)r}{p}\right)\left(\frac{f(r)r + kf(r)}{p}\right)$$

Note that

$$\left(\frac{f(r)r}{p}\right) = \left(\frac{1}{p}\right) = 1$$

since $f(r)r \equiv 1 \pmod{p}$. Similarly, we have

$$\left(\frac{f(r)r + kf(r)}{p}\right) = \left(\frac{1 + kf(r)}{p}\right)$$

since $f(r)r + kf(r) \equiv 1 + kf(r) \pmod{p}$. Using these two facts, we find that

$$\left(\frac{f(r)r}{p}\right)\left(\frac{f(r)r + kf(r)}{p}\right) = \left(\frac{1 + kf(r)}{p}\right)$$

Since f is bijective, $\{f(r) \mid r \in R\} = R$ is a reduced system of residues modulo p. Because $(k,p) = 1$, we find that $\{kf(r) \mid r \in R\}$ is also a reduced system of residues modulo p. Thus, we deduce that

$$\sum_{r=1}^{p-1}\left(\frac{r(r+k)}{p}\right) = \sum_{r\in R}\left(\frac{r(r+k)}{p}\right) = \sum_{r\in R}\left(\frac{1+kf(r)}{p}\right) = \sum_{r\in R}\left(\frac{1+r}{p}\right) = -1$$

by part (ii) of problem 5.