Math 115A Homework 3

Ethan Martirosyan

February 23, 2024

Problem 1

We claim that the function

$$\frac{\mu(d)}{d}$$

is multiplicative. Let us suppose that m and n are positive integers such that $(m, n) = 1$. Notice that

$$\frac{\mu(mn)}{mn} = \frac{\mu(m)\mu(n)}{mn} = \frac{\mu(m)}{m} \cdot \frac{\mu(n)}{n}$$

since μ is multiplicative. In class, we proved that if a function is multiplicative, so is its mobius transform. Thus, the function

$$g(n) = \sum_{d|n} \frac{\mu(d)}{d}$$

is multiplicative. Since $n = p_1^{e_1} \cdots p_k^{e_k}$, we have

$$g(n) = g(p_1^{e_1} \cdots p_k^{e_k}) = g(p_1^{e_1}) \cdots g(p_k^{e_k})$$

For any i, we have

$$g(p_i^{e_i}) = \sum_{d|p_i^{e_i}} \frac{\mu(d)}{d} = \sum_{j=0}^{e_i} \frac{\mu(p_i^j)}{p_i^j}$$

If $j > 1$, then

$$\frac{\mu(p_i^j)}{p_i^j} = 0$$

by the definition of μ. If $j = 1$, then

$$\frac{\mu(p_i^j)}{p_i^j} = \frac{\mu(p_i)}{p_i} = -\frac{1}{p_i}$$

If $j = 0$, then

$$\frac{\mu(p_i^j)}{p_i^j} = \frac{\mu(p_i^0)}{p_i^0} = \frac{\mu(1)}{1} = 1$$

Thus, we find that

$$g(p_i^{e_i}) = \sum_{j=0}^{e_i} \frac{\mu(p_i^j)}{p_i^j} = \left(1 - \frac{1}{p_i}\right)$$

Therefore, we may deduce that

$$\sum_{d|n} \frac{\mu(d)}{d} = g(n) = g(p_1^{e_1}) \cdots g(p_k^{e_k}) = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Problem 2

To prove that the set

$$T = \{am + b : \ m \in S\}$$

is a complete system of residues modulo n, we must show that $|T| = n$ and that T is incongruent modulo n. To prove that $|T| = n$, we may define the function $f : S \to T$ as follows:

$$f(m) = am + b$$

First, we claim that f is injective. Suppose that $m_1, m_2 \in S$ and that

$$f(m_1) = f(m_2)$$

or

$$am_1 + b = am_2 + b$$

Since a is nonzero, we find that

$$m_1 = m_2$$

Thus f is injective. Next, we claim that f is surjective. Suppose that $am + b \in T$ where $m \in S$. Then, it is evident that

$$f(m) = am + b$$

so that f is surjective. We deduce that f is bijective. Thus, we have $|T| = |S| = n$ (we know that $|S| = n$ since S is a complete system of residues modulo n). Next, we claim that T is incongruent modulo n. Suppose that

$$am_1 + b \equiv am_2 + b \pmod{n}$$

Subtracting b yields

$$am_1 \equiv am_2 \pmod{n}$$

Since $(a, n) = 1$ by assumption, we may divide by a to deduce that

$$m_1 \equiv m_2 \pmod{n}$$

Since $m_1, m_2 \in S$ and S is incongruent modulo n, we may deduce that $m_1 = m_2$ so that

$$am_1 + b = am_2 + b$$

This proves that T is incongruent modulo n, so we know that T is a complete system of residues modulo n.

Problem 3

To prove that the set

$$Y = \{am : \ m \in X\}$$

is a reduced system of residues modulo n, we must show that $|Y| = \varphi(n)$, that every element of Y is coprime to n, and that Y is incongruent modulo n. To show that $|Y| = \varphi(n)$, we may define the function $f : X \to Y$ as follows:

$$f(m) = am$$

First, we claim that f is injective. Let

$$f(m_1) = f(m_2)$$

where $m_1, m_2 \in X$. Then we have

$$am_1 = am_2$$

so that $m_1 = m_2$. Thus f is injective. Next, we claim that f is surjective. Let $am \in Y$, where $m \in X$. Then, we have

$$f(m) = am$$

so that f is surjective. Thus f is bijective, and we know that $|Y| = |X| = \varphi(n)$ (we know that $|X| = \varphi(n)$ because X is assumed to be a reduced system of residues modulo n). Next, we claim that every element of Y is coprime to n. Let $am \in Y$, where $m \in X$. Notice that $(a, n) = 1$ by assumption and $(m, n) = 1$ since X is a reduced system of residues modulo n. Thus, we find that $(am, n) = 1$. Finally, we claim that Y is incongruent modulo n. Suppose that

$$am_1 \equiv am_2 \pmod{n}$$

Since $(a, n) = 1$, we find that

$$m_1 \equiv m_2 \pmod{n}$$

Because X is incongruent modulo n, we know that $m_1 = m_2$ so that $am_1 = am_2$. This means that Y is incongruent modulo n. Thus, we may deduce that Y is a reduced system of residues modulo n.

Problem 4

First, we may let $n = 1$. Notice that $1^p - 1 = 0$ is a multiple of p, so we have

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

Next, we may suppose that $n \geq 1$ and

$$n^p \equiv n \pmod{p}$$

We claim that this congruence holds for $n + 1$. Notice that

$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k 1^{p-k} = \sum_{k=0}^{p} \binom{p}{k} n^k$$

Notice that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

We know that p divides $p!$. For $1 \leq k \leq p-1$, we claim that p does not divide $k!(p-k)!$. If p did divide $k!(p-k)!$, then p must divide $k!$ or $(p-k)!$ because p is prime. This means that p must divide some number less than or equal to k or some number less than or equal to $p - k$, which is not true. Thus, we find that

$$p \mid \binom{p}{k}$$

for $1 \leq k \leq p-1$. Finally, we obtain

$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k \equiv 1 + n^p \equiv n + 1 \pmod{p}$$

since

$$n^p \equiv n \pmod{p}$$

by our induction hypothesis.

Problem 5

First, we will compute $(256, 337)$ as follows:

$$\begin{aligned} 337 &= 256 \cdot 1 + 81 \\ 256 &= 81 \cdot 3 + 13 \\ 81 &= 13 \cdot 6 + 3 \\ 13 &= 3 \cdot 4 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

Thus, we find that $(256, 337) = 1$. That means that there is one solution to this congruence. To find it, we will first compute the inverse of 256 modulo 337 as follows:

$$\begin{aligned} 1 &= 13 - 3 \cdot 4 = 13 - (81 - 13 \cdot 6) \cdot 4 = 13 \cdot 25 + 81 \cdot -4 = (256 - 81 \cdot 3) \cdot 25 + 81 \cdot -4 \\ &= 256 \cdot 25 + 81 \cdot -79 = 256 \cdot 25 + (337 - 256 \cdot 1) \cdot -79 = 256 \cdot 104 + 337 \cdot -79 \end{aligned}$$

Thus, we find that

$$256 \cdot 104 \equiv 1 \pmod{337}$$

Multiplying both sides of the congruence

$$256x \equiv 179 \pmod{337}$$

by 104 yields

$$x \equiv 104 \cdot 179 \equiv 81 \pmod{337}$$

Problem 6

First, we will compute $(1215, 2755)$ as follows:

$$\begin{aligned}
2755 &= 1215 \cdot 2 + 325 \\
1215 &= 325 \cdot 3 + 240 \\
325 &= 240 \cdot 1 + 85 \\
240 &= 85 \cdot 2 + 70 \\
85 &= 70 \cdot 1 + 15 \\
70 &= 15 \cdot 4 + 10 \\
15 &= 10 \cdot 1 + 5 \\
10 &= 5 \cdot 2
\end{aligned}$$

Thus, we find that $(1215, 2755) = 5$. Since $5 \mid 560$, there are five solutions to this congruence. Now, we may divide the congruence

$$1215 \equiv 560 \pmod{2755}$$

by 5 to obtain

$$243x \equiv 112 \pmod{551}$$

To compute the inverse of 243 modulo 551, we must first perform the Euclidean Algorithm:

$$\begin{aligned}
551 &= 243 \cdot 2 + 65 \\
243 &= 65 \cdot 3 + 48 \\
65 &= 48 \cdot 1 + 17 \\
48 &= 17 \cdot 2 + 14 \\
17 &= 14 \cdot 1 + 3 \\
14 &= 3 \cdot 4 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 2 \cdot 1
\end{aligned}$$

Then, we write

$$\begin{aligned}
&1 = 3 - 2 \cdot 1 = 3 - (14 - 3 \cdot 4) \cdot 1 = 3 \cdot 5 + 14 \cdot -1 = (17 - 14 \cdot 1) \cdot 5 + 14 \cdot -1 \\
&= 14 \cdot -6 + 17 \cdot 5 = (48 - 17 \cdot 2) \cdot -6 + 17 \cdot 5 = 17 \cdot 17 + 48 \cdot -6 \\
&= (65 - 48 \cdot 1) \cdot 17 + 48 \cdot -6 = 65 \cdot 17 + 48 \cdot -23 = 65 \cdot 17 + (243 - 65 \cdot 3) \cdot -23 \\
&= 65 \cdot 86 + 243 \cdot -23 = (551 - 243 \cdot 2) \cdot 86 + 243 \cdot -23 = 551 \cdot 86 + 243 \cdot -195
\end{aligned}$$

Thus -195 is an inverse of 243 modulo 551. To obtain a positive inverse, we may add 551 to -195 to obtain 356. That is, we have

$$356 \cdot 243 \equiv 1 \pmod{551}$$

We may multiply both sides of the congruence

$$243x \equiv 112 \pmod{551}$$

by 356 to obtain

$$x \equiv 356 \cdot 112 \equiv 200 \pmod{551}$$

Thus, 200 (mod 551) is one solution of the congruence $243x \equiv 112 \pmod{551}$. It is also a solution of the congruence $1215x \equiv 560 \pmod{2755}$. The four other solutions are obtained by adding multiples of 551; they are

$$200 + 551 \cdot 1,\ 200 + 551 \cdot 2,\ 200 + 551 \cdot 3,\ 200 + 551 \cdot 4 \pmod{2755}$$

Therefore, the five solutions of this congruence are

$$200,\ 751,\ 1302,\ 1853,\ 2404 \pmod{2755}$$