SECOND MIDTERM
MATH 104A, UCSD, AUTUMN 17

You have 80 minutes.

There are 6 problems, and the total number of points is 70. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:________________________________

Signature:________________________________

Student ID #:________________________________

Section Time:________________________________

Problem	Points	Score
1	15	
2	10	
3	10	
4	15	
5	10	
6	10	
7	10	
8	10	
Total	70	

1. (15pts) (i) *Give the definition of a congruent to b modulo m.*

Two integers a and b are congruent modulo the natural number m if $a - b$ is divisible by m.

(ii) *Give the definition of a complete residue system.*

A complete residue system modulo a natural number m is a set of integers S such that every integer is congruent to exactly one element of S modulo m.

(iii) *Give the definition of a multiplicative function.*

A function $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ is multiplicative if $f(mn) = f(m)f(n)$ whenever m and n are coprime.

2. (10pts) *Find all solutions of* $19x + 20y = 1909$ *in natural numbers* x *and* y.

We first find x and y such that

$$19x + 20y = 1.$$

This is easy, take $y = 1$ and $x = -1$. Now multiply by 1909 to get a pair of integer solutions $(-1909, 1909)$ to the equation $19x + 20y = 1909$. As 19 and 20 are coprime, any integer solution (x, y) to this equation is of the form $(20t - 1909, 1909 - 19t)$.
The condition that the first coordinate is positive means that

$$20t > 1909 \qquad \text{so that} \qquad t > 95.$$

The condition that the second coordinate is positive means that

$$19t < 1909 \qquad \text{so that} \qquad t < 101.$$

Thus the possible values of t are 96, 97, 98, 99 and 100. The possible values of (x, y) are then

$$(11, 85), \qquad (31, 66), \qquad (51, 47), \qquad (71, 28), \qquad \text{and} \qquad (91, 9).$$

3. (10pts) *Show that if g and m are natural numbers then there are integers a and b, not both zero, such that $(a, b) = g$ and $[a, b] = m$ if and only if $g|m$.*

Suppose that $g|m$. Then take $a = g$ and $b = m$.
$g|a$ and $g|b$ so that g is common divisor. If $d|a$ and $d|b$ is a common divisor then $d|g$. Thus $g = (a, b)$ is the greatest common divisor.
$a|m$ and $b|m$ so that m is a common multiple. If $a|l$ and $b|l$ then $m|l$ so that $m = [a, b]$ is the least common multiple.
Now suppose that $(a, b) = g$ and $[a, b] = m$. We may suppose that a is non-zero. As g is A common divisor, $g|a$. As m is a common multiple, $a|m$. Thus $g|m$.

4. (15pts) *Show that if r and s are odd then*
(i)
$$\frac{rs-1}{2} = \frac{r-1}{2} + \frac{s-1}{2} \mod 2.$$

As r and s are odd, there are integers a and b such that $r = 2a+1$ and $s = 2b+1$. Therefore
$$\begin{aligned}\frac{rs-1}{2} &= \frac{(2a+1)(2b+1)-1}{2}\\ &= \frac{4ab+2a+2b}{2}\\ &= 2ab+a+b\\ &= a+b \mod 2\\ &= \frac{r-1}{2} + \frac{s-1}{2}.\end{aligned}$$

(ii) $r^2 \equiv 1 \mod 8$.

Note that $a(a+1)$ is even, so that $4a(a+1)$ is divisible by 8. Therefore
$$\begin{aligned}r^2 &= (2a+1)^2\\ &= 4a^2+4a+1\\ &= 4a(a+1)+1\\ &\equiv 1 \mod 8.\end{aligned}$$

(iii)
$$\frac{r^2s^2-1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \mod 8.$$

We have
$$\begin{aligned}
\frac{r^2s^2-1}{8} &= \frac{(2a+1)^2(2b+1)^2-1}{8}\\
&= \frac{(4a^2+4a+1)(4b^2+b4+1)-1}{8}\\
&= \frac{16a(a+1)b(b+1)+4a^2+4a+4b^2+4b+1-1}{8}\\
&= 2a(a+1)b(b+1) + \frac{a(a+1)+b(b+1)}{2}\\
&\equiv \frac{a(a+1)+b(b+1)}{2} \mod 8\\
&= \frac{4a(a+1)+4b(b+1)}{8}\\
&= \frac{r^2-1}{8} + \frac{s^2-1}{8}.
\end{aligned}$$

5. (10pts) *If p is a prime number then show that*

$$(a+b)^p \equiv a^p + b^p \mod p,$$

for all integers a and b.

Note that

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

is divisible by p for all $0 < i < p$, since the denominator is a product of natural numbers less than p. Thus

$$\binom{p}{i} \equiv 0 \mod p.$$

Applying the binomial theorem we have

$$\begin{aligned}(a+b)^p &= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \dots \binom{p}{i}a^{p-i}b^i + \dots + \binom{p}{p-1}ab^{p-1} + \binom{p}{p}b^p \\ &\equiv a^p + b^p \mod p.\end{aligned}$$

6. (10pts) *Show that if $d|n$ then $\varphi(d)|\varphi(n)$.*

As both φ is multiplicative, we may assume that n is a power of a prime, $n = p^e$, where e is a non-negative integer. If $n = 1$ then $d = 1$ and the result is clear. Thus we may assume that e is a natural number. As d divides n we have $d = p^f$, for some non-negative integer f.
In this case

$$\varphi(n) = p^e - p^{e-1} = (p-1)p^{e-1} \qquad \text{and} \qquad \varphi(d) = p^f - p^{f-1} = (p-1)p^{f-1}$$

and the result is clear.

Bonus Challenge Problems

7. (10pts) *Show that the Euler φ-function is multiplicative.*

Suppose that $m = 1$. Then $mn = 1 \cdot n = n$ so that

$$\begin{aligned} \phi(m)\phi(n) &= \phi(1)\phi(n) \\ &= \phi(n) \\ &= \phi(1 \cdot n) \\ &= \phi(mn). \end{aligned}$$

Thus the result holds if $m = 1$. Similarly the result holds if $n = 1$. Thus we may assume that m and $n > 1$. Consider the array

$$\begin{array}{ccccc} 0 & 1 & 2 & \dots & m-1 \\ m & m+1 & m+2 & \dots & m+(m-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n-1)m & (n-1)m+1 & (n-1)m+2 & \dots & (n-1)m+(m-1). \end{array}$$

The last entry is $nm - 1$ and so this is a complete residue system, modulo mn. Therefore $\varphi(mn)$ is the number of elements of the array comprime to mn.

Pick a column and suppose the first entry is a. The other entries in that column are $m + a$, $2m + a$, $\dots$, $(n-1)m + a$ and so every entry in that column is congruent to a modulo m. So if a is not coprime to m then no entry in that column is coprime to m, let alone mn. Thus we can focus on those columns whose first entry a is coprime to a.

The first row is a complete residue system modulo m, so that $\varphi(m)$ elements of the first row are coprime to m. Thus there are only $\varphi(m)$ columns we need to focus on. On the other hand, the entries in this column are the numbers $m \cdot 1 + a$, $m \cdot 2 + a$, $m \cdot 3 + a$, and so they are a complete residue system modulo n. Thus $\varphi(n)$ elements of this column are coprime to n.

Thus $\varphi(m)\varphi(n)$ elements of the array are coprime to both m and n. But as m and n are coprime, it follows that an integer l is coprime to mn if and only if it is coprime to m and n. Thus $\varphi(m)\varphi(n)$ elements of the array are coprime to mn.

8. (10pts) *Fix a natural number k. Show that there are arbitrarily long blocks of consecutive integers, all of which are divisible by the kth power of a natural number bigger than one.*

Let $p_1, p_2, \dots, p_r$ be distinct primes, for example

$$2, 3, 5, \dots, p_r.$$

Let $m_i = p_i^k$. Then

$$m_1, m_2, \dots, m_r$$

are pairwise coprime. Let

$$c_i = m_i - i - 1,$$

so that

$$\begin{aligned} c_1 &\equiv 0 \mod m_1 \\ c_2 &\equiv -1 \mod m_2 \\ c_3 &\equiv -2 \mod m_3 \\ \vdots & \ \ddots \qquad \vdots \\ c_r &\equiv -r+1 \mod m_r. \end{aligned}$$

Then, by the Chinese remainder theorem, we can find a natural number x congruent to c_i, modulo m_i, for every $1 \leq i \leq r$. Note that

$$x \equiv 0 \mod m_1,$$

so that $m_1 = p_1^k$ divides x. Thus x is divisible by a kth power. But

$$x + 1 \equiv 0 \mod m_2,$$

so that p_2^k divides $x+1$. Thus $x+1$ is divisible by a kth power. In general

$$x + (i-1) \equiv 0 \mod m_i,$$

so that p_i^k divides $x + i = 1$. Thus $x + i - 1$ is divisible by a kth power. It follows that every one of the r consecutive integers

$$x, \qquad x+1, \qquad x+2, \qquad \dots \qquad x+r-1$$

is divisible by a kth power.