Math 4400 Midterm 1

June 15, 2017

Name: Solutions

Question	Points	Score
1	15	
2	15	
3	15	
4	15	
5	20	
6	20	
7	0	
Total:	100	

1. (15 points) Find the continued fraction expansion of $\frac{81}{30}$

$81 = 2 \cdot 30 + 21$

$30 = 1 \cdot 21 + 9$

$21 = 2 \cdot 9 + 3$

$9 = 3 \cdot 3$

So $$\frac{81}{30} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{3}}}$$

$$= [2; 1, 2, 3]$$

2. (15 points) Find a natural number x with $0 \leq x < 175$, such that $6^{242} \equiv x \mod 175$

$175 = 5^2 \cdot 7$, so

$$\varphi(175) = 175 \cdot \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$$

$$= 175 \cdot \frac{4}{5} \cdot \frac{6}{7} = 5 \cdot 4 \cdot 6 = 120$$

~~Thus~~ $\gcd(6, 175) = 1$, since $2 \nmid 175$ and $3 \nmid 175$,

so, using Euler's formula,

$$6^{242} \equiv 6^{2 \cdot 120 + 2} \equiv \left(6^{120}\right)^2 \cdot 6^2 \equiv 1 \cdot 36 \equiv 36 \mod 175$$

3. (15 points) Given the following equations, and the fact that $438/3 = 146$, find all incongruent solutions to the equation $303x \equiv 3 \mod 438$.

$$\begin{aligned} 438 &= 1 \cdot 303 + 135 \\ 303 &= 2 \cdot 135 + 33 \\ 135 &= 4 \cdot 33 + 3 \\ 33 &= 11 \cdot 3 \end{aligned}$$

$135 - 4 \cdot 33 = 3$

$\Rightarrow 135 - 4 \cdot (303 - 2 \cdot 135) = 3$

$\Rightarrow 9 \cdot 135 - 4 \cdot 303 = 3$

$\Rightarrow 9 \cdot (438 - 303) - 4 \cdot 303 = 3$

$\Rightarrow 9 \cdot 438 - 13 \cdot 303 = 3$

$\Rightarrow -13 \cdot 303 \equiv 3 \mod 438.$

So the incongruent solutions are:

$x = -13$, $x \equiv -13 + 146$, $x \equiv -13 + 2 \cdot 146$

i.e. $x \equiv 133$, $x \equiv 279$, and $x \equiv 425 \mod 438$

(There are 3 solutions since $\gcd(438, 303) = 3$).

4. (15 points) Suppose $a, b, c, m \in \mathbb{Z}$, $m \neq 0$, and $\gcd(c, m) = 1$. Suppose also that $ac \equiv bc \mod m$. Show that $a \equiv b \mod m$.

Since $\gcd(c,m) = 1$, $\exists x \in \mathbb{Z}: cx \equiv 1 \mod m$.

Then $ac \equiv bc \mod m$

$\Rightarrow acx \equiv bcx \mod m$

$\Rightarrow a \cdot 1 \equiv b \cdot 1 \mod m$

$\Rightarrow$ $a \equiv b \mod m$.

5. (20 points) Suppose $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$. Show that $\gcd(a, mn) = 1$.

Let $d \in \mathbb{N}$ such that $d \mid a$ and $d \mid mn$.

Suppose $d > 1$. Then we must have $\gcd(d, m) = 1$. Otherwise, $\exists e \in \mathbb{N}$, $e > 1$, such that $e \mid d$ and $e \mid m$. But, since $e \mid d$, we know $e \mid a$. Then $\gcd(a, m) \geq e$, a contradiction.

Since $d \mid mn$ and $\gcd(d, m) = 1$, we know $d \mid n$. Thus $\gcd(a, n) \geq d > 1$, a contradiction.

6. (a) (5 points) Let $x, n \in \mathbb{Z}$ and suppose $\gcd(x, n) = d$. Prove that $\gcd\left(\frac{x}{d}, \frac{n}{d}\right) = 1$.

Let $f \in \mathbb{N}$, such that $f \mid \frac{x}{d}$ and $f \mid \frac{n}{d}$.

Then $df \mid x$, $df \mid n$, so $df \le \gcd(x,n) = 1$.

Thus $f = 1$.

(b) (5 points) Let $x, n, d \in \mathbb{Z}$ and suppose $\gcd(x, n) = 1$. Prove that $\gcd(xd, nd) = d$.

Since $d \mid xd$ and $d \mid nd$, we know $d \mid \gcd(xd, nd)$.

Since $\gcd(xd, nd) \mid xd$ and $\gcd(xd,nd) \mid nd$, we have $\frac{\gcd(xd,nd)}{d} \mid x$, $\frac{\gcd(xd,nd)}{d} \mid n$. $\Rightarrow \frac{\gcd(xd,nd)}{d} = 1$,

so $\gcd(xd,nd) = d$.

(c) (10 points) Let $d, n \in \mathbb{N}$ with $n > 1$ and $d \mid n$. Show that $\varphi\left(\frac{n}{d}\right) = \#S$, where $S = \{x \in \mathbb{N} \mid 1 \le x \le n, \gcd(x, n) = d\}$. (Use the back of the page if you run out of space)

Let $T = \{x \in \mathbb{N} \mid 1 \le x \le \frac{n}{d}, \gcd(x, \frac{n}{d}) = 1\}$,

Then $\varphi(\frac{n}{d}) = \#T$, so <u>WTS</u>: $\#T = \#S$.

Define $f : S \longrightarrow T$ by $x \longmapsto x/d$.

(<u>Note</u>: if $x \in S$, then $1 \le x/d \le n/d$ and, by (a), $\gcd(\frac{x}{d}, \frac{n}{d}) = 1$, so $x/d \in T$)

If $\frac{x_1}{d} = \frac{x_2}{d}$, then $x_1 = x_2$, so f injective.

If $y \in T$, then $1 \le dy \le n$ and $\gcd(dy, n) = d$, by (b), and $y = f(dy)$. So f is surjective $\boxtimes$

7. (10 points (bonus)) Use the last problem to prove that $\sum_{\substack{1 \leq d \leq n \\ d \mid n}} \varphi(d) = n$.

$$\{1, 2, \ldots, n\} = \underbrace{\bigsqcup_{d \mid n}}_{\text{disjoint union,}} \{x \mid 1 \leq x \leq n, \gcd(x, n) = d\}$$

Scratch Paper (feel free to tear this off)