Name: SOLUTIONS

Tuesday March 1, 2011
MATH 42 – Exam 1

For full credit, all work must be shown and clearly presented. No calculators.

1	
2	
3	
4	
5	
6	

1. (5 points each)

a. Find the GCD of 654 and 163.

$$654 = 163 \cdot 4 + 2$$
$$163 = 2 \cdot 81 + 1$$
$$2 = 1 \cdot 2 + 0$$

The GCD is 1.

b. Write $\frac{654}{163}$ as a simple continued fraction.

$$\frac{654}{163} = 4 + \cfrac{1}{81 + \cfrac{1}{2}}.$$

c. Find ***all*** integral solutions to the equation $654x + 163y = 1$.

		4	81	2
0	1	4	325	654.
1	0	1	81	163

$654(-81) + 163(325) = 1.$

All solutions:

$x = -81 + 163k, \quad y = 325 - 654k, \quad k \in \mathbb{Z}.$

d. What is the multiplicative inverse of 163 in $\mathbb{Z}_{654}$?

Since $163 \cdot 325 = 1 + 654 \cdot 81$, the multiplicative inverse of 163 is 325 in $\mathbb{Z}_{654}$.

2. Consider the following four functions. Put them into the chart based on whether they are one-to-one and/or onto. No partial credit will be given unless work is shown. (10 points)

I $f(x) = 2x$ as a function from $\mathbb{Z}_7$ to $\mathbb{Z}_7$.

II $g(x) = 2x$ as a function from $\mathbb{Z}_6$ to $\mathbb{Z}_6$.

III $h(x) = 2x$ as a function from $\mathbb{Z}_4$ to $\mathbb{Z}_8$.

IV $j(x) = 2x \mod 5$ as a function from $\mathbb{Z}$ to $\mathbb{Z}_5$.

	One-to-one	Not one-to-one
Onto	I.	IV.
Not onto	III	II.

3. Decide which of these congruences have 0 solutions, 1 solution, or 2 solutions. No partial credit will be given if no work is shown. (10 points)

I $50x \equiv 17 \mod 67$

II $50x \equiv 17 \mod 166$

III $50x \equiv 16 \mod 166$

No solutions	II.
One solution	I.
Two solutions	III.

4. Compute 3^{2402} mod 3500. *(Hint: First compute $\varphi(3500)$.)* (10 points)

$3500 = 7 \cdot 500 = 7 \cdot 4 \cdot 125.$

So $\varphi(3500) = \varphi(7)\,\varphi(4)\,\varphi(125) = 6 \cdot (4-2)(125-25)$

$= 6 \cdot 2 \cdot 100 = 1200.$

Then $3^{1200} \equiv 1 \mod 3500.$

So $3^{2402} = 3^{1200} \cdot 3^{1200} \cdot 3^2 = 9 \mod 3500.$

5. Prove that if $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$. (10 points)

$a \equiv b \mod m$ means $m | a-b$.

$c \equiv d \mod m$ means $m | c-d$.

Then $a-b = mk$ and $c-d = m\ell$ for some $k, \ell \in \mathbb{Z}$.

So $a-b+c-d = mk + m\ell = m(k+\ell)$

Rearranging terms, we get

$m(k+\ell) = (a+c) - (b+d)$,

so $m \mid [(a+c)-(b+d)]$.

Thus, $a+c \equiv b+d$ mod m by definition.

6. Prove that for integers a, b and c, if $a \mid c$ and $b \mid c$, and if $(a,b) = 1$, then $ab \mid c$. You may use the fact that if $(a,b) = 1$, then there are integers x and y such that $ax + by = 1$. *(Hint: Think of the proof of the Fundamental Theorem of Arithmetic.)* (10 points)

If $(a,b)=1$, then there exists $x, y \in \mathbb{Z}$ s.t. $ax+by=1$.

Multiplying through by c, we get

$$acx + bcy = c.$$

But $a \mid c \Rightarrow c = ak$ for some $k \in \mathbb{Z}$

and $b \mid c \Rightarrow c = bl$ for some $l \in \mathbb{Z}$.

Substituting, we get

$$c = a(bl)x + b(ak)y$$
$$= ab(lx + ky).$$

Thus, $ab \mid c$.

7. **Extra Credit:** Verify for at least 4 natural numbers n that

$$n = \sum_{\substack{d|n \\ d>0}} \varphi(d).$$

Prove this fact for all n in $\mathbb{N}$. (5 points)

Verification:

For example, if $n=1$, $1 = \varphi(1)$. ✓

If $n=2$, $2 = \varphi(1)+\varphi(2) = 1+1$ ✓

If $n=3$, $3 = \varphi(1)+\varphi(3) = 1+2$ ✓

If $n=6$, $6 = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)$

$= 1+1+2+2 = 6$ ✓

For the proof:

We will count natural numbers k satisfying

$1 \le k \le n$, and $(k,n) = \frac{n}{d}$, where d is a divisor of n.

I claim there are $\varphi(d)$ such k:

There are d multiples of $\frac{n}{d}$ less than or equal to n,

namely $\frac{n}{d}, \frac{2n}{d}, \frac{3n}{d}, \ldots, \frac{dn}{d} = n$.

Clearly if $(k,n) = \frac{n}{d}$, $k = \frac{l \cdot n}{d}$. for some $1 \le l \le d$.

(i.e. k is in the list of multiples of $\frac{n}{d}$ above).

But if $(l,d) \ne 1$, then $(k,n) > \frac{n}{d}$ since if $c>1$ and

$c|l$, $c|d$, i.e. $l = c \cdot l'$ and $d = c \cdot d'$,

$k = \frac{\cancel{c}l'n}{\cancel{c}d'} = \frac{l'n}{d'}$.

Now since $d' < d$, k is a multiple of $\frac{n}{d'}$, which is

greater than $\frac{n}{d}$. That is, (k,n) is at least $\frac{n}{d'} > \frac{n}{d}$.

Now if $(l,d)=1$, then $(k,n) = \frac{n}{d}$ because $\frac{n}{d}$ divides both

but if something larger, $\frac{an}{d}$ divided both n and k, then

$a|l$ and $a|d$ since $n = \frac{dn}{d}$.

Proof cont:

In summary, there are $\varphi(d)$ numbers k satisfying $1 \leq k \leq n$ and $(k,n) = \frac{n}{d}$.

Every integer k s.t. $1 \leq k \leq n$ has $(k,n) = \frac{n}{d}$ for some divisor d of n. (since $\frac{n}{d}$ will range over all divisors of n).

Therefore, we see that

$$n = \underset{(k,n)=\frac{n}{d_1}}{\#\text{ of } k \text{ with}} + \underset{(k,n)=\frac{n}{d_2}}{\#\text{ of } k \text{ with}} + \dots$$

$$= \sum_{\substack{d|n \\ d>0}} \varphi(d).$$

Alternate proof:

Induct on the number of distinct prime divisors of n.

Base cases: $n=1$: If $n=1$, $\varphi(1)=1$ and $1=1$ ✓

If n is prime or a prime power:

$n = p^k$ where p is prime.

Then
$$\sum_{\substack{d|n \\ d>0}} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^k)$$
$$= \cancel{1} + (p - \cancel{1}) + (p^2 - p) + \dots + (p^k - p^{k-1})$$
$$= p^k \quad \text{(Telescoping sum).}$$
$$= n \quad ✓.$$

Inductive step: Assume the statement is true for n the product of powers of at most $r-1$ primes. Now let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and show the statement is true for n.

If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, write $m = p_1^{k_1} p_2^{k_2} \cdots p_{r-1}^{k_{r-1}} = \dfrac{n}{p_r^{k_r}}$.

Then we know by assumption that

$$m = \sum_{\substack{d \mid m \\ d > 0}} \varphi(d)$$

Of course, if $d \mid m$, $d \mid n$;

So the sum

$\displaystyle\sum_{\substack{d \mid n \\ d > 0}} \varphi(d)$ has all the terms from the sum above,

plus a few more.

Namely, $$\sum_{\substack{d \mid n \\ d > 0}} \varphi(d) = \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) + \sum_{\substack{d \mid m \\ d > 0}} \sum_{l=1}^{k_r} \varphi(p_k^l d)$$

(In the far right sum, we're summing over divisors of n that are divisible by p^k, and these divisors can be written as $d \cdot p_k^l$ where $d \mid m$ and $1 \le l \le k_r$)

So $$\sum_{\substack{d \mid n \\ d > 0}} \varphi(d) = \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) + \sum_{\substack{d \mid m \\ d > 0}} \sum_{l=1}^{k_r} \left[\varphi(p_k^l)\varphi(d)\right]$$ (since p_k^l and d are rel. prime).

$$= \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) + \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) \sum_{l=1}^{k_r} \varphi(p_k^l)$$

$$= \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) + \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) \left[\varphi(p) + \varphi(p^2) + \dots + \varphi(p^{k_r})\right]$$

$$= \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) + \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) \left[\cancel{p} - 1 + p^2 - \cancel{p} + \dots + p^{k_r} - p^{k_r - 1}\right]$$

$$\overset{*}{=} \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) + (p^{k_r} - 1) \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) = p^{k_r} \sum_{\substack{d \mid m \\ d > 0}} \varphi(d) = p^{k_r} \cdot m = n$$