Midterm Examination 1 - Math 580, Frank Thorne (thorne@math.sc.edu)

Thursday, October 3, 2013

Please work without books, notes, calculators, or any assistance from others. Be sure to show all your work and explain what you are doing!

If you need either of the following two results, quote them by the names given here:

Euclidean Algorithm Theorem. For any nonzero integers a and b, there are integers x and y with $ax + by = (a, b)$.

Euclid's Lemma. If $d|ab$ and $(d, a) = 1$, then $d|b$.

1. (10 points) Let a, b, and m be integers. Give *precise* definitions for what it means to say that $a|b$ and to say that $a \equiv b \pmod{m}$.

2. (10 points) Determine the last digit of 79^{1843}.

3. (12 points) Find all the solutions to $74x + 44y = 26$.

4. (16 points) Solve the system of equations $x \equiv 4 \pmod{15}$, $x \equiv 6 \pmod{22}$. (Express your answer as a congruence.)

   For this problem, solve using methods which would also be practical for larger numbers (no guess and check please).

5. (10 points) If $d|ab$ for positive integers, must we have either $d|a$ or $d|b$? Prove or give a counterexample.

6. (20 points) Suppose that $(a, m) = 1$, and that c is any integer. Prove that there exists a unique solution $x \pmod{m}$ to the congruence $ax \equiv c \pmod{m}$.

   (There are two parts to a correct solution.)

7. (10 points) Suppose you were to write out a multiplication table $\pmod{113}$. How many different integers $\pmod{113}$ would you see in each row of the table? How many times would each integer $\pmod{113}$ repeat?

   Explain your answer.

8. (12 points) Can the difference of two consecutive fifth powers be divisible by 3? Prove your assertion.

9. (**Bonus.** 5 points) Let T be the set of odd positive integers. Does unique factorization hold in T? Prove or disprove.

Exam 1.

1. $a|b$ means that $b = na$ for some integer n.

$a \equiv b \pmod{m}$ means $m \mid b-a$.

2. Look at $79^{1843} \pmod{10}$.

$$79^{1843} \equiv (-1)^{1843} \pmod{10}$$
$$\equiv (-1)^{2\cdot 921}(-1) \pmod{10}$$
$$\equiv 1^{921}\cdot(-1) \pmod{10} \equiv -1 \pmod{10}.$$

So the last digit is 9.

3. $74x + 44y = 26$ is the same as $37x + 22y = 13$.

First solve $37r + 22s = 1$:

$$37 = 1\cdot 22 + 15$$
$$22 = 1\cdot 15 + 7$$
$$15 = 2\cdot 7 + 1 \Longrightarrow 1 = 15 - 2\cdot 7$$
$$= 15 - 2(22-15)$$
$$= -2\cdot 22 + 3\cdot 15$$
$$= -2\cdot 22 + 3(37-22)$$
$$= 3\cdot 37 - 5\cdot 22.$$

(= 111 − 110. It checks out!)

So $37\cdot 3 + 22\cdot(-5) = 1$, so

$$37\cdot(39) + 22\cdot(-65) = 1.$$

Since $(37, 22) = 1$ we get all solutions by adding multiples of 22 to 39 and subtracting multiples of 37 from -65:

$$x = 39 + 22t$$
$$y = -65 - 37t$$

for all integers t.

4. First solve two easier problems:

(1) $x_1 \equiv 1 \pmod{15}$, $x_{\cancel{2}} \equiv 0 \pmod{22}$.

So solve $22 \cancel{s} r - 15s = 1$.

$$22 = 1\cdot 15 + 7$$
$$15 = 2\cdot 7 + 1$$

So ~~22=~~

$$\begin{aligned} 1 &= 15 - 2\cdot 7 \\ &= 15 - 2(22 - 15) \\ &= 3\cdot 15 - 22. \end{aligned}$$

$1 = 3\cdot 15 - 2\cdot 22$, so take $s = -3$, $r = -2$.

In other words, $x_1 = 22r = -44$.

Then $x_1 \equiv 1 \pmod{15}$, $x_1 \equiv 0 \pmod{22}$.

(2) $x_2 \equiv 0 \pmod{15}$, $x_2 \equiv 1 \pmod{22}$.

Here we use $15\cdot(-s)$, with $-s = 3$.

$45 \equiv 0 \pmod{15}$ and $\equiv 1 \pmod{22}$

because $1 = 3\cdot 15 - 2\cdot 22$,

So, take $x = 4\cdot x_1 + 6\cdot x_2$.

Then, (mod 15), $x \equiv 4 + 0 \equiv 4$

(mod 22), $x \equiv 0 + 6 \equiv 6$

so x will be a solution.

$$4\cdot(-44) + 6\cdot(45) = 4\cdot(-44 + 45) + 2\cdot 45 = 94.$$

So $x = 94$ is one solution.

By the Chinese Remainder Theorem this is unique (mod $15\cdot 22$) = (mod 330) so the solution is

$$x \equiv 94 \pmod{330}.$$

5. Not always: Let $d=4$, $a=2$, $b=2$.

Then $d \mid a\cdot b$ ($4 \mid 4$) but $d \nmid a$ and $d \nmid b$.

6. Given $(a,m)=1$. Prove there is a unique solution $x \pmod m$ to $ax \equiv c \pmod m$.

<u>Existence</u>:

First we want to solve $ab \equiv 1 \pmod m$.

This is the same as $ab - mr = 1$ for some r.

We know that $ab + ms = 1$ has a solution (b,s) <u>by the Euclidean algorithm</u> (because a and m are coprime). So take $r=-s$.

We have $ab \equiv 1 \pmod m$.

Now, take $x = c\cdot b$, and

$$ax = a\cdot c\cdot b \equiv c \pmod m.$$

So there <u>exists</u> a solution x.

Now suppose there are two different solutions x and y. Then

$$ax \equiv c \pmod m$$
$$ay \equiv c \pmod m$$

So $ax - ay \equiv 0 \pmod m$,

which says $m \mid a(x-y)$. Since m and a are coprime, $m \mid x-y$ which says that $x \equiv y \pmod m$.

So x must be unique $\pmod m$.

7. 113 is a prime number.

In the 0 row we would see 0 113 times.

In every other row ~~number~~ we would see every number between 0 and 112 exactly once.

		x					
		0	1	2	3	4	...
	0	0	0	0	0	0	
	1	0	1	2	3	4	
	2	0	2	4	6	8	
a	3	0	3	6	9	12	
	4	0					
	⋮						

The numbers to be multiplied are a and x and the product is c. The previous problem tells us that for each c, (and every $a \neq 0$) there is exactly one x for which $ax \equiv c \pmod{113}$, which is the same thing as saying that each c appears once in each row other than the a = 0 row.

8. We want to know if we can have $(x+1)^5 - x^5 \equiv 0 \pmod 3$

This depends only on what x is $\pmod 3$.

If $x \equiv 0 \pmod 3$, $(x+1)^5 - x^5 \equiv 1^5 - 0^5 \equiv 1 \pmod 3$

If $x \equiv 1 \pmod 3$, $(x+1)^5 - x^5 \equiv 2^5 - 1^5 \equiv 31 \pmod 3$

$\not\equiv 0 \pmod 3$

If $x \equiv 2 \pmod 3$, $(x+1)^5 - x^5 \equiv 0^5 - 2^5 \equiv -32 \pmod 3$

$\not\equiv 0 \pmod 3$.

In no case do we ever get $(x+1)^5 - x^5 \equiv 0 \pmod 3$.
So this is impossible.

9. Yes! It does. This is because factorization in T is the same thing as factorization in the ordinary integers: each integer in T has only odd factors and so the even integers make no appearance.

So unique factorization holds because it does in the ordinary integers.

This contrasts with the set S of integers $\equiv 1 \pmod 4$, which are allowed to have factors not in the set.

Midterm Examination 2 - Math 580, Frank Thorne (thorne@math.sc.edu)

Tuesday, November 12, 2013

1. (6 points) Define what it means for a function to be *multiplicative.*

2. (12 points) Compute $d(84)$, $\phi(84)$, and $\sigma(84)$.

3. (10 points) Determine the remainder when 4^{400} is divided by 37.

4. (10 points) Perform the base 7 multiplication $45_7 \times 34_7$ without converting into base 10.

5. Find at least two values of n satisfying each of the conditions below. (The parts are separate! You don't need to find n that work with all of them.)

   Bonus: find all values of n, with proof.

   - (6 points) $\phi(n) = 12$
   - (6 points) $d(n) = 10$
   - (8 points) $\sigma(n) < \frac{3}{2}n$, but n is not prime.

6. Let p and q be primes, and let a and b be positive integers.

   - (12 points) Prove a formula for $\sigma(p^a q^b)$.
   - (12 points) Prove a formula for $d(p^a q^b)$.

   In your proofs, do not use any facts about $\sigma(n)$ and $d(n)$ other than their definitions – but feel free to appeal to any other theorems or facts we have studied.

7. (18 points) Prove the following lemma, which was used in the proof of Fermat's Theorem.

   Lemma. Let p be a prime and suppose that $(a, p) = 1$. Then the least residues of

   $$a, 2a, 3a, \cdots, (p-1)a \pmod{p},$$

   are

   $$1, 2, 3, \cdots, p-1$$

   in some order.

   (Note: your proof might work equally well even if p is not a prime.)

Exam 2.

1. f is multiplicative if $f(mn) = f(m)f(n)$ whenever m and n are coprime integers.

2. Use multiplicativity.

$$84 = 3 \cdot 2^2 \cdot 7.$$

$$d(84) = d(3)\,d(2^2)\,d(7) = 2 \cdot 3 \cdot 2 = 12$$

$$\phi(84) = \phi(3)\,\phi(2^2)\,\phi(7) = 2 \cdot 2 \cdot 6 = 24$$

$$\sigma(84) = \sigma(3)\,\sigma(2^2)\,\sigma(7) = 4 \cdot (1+2+4) \cdot 8$$

$$= 32 \cdot 7 = 224.$$

3. By Euler's Theorem $4^{36} \equiv 1 \pmod{37}$.

So $4^{400} = 4^{11 \cdot 36 + 4} \equiv (4^{36})^{11} \cdot 4^4 \pmod{37}$

$$\equiv 1^{11} \cdot 4^4 \pmod{37}$$

$$\equiv 256 \pmod{37}.$$

185
222
259

$222 = 37 \cdot 6$,

So $256 \equiv 34 \pmod{37}$.

(4 late)

45. $\phi(13) = 13 - 1 = 12.$

$\phi(21) = (7-1)(3-1) = 12.$

d: If p is any prime, $d(p^9) = 10$.

So 2^9 and 3^9 work.

We also have $d(p^4 \cdot q) = 10$ for any primes p and q, etc.

If n is divisible by two (slightly) big primes this works.

Try $n = 35 = 5 \cdot 7$.

Then $\sigma(n) = (1+5)(1+7) = 6 \cdot 8 = 48 < \frac{3}{2} \cdot 35$.

6. The divisors of $p^a q^b$ are all integers of the form $p^r q^s$, where $0 \le r \le a$ and $0 \le s \le b$.

There are $a+1$ possibilities for r and $b+1$ possibilities for s, so $d(p^a q^b) = (a+1)(b+1)$.

We have

$\sigma(p^a q^b) = (1 + p + p^2 + \cdots + p^a)(1 + q + q^2 + \cdots + q^b)$, because when we multiply out the product, every divisor of $p^a q^b$ appears exactly once.

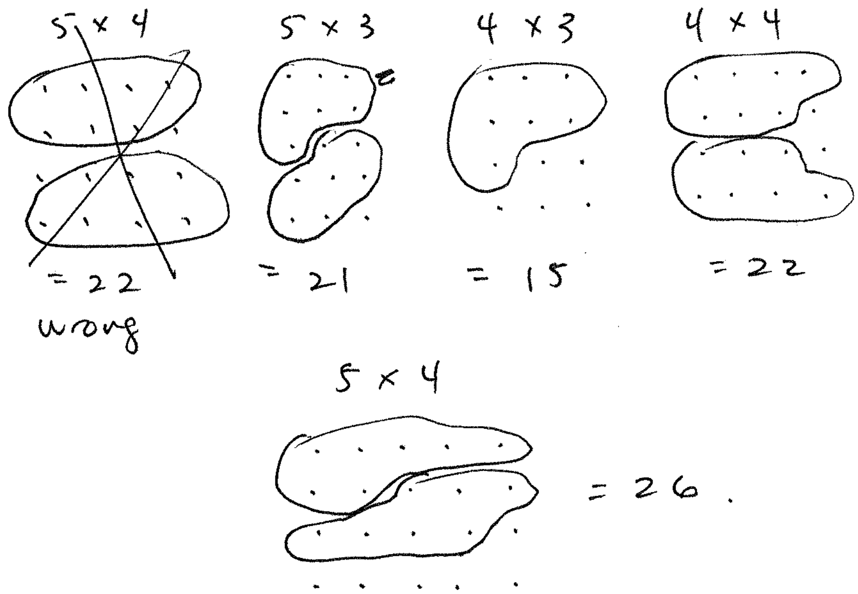
And $1 + p + p^2 + \cdots + p^a = \dfrac{p^{a+1} - 1}{p - 1}$

$1 + q + \cdots + q^b = \dfrac{q^{b+1} - 1}{q - 1}$,

so $\sigma(p^a q^b) = \dfrac{p^{a+1} - 1}{p - 1} \cdot \dfrac{q^{b+1} - 1}{q - 1}$.

4. In base 7:

$$\begin{array}{r} {}^{2}_{2}\ \ \\ 45 \\ \times\ \ 34 \\ \hline 246 \\ 201\ \ \\ \hline 2256 \end{array}.$$



7. Let p be a prime and let $(a,p)=1$.
Look at $a, 2a, \cdots, (p-1)a \pmod p$.

They are all coprime to p because a is and because each of $1, 2, \cdots, p-1$ is.

I claim that each represents a distinct residue class $(\text{mod } p)$. To see this, suppose that $ra \equiv sa \pmod p$ for some $1 \le r, s \le p-1$. Then $p \mid ra - sa$, so $p \mid a(r-s)$. Because p is prime and $p \nmid a$, $p \mid r-s$. But because $1 \le r, s \le p-1$, we must have $r = s$, proving the claim.

So, the least residues of $a, 2a, \cdots, (p-1)a$ are $p-1$ different numbers between 1 and $p-1$. Since there are only $p-1$ of them, these least residues must include all of them.