MATH 540: STUDY GUIDE AND PRACTICE PROBLEMS FOR EXAM I

The following is a list of topics and types of problems you should know for Exam I.

1. Be able to state the various theorems and definitions from class, and answer true-false type questions regarding them.

2. Mathematical Induction. Be able to apply mathematical induction to prove an elementary statement.

3. The Well Ordering Principle. Know how to state it and how to use it.

4. The Division Algorithm and its consequences. Be able to apply the division algorithm to find the GCD of two positive integers and use it to find the coefficients required in Bezout's principle. Similarly, be able to use Blankinship's method to write the GCD of A and b as an integer combination of A and b.

5. Know the relationship between the LCM and GCD of two positive integers.

7. Know the Fundamental Theorem of Arithmetic and its consequences, especially in regards to finding LCMs and GCDs.

8. Be able to verify that a given relation is an equivalence relation.

9. Know the formulas for $\tau(n)$, the number of divisors of n, and $\sigma(n)$, the sum of the divisors of n, and how to use them.

10. Know basic properties of and how to compute with integers modulo n, including solving simple linear equations.

11. Know the definition and properties of Euler's totient function.

12. Be able to work problems using Euler's theorem, Euler's product formula and Gauss's theorem.

13. Be able to work problems involving equivalence relations.

14. Be able to reproduce the proof of any one of the following three theorems:

(i) Every positive integer can be written as a product of prime numbers, i.e., the existence part of the Fundamental Theorem of Arithmetic.

(ii) If p is a prime number and $p|ab$, then $p|a$ or $p|b$.

(iii) Euler's Formula.

Practice Problems

1. Prove the following two statements by induction:

(a) $\sum_{k=1}^{n}(-1)^k k^2 = \frac{(-1)^n n(n+1)}{2}$.

(b) $\sum_{k=1}^{n}\frac{1}{k(k+1)} = \frac{n}{n+1}$.

2. Let $d_1 = \frac{2}{3}$ and $d_2 = \frac{3}{5}$. For $n \geq 3$, set $d_n := d_{n-1} \cdot d_{n-2}$. Use the Well Ordering Principle to show that $d_n < 1$, for all $n \geq 1$.

3. Use Let $a = \sigma(24)$ and $b = \tau(24)$. Here $\sigma(24)$ means the sum of the divisors of 24 and $\tau(24)$ means the number of divisors of 24. Use the division algorithm to find $\mathrm{GCD}(a, b)$. Then use Bezout's Principle to write $\mathrm{GCD}(a, b)$ as a combination of a and b. Finally, find $\mathrm{LCM}(a, b)$.

4. Use the Fundamental Theorem of arithmetic to find the GCD and LCM of 63,000 and 36,690.

5. Consider the relation on $\mathbb{Z}^+ \times \mathbb{Z}^+$ given by $(a, b) \sim (c, d)$ if and only if $a + d = b + c$.
   (a) Prove that $\sim$ is an equivalence relation.
   (b) Describe the equivalence class of $(3, 5)$.
   (c) Let X be the set of equivalence classes of $\sim$. Define $f : X \to \mathbb{Z}$, by $f([(a, b]) = a - b$. Prove that f is well defined, in other words, the value of f does not change if we use a different representative for the class $[(a, b)]$.

6. For $n \geq 2$, let $\mathbb{Z}_n$ denote the integers modulo n.
   (a) Write out addition and multiplication tables for $\mathbb{Z}_7$.
   (b) Can you explain why every non-zero element of $\mathbb{Z}_7$ has a multiplicative inverse?
   (c) Find a solution to the congruence $7x \equiv 5 \pmod{12}$.
   (d) Find an integer n so that the congruence $7x \equiv 5 \pmod{n}$ does *not* have a solution.
   (e) Find all solutions to $12x \equiv 15 \bmod 21$, both in $\mathbb{Z}_{21}$ and in $\mathbb{Z}$.
   (f) Find all solutions to the equation $x^2 - 1 \equiv 0 \bmod 35$.

7. Find the multiplicative inverse of 27 modulo each of 31, 33, 34. Hint: Euler's theorem might be useful.

8. Find $139^{112} \bmod 27$.

9. Find $\phi(1492), \phi(1776), \phi(2001)$.

10. Find all positive integers n such that $\frac{\phi(n)}{n} = \frac{1}{2}$.

Solutions To Practice Problems

#1 (a) When $n=1$, both sides equal -1.

Assume the formula is valid for n. Then

$$\sum_{k=1}^{n} (-1)^k k^2 = \frac{(-1)^n n(n+1)}{2}. \quad \text{Adding } (-1)^{n+1}(n+1)^2$$

to both sides we get:

$$\sum_{k=1}^{n+1} (-1)^k k^2 = \frac{(-1)^n n(n+1)}{2} + (-1)^{n+1}(n+1)^2 =$$

$$\frac{(-1)^n n(n+1)}{2} + \frac{(-1)^{n+1} 2(n+1)^2}{2} = (-1)^{n+1}\left\{\frac{-(n)(n+1) + 2(n+1)^2}{2}\right\}$$

$$= (-1)^{n+1}\left\{\frac{-n^2-n+2n^2+4n+2}{2}\right\} = (-1)^{n+1}\frac{n^2+3n+2}{2} = (-1)^{n+1}\frac{(n+1)(n+2)}{2} \quad //$$

(b) When $n=1$: Both sides of the equation equal $1/2$. Assume the formula holds for n, i.e. $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$.

Adding $\dfrac{1}{(n+1)(n+2)}$ to both sides gives: $\displaystyle\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \frac{n}{n+1} + \frac{1}{(n+1)(n+2)}$

$$= \frac{n(n+2)+1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{1}{(n+1)(n+2)}. \;//$$

#2. Let S denote all elements of the sequence $\{d_n\}_{n\geq 1}$ such that $d_n \geq 1$. If $S = \phi$, we are done. Suppose $S \neq \phi$. By the Well Ordering Principle, $\exists\, d_r \in S$, a least element. Note $d_1 = 2/3$, $d_2 = 3/5$ are Not in $S \Rightarrow r \geq 3$.

Thus $d_r = d_{r-1} \cdot d_{r-2}$. Since d_{r-1}, d_{r-2} are less than d_r

$d_{r-1} \notin S$, $d_{r-2} \notin S \Rightarrow d_{r-1} < 1$ and $d_{r-2} < 1$. But then $d_r = d_{r-1} \cdot d_{r-2} < 1$, which gives the required contradiction

#3) Divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24

$\tau(24) = 8$ and $\sigma(24) = 60$

$$\Rightarrow \text{GCD}(8,60) = 4$$

$$\text{LCM}(8,60) = \frac{8 \cdot 60}{4} = 120.$$

Bezout: $4 = 8 \cdot 8 + (-1) \cdot 60$

4. $63{,}000 = 2^3 \cdot 3^2 \cdot 5^3 \cdot 7$
$36{,}690 = 2 \cdot 3 \cdot 5 \cdot 1223$ } prime decompositions as in FTA.

$GCD = 2 \cdot 3 \cdot 5 = 30$

$LCM = 7 \cdot 1223 \cdot 2^3 \cdot 3^2 \cdot 5^3 = 77{,}049{,}000$

5. (a) (i) $(a,b) \sim (a,b)$ Since $a+b = b+a$

(ii) If $(a,b) \sim (c,d)$, then $a+d = b+c \Rightarrow c+b = d+a \Rightarrow$
$(c,d) \sim (a,b)$

(iii) If $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f) \Rightarrow a+d = b+c$
$c+f = d+e$

Adding we get $a+d+c+f = b+c+d+e \Rightarrow a+f = b+e \Rightarrow (a,b) \sim (e,f)$
$\therefore \sim$ is an equivalence relⁿ

(b) $(3,5) \sim (a,b)$ if and only if $3+b = 5+a$ iff
$b = a+2$ i.e. $\Leftrightarrow$ (a,b) lies on the line $y = x+2$.

(c) Suppose $[(a,b)] = [(c,d)]$ Then $(a,b) \sim (c,d)$
$\Rightarrow a+d = b+c \Rightarrow a-b = c-d \Rightarrow f([(a,b)]) = f([(c,d)])$.

#6. (a)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) 1 appears in every Non-zero Row/Column of the multiplication table.

Better: $GCD(a,7) = 1$ for $a = 1, 2, 3, 4, 5, 6$.

(c) Note $7 \cdot 7 \equiv 1 \mod 12$. Thus if we multiply both sides of the congruence $7X \equiv 5 \pmod{12}$

by 7 we get: $49X \equiv 35 \pmod{12}$

$$\Downarrow$$

$$X \equiv 11 \pmod{12}.$$

(d) Take $n = 14$. Then:

$$
\begin{aligned}
7 \cdot 0 &\equiv 0 \mod 14 \\
7 \cdot 1 &\equiv 7 \mod 14 \\
7 \cdot 2 &\equiv 0 \mod 14 \\
7 \cdot 3 &\equiv 7 \mod 14 \\
7 \cdot 4 &\equiv 0 \mod 14 \\
7 \cdot 5 &\equiv 7 \mod 14 \\
7 \cdot 6 &\equiv 0 \mod 14 \\
&\vdots \\
7 \cdot 13 &\equiv 7 \mod 14
\end{aligned}
$$

This shows that $7 \cdot X \equiv 5$ has no sol^{n} mod 14.

OR. Suppose a is a Sol$^{\underline{n}}$ to the Congruence $\Rightarrow 7a \equiv 5 \mod 14 \Rightarrow$

$14 \mid 7a-5 \Rightarrow 7a-5 = 14 \cdot n \Rightarrow 7a = 14 \cdot n + 5$

$\Rightarrow 7 \mid 5$, $\times\!\!\times$. So No Sol$^{\underline{n}}$ exists.

6e $12x \equiv 15 \mod 21$

$\Rightarrow 4x \equiv 5 \mod 7$, $3 = GCD(12, 21)$

$x = 3$ is one sol$^{\underline{n}}$ mod 21

adding $\frac{21}{3} = 7 \Rightarrow x = 10$ is a sol$^{\underline{n}}$

$x = 17$ is a sol/n

$\therefore$ Over $\mathbb{Z}_{12}$: ~~3, 17,~~ 3, 10, 17 are sol$^{\underline{n}}$s

Over $\mathbb{Z}$: $\{21n + 3 \mid n \in \mathbb{Z}\}$

$\{21n + 17 \mid n \in \mathbb{Z}\}$ are sol$^{\underline{n}}$s

$\{21n + 10 \mid n \in \mathbb{Z}\}$

6f: If a is a sol$^{\underline{n}}$ $\Rightarrow a^2 - 1 \equiv 0 \mod 35$

This problem was given as a challenge.

$\Rightarrow a^2 \equiv 1 \mod 35$

So at least a has an inverse $\Rightarrow gcd(a, 35) = 1$

In Lecture 6, we set up a correspondence $\mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$ where $n = ab$

$gcd(a, b) = 1$, given by

$\tilde{i} \longrightarrow (\bar{i}, \bar{i})$ and we showed

this correspondence respected multiplication

Thus we have $\mathbb{Z}_{35} \longrightarrow \mathbb{Z}_5 \times \mathbb{Z}_7$

If $\tilde{a} \in \mathbb{Z}_{35}$ satisfies $\tilde{a}^2 \equiv 1 \bmod 35$

$\Rightarrow (\bar{a}, \hat{a})^2 \equiv (1,1)$ in $\mathbb{Z}_5 \times \mathbb{Z}_7$

i.e. $(\bar{a})^2 \equiv 1$ in $\mathbb{Z}_5$

$(\hat{a})^2 \equiv 1$ in $\mathbb{Z}_7$

Thus $\bar{a} \equiv 1$ or 4 in $\mathbb{Z}_5$

$\hat{a} \equiv 1$ or 6 in $\mathbb{Z}_7$

$\therefore (\bar{1}, \hat{1}), (\bar{4}, \hat{1}), (\bar{1}, \hat{6}), (\bar{4}, \hat{6})$

each square to $(1,1)$ in $\mathbb{Z}_5 \times \mathbb{Z}_7$

Under the correspondence

$\tilde{1} \longleftrightarrow (\bar{1}, \hat{1})$

$\widetilde{29} \to (\bar{4}, \hat{1})$

$\tilde{6} \to (\bar{1}, \hat{6})$

$\widetilde{34} \to (\bar{4}, \hat{6})$

$\therefore \tilde{1}, \widetilde{29}, \tilde{6}, \widetilde{34}$ are sol$^{\underline{n}}$s to $x^2 - 1 \equiv 0 \bmod 35$

7) mod 31, $(27)^{-1} \equiv 23$

mod 33, No inverse

mod 34, $(27)^{-1} \equiv 29$

8) $139^{112} \bmod 27$ $\qquad \phi(27) = 3^3 - 3^2 = 27 - 9 = 18$

$\parallel$

$4^{112} \bmod 27$

$\parallel$

$(4^{18})^6 \cdot 4^4 \bmod 27$

$\parallel$

$1 \cdot 4^4 \bmod 27 \equiv 256 \bmod 27 \equiv \boxed{13 \bmod 27}$

9) $\phi(1492) = \phi(4)\phi(373) = 2(372)$, since 373 is prime

$= 744$

$\phi(1776) = \phi(2^4 \cdot 3 \cdot 37) = \phi(2^4)(\phi(3))\phi(37)$

$= (2^4 - 2^3)(2)(36) = 16 \cdot 36 = 576$

$\phi(2001) = \phi(3) \cdot \phi(23)\phi(29)$

$= 2 \cdot 22 \cdot 28 = 1232$

10. 1^{st} note if $n = 2^e$

Then $\frac{\phi(n)}{n} = \frac{2^e - 2^{e-1}}{2^e} = 1 - \frac{1}{2} = \frac{1}{2}$

Conversely if $n = p^e$

and $\frac{1}{2} = \frac{\phi(n)}{n} = \frac{p^e - p^{e-1}}{p^e} = 1 - \frac{1}{p}$

$\Rightarrow 1 - \frac{1}{2} = 1 - \frac{1}{p} \Rightarrow \frac{1}{2} = \frac{1}{p} = p = 2.$

$\therefore$ The only n with one prime factor s.t. $\frac{\phi(n)}{n} = \frac{1}{2}$ is $n = 2^e$, $e \geq 1$.

Suppose $n = p_1^{e_1} \cdots p_r^{e_r}$ with $r > 1$. Claim ~~it~~ can't have $\frac{\phi(n)}{n} = \frac{1}{2}$. Spose otherwise:

$$\frac{1}{2} = \frac{\phi(n)}{n} = \frac{(p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p_r^{e_r-1})}{p_1^{e_1} \cdots p_r^{e_r}}$$

$$\Rightarrow \frac{1}{2} = \left(\frac{p_1 - 1}{p_1}\right) \cdots \left(\frac{p_r - 1}{p_r}\right)$$

$$\Rightarrow 2(p_1 - 1) \cdots (p_r - 1) = p_1 \cdots p_r.$$

2 divides LHS $\Rightarrow 2 \mid$ RHS $\Rightarrow 2 \mid p_i$ some i, say $2 \mid p_1$

Then $2 = p_1$.

$\therefore 2(2-1)(p_2-1)\cdots(p_r-1) = 2\cdot p_2\cdots p_r$

$\Rightarrow (p_2-1)\cdots(p_r-1) = p_2\cdots p_r$, a contradiction. Thus $r=1$

and only $n = 2^e$, some $e\geq 1$

satisfies $\dfrac{\phi(n)}{n} = \dfrac{1}{2}$.