Math 241

12 March 2010
Second Midterm

NAME (Print!): Key

Problem	Points	Score
1	20	
2	20	
3	20	
4	20	
5	10	
6	10	
Total	100	

Problem 1 (20 points): Show that $n^2 + 1000n = O(n^3)$.

I need a C so that $n^2 + 1000n < Cn^3$ whenever $n \geq n_0$. i.e.,

$$\frac{1}{n} + \frac{1000}{n^2} \leq C$$

$C = 1001$ and $n_0 = 1$ works since $\frac{1}{n} + \frac{1000}{n^2}$ is always decreasing and at $n_0 = 1$ we have 1001.

Problem 2 (20 points): Solve for x in the following (not by brute force):

(a) For an odd integer n, $2x \equiv 1 \pmod{n}$.

$x \equiv \frac{n+1}{2} \pmod{n}$. $2 \cdot \left(\frac{n+1}{2}\right) \equiv (n+1) \bmod n \equiv 1 \bmod n$

(b) $2x \equiv 7 \pmod{17}$

~~56~~

$2^{-1} = \frac{17+1}{2} = 9$

$2x \equiv 7 \pmod{17}$

$x \equiv 63 \pmod{17}$

$x \equiv 12 \pmod{17}$

Problem 3 (20 points): Prove that $3^{3n+1} + 2^{n+1}$ is divisible by 5 f

$n=0$:

$3 + 2$ is divisible by 5

~~Assume~~ Let $f(n) = 3^{3n+1} + 2^{n+1}$

Assume $f(n)$ is divisible by 5 an

$f(n+1)$ is

$3^{3(n+1)+1}$

$+ 2^{n+1+1}$

$= 3^{3n+4}$

$+ 2$

$= 27\, 3^{3n+1}$ +

$= 27\, 3^{3n+1} - 27$

$= 27(3^{3n+1} - 2^{n+}$

Problem 4 (20 points): Find all solutions to the system of congruences (only partial credit will be given if you do this by brute force):

$$x \equiv 2 \pmod 3$$
$$x \equiv 1 \pmod 4$$
$$x \equiv 3 \pmod 5$$

$M_1 = 20$

$M_2 = 15$

$M_3 = 12$

$M_1 y_1 \equiv 1 \pmod{m_1}$

$\Rightarrow$

$20 y_1 \equiv 1 \pmod 3$

$2 y_1 \equiv 1 \pmod 3$ $\quad y_1 = 2$

$M_2 y_2 \equiv 1 \pmod{m_2}$

$15 y_2 \equiv 1 \pmod 4$

$3 y_2 \equiv 1 \pmod 4$

$y_2 = 3$

$M_3 y_3 \equiv 1 \pmod{m_3}$

$12 y_3 \equiv 1 \pmod 5$ $\quad 2 y_3 \equiv 1 \pmod 5$

$y_3 = 3$

$x = 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 3$

$= 80 + 45 + 108$

$= 20 - 15 + 48$

$= 53$

$53 + k60$

$k \in \mathbb{Z}$.

Problem 5 (10 points): Alice wants to send an RSA encrypted message M to her friends Bob and Carol. She uses key (e_1, n) to send the message to Bob and (e_2, n) to send the message to Carol where e_1 and e_2 are distinct primes. Alice sends $C_1 = M^{e_1} \pmod{n}$ to Bob and $C_2 = M^{e_2} \pmod{n}$. to Carol. If you intercept C_1, C_2 and knew e_1, e_2, n, describe how you would find M.

I need an M' some how.

Since e_1, e_2 are distinct primes $\gcd(e_1, e_2) = 1$

$\Rightarrow$ $\exists\ x, y$ so that $e_1 x + e_2 y = 1$. Find them.

Take $C_1 = M^{e_1}$

$C_2 = M^{e_2}$

Then

$C' = (M^{e_1})^x \cdot (M^{e_2})^y \pmod{n}$

$= M^{e_1 x + e_2 y} \pmod{n}$

$\equiv M' \pmod{n}$

$\equiv M \pmod{n}$.

Problem 6 (10 points): For a string w, let w^i be the concatentation of w with itself i times. Give a recursive definition of w^i and use it to prove $\ell(w^i) = i\ell(w)$ ~~via structural induction.~~

Recursive defn:

$w^0 = \lambda$ (empty string)

$w^i = w \cdot w^{i-1}$

~~pf: $\ell(\lambda^i) = \ell(\lambda) = 0$.~~

$x \in \Sigma$

~~$\ell((wx)^i) = \ell((wx)(wx)^{i-1})$~~

pf:

$$\begin{aligned} \ell(w^i) &= \ell(w\, w^{i-1}) \\ &= \ell(w) + \ell(w^{i-1}) \\ &= \ell(w) + (i-1)\ell(w) \\ &= i\,\ell(w). \end{aligned}$$

(THIS PAGE INTENTIONALLY BLANK)