Exam II – 11/18/09
SOLUTIONS

Math 406

1. (15 points) Using the Chinese Remainder Theorem, find all solutions to the following system:

$$7x \equiv 4 \pmod{11}$$
$$x \equiv 3 \pmod{7}.$$

First note that since $7^{-1} \equiv 8$ modulo 11, the first equation can be replaced with $x \equiv -1$ modulo 11. Then we solve using the Chinese Remainder Theorem: $m_1 = 11$, $M_1 = 7$ and $m_2 = 7$, $M_2 = 11$, and $a_1 = -1$, and $a_2 = 3$. We solve

$$y_1 M_1 \equiv 7y_1 \equiv 1 \ (11)$$
$$y_2 M_2 \equiv 11y_2 \equiv 1 \ (7)$$

to find $y_1 = 8$ and $y_2 = 2$. Then the general solution is

$$x \equiv a_1 y_1 M_1 + a_2 y_2 M_2 = (-1) \cdot 8 \cdot 7 + 3 \cdot 2 \cdot 11 = 10 \ (77).$$

2. (20 points) If the ciphertext message produced by RSA encryption with the key $(e, n) = (139, 2747)$ is 1439, what is the plaintext message? (Give the answer as a block of 4 digits. Use the back of this page if necessary.)

We have the prime factorization $2747 = 41 \cdot 67$, so $\phi(2747) = 40 \cdot 66 = 2640$. The solution to $139d \equiv 1 \ (2640)$ is $d = 19$. Thus we need to compute $1439^{19} \ (2747)$. We can do this calculating $1439^2 \ (2747)$, then $1439^4 \ (2747)$, and so on, up to $1439^{16} \ (2747)$. Using this we compute $1439^{19} \equiv 113 \ (2747)$. Thus, the plaintext message is 0113.

3. (a) (10 points) Find $\text{ord}_{14}5$.

Note $\phi(14) = 6$, so the order of 5 is a divisor of 6. Easy to see: $5^2 \equiv 11$ and $5^3 \equiv -1$ modulo 14, so the order of 5 is not a divisor of 2 or 3. Thus the order is 6.

(b) (5 points) Find all the primitive roots for 14. (Hint: first determine the number of primitive roots.)

There are $\phi(\phi(14) = \phi(6) = 2$ primitive roots. One is 5, henc the other is 5^{-1} modulo 14, that is, 3. So the two primitive roots are 3 and 5 modulo 14.

4. (10 points) Let p be a prime number. Show that for all integers a, b, we have $(a+b)^p \equiv a^p + b^p \pmod{p}$. Does this remain true if p is replaced by an arbitrary integer n? (Explain.)

A form of Fermat's Little Theorem says $x^p \equiv x\ (p)$, for all integers x. Taking $x = a + b$ and $x = a$ and $x = b$, we see that both sides of the equation $(a + b)^p \equiv a^p + b^p\ (p)$ are simply $a + b$. Hence the equation is true.

The equation fails if p is replaced by a composite number. For example, take $n = 4$, $a = 1$ and $b = -1$. Then note

$$(1 + -1)^4 \equiv 0\ (4)$$

but

$$1^4 + (-1)^4 \equiv 2\ (4).$$

5. (a) (10 points) Let m, n be positive integers. Prove that $m \,|\, n \Rightarrow \phi(m) \,|\, \phi(n)$.

Write $m = p_1^{a_1} \cdots p_r^{a_r}$, where the p_i's denote distinct primes and $a_i > 0$ for each i. Write $n = p_1^{b_1} \cdots p_r^{b_r} q_1^{c_1} \cdots q_s^{c_s}$, for some integers $b_i, c_j > 0$ and primes q_j (pairwise distinct and distinct from the p_i's; note we have to allow $s = 0$ as a possibility). We have $a_i \leq b_i$ for each i, since $m|n$.

By a formula for ϕ, we have

$$\begin{aligned}\phi(m) &= p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1) \\ \phi(n) &= p_1^{b_1-1}(p_1 - 1) \cdots p_r^{b_r-1}(p_r - 1)\, q_1^{c_1-1}(q_1 - 1) \cdots q_s^{c_s-1}(q_s - 1).\end{aligned}$$

Since $a_i - 1 \leq b_i - 1$ for each i, it is now evident that $\phi(m)|\phi(n)$.

(b) (5 points) Is it true that $m \mid n \Rightarrow \sigma(m) \mid \sigma(n)$? Prove, or disprove with a counterexample.

No, in general this is false. Consider $m = 3$ and $n = 9$. Then $\sigma(3) = 1 + 3 = 4$ but $\sigma(9) = 1 + 3 + 9 = 13$, and 4 does not divide 9.

(c) (5 points) Is it true that $m \mid n \Rightarrow \mu(m) \mid \mu(n)$? Prove, or disprove with a counterexample.

Yes, this is true. Here's the proof. Note that μ takes values in $\{0, 1, -1\}$. Since 1 and -1 divide every integer, we have $\mu(m)|\mu(n)$ for any n, if $\mu(m) \in \{1, -1\}$. We just need to consider the case $\mu(m) = 0$ and show that in that case, if $m|n$, then we must have $\mu(n) = 0$ as well. Then we'd be done, since $0|0$.

But $\mu(m) = 0$ if and only if m is divisible by the square of a prime number. But in that case, since $m|n$, we have n is also divisible by a square of a prime, and so $\mu(n) = 0$ too.

6. (10 points) Let p be a prime number. Show that $(2p-1)! \equiv p \pmod{p^2}$. (Use the back of this page if necessary.)

Write $(2p-1)! = [(p+p-1)(p+p-2)\cdots(p+1)] \cdot p \cdot (p-1)!$. The bracketed term $[\cdots]$ is congruent modulo p to $(p-1)!$, so by Wilson's theorem it is congruent to -1 modulo p. Write $[\cdots] = -1 + kp$ for an integer k, and write $(p-1)! = -1 + lp$ for an integer l.

Then

$$(2p-1)! = (-1 + kp) \cdot p \cdot (-1 + lp).$$

It is the right hand side is congruent to p modulo p^2.