**July 8, 2004**

# Math 490A
# Number Theory
# Midterm Exam
# Solution

**Instructions:** Give a complete solution to each problem. You may use any result from class or the homework (except the result in question or a result whose proof depends on the result in question). When using a result be sure to either give it's name, or allude to its content. Be sure to work the problems in an order that will maximize *your* score. You may use a (non programmable) calculator.

**1. (6 points)** Prove that there is no pair of integers satisfying $(x, y) = 7$ and $x+y = 1000$.

*Solution.* If $(x, y) = 7$, then $7|x + y$. Thus, if $(x, y) = 7$ and $x + y = 1000$, we would have $7|1000$, which is a contradiction.

**2. (8 points)** Use the Euclidean algorithm to find $d = (3672, 1566)$. Write $d$ as an integer linear combination of 3672 and 1566.

*Solution.* we iterate the Division Algorithm:

$$\begin{aligned} 3672 &= 2 \cdot 1566 + 540 \\ 1566 &= 2 \cdot 540 + 486 \\ 540 &= 1 \cdot 486 + 54 \\ 486 &= 9 \cdot 54 + 0. \end{aligned}$$

Thus, $d = 54$. We now back substitute:

$$54 = 540 - 486 = 540 - (1566 - 2 \cdot 540) = 3 \cdot 540 - 1566 =$$
$$3(3672 - 2 \cdot 1566) - 1566 = 3 \cdot 3672 - 7 \cdot 1566.$$

**3.**

(a) **(15 points)** State and Prove Euler's Theorem.

(b) **(8 points)** Show that, for any integer $n$, $n^7 - n$ is divisible by 42.

(a)

EULER'S THEOREM. *If $m > 0$ and $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1(\mod m)$.*

*Proof.* Let $r_1, r_2, \ldots, r_{\varphi(m)}$ be a reduced residue system modulo $m$. Then, since $(a, m) = 1$, $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ is another reduced residue system modulo $m$. Thus,

$$\begin{aligned} ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(m)} &\equiv r_1 r_2 \ldots r_{\varphi(m)} (\mod m) \\ \Rightarrow a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} &\equiv r_1 r_2 \ldots r_{\varphi(m)} (\mod m) \\ \Rightarrow a^{\varphi(m)} &\equiv 1 (\mod m), \end{aligned}$$

since each $r_i$ is invertible, modulo $m$. □

(b)

*Proof.* Since $42 = 2 \cdot 3 \cdot 7$, we need to show $n^7 \equiv n(\mod p)$, for $p = 2, 3$, and 7. Note $n^7 \equiv n(\mod 2)$ since $n^7$ is odd if and only if $n$ is. By Fermat's Theorem, $n^3 \equiv n(\mod 3)$, for any $n$. Thus $n^7 \equiv (n^3)^2 \equiv n^3 \equiv n(\mod 3)$, as we claim. Finally, Fermat's Theorem implies $n^7 \equiv n(\mod 7)$ for all $n$. Thus, $n^7 - n$ is divisible by $2, 3$, and 7, and hence by 42. □

**4. (10 points)** Find all solutions to the congruence

$$20x \equiv 30 \,(\mathrm{mod}\ 35).$$

We give two solutions:

*Solution 1.* Since $(20, 35) = 5$, and $5|30$, there are 5 solutions to this congruence, $(\mod 35)$. Morevoer, these are given by all solutins to

$$\frac{20}{5}x \equiv \frac{30}{5} (\mod \frac{35}{5}),$$

which gives

$$4x \equiv 6(\mod 7).$$

Since $2 \cdot 4 \equiv 1 (\mod 7)$, we get $x \equiv 5 (\mod 7)$. Thus, the solutions are $x \equiv 5, 12, 19, 26, 33 (\mod 35)$. □

*Solution 2.* Note, by the Chinese Remainder Theorem, $20x \equiv 30 (\mod 35)$ is equivalent to

$$\begin{cases} 20x \equiv 30 (\mod 5) \\ 20x \equiv 30 (\mod 7) \end{cases} \Leftrightarrow \begin{cases} 0x \equiv 0(\mod 5) \\ 6x \equiv 2 (\mod 7). \end{cases}$$

The first congruence is always satisfied. Further, since $6^2 \equiv 1 \pmod 7$, we have $x \equiv 6 \cdot 2 \equiv 5 \pmod 7$. Thus

$$x \equiv 5, 12, 19, 26, \text{ and } 33 \pmod{35}$$

are all of the solutions. □

**5. (13 points)** Let $f(x) = x^3 + 4x^2 + 2x + 8$. Determine the **number** of solutions to $f(x) \equiv 0 \pmod{27}$.

*Solution.* We first solve $f(x) \equiv 0 \pmod 3$. By Fermat's Theorem, and reduction modulo 3, we have

$$f(x) \equiv x^2 + 2 \pmod 3.$$

This has solutions $x \equiv \pm 1 \pmod 3$. Note that

$$f'(x) = 3x^2 + 8x + 2 \equiv 2x + 2 \pmod 3.$$

Since $f'(1) \not\equiv 0 \pmod 3$ we know there is a unoque solution $s_0$ to $f(x) \equiv 0 \pmod{27}$, with $s_0 \equiv 1 \pmod 3$. Note $f'(-1) \equiv 0 \pmod 3$. Further $f(-1) = 9 \equiv 0 \pmod 9$. Thus all of the integers $-1 + 3t$, for $t = 0, 1$, and 2, are solutions to $f(x) \equiv 0 \pmod{27}$. So, $x \equiv -1, 2, 5 \pmod 9$ are solutions modulo 9. Note that $f(-1) \not\equiv 0 \pmod{27}$. Further $f(2) = 36 \not\equiv 0 \pmod{27}$. finally,

$$f(5) = 5^3 + 4 \cdot 5^2 + 2 \cdot 5 + 8 \equiv 5(-2) + 4(-2) + 5(2) + 8 \equiv 0 \pmod{27}.$$

Thus $x \equiv 5, 14, 23 \pmod{27}$ are all solutions. Hence there are 4 solutions. □

**6. (7 points each)** Determine for which of the following values of $n$, $x^n - 1$ has $n$ solutions modulo 17.

(a) $n = 8$.
(b) $n = 9$.

*Solution.*

(a) Since 17 is prime, and $8|16$, we know there are 8 solutions to $x^8 - 1 \equiv 0 \pmod{17}$.
(b) Note that, using the division algorithm for polynomials,

$$x^{17} - x = (x^9 - 1)x^8 + (x^8 - x).$$

Since the remainder $x^8 - x$ does not have all of its coefficients divisible by 17, Chebyshev's Theorem implies $x^9 - 1 \equiv 0 \pmod{17}$ has fewer than 9 solutions. □

**7. (15 points)** Prove that for every prime $p > 5$ either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.

*Proof.* . Since $p > 5$, and $p$ is prime, we have $p$ is odd. Thus, $2|p^2 - 1$ and $2|p^2 + 1$. Also, since $5 \not| p$, we have $p \equiv 1, 2, 3, \text{ or} 4 \pmod{5}$. Thus $p^2 \equiv \pm 1 \pmod{5}$. Thus either $5|p^2 - 1$ or $5|p^2 + 1$. Thus, one of $p^2 - 1$ or $p^2 + 1$ is a multiple of 10.

*Alternate proof.* Since $p > 5$, we know $5 \not| p$, and thus $p \equiv 1, 3, 7, \text{ or } 9 \pmod{10}$. Thus $p^2 \equiv 1, \text{ or } 9 \pmod{10}$. Thus $10|p^2 - 1$, or $10|p^2 + 1$. □

**8. (11 points)** Prove that, $\varphi(12^k) = \varphi(12) \cdot 12^{k-1}$.

*Solution.* Note that

$$\varphi(12) = \varphi(2^2)\varphi(3) = 2 \cdot 2 = 4.$$

Further,

$$\begin{aligned}\varphi(12^k) = vp(2^{2k}3^k) = \varphi(2^{2k})\varphi(3^k) = 2^{2k-1} \cdot (2-1)3^{k-1}(3-1) \\ = 2^{2k}3^{k-1} = 4 \cdot 2^{2(k-1)}3^{k-1} = \varphi(12)12^{k-1}.\end{aligned}$$

□

**Extra Credit: (10 points)** Find all solutions to $f(x) \equiv 0 \pmod{27}$, with $f(x)$ as in problem 5.

*Solution.* We need only find the solution $s_0 \equiv 1 \pmod{3}$. Since $f'(1) \equiv 1 \pmod{3}$, we have a unique solution $s_2 \equiv 1 \pmod{3}$ with $f(s_2) \equiv 0 \pmod{9}$, and $s_2 = 1 + 3t$, where

$$f'(1)t \equiv \frac{-f(1)}{3} \pmod{3}.$$

Thus $t \equiv \dfrac{-15}{3} \equiv 1 \pmod{3}$, and $s_2 \equiv 4 \equiv (-5) \pmod{9}$. note

$$f(5) \equiv -5(-2) + 4(-2) + 2(-5) + 8 \equiv 0 \pmod{27}.$$

Thus $s_3 \equiv -5 \,(mod 27)$ is the unique solution with $s - 3 \equiv 1 \pmod{3}$. therefore, the four solutions are $x \equiv 5, 14, 22, 23 \pmod{27}$.

Note: An alternative way to compute the solution $s_3$ :

$$f(4) = 4^3 = 4 \cdot 4^2 + 2(4) + 8 \equiv 10 + 10 + 8 + 8 \equiv 9 \,(\mod 27).$$

Thus, $s_3 = s_2 + 9t$, with

$$f'(s_2)t \equiv \frac{-f(4)}{9} \,(\mod 3),$$

which says $t \equiv -1 \,(\mod 3)$, so we get $s_3 \equiv 4 - 9 = -5 \,(\mod 27)$. □