MATH 362 Midterm 1 Time: 50 minutes

Friday October 11, 2019

1. [6] Let $n = 693 = 3^2 \times 7 \times 11$. Complete – just write down the answers, no explanations necessary. Use the last page for rough work if necessary.

   (a) $d(n) = 3 \times 2 \times 2$

   (b) $\sigma(n) = (\frac{3^3-1}{2})(\frac{7^2-1}{6})(\frac{11^2-1}{10}) = 1248$

   (c) The least residue of $n^{34} \pmod 5$ is 4.

2. [3] Let $p > 3$ be a prime number. Prove that $p \equiv 1$ or $5 \pmod 6$.

   Since p is odd, $p \equiv 1,\ 3$ or $5 \pmod 6$. If $p \equiv 3 \pmod 6$, then $p = 6k + 3$ for some integer k. Then $3|p$. Since $p \neq 3$, this implies p is not prime, a contradiction. Therefore $p \equiv 1$ or $5 \pmod 6$.

3. [3] Solve the congruence $39x \equiv 9 \pmod{21}$.

   Since $(39, 21) = 3$ and $3|9$, the congruence has three solutions.

   Simplify:
   $$39x \equiv 9 \pmod{21} \Rightarrow 13x \equiv 3 \pmod 7 \Rightarrow 6x \equiv 3 \pmod 7.$$

   Hence
   $$2x \equiv 1 \equiv 8 \pmod 7 \quad \text{since } (3, 7) = 1.$$

   Therefore $x \equiv 4 \pmod 7$. The solutions are $4,\ 11,\ 18$.

4. [4] Does the congruence $899x \equiv 17 \pmod{1479}$ have a solution? Why or why not?

Using the Euclidean algorithm (or another suitable method), we see that $(899, 1479) = 29$. Since 29 does not divide 17, the congruence has no solutions.

5. [4] Find the smallest integer $a > 2$ such that $2|a,\ 5|(a+1)$ and $9|(a+2)$.

From the statements $2|a,\ 5|(a+1)$ and $9|(a+2)$, we deduce that

$$a \equiv 0 \pmod{2} \tag{1}$$
$$a \equiv -1 \pmod 5 \tag{2}$$
$$a \equiv -2 \pmod{9}. \tag{3}$$

From (1) we deduce that $a = 2r$ for some $r \in \mathbb{Z}$. Substitute in (2):

$$2r \equiv -1 \equiv 4 \pmod{5},$$

hence $r \equiv 2 \pmod{5}$ since $(2, 5) = 1$. Say $r = 5s + 2,\ s \in \mathbb{Z}$. Then $a = 2(5s + 2) = 10s + 4$. Substitute in (3):

$$10s + 4 \equiv s + 4 \equiv -2 \pmod{9}.$$

Hence $s \equiv -6 \equiv 3 \pmod{9}$. Say $s = 9t + 3,\ t \in \mathbb{Z}$. Then $a = 10(9t + 3) + 4 = 90t + 34$. Putting $t = 0$ we see that 34 is the smallest number a with the given properties.

6. [3] Prove that if $a^k - 1$ is prime, then $a = 2$.

(Sorry, the question should have stipulated that $k > 1$, otherwise there is a counterexample with $a = 3$ and $k = 1$.)

From Assignment 1, Question 2, we know that

$$\sum_{i=0}^{k-1} a^i = \frac{a^k - 1}{a - 1}, \quad a \neq 1.$$

Hence

$$a^k - 1 = (a - 1)(a^0 + a^1 + \cdots a^{k-1}).$$

Since $a^k - 1$ is prime, $a - 1 = 1$ or $a^0 + a^1 + \cdots a^{k-1} = 1$. Since $k > 1$, $a^0 + a^1 + \cdots a^{k-1} > 1$. Hence $a = 2$.

7. [5] Prove Wilson's Theorem: The integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$. You don't need to prove the lemmas you use.

Suppose p is prime. If $p = 2$ the result is obvious, so assume p is odd. By a lemma we can arrange the $p-3$ numbers

$$2,\ 3,\ \ldots,\ p-2$$

as $(p-3)/2$ pairs such that each pair consists of an integer a and its associated integer a', which is different from a, such that $aa' \equiv 1 \pmod{p}$. Since the product of the two integers in each pair is congruent to $1 \pmod{p}$, it follows that

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

hence

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}.$$

Conversely, suppose that for some integer n,

$$(n-1)! \equiv -1 \pmod{n}. \tag{4}$$

We must prove that n is prime. Suppose $n = ab$ for some positive integers a, b such that $a \neq n$. From (4) we have

$$n|((n-1)!+1)$$

and since $a|n$ we have

$$a|((n-1)!+1). \tag{5}$$

But since $a \leq n-1$ it follows that a is one of the factors of $(n-1)!$. Thus

$$a|(n-1)! \tag{6}$$

But (5) and (6) imply that $a|1$, so $a = 1$. Therefore the only positive divisors of n are 1 and n, thus n is a prime.

8. [4] Prove that if $2^p - 1$ is prime and $n = 2^{p-1}(2^p - 1)$, then n is perfect.

Let $n = 2^{p-1}(2^p-1)$. Since $2^p - 1$ is prime, $\sigma(2^p-1) = 2^p - 1 + 1 = 2^p$. Also, 2^{p-1} is a prime power, hence

$$\sigma(2^{p-1}) = 2^p - 1.$$

Now, σ is a multiplicative function and $(2^{p-1}, 2^p - 1) = 1$ (because 2 is the only prime divsor of 2^{p-1} while $2^p - 1$ is odd), hence

$$\sigma(n) = \sigma(2^{p-1}(2^p-1)) = \sigma(2^{p-1})\sigma(2^p-1) = (2^p-1)(2^p) = 2n.$$

Thus n is perfect.