Nathan Ha SID 862377326

CS 111 ASSIGNMENT 2
due February 5

Problem 1: Prove the following statement:
If $p > 5$ and $gcd(p, 20) = 1$, then $(p^2 - 21)(p^2 + 16) \equiv 0 \pmod{20}$.

Hint: The product of any k consecutive integers is divisible by k.

Solution 1: SOLUTION 1 GOES HERE

Problem 2: PROBLEM 2 GOES HERE

Solution 2: SOLUTION 2 GOES HERE

Problem 3:

(a) Compute $5^{1627} \pmod{12}$. Show your work.

(b) Compute $8^{-1} \pmod{17}$ by listing the multiples. Show your work.

(c) Compute $8^{-1} \pmod{17}$ using Fermat's Little Theorem. Show your work.

(d) Compute $8^{-11} \pmod{17}$ using Fermat's Little Theorem. Show your work.

(e) Find an integer x, $0 \leq x \leq 40$, that satisfies the following congruence: $31x + 54 \equiv 16 \pmod{41}$. Show your work. You should not use brute force approach.

Solution 3:

(a) $5^{1627} \pmod{12}$
$\equiv 5 \cdot (5^2)^{813} \pmod{12}$
$\equiv 5 \cdot (25)^{813} \pmod{12}$
$\equiv 5 \cdot (1)^{813} \pmod{12}$
$\equiv 5 \pmod{12}$.

(b) $8^{-1} \pmod{17} \implies 8a \equiv 1 \pmod{17} \implies 8a = 17b + 1$. We need to find an a to make this equation true.
Multiples of 8: $8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120$
Multiples of 17 (and then +1): $18, 35, 52, 69, 86, 103, 120$
We can see that the equation is true when $a = 15$ and $b = 7$. This means that $8^{-1} \pmod{17} \equiv 15$.

(c) According to Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, where p is prime. Since $8^{-1} \pmod{17}$, and 17 is prime, then $8x \equiv 1 \pmod{17}$, for some a. By Fermat's Little Theorem, we can say: $8^{16} \equiv 8^{17-1} \equiv 1 \pmod{17} \implies 8 \cdot 8^{15} \equiv 1 \pmod{17}$
$\implies 8^{-1} \equiv 8^{15} \pmod{17}$
$\equiv 8(8^2)^7 \pmod{17}$
$\equiv 8(64)^7 \pmod{17}$
$\equiv 8(13)^7 \pmod{17}$
$\equiv (8)(13)(13^2)^3 \pmod{17}$
$\equiv 104(169)^3 \pmod{17}$
$\equiv 2(16)^3 \pmod{17}$
$\equiv 2(16)(16)^2 \pmod{17}$
$\equiv 32(256) \pmod{17}$
$\equiv 15(256) \pmod{17}$
$\equiv 15(1) \pmod{17}$
$\equiv 15 \pmod{17}$.
Therefore, $8^{-1} \pmod{17} = 15$.

(d) $8^{-11} \pmod{17}$ is the same as $(8^{-1})^{11} \pmod{17}$. we know that, by the result found in parts b and c, that $8^{-1} \pmod{17} = 15$. This means that $(8^{-1})^{11} \equiv 15^{11} \pmod{17}$. From here, since we want to use Fermat's Little Theorem, we should multiply by $(8^5)(8^{-1})^5 \equiv (8^5)(15)^5 \equiv 1 \pmod{17}$. We know this to be true because of the properties of inverses. We now have $8^5(15^5)(15^{11})$
$\equiv 8^5(15)^{16} \pmod{17}$. By Fermat's Little Theorem (as stated in part c), we can substitute 15^{16} with 1: $8^5(15)^{16} \pmod{17} \equiv 8^5 \pmod{17}$. Now, we can simplify by squaring:
$8^5 \equiv 8 \cdot 64^2 \pmod{17}$
$\equiv 8 \cdot 13^2 \pmod{17}$
$\equiv 8 \cdot 169 \pmod{17}$
$\equiv 8 \cdot 16 \pmod{17}$
$\equiv 128 \pmod{17}$
$\equiv 9 \pmod{17}$.

(e) $31x + 54 \equiv 16 \pmod{41}$. First, we can subtract both sides by 54: $31x \equiv -38 \pmod{41}$
$\equiv 3 \pmod{41}$. Now, we have to find the inverse $31^{-1} \pmod{41}$. We can list multiples to find the solution of $31a = 41k + 1$:
multiples of 31: 31, 62, 93, 124
multplies of 41(+1): 42, 83, 124
As we can see, the equation is true when $a = 4$ and $k = 3$. This means that the inverse of 31 is 4.
Going back to the original equation, we can multiply both sides by 31^{-1}:
$31 \cdot 31^{-1}x \equiv 31^{-1} \cdot 3 \pmod{41} \implies x \equiv 4 \cdot 3 \pmod{41} \equiv 12 \pmod{41}$. Therefore, $x = 12$.
