Name: ______________________________

MATH 580: TEST 1, FALL 2019

Instructions and Point Values: There are 8 problems. For each problem below, show ALL of your work. If a box is given, put your answer in the box. If a problem says to simplify your answer, you should in particular not leave your answer in a product form - multiply it out. Do NOT use a calculator.

There are 100 total points possible on this exam.

20 pts (1) Give short answers for each of the following.

(a) If $a = 2^2 \cdot 3 \cdot 5^2 \cdot 7$ and $b = 2 \cdot 3^2 \cdot 7$, then calculate $\gcd(a, b)$. Simplify your answer.

Answer: $\boxed{}$

(b) Given $2019 = 3 \cdot 673$, where both 3 and 673 are primes, what is the value of $\phi(2019)$? Show appropriate work and simplify your answer.

Answer: $\boxed{}$

(c) Let n be a positive integer for which $\phi(n) = 1000$. Fill in the two boxes below with integers in the set $\{0, 1, 2, \ldots, 999\}$ to make a correct statement.

Exactly one of the following must be true:

The number $2^{\phi(n)}$ is congruent to $\boxed{}$ mod n or the number $\boxed{}$ divides n.

(d) The value of $\phi(1000)$ is 400. What are the last three digits (the three right-most digits) of the number 5^{2003}? Justify your answer with appropriate work and put the digits in the correct order as they appear from left to right.

Answer: $\boxed{}$

$\boxed{\text{10 pts}}$ (2) Let a, b and c be integers. Using the definition of what it means for one number to divide another, prove that if a divides both b and $b+c$, then a divides c. Use complete English sentences throughout your proof.

$\boxed{\text{10 pts}}$ (3) Note that $111 = 3 \cdot 37$, where both 3 and 37 are primes. Find $x \in \{0, 1, \ldots 110\}$ satisfying

$$2^{222} \equiv x \pmod{111}.$$

In other words, what is the remainder when 2^{222} is divided by 111?

Answer: $\boxed{}$

$\boxed{\text{10 pts}}$ (4) Using the Euclidean algorithm, calculate $\gcd(2501, 7747)$.

Answer: $\boxed{}$

$\boxed{\text{10 pts}}$ (5) The factorization of n and $n-1$ into prime factors are given for each part below. Given that

$$2^{30} \equiv 1 \pmod{331},$$

determine if the following values of n are pseudoprimes. Be careful when treating the primes < 331. Justify with short answers, but mention important theorems from class that you use.

(a) $n = 11305 = 5 \cdot 7 \cdot 17 \cdot 19$
$n - 1 = 11304 = 2^3 \cdot 3^2 \cdot 157$

Check the correct box below.

n is a pseudoprime. $\square$

n is not a pseudoprime. $\square$

(b) $n = 30121 = 7 \cdot 13 \cdot 331$
$n - 1 = 30120 = 2^3 \cdot 3 \cdot 5 \cdot 251$

Check the correct box below.

n is a pseudoprime. $\square$

n is not a pseudoprime. $\square$

$\boxed{\text{10 pts}}$ (6) The last prime year was 2017. What is the remainder when

$$2^{2017} - 2016!$$

is divided by 2017 ? Give an explanation for your answer, indicating clearly what results you are using from class.

Answer: $\boxed{}$

$\boxed{\text{15 pts}}$ (7) Find the smallest positive integer x satisfying

$$4104\, x \equiv 3 \pmod{8249}.$$

Answer: $\boxed{}$

$\boxed{\text{15 pts}}$ (8) Let

$$N = \underbrace{1111111\ldots111111}_{\text{a string of 400 digits that are 1}} .$$

In other words, N is a 400 digit number with each digit in base 10 equal to 1. Prove that N is not the sum of two cubes by looking at what cubes can be modulo 9. Use complete English sentences throughout your proof. (Note that looking at negative values modulo 9 can simplify some of the work. For example, $7^3 \equiv (-2)^3 \equiv -8 \equiv 1 \pmod 9$.)