Name **Solutions**

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: $\boxed{42}$

Solution. The answer is $2 \cdot 3 \cdot 7 = 42$.

(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: $\boxed{1344}$

Solution. $\phi(2019) = 2019 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{673}\right) = 3 \cdot 673 \cdot \frac{2}{3} \cdot \frac{672}{673} = 2 \cdot 672 = 1344$

(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 $\boxed{1}$ mod n or the number $\boxed{2}$ 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: $\boxed{125}$

Solution. This was trickier than I intended in that Euler's Theorem does not apply directly since $\gcd(5, 1000) \neq 1$. In other words, it is not true that $5^{400} \equiv 1 \pmod{1000}$ like most of you wrote. We did discuss how to do this correctly during the review. The answer is 125 but doing the problem correctly takes more work than intended. I am giving everyone credit for this.

$\boxed{\text{10 pts}}$ (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.

Solution. Since a divides both b and $b+c$, we obtain from the definition of what it means for one number to divide another that there are integers k and ℓ such that

$$b = ka \quad \text{and} \quad b + c = \ell a.$$

Hence,

$$c = (b+c) - b = \ell a - ka = (\ell - k)a.$$

Thus, we see that c is an integer (namely $\ell - k$) times a. By using the definition of what it means for one number to divide another again, we deduce that a divides c, which completes the 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: $\boxed{64}$

Solution. Since $\phi(111) = 3 \cdot 37 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{37}\right) = 3 \cdot 37 \cdot \frac{2}{3} \cdot \frac{36}{37} = 2 \cdot 36 = 72$, we deduce from Euler's Theorem that

$$2^{72} \equiv 1 \pmod{111}.$$

Since $222 = 72 \cdot 3 + 6$ (by dividing 222 by 72), we see that

$$2^{222} \equiv 2^{72 \cdot 3 + 6} \equiv \left(2^{72}\right)^3 2^6 \equiv 2^6 \equiv 64 \pmod{111},$$

the answer is 64. ■

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

Answer: $\boxed{61}$

$$\begin{aligned} 7747 &= 2501 \cdot 3 + 244 \\ 2501 &= 244 \cdot 10 + 61 \\ 244 &= 61 \cdot 4 + 0 \end{aligned}$$

Solution. Use the Euclidean algorithm as shown in the box.

$\boxed{\text{10 pts}}$ (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. $\boxed{\checkmark}$

n is not a pseudoprime. $\boxed{}$

Solution. By Fermat's Little Theorem, $2^4 \equiv 1 \pmod 5$, $2^6 \equiv 1 \pmod 7$ and $2^{18} \equiv 1 \pmod{19}$. From the given factorization of 11304, we then deduce that

$$2^{11304} \equiv \left(2^4\right)^{2 \cdot 3^2 \cdot 157} \equiv 1 \pmod 5, \qquad 2^{11304} \equiv \left(2^6\right)^{2^2 \cdot 3 \cdot 157} \equiv 1 \pmod 7,$$

$$\text{and} \qquad 2^{11304} \equiv \left(2^{18}\right)^{2^2 \cdot 157} \equiv 1 \pmod{19}.$$

For the prime 17 dividing n, observe that $2^4 \equiv -1 \pmod{17} \implies 2^8 \equiv 1 \pmod{17}$. Hence,

$$2^{11304} \equiv \left(2^8\right)^{3^2 \cdot 157} \equiv 1 \pmod{17}.$$

The above now implies that $2^{11304} - 1$ is divisible by each of 5, 7, 17, 19 and, hence, their product 11305. Thus, $2^{11304} \equiv 1 \pmod{11305} \implies 2^{11305} \equiv 2 \pmod{11305}$. Since 11305 is > 1 and composite, we deduce 11305 is a pseudoprime. Note that I said to keep it short, so all these details are not necessary. See what I did for the next part.

(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. $\boxed{\checkmark}$

n is not a pseudoprime. $\boxed{}$

Solution. Using Fermat's Little Theorem and noting that 6 and 12 divide 30120, we see that $2^{30120} \equiv 1$ modulo 7 and 13. We're given that $2^{30} \equiv 1 \pmod{331}$ and 30 divides 30120, so we also have $2^{30120} \equiv 1$ modulo 331. Therefore, $2^{30120} \equiv 1 \pmod{30121}$ or $2^{30121} \equiv 2 \pmod{30121}$. Since $30121 > 1$ and 30121 is composite, 30121 is a pseudoprime.

$\boxed{\text{10 pts}}$ (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: $\boxed{3}$

Solution. By Fermat's Little Theorem, $2^{2017} \equiv 2 \pmod{2017}$. By Wilson's Theorem, $2016! \equiv -1 \pmod{2017}$. Therefore,

$$2^{2017} - 2016! \equiv 2 - (-1) \equiv 3 \pmod{2017}.$$

Hence, the remainder is 3.

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

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

$$\boxed{\begin{aligned} 8249 &= 4104 \cdot 2 + 41 \\ 4104 &= 41 \cdot 100 + 4 \\ 41 &= 4 \cdot 10 + 1 \end{aligned}}$$

Answer: $\boxed{2213}$

Solution. We begin by using the Euclidean algorithm until we get a remainder of 1 as shown in the box above. Then

$$\begin{aligned} 1 &= 41 - 4 \cdot 10 = 41 - (4104 - 41 \cdot 100) \cdot 10 = 41 \cdot 1001 - 4104 \cdot 10 \\ &= (8249 - 4104 \cdot 2) \cdot 1001 - 4104 \cdot 10 = 8249 \cdot 1001 - 4104 \cdot 2012. \end{aligned}$$

Reducing modulo 8249, we obtain

$$4104\,(-2012) \equiv 1 \pmod{8249} \implies 4104\,(-6036) \equiv 3 \pmod{8249}.$$

For the minimum positive integer, we take $-6036 + 8249 = 2213$.

$\boxed{\text{15 pts}}$ (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, $7^3 \equiv (-2)^3 \equiv -8 \equiv 1 \pmod 9$.)

Solution. Assume $N = a^3 + b^3$ for some integers a and b. Since every integer is congruent to an integer in $\{0, 1, \ldots, 8\}$ modulo 9 and since

$$0^3 \equiv 0 \pmod 9,$$
$$1^3 \equiv 1 \pmod 9,$$
$$2^3 \equiv 8 \equiv -1 \pmod 9,$$
$$3^3 \equiv 0 \pmod 9,$$
$$4^3 \equiv 64 \equiv 1 \pmod 9,$$
$$5^3 \equiv (-4)^3 \equiv -4^3 \equiv -1 \pmod 9,$$
$$6^3 \equiv (-3)^3 \equiv -3^3 \equiv 0 \pmod 9,$$
$$7^3 \equiv (-2)^3 \equiv -2^3 \equiv 1 \pmod 9,$$

and

$$8^3 \equiv (-1)^3 \equiv -1 \pmod 9,$$

we see that each of a^3 and b^3 is congruent to an integer in $\{0, 1, -1\}$ modulo 9. Thus, one of

$$a^3 + b^3 \equiv 0 + 0 \equiv 0 \pmod 9,$$
$$a^3 + b^3 \equiv 0 + 1 \equiv 1 \pmod 9,$$
$$a^3 + b^3 \equiv 0 + -1 \equiv 8 \pmod 9,$$
$$a^3 + b^3 \equiv 1 + 1 \equiv 2 \pmod 9,$$
$$a^3 + b^3 \equiv 1 - 1 \equiv 0 \pmod 9,$$

and

$$a^3 + b^3 \equiv -1 - 1 \equiv 7 \pmod 9$$

holds, so that the remainder when we divide N by 9 is in $\{0, 1, 2, 7, 8\}$. On the other hand, the sum of the digits of N is $400 \cdot 1 \equiv 400 \equiv 4 + 0 + 0 \equiv 4 \pmod 9$, so the remainder when N is divided by 9 is 4. This is a contradiction; hence, N is not the sum of two cubes. ■