Name: ______________________

Math 580/780I: Test 2, Fall 2019

Instructions and Point Values: Put your name at the top of this page and at the top of the first page of the packet of blank paper given to you. There are 8 problems below. Show ALL of your work in the packet of blank paper. Work each problem on the paper provided, making your work clear and organized. Put your answers in the boxes below where appropriate. Do NOT use a calculator.

There are 100 total points possible on this exam. The point value for each problem appears to the left of each problem.

---

10 pts (1) (a) What is the order of 2 modulo 13 ? Justify your answer.

Order of 2 modulo 13: ☐

(b) Is 2 a primitive root modulo 13 ? Explain your answer.

Answer: ☐ (YES or NO)

---

8 pts (2) The number 3 is a primitive root modulo the prime 113. What is the order of 9 modulo 113? Justify your answer.

Order of 9 modulo 113: ☐

---

10 pts (3) In class, we showed a theorem that, for p an odd prime, the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$. You were to have known the proof of this theorem for the test. Let p be a prime with $p \equiv 3 \pmod{4}$. Without using the theorem, prove that there are no integers a such that $a^2 \equiv -1 \pmod{p}$. (This is part of the proof of the theorem.)

---

10 pts (4) Calculate

$$\gcd\left(x^9 + x^8 + x^5 - 2\,x - 1, x^8 + x^7 - x^3 - 1\right).$$

gcd: ☐

Did you remember to put your name on this page and on your packet of blank paper given to you?

12 pts

(5) (a) What is the remainder when

$$f(x) = x^{2019} - 2\,x^{2018} - 4\,x^{2017} + 8\,x^{2016} + x^9 - 4\,x^7 + x^3 - x + 1$$

is divided by $x - 2$?

Remainder: $\boxed{}$

(b) What is the remainder when the polynomials $f(x)$ in part (a) is divided by $x^3 + 1$?

Remainder: $\boxed{}$

---

16 pts

(6) Find the smallest positive integer solution to the system of congruences below. Justify your answer with appropriate work.

$$\begin{aligned} x &\equiv 1 \pmod{12} \\ x &\equiv 7 \pmod{18} \\ x &\equiv 16 \pmod{21} \\ x &\equiv 9 \pmod{28} \end{aligned}$$

Smallest Positive Integer: $\boxed{}$

---

16 pts

(corrected version)

(7) The number 2019 factors as $3 \cdot 673$ where 3 and 673 are primes. You know (in theory) how to compute the inverse of 3 modulo 673, but your nice teacher has decided to tell you that $3 \cdot 449 \equiv 1 \pmod{673}$. What is the value of 3^{672} modulo 2019 ? Give an answer in the set $\{0, 1, 2, \ldots, 2018\}$. Justify your answer with appropriate work.

Answer in $\{\mathbf{0, 1, 2, \ldots, 2018}\}$: $\boxed{}$

---

18 pts

(8) You should use that

$$x^3 + 2\,x^2 - 3\,x + 2 \equiv (x - 2044)\,(x - 2765)\,(x - 3507) \pmod{4159}$$

for this problem. Do NOT verify it - just use it. What is the value of

$$2044^3 + 2765^3 + 3507^3 \pmod{4159}\,?$$

Show all work justifying your answer. Do not multiply any numbers together that are greater than 20 to get your answer. Give an answer that is in the set $\{0, 1, 2, \ldots, 4157, 4158\}$.

Answer in $\{\mathbf{0, 1, 2, \ldots, 4157, 4158}\}$: $\boxed{}$