Name **Solutions**

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: 12

Solution. Since $2^1 \equiv 2 \pmod{13}$, $2^2 \equiv 4 \pmod{13}$, $2^3 \equiv 8 \pmod{13}$, $2^4 \equiv 3 \pmod{13}$, $2^5 \equiv 6 \pmod{13}$ and $2^6 \equiv 12 \pmod{13}$, we see that the order of 2 modulo 13 is > 6. Since $\phi(13) = 12$, the order of 2 modulo 13 must divide 12. This implies the order is 12.

- -

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

Answer: YES (YES or NO)

Solution. Since $\phi(13) = 12$ is the order of 2 modulo 13, by the definition of a primitive root, we deduce 2 is a primitive root modulo 13.

---

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: 56

Solution. By Fermat's Little Theorem, we have $9^{56} \equiv (3^2)^{56} \equiv 3^{112} \equiv 1 \pmod{113}$. Thus, the order of 9 modulo 113 is ≤ 56. Now suppose k is a positive integer such that $9^k \equiv 1 \pmod{113}$. Since 3 is a primitive root modulo the prime 113, the order of 3 modulo 113 is 112. Since $3^{2k} \equiv 9^k \equiv 1 \pmod{113}$, we obtain $2k \ge 112$ or, equivalently, $k \ge 56$. This shows the order of 9 modulo 113 is ≥ 56. The answer follows.

---

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.)

Solution. Assume a is an integer such that $a^2 \equiv -1 \pmod{p}$. Since $0 \not\equiv -1 \pmod{p}$, we see that $p \nmid a$. Since $p \equiv 3 \pmod{4}$, there is an integer k such that $p = 4k+3$. Hence, $(p-1)/2 = (4k+2)/2 = 2k+1$, an odd number. Raising both sides of the congruence $a^2 \equiv -1 \pmod{p}$ to the $(p-1)/2$ power, we deduce

$$a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p},$$

which contradicts Fermat's Little Theorem. Thus, there are no integers a such that $a^2 \equiv -1 \pmod{p}$.

---

10 pts (4) Calculate

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

gcd: $x^4 - 1$

Solution. Applying the Euclidean Algorithm,

$$\begin{aligned} x^9 + x^8 + x^5 - 2x - 1 &= (x^8 + x^7 - x^3 - 1)\,x + x^5 + x^4 - x - 1 \\ x^8 + x^7 - x^3 - 1 &= (x^5 + x^4 - x - 1)\,x^3 + x^4 - 1 \\ x^5 + x^4 - x - 1 &= (x^4 - 1)(x + 1) + 0, \end{aligned}$$

we see that $\gcd\left(x^9 + x^8 + x^5 - 2x - 1, x^8 + x^7 - x^3 - 1\right) = x^4 - 1$.

---

12 pts (5) (a) What is the remainder when

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

is divided by $x - 2$?

Remainder: 7

Solution. The answer follows from the Remainder Theorem and

$$\begin{aligned} f(2) &= 2^{2019} - 2 \cdot 2^{2018} - 4 \cdot 2^{2017} + 8 \cdot 2^{2016} + 2^9 - 4 \cdot 2^7 + 2^3 - 2 + 1 \\ &= 2^{2019} - 2^{2019} - 2^{2019} + 2^{2019} + 2^9 - 2^9 + 2^3 - 2 + 1 = 2^3 - 2 + 1 = 7. \end{aligned}$$

- -

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

Remainder: $-2x^2 - 9x + 6$

Solution. Since $x^3 \equiv -1 \pmod{x^3+1}$, we have $x^6 \equiv 1 \pmod{x^3+1}$. Let $k = 336$ so that $2016 = 6k$. Then

$$\begin{aligned} f(x) &\equiv x^{2019} - 2\,x^{2018} - 4\,x^{2017} + 8\,x^{2016} + x^9 - 4\,x^7 + x^3 - x + 1 \\ &\equiv (x^6)^k x^3 - 2(x^6)^k x^2 - 4(x^6)^k x + 8(x^6)^k + (x^6)x^3 - 4(x^6)x + x^3 - x + 1 \\ &\equiv x^3 - 2x^2 - 4x + 8 + x^3 - 4x + x^3 - x + 1 \equiv 3x^3 - 2x^2 - 9x + 9 \\ &\equiv -3 - 2x^2 - 9x + 9 \equiv -2x^2 - 9x + 6 \pmod{x^3+1}, \end{aligned}$$

giving the answer.

---

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: 205

Solution. The above congruences are equivalent to the congruences $x \equiv 1 \pmod 4$, $x \equiv 7 \pmod 9$ and $x \equiv 2 \pmod 7$. As the moduli 4, 9 and 7 are relatively prime with their product equal to 252, we can apply the Chinese Remainder Theorem to obtain

$$x \equiv 1 \cdot 63 \cdot (-1) + 7 \cdot 28 \cdot 1 + 2 \cdot 36 \cdot 1 \equiv -63 + 196 + 72 \equiv 205 \pmod{252}.$$

The smallest positive solution is therefore 205.

---

16 pts (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.

(corrected version)

Answer in $\{0, 1, 2, \ldots, 2018\}$: 1347

Solution. Let $x = 3^{672}$. Since x is divisible by 3, we have $x \equiv 0 \pmod 3$. By Fermat's Little Theorem, we have $x \equiv 1 \pmod{673}$. From the statement of the problem, the inverse of 3 modulo 673 is 449. By the Chinese Remainder Theorem construction, we deduce

$$x \equiv 0 \cdot (\text{something}) + 1 \cdot 3 \cdot 449 \equiv 1347 \pmod{2019}.$$

---

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 $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \mathbf{4157}, \mathbf{4158}\}$: 4127

Solution. Let $f(x) = (x - 2044)\,(x - 2765)\,(x - 3507)$, and let α_1, α_2 and α_3 be its roots. Let σ_j be the corresponding elementary symmetric functions for α_1, α_2 and α_3. Let $S_k = \alpha_1^k + \alpha_2^k + \alpha_3^k$ for each integer $k \geq 0$. Since $f(x) \equiv x^3 + 2\,x^2 - 3\,x + 2 \pmod{4159}$, we deduce that

$$S_0 = \alpha_1^0 + \alpha_2^0 + \alpha_3^0 \equiv 1 + 1 + 1 \equiv 3 \pmod{4159},$$

$$S_1 = \alpha_1 + \alpha_2 + \alpha_3 \equiv \sigma_1 \equiv -2 \pmod{4159},$$

$$S_2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \equiv \sigma_1^2 - 2\sigma_2 \equiv (-2)^2 - 2(-3) \equiv 10 \pmod{4159}, \text{ and}$$

$$S_3 = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 \equiv -2\,S_2 + 3\,S_1 - 2\,S_0 \equiv -20 - 6 - 6 \equiv -32 \equiv 4127 \pmod{4159}.$$

Therefore, the answer is 4127.