

**Instructions:**

Please write your answers on separate paper. Please write clearly and legibly, using a large font and plenty of white space (I need room to put my comments). Staple all your pages together, with your problems in order, when you turn in your exam. Make clear what work goes with which problem. Put your name on every page. To get credit, you must show adequate work to justify your answers. If unsure, show the work. You may use one 8.5x11 page of notes, both sides. No other outside materials are permitted on this exam – notes, papers, books, calculators, phones, smartwatches, or computers – only pens and pencils, and this one page you produce and bring. No formulas will be provided. You may cite and use any theorem from the course (except to prove itself), but not any exercise. Twelve problems are out of 12 points, four are out of 14 points, 200 points maximum. You have 120 minutes.

1. (12pts) Let  $a, b, c \in \mathbb{Z}$ . Suppose that  $c$  is a common divisor of  $a, b$ . Prove that  $c|(a^2 - b^2)$ .
2. (12pts) Let  $a = 17, b = 57$ , integers. Use the Euclidean algorithm to find  $\gcd(a, b)$  and also  $u, v \in \mathbb{Z}$  satisfying  $ua + bv = \gcd(a, b)$ .
3. (12pts) Prove or disprove: For all nonzero  $a, b, c \in \mathbb{Z}$ , if  $\gcd(a, b) = 1$  then  $\gcd(a, bc) = \gcd(ab, c)$ .
4. (12pts) Prove that for all rings  $R$ , and for all  $a \in R$ ,  $a \cdot 0_R = 0_R$ .
5. (12pts) Prove that for all rings  $R$ , and for all  $a, b \in R$ ,  $(-a) \cdot b = -(a \cdot b)$ .
6. (12pts) Let  $a(x) = x^3 + 2ix^2 - 3x - 2i$ ,  $b(x) = x^3 + x$ , elements of  $\mathbb{C}[x]$ . Use the Euclidean algorithm to find  $\gcd(a, b)$  and also  $u, v \in \mathbb{C}[x]$  satisfying  $ua + bv = \gcd(a, b)$ .
7. (12pts) Find an irreducible polynomial of degree 4 in  $\mathbb{Z}_2[x]$ . Be sure to fully justify.
8. (12pts) Find at least three different finite fields  $\mathbb{F}$ , such that  $x^2 - 2 (= x^2 - 1_{\mathbb{F}} - 1_{\mathbb{F}})$  is reducible in  $\mathbb{F}[x]$ .
9. (12pts) Consider  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  given by  $f(x) = -x$ . Prove or disprove that  $f$  is an isomorphism.
10. (12pts) Let  $m, n \in \mathbb{Z}$  and consider the principal ideals  $I = (m), J = (n)$ . Prove that  $I \subseteq J$  if and only if  $n|m$ .
11. (12pts) Let  $R, S$  be rings, and consider the homomorphism  $f : R \times S \rightarrow S$  given by  $f((a, b)) = b$ . Find its kernel, and express it as a principal ideal.
12. (12pts) Consider  $I = (2, x^2)$ , an ideal in  $R = \mathbb{Z}[x]$ . Compute all elements of  $R/I$ , and determine whether  $I$  is maximal.
13. (14pts) State and prove the  $\mathbb{Z}_p$  Theorem.
14. (14pts) State and prove the Injective Homomorphism Theorem.
15. (14pts) State and prove the Ideal to Kernel Theorem.
16. (14pts) State and prove the Quotient Ring Theorem.