

- (18) 1. (a) Use the Euclidean algorithm to find the gcd of 71 and 150 and express it as a sum of multiples of 71 and 150.

(b) Find the additive inverse and the multiplicative inverse of $[71]$ in \mathbb{Z}_{150} . Express your answers in reduced form.

- (16) 2. Prove by induction that

$$[4]^n = [3n + 1]$$

in \mathbb{Z}_9 for all integers $n \geq 1$.

- (16) 3. (a) Carefully state the fundamental theorem of arithmetic.

(b) Suppose that a, b, c are nonzero integers, and suppose that a and b are relatively prime. Prove without using the fundamental theorem that

$$a \mid bc \implies a \mid c.$$

Hint: The proof is very similar to the proof of Euclid's lemma which was done in class.

- (16) 4. Let $R = \mathbb{R}$ (the ring of real numbers) and let $\alpha = \frac{1+\sqrt{5}}{2} \in \mathbb{R}$. Recall from class that $\alpha^2 = \alpha + 1$. Let

$$S = \{a + b\alpha : a, b \in \mathbb{Z}\}$$

in R . Determine whether or not S is a subring of R .

- (16) 5. An *idempotent* in a ring R is an element $e \in R$ such that $e^2 = e$.

(a) Define what is meant by an *integral domain*.

(b) If R is an integral domain, prove that the only idempotents in R are 0 and 1. Indicate where in your argument you are using the fact that R is an integral domain.

(c) Give an example of a ring R with identity and an idempotent $e \in R$ such that $e \neq 0$ and $e \neq 1$.

(18) 6. Give an example if possible of each of the following. Otherwise, briefly indicate why an example is not possible (for example by quoting a proposition from class).

(a) A finite ring that is not commutative.

(b) A field that is not an integral domain.

(c) Three nonzero elements in \mathbb{Z}_{68} that are not units.

(d) A \sim relation on the set \mathbb{Z} of integers that is reflexive and transitive but not symmetric.