Mathematics 546 Homework.

Here are some practice problems for the test.

Problem 1. Solve the following congruences or explain why they have no solutions.

(a) $15x \equiv 25 \mod 85$.
(b) $-33x + 9 \equiv 102 \mod 45$.
(c) $1236x \equiv 17 \mod 3219123$. *Hint:* Rather than doing a long commutation, show that both 1236 and 3219123 are divisible by 3 which will be enough to show 17 is not divisible by $\gcd(1236, 3219123)$.

Problem 2. Show that if $m \equiv 3 \mod 4$, then m is not the sum of two perfect squares. *Hint:* What are the possible values of $(x^2+y^2) \mod 4$? □

Problem 3. Let $[a]_n$ be a unit in $\mathbb{Z}_n$. Show that the equation

$$[a]_n[b]_n = [0]_n$$

implies $[b]_n = [0]_n$.

Problem 4. Let p be a prime. Show that $[a]_p[b]_p = [0]_p$ in $\mathbb{Z}_p$, then $[a]_p = [0]_p$ or $[b]_p = [0]_p$. □

Problem 5. Let p be a prime number. Show that the only solutions to

$$[a]_p^2 = [1]_p$$

are $[a]_p = \pm[1]_p$. □

Problem 6. Find all the solutions to

$$[a]_8^2 = [1]_8$$

in $\mathbb{Z}_8$. □

Proposition 1 (Rational root test for cubics.). *Let a, b, c, d be integers with $a \neq 0$. Let*

$$r = \frac{p}{q}$$

be a rational root in lowest term (that is $\gcd(p, q) = 1$) of

$$ax^3 + bx^2 + cx + d = 0.$$

Then

$$p \mid a \quad \text{and} \quad q \mid d.$$

Problem 7. Prove this. □

Problem 8. Prove $\sqrt[3]{5}$ is irrational. □

Problem 9. Review what it means for a subset, I, of $\mathbb{Z}$ to be an ***ideal***, and recall that we have shown that if I is an ideal, then either $I = \{0\}$ or there is a positive integer d such that

$$I = d\mathbb{Z} := \{qd : q \in \mathbb{Z}\} = \text{all integral multiples of } d.$$

Show that if $a, b, c \in Z$ and

$$I = \{ax + by + cz : x, y, z \in \mathbb{Z}\}$$

is the set of all integral linear combinations of a, b, and c, then I is an ideal. □

Problem 10. Let a, b, c be integers, not all zero. Define what it means for d to be a greatest common divisor of a, b, and c. Show that there are integers x_0, y_0, and z_0 such that

$$ax_0 + by_0 + cz_0 = d.$$

Hint: Consider the set $I = \{ax + by + cz : x, y, z \in \mathbb{Z}\}$ and show that the least positive element of I is $\gcd(a, b, c)$. □