HW2

(Due 5:00pm Wednesday, March 26, 2025, on WyoCourses)

Instructions: For this assignment, I am expecting that you will use appropriate computer software (such as Mathematica) whenever this is helpful. (The software will not write proofs for you; but it can help you search for examples and counterexamples.) *Check your answers* wherever possible. Submit solutions through WyoCourses. See the syllabus and FAQ for general expectations regarding homework.

1. (*50 points*) Determine whether each of the following Diophantine equations has any integer solutions. If solutions exist, find a solution $(x, y) \in \mathbb{Z}^2$. (You are not required to find *all* solutions. Zero values for x, y are allowed.) If no solution exists, prove this using modular arithmetic.

   (a) $29x^2 - y^2 = 5$
   (b) $29x^2 - y^2 = 10$
   (c) $29x^2 - y^2 = 1$
   (d) $29x^2 - y^2 = 3$
   (e) $29x^2 - y^2 = -13$
   (f) $61x^2 - y^2 = 12$
   (g) $61x^2 - y^2 = 2$
   (h) $61x^2 - y^2 = 3$
   (i) $61x^2 - y^2 = 24$
   (j) $61x^2 - y^2 = 1$

2. (*25 points*) Let $p = 9080706050401$. Making use of appropriate software,
   (a) Verify that p is prime. (In Mathematica, you may use the `PrimeQ[]` command.)
   (b) Find the smallest positive integer b such that $1234b \equiv 56789 \mod p$.
   (c) Find the smallest positive integer c such that $c \equiv 123456789^{9876543210} \mod p$.
   (d) Find an integer x satisfying
   $$x^{263} \equiv 1975712412050 \mod p.$$
   (*Hint*: First find the inverse of 263 mod $p-1$. Then use Fermat's Little Theorem. To make sure you use the correct values above, use a mouse to copy them from this pdf document and paste them into your Mathematica notebook.)

3. (*15 points*) In each case, indicate *how many* pairs of integers (x, y) satisfy the given equation. You are not required to list all solutions. Be sure to remember that integers can be positive, negative or zero.
   (a) $x^2 + y^2 = 400$
   (b) $x^2 - y^2 = 400$
   (c) $xy = 400$

4. (*30 points*) In the ring $\mathbb{Z}[i]$ of Gaussian integers, show that
   (a) 1009 is reducible, and
   (b) 2003 is irreducible.