E. Dummit's Math 3527 ~ Number Theory I, Spring 2023 ~ Homework 10, due Fri Apr 7th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Submit scans of your responses via Canvas.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. For each integer, determine whether it can be written as a sum of two squares (of integers), and for those that can, give at least one such way:
   (a) The integer 2600.
   (b) The integer 2020.
   (c) The integer 2023.
   (d) The integer 77077.
   (e) The prime 2909, given that $878^2 \equiv -1 \pmod{2909}$.
   (f) The prime 5813, given that $796^2 \equiv -1 \pmod{5813}$.

---

2. The goal of this problem is to find all of the Pythagorean right triangles with one side of length $2023 = 7 \cdot 17^2$.
   (a) Find the eight Pythagorean triangles having one leg of length 2023. [Hint: Note that $k(s^2 - t^2)$ factors as $k(s-t)(s+t)$, then break into cases based on k.]
   (b) Find the two Pythagorean triangles having hypotenuse of length 2023. [Hint: If $k(s^2 + t^2) = 2023$, why must k be divisible by 7?]

---

3. List all of the (nonzero) quadratic residues, and all of the quadratic nonresidues, modulo 13 and modulo 19.

---

4. Calculate the following Legendre symbols (i) using Euler's criterion, and (ii) using quadratic reciprocity.
   (a) $\left(\frac{3}{17}\right)$.
   (b) $\left(\frac{11}{733}\right)$.
   (c) $\left(\frac{-5}{67}\right)$.
   (d) $\left(\frac{67}{101}\right)$.
   (e) $\left(\frac{15}{23}\right)$.
   (f) Which method is easier to implement by hand?

Part II: Solve the following problems. Justify all answers with rigorous, clear explanations.

5. Prove that if an integer is the sum of squares of two rational numbers, then it is the sum of squares of two integers: for example, $5 = (22/13)^2 + (19/13)^2 = 2^2 + 1^2$. [Hint: Clear denominators and use the characterization of sums of two squares.]

---

6. We have given a geometric description for finding residue class representatives for $\mathbb{Z}[i]$ modulo α. In certain cases, we can give a more direct description.

   (a) If $\alpha = n$ is an integer (in $\mathbb{Z}$), show that the residue classes modulo α are represented by the elements $c + di$, with $0 \leq c \leq n-1$ and $0 \leq d \leq n-1$. [Hint: Draw the fundamental region.]

   (b) If $\pi = a + bi$ is a prime element with $N(\pi) = p$ a prime congruent to 1 modulo 4 (e.g., such as $\pi = 2 + i$ or $\pi = 3 - 2i$), show that the residue classes modulo π are represented by the elements 0, 1, ... , $p - 1$. [Hint: Count the residue classes and then show the given ones are distinct.]

---

7. Recall (cf. Homework 1) that the Fibonacci-Virahanka numbers F_n are defined by $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. The goal of this problem is to show that if F_k is a prime congruent to 1 modulo 4, then (i) F_k is the sum of two squares of Fibonacci numbers and (ii) the two square roots of -1 modulo F_k are also Fibonacci numbers.

   (a) Verify the results for the Fibonacci primes $F_5 = 5$, $F_7 = 13$, and $F_{11} = 89$.

   (b) Suppose F_k is prime and $k > 4$. Show that k must be odd. [Hint: Use an identity from problem 4(d) of homework 1.]

   (c) Suppose that F_k is a prime congruent to 1 modulo 4: then F_k can be written uniquely as the sum of two squares $F_k = a^2 + b^2$ for positive a, b. Show that both a and b are Fibonacci numbers. [Hint: Use the other identity from problem 4(d) of homework 1.]

   (d) Suppose that F_k is a prime congruent to 1 modulo 4: then -1 is a square modulo F_k. Show that the two square roots of -1 modulo F_k are F_{k-1} and F_{k-2}. [Hint: Use 4(c) from homework 1.]

---

8. Let p be a prime.

   (a) If $p \neq 2$, show that $x^4 + 1$ divides $x^{p^2} - x$ in $\mathbb{F}_p[x]$. [Hint: Observe that $x^4 + 1$ divides $x^8 - 1$, and that 8 divides $p^2 - 1$.]

   (b) Show that $x^4 + 1$ is reducible modulo p for every prime p. [Hint: What does (a) say about the possible degrees of irreducible factors?]

   (c) If $p \neq 2, 3$, show that at least one of 2, 3, and 6 is a quadratic residue modulo p.

   (d) Show that the polynomial $q(x) = (x^2 - 2)(x^2 - 3)(x^2 - 6)$ has a root modulo p for every prime p.
