E. Dummit's Math 3527 ~ Number Theory I, Spring 2022 ~ Homework 10, due Fri Apr 22nd.

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 $m$, either find a primitive root modulo $m$ and the total number of primitive roots modulo $m$, or explain briefly why there are none:

   (a) $m = 13$.
   (b) $m = 13^3$.
   (c) $m = 32^{2022}$.
   (d) $m = 33^{2022}$.
   (e) $m = 5^{2022}$.
   (f) $m = 2 \cdot 5^{2022}$.

---

2. For each Gaussian integer $\alpha$, find (i) the number of residue classes in $\mathbb{Z}[i]$ modulo $\alpha$, and (ii) the prime factorization of $\alpha$ in $\mathbb{Z}[i]$:

   (a) $\alpha = 19 + 48i$.
   (b) $\alpha = 28 - 4i$.
   (c) $\alpha = 20 + 7i$.
   (d) $\alpha = 60 - 11i$.
   (e) $\alpha = 2022$.

---

3. Let $R = \mathbb{Z}[i]$ and $r = 4 + 2i$.

   (a) Determine the total number of residue classes in $R/rR$.
   (b) Draw a fundamental region for $R/rR$, and use it to find an explicit list of residue class representatives.
   (c) Find the prime factorization of $r$ in $\mathbb{Z}[i]$.
   (d) How many units are there in $R/rR$? [Hint: Use the Chinese Remainder Theorem and the factorization of $r$.]
   (e) Verify Euler's Theorem for the element $x = 1 + 2i$ in $R/rR$.

---

4. 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 2022.
   (d) The integer 77077.

---

5. Solve the following problems:

   (a) Given that $878^2 \equiv -1 \pmod{2909}$, find a representation of the prime 2909 as the sum of two squares.

   (b) Given that $796^2 \equiv -1 \pmod{5813}$, find a representation of the prime 5813 as the sum of two squares.

   (c) Find the three right triangles having one leg of length 20, and whose other two side lengths are integers.

   (d) Find the unique right triangle with integer leg lengths whose hypotenuse has length 2022.

---

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

---

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

7. 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.]

---

8. We have given a geometric description for finding residue class representatives for $\mathbb{Z}[i]$ modulo $\alpha$. 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 $\alpha$ 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 $\pi$ are represented by the elements 0, 1, ... , $p - 1$. [Hint: Count the residue classes and then show the given ones are distinct.]

---

9. [Optional, but fun!] Let $f(n)$ be the number of different ways of writing $n = A^2 + B^2$ for integers $(A, B)$; recall that we gave an exact formula for this quantity based on the prime factorization of $n$. In Mathematica, the command `SquaresR[2,n]` will give the value of the function $f(n)$.

   (a) Find the average value of $f(n)$ for the integers $n$ satisfying $0 \leq n \leq M$, for $M = 100$, 1000, 10000, and 100000. In other words, compute $\dfrac{1}{M}\displaystyle\sum_{i=1}^{M} f(i)$ for those four values of $M$.

   (b) Based on the results in part (a), what do you think the average value approaches as $M$ grows very large?

   (c) Prove that your conjecture from part (b) is correct.

---