---

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

   - We proved using geometry that the number of residue classes is $N(\alpha)$.
   - To factor $\alpha \in \mathbb{Z}[i]$ we first factor $N(\alpha)$ in $\mathbb{Z}$, then we find the factorization in $\mathbb{Z}[i]$ of each rational prime in the factorization of $N(\alpha)$, and finally determine which terms divide α and to what powers.

   (a) $\alpha = 19 + 48i$.

   - The number of residue classes is $N(\alpha) = 19^2 + 48^2 = \boxed{2665} = 5 \cdot 13 \cdot 41$.
   - Since $5 = (2+i)(2-i)$, $13 = (3+2i)(3-2i)$, and $41 = (5+4i)(5-4i)$, the possible prime factors of a are $2 \pm i$, $3 \pm 2i$, and $5 \pm 4i$.
   - Checking which of these actually divide $19+48i$ yields the factorization $19+48i = \boxed{i(2-i)(3-2i)(5+4i)}$.

   (b) $\alpha = 28 - 4i$.

   - The number of residue classes is $N(\alpha) = 28^2 + 4^2 = \boxed{800} = 2^5 5^2$.
   - Since $2 = -i(1+i)^2$ and $5 = (2+i)(2-i)$, the possible prime factors of b are $1+i$ and $2 \pm i$.
   - Checking which of these divide $28 - 4i$, and to which powers, yields $28 - 4i = \boxed{-(1+i)^5(2-i)^2}$.

   (c) $\alpha = 20 + 7i$.

   - The number of residue classes is $N(\alpha) = 20^2 + 7^2 = \boxed{449}$, which is prime. So $20 + 7i$ is prime (irreducible) in $\mathbb{Z}[i]$ and its factorization is simply $\boxed{20 + 7i}$.

   (d) $\alpha = 60 - 11i$.

   - The number of residue classes is $N(\alpha) = 60^2 + 11^2 = \boxed{3721} = 61^2$.
   - Since $61 = (6+5i)(6-5i)$, the possible prime factors of c are $6 \pm 5i$.
   - Checking which of these divide $60 - 11i$, and to which powers, yields $60 - 11i = \boxed{-i(6+5i)^2}$.

   (e) $\alpha = 2025$.

   - The number of residue classes is $N(\alpha) = 2025^2 = \boxed{4100625}$.
   - Since $2025 = 3^4 5^2$, we can just use the factorizations of these integers in $\mathbb{Z}[i]$, namely, $3 = 3$ and $5 = (2+i)(2-i)$. Hence, $2025 = \boxed{3^4(2+i)^2(2-i)^2}$.

   (f) $\alpha = 2465$.

   - The number of residue classes is $N(\alpha) = 2465^2 = \boxed{6076225}$.
   - Since $2465 = 5 \cdot 17 \cdot 29$ we need to factor these integers in $\mathbb{Z}[i]$. The odd primes are all 1 mod 4 so they do factor: $5 = (2+i)(2-i)$, $17 = (4+i)(4-i)$, and $29 = (5+2i)(5-2i)$.
   - Hence, $2465 = \boxed{(2+i)(2-i)(4+i)(4-i)(5+2i)(5-2i)}$.

---

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

   (a) Find the prime factorization of r in $\mathbb{Z}[i]$.

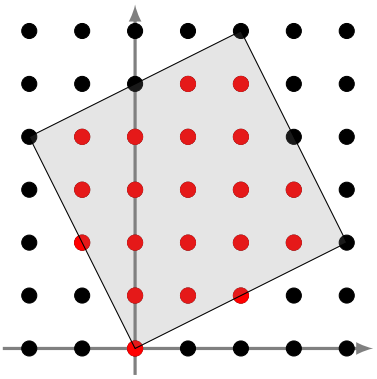
   - As $N(r) = 20$ with $2 = -i(1+i)^2$ and $5 = (2+i)(2-i)$, the possible factors are $1+i$ and $2 \pm i$.
   - Checking which of these actually divide $4 + 2i$ yields the factorization $4 + 2i = \boxed{-i(1+i)^2(2+i)}$.

   (b) Determine the total number of residue classes in R/rR.

   - From our results, the number of residue classes is $N(r) = 4^2 + 2^2 = \boxed{20}$.

(c) Draw a fundamental region for R/rR, and use it to find an explicit list of residue class representatives.

- To find the residue class representatives, we draw the square whose vertices are 0, r, ir, and $(1+i)r$, and list all of the lattice points that lie inside, or on the left or bottom edges:



- The representatives are $-1+2i$, $-1+3i$, $-1+4i$, 0, i, $2i$, $3i$, $4i$, $1+i$, $1+2i$, $1+3i$, $1+4i$, $1+5i$, $2+i$, $2+2i$, $2+3i$, $2+4i$, $2+5i$, $3+2i$, and $3+3i$.

---

3. 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:

- We know that if $n = 2^k p_1^{n_1} \cdots p_k^{n_k} q_1^{m_1} \cdots q_d^{m_d}$, where $p_1, \cdots, p_k$ are distinct primes congruent to 1 modulo 4 and $q_1, \cdots, q_d$ are distinct primes congruent to 3 modulo 4, then n can be written as a sum of two squares in $\mathbb{Z}$ if and only if all the m_i are even. Such representations all arise from finding the real and imaginary parts of the Gaussian integer factorization of each term in $n = 2^k p_1^{n_1} \cdots p_k^{n_k} q_1^{m_1} \cdots q_d^{m_d}$.

(a) The integer 2600.

- We have the prime factorization $2600 = 2^3 5^2 13^1$, so since there are no primes congruent to 3 mod 4, it can be written as a sum of two squares.
- One such way can be found by multiplying out $(1+i)^3(2+i)^2(3+2i) = -38-34i$, yielding $2600 = \boxed{38^2+34^2}$. Two others, $\boxed{22^2+46^2}$ and $\boxed{50^2+10^2}$, can be found by taking different choices of primes in the product above.

(b) The integer 2024.

- We have the prime factorization $2024 = 2^3 \cdot 11 \cdot 23$. This $\boxed{\text{cannot be written as a sum of two squares}}$ because of the factors 11 and 23.

(c) The integer 2026.

- We have the prime factorization $2024 = 2 \cdot 1013$ and since 1013 is 1 modulo 4, 2026 can be written as a sum of two squares. We could write 1013 as a sum of two squares, but it is easier just to notice that $45^2 = 2025$ so $2026 = \boxed{45^2+1^2}$.

(d) The integer 77077.

- We have the prime factorization $77077 = 7^2 11^2 13^1$, so since both 7 and 11 appear with an even exponent, it can be written as a sum of two squares.
- Essentially the only possibility is given by multiplying out $7 \cdot 11 \cdot (3+2i) = 231+154i$, yielding $77077 = \boxed{231^2+154^2}$.

(e) The prime 2909, given that $878^2 \equiv -1 \pmod{2909}$.

- Per the algorithm discussed in the lectures, we compute the gcd of $878+i$ and 2909 in $\mathbb{Z}[i]$ using the Euclidean algorithm:

$$\begin{aligned} 2909 &= 3(878+i) + (275-3i) \\ 878+i &= 3(275-3i) + (53+10i) \\ 275-3i &= (5-i)(53+10i) \end{aligned}$$

- The last nonzero remainder is $53+10i$, and indeed we can see that $2909 = \boxed{53^2+10^2}$.

(f) The prime 5813, given that $796^2 \equiv -1 \pmod{5813}$.

- Per the algorithm discussed in the lectures, we compute the gcd of $796+i$ and 5813 in $\mathbb{Z}[i]$ using the Euclidean algorithm:

$$\begin{aligned} 5813 &= 7(796+i) + (241-7i) \\ 796+i &= 3(241-7i) + (73+22i) \\ 241-7i &= (3-i)(73+22i) \end{aligned}$$

- The last nonzero remainder is $73+22i$, and indeed we can see that $5813 = \boxed{73^2+22^2}$.

---

4. Find all of the Pythagorean right triangles (i.e., with integer side lengths) where one side length is 2026.

- First note that $2026 = 2 \cdot 1013$, where 1013 is prime and congruent to 1 modulo 4.
- As we showed in class, any Pythagorean right triangle has legs of lengths $2stk$ and $(s^2-t^2)k$, with hypotenuse $(s^2+t^2)k$, where $s > t$ are unique relatively prime positive integers of opposite parity and k is a positive integer. So we just set each of these equal to 2026 and solve.
- If $2stk = 2026$ then $stk = 1013$ which can only occur with $s = 1013$, $t = k = 1$, but then s, t have the same parity.
- If $(s^2-t^2)k = 2026$ then since $s^2 - t^2 \geq 3$ the only possibilities are $(s^2-t^2, k) = (1013, 2)$ or $(2026, 1)$.
  - In the first case, $(s-t)(s+t) = 1013$ forces $s-t = 1$ and $s+t = 1013$ so $s = 507$, $t = 506$, $k = 1$, yielding the triple $\boxed{(2026, 1026168, 1026170)}$.
  - In the second case, we see $(s-t)(s+t) = 2 \cdot 1013$ is impossible because the two terms $s-t$ and $s+t$ have the same parity hence their product is either odd or a multiple of 4, hence cannot be twice an odd number.
- If $(s^2+t^2)k = 2026$ then since $s^2 + t^2 \geq 5$ the only possibilities are $(s^2+t^2, k) = (1013, 2)$ or $(2026, 1)$.
  - In the first case, $s^2 + t^2 = 1013$ requires decomposing 1013 as the sum of two squares. Since $2026 = 45^2 - 1$ we see $45^2 \equiv -1 \pmod{2026}$, so using the method illustrated in the previous problem we can readily compute $\gcd(45+i, 1013) = 22+23i$, and so $1013 = 22^2 + 23^2$. Then $s = 23$, $t = 22$, $k = 2$ yielding the triple $\boxed{(90, 2024, 2026)}$.
  - In the second case, since 2026 is 2 modulo 4, having $s^2 + t^2 = 2026$ would require both s, t to be odd, but they must be of opposite parity. So there are no additional triples here.

---

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

- From our discussion, the quadratic residues modulo p are $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$.
- For $p = 13$ these are $\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \equiv \boxed{\{1, 4, 9, 3, 12, 10\}}$ so the quadratic nonresidues are the remaining classes $\boxed{\{2, 5, 6, 7, 8, 11\}}$.
- For $p = 19$ these are $\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2\} \equiv \boxed{\{1, 4, 9, 16, 6, 17, 11, 7, 5\}}$ so the quadratic nonresidues are the remaining nonzero residue classes $\boxed{\{2, 3, 8, 10, 12, 13, 14, 15, 18\}}$.

---

6. Calculate the following Legendre symbols (i) using Euler's criterion, and (ii) using quadratic reciprocity.

(a) $\left(\frac{3}{17}\right)$.

- Using Euler's criterion, we have $3^{(17-1)/2} \equiv 3^8 \equiv \boxed{-1} \pmod{17}$.
- Using quadratic reciprocity, we have $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = \boxed{-1}$.

(b) $\left(\frac{11}{733}\right)$.

- Using Euler's criterion, we have $11^{(733-1)/2} \equiv 11^{366} \equiv \boxed{-1} \pmod{733}$.
- Using quadratic reciprocity, we have $\left(\frac{11}{733}\right) = \left(\frac{733}{11}\right) = \left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = \boxed{-1}$.

(c) $\left(\frac{-5}{67}\right)$.

- Using Euler's criterion, we have $(-5)^{(67-1)/2} \equiv (-5)^{33} \equiv \boxed{+1} \pmod{67}$.
- Using quadratic reciprocity, we have $\left(\frac{-5}{67}\right) = \left(\frac{-1}{67}\right)\left(\frac{5}{67}\right) = -1 \cdot \left(\frac{67}{5}\right) = -1 \cdot \left(\frac{2}{5}\right) = \boxed{+1}$ since $\left(\frac{-1}{67}\right) = -1$ because 67 is 3 mod 4.

(d) $\left(\frac{67}{101}\right)$.

- Using Euler's criterion, we have $67^{(101-1)/2} \equiv 67^{50} \equiv \boxed{-1} \pmod{101}$.
- Using quadratic reciprocity, we have $\left(\frac{67}{101}\right) = \left(\frac{101}{67}\right) = \left(\frac{34}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{17}{67}\right) = (-1) \cdot \left(\frac{67}{17}\right) = (-1) \cdot \left(\frac{-1}{17}\right) = \boxed{-1}$ since $\left(\frac{2}{67}\right) = -1$ as 67 is 3 mod 8, and $\left(\frac{-1}{17}\right) = +1$ as 17 is 1 mod 4.

(e) $\left(\frac{15}{23}\right)$.

- Using Euler's criterion, we have $15^{(23-1)/2} \equiv 15^{11} \equiv \boxed{-1} \pmod{23}$.
- Using quadratic reciprocity, we have $\left(\frac{15}{23}\right) = \left(\frac{3}{23}\right)\left(\frac{5}{23}\right) = -\left(\frac{23}{3}\right)\left(\frac{23}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = -(-1)(-1) = \boxed{-1}$.

(f) Which method is easier to implement by hand?

- For Euler's criterion, even though the calculations shown above omit the details, the successive squarings are quite lengthy. (The calculation for (a) is fairly short, but the rest are quite a bit more involved.)
- Quadratic reciprocity is much easier when the numbers are even moderately large, though it does require factoring the number on the top. (If we used Jacobi symbols, we could go even faster.)

---

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.]

- If $n = (a/b)^2 + (c/d)^2$ is an integer, by rescaling if necessary we may assume the denominators are equal: then $n = (a^2 + c^2)/b^2$, so that $b^2 n = a^2 + c^2$.
- By our classification of integers that are the sum of two squares, we know that any prime congruent to 3 modulo 4 must appear to an even power in the factorization of $b^2 n$, and hence also in the factorization of n. But this means n is the sum of two squares, as claimed.

---

8. 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.]

   - We can simply draw the fundamental region: it is a square with vertices 0, n, ni, and $n + ni$. The points $c + di$ with $0 \leq c \leq n-1$ and $0 \leq d \leq n-1$ then clearly give a full set of representatives since they hit all points in the interior and all points on the left and bottom sides of the square.
   - Alternatively, we could use the fact that we know there are $N(n) = n^2$ residue classes, and there are n^2 such elements, so all we need to do is see that they are distinct modulo n in $\mathbb{Z}[i]$. But this is immediate, because $a + bi \equiv c + di \pmod{n}$ only when n divides $a - c$ and $b - d$.

   (b) If $\pi = a + bi$ is a prime element with $N(\pi) = p$ a prime congruent to 1 modulo 4 (e.g., $\pi = 2 + i$ or $\pi = 3 - 2i$), show that the residue classes modulo π are represented by the elements 0, 1, ... , $p - 1$. [Hint: Show $a \in \mathbb{Z}$ is divisible by π only if it is divisible by p; deduce 0, 1, ... , $p - 1$ are distinct mod π.]

   - We know that there are $N(a + bi) = p$ residue classes, and there are p elements listed, so all we need to do is see that they are distinct modulo π in $\mathbb{Z}[i]$.
   - Now observe that if $a \in \mathbb{Z}$ is divisible by π then $a = \overline{a}$ is divisible by $\overline{\pi}$, so since π and $\overline{\pi}$ are relatively prime, a is divisible by $\pi\overline{\pi} = p$. So, since the given integers are distinct mod p, they are distinct mod π, as claimed.

---

9. The goal of this problem is to discuss some results on consecutive integers that are sums of two squares.

   (a) If N is the sum of two squares, show that N must be congruent to 0, 1, 2, 4, or 5 modulo 8.

   - As shown on a previous homework, squares are 0, 1, or 4 modulo 8, so the sum of two squares can only be $0 + 0 = 0$, $1 + 0 = 1$, $1 + 1 = 2$, $4 + 0 = 4$, or $4 + 1 = 5$ modulo 8, as claimed.

   (b) Deduce that there do not exist four consecutive integers all of which are the sum of two squares.

   - Any four consecutive integers must contain one that is 3 or 7 modulo 8, so by part (a) that integer is not a sum of two squares.

   (c) Show that there exist infinitely many N for which N, $N+1$, $N+2$ are all the sum of two squares. [Hint: Try $N = 4a^4 + 4a^2$.]

   - Following the hint we observe that for $N = 4a^4 + 4a^2$ we have $N = (2a^2)^2 + (2a)^2$, $N + 1 = (2a^2 + 1)^2 + 0^2$, and $N + 2 = (2a^2 + 1)^2 + 1^2$, so each of N, $N + 1$, $N + 2$ are the sum of two squares.
