---

1. (a) Express 46, 57, 88, and 114 as the sum of three squares.
   - We have $46 = 6^2+3^2+1^2$, $57 = 7^2+2^2+2^2$, $88 = 6^2+6^2+4^2$, and $114 = 8^2+7^2+1^2 = 8^2+5^2+5^2$.

   (b) Express 87, 135, 2023, and 2024 as the sum of four squares.
   - We have $87 = 7^2+5^2+3^2+2^2$, $135 = 10^2+5^2+3^2+1^2$, $2023 = 34^2+17^2+17^2+17^2$, $2024 = 38^2+20^2+12^2+6^2$. (There are many other possible solutions.)

---

2. For each quadratic integer ring (i) identify the value given by the Minkowski bound, (ii) find the splitting of all prime ideals up to the Minkowski bound, and (iii) determine the structure of the ideal class group:

   (a) $\mathbb{Z}[\sqrt{3}]$.
   - Here $\Delta = 12$ so $\mu = \frac{1}{2}\sqrt{\Delta} = \sqrt{3} \approx 1.7321$.
   - Since $\mu < 2$, there are no prime ideals of norm at most μ, so we see immediately that the class group is trivial.

   (b) $\mathcal{O}_{\sqrt{13}}$.
   - Here $\Delta = 13$ so $\mu = \frac{1}{2}\sqrt{\Delta} = \frac{1}{2}\sqrt{13} \approx 1.8028$.
   - Since $\mu < 2$, there are no prime ideals of norm at most μ, so we see immediately that the class group is trivial.

   (c) $\mathbb{Z}[\sqrt{-6}]$.
   - Here $\Delta = -24$ so $\mu = \frac{2}{\pi}\sqrt{24} \approx 3.1188$.
   - Since $\mu < 4$, the only possible prime ideals of norm less than μ are the ideals of norm 2 and norm 3.
   - The minimal polynomial of the generator is $x^2 - 6$.
   - For (2) we see the polynomial has a double root at 0 mod 2 so we get $(2) = (2, \sqrt{-6})^2$. This ideal $I_2 = (2, \sqrt{-6})$ is not principal, since any generator would necessarily have norm ± 2, but there are no such elements since there are no solutions to $x^2 + 6y^2 = \pm 2$. Thus, $[I_2]$ is an element of order 2 in the class group.
   - For (3) we see the polynomial has a double root at 0 mod 3 so we get $(3) = (3, \sqrt{-6})^2$, and as above the ideal $I_3 = (3, \sqrt{-6})$ is not principal since there are no elements of norm ± 3. Thus, $[I_3]$ is an element of order 2 in the class group.
   - To identify the relationship between I_2 and I_3 we observe $I_2 I_3 = (6, 2\sqrt{-6}, 3\sqrt{-6}, -6) = (\sqrt{-6})$ is principal, so $[I_2] = [I_3]^{-1} = [I_3]$.
   - We therefore have a single nonprincipal ideal class, so the class group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

   (d) $\mathbb{Z}[\sqrt{14}]$.
   - Here $\Delta = 56$ so $\mu = \frac{1}{2}\sqrt{56} \approx 3.7417$.
   - Since $\mu < 4$, the only possible prime ideals of norm less than μ are the ideals of norm 2 and norm 3.
   - The minimal polynomial of the generator is $x^2 - 14$.
   - For (2) we see the polynomial has a double root at 0 mod 2 so we get $(2) = (2, \sqrt{14})^2$. If this ideal $I_2 = (2, \sqrt{14})$ were principal then it would be generated by an element of norm 2, and searching for solutions to $x^2 - 14y^2 = \pm 2$ reveals that $4 + \sqrt{14} \in I_2$ has norm 2. Thus $I_2 = (4 + \sqrt{14})$ is principal so it is the trivial class.
   - For (3) we see that $x^2 - 14$ is irreducible modulo 3, so (3) is inert and has norm 9. Thus there are no ideals of norm 3.
   - We have identified all of the possible prime ideals of norm up to μ and they are all principal, so the class group is trivial.

(e) $\mathcal{O}_{\sqrt{-163}}$.

- Here $\Delta = 163$ so $\mu = \frac{2}{\pi}\sqrt{163} \approx 8.1278$.
- Since $\mu < 9$, the only possible prime ideals of norm less than μ are the ideals of norm 2, 3, 5, and 7.
- The minimal polynomial of the generator is $x^2 - x + 41$.
- However, it is not hard to check that the polynomial is irreducible modulo (2), (3), (5), and (7) (the quick way is to note that -163 is 2 mod 3, 2 mod 5, and 6 mod 7, so it is not a quadratic residue modulo any of these primes).
- Therefore, all of these primes are inert, so there are no nonprincipal prime ideals up to the Minkowski bound, so the class group is trivial.

(f) $\mathcal{O}_{\sqrt{-23}}$. [Hint: Show I_2^3 and $I_2 I_3$ are both principal.]

- Here $\Delta = 24$ so $\mu = \frac{2}{\pi}\sqrt{23} \approx 3.0531$.
- Since $\mu < 4$, the only possible prime ideals of norm less than μ are the ideals of norm 2 and norm 3.
- The minimal polynomial of the generator $\omega = \frac{1+\sqrt{-23}}{2}$ is $x^2 - x + 6$.
- For (2) we see the polynomial has roots 0 and 1 so we get $(2) = (2, \frac{1+\sqrt{-23}}{2})(2, \frac{1-\sqrt{-23}}{2})$. If the ideal $I_2 = (2, \frac{1+\sqrt{-23}}{2})$ were principal then it would be generated by an element of norm 2, but there are no elements of norm 2 since there are no solutions to $x^2 + 23y^2 = 8$. The ideal I_2^2 cannot be principal either, since it would have to be generated by an element of norm 4, but the only such elements are ± 2 and we already have the ideal factorization $(2) = I_2 I_2'$ and $I_2 \neq I_2'$ since 2 is not ramified.
- On the other hand, I_2^3 has norm 8, and there are elements of norm 8, namely, $\dfrac{3 \pm \sqrt{-23}}{2}$. Indeed, we can see that $I_2^3 = (8, 2 + 2\sqrt{-23}, -11 + \sqrt{-23}, \frac{-17-5\sqrt{-23}}{2})$ so this ideal contains $8 + (2 + 2\sqrt{-23}) + \frac{-17-5\sqrt{-23}}{2} = \frac{3-\sqrt{-23}}{2}$. Thus $I_2^3 = (\frac{3-\sqrt{-23}}{2})$ is principal, and so $[I_2]$ is an element of order 3 in the class group.
- For (3) we see the polynomial has roots 0 and 1 so we get $(3) = (3, \frac{1+\sqrt{-23}}{2})(3, \frac{1-\sqrt{-23}}{2})$. In a similar way we can see I_3 and I_3^2 are not principal, but I_3^3 is. To determine the relationship between $[I_2]$ and $[I_3]$ we search for elements of norm equal to a power of 2 times a power of 3. We can see that $\dfrac{1 + \sqrt{-23}}{2}$ has norm 6 and is contained in I_2 and I_3, so in fact $I_2 I_3 = (\frac{1+\sqrt{-23}}{2})$ is principal, so $[I_3] = [I_2]^{-1}$.
- Thus the class group is generated by $[I_2]$ and is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

---

3. The goal of this problem is to discuss runs of consecutive integers none of which are the sum of 2 or 3 squares.

(a) For any positive integer k, show that there exist k consecutive positive integers none of which are the sum of two squares. [Hint: Take $N \equiv 3 \pmod 9$, $N + 1 \equiv 7 \pmod{49}$, etc.]

- Let $p_1, p_2, \ldots, p_k$ be distinct primes congruent to 3 modulo 4. By the Chinese remainder theorem, there exists a solution to the simultaneous congruences $N \equiv p_1 \pmod{p_1^2}$, $N + 1 \equiv p_2 \pmod{p_2^2}$, ... , $N + k - 1 \equiv p_k \pmod{p_k^2}$, since the moduli are relatively prime.
- Taking N to be a positive solution of this system of congruences, we see that N, $N+1$, ... , $N+k-1$ are all divisible by a 3 mod 4 prime to an odd power, meaning that none of them are the sum of two squares.

(b) Show that of any 3 consecutive positive integers, at least one is the sum of three squares.

- As we showed, the integers that are not the sum of three squares are of the form $4^a(8b+7)$ for some nonnegative integers a, b. Such integers are either 7 mod 8 or 0 mod 4, hence are 0, 4, or 7 mod 8. Any three consecutive integers necessarily has at least one that is not 0, 4, or 7 mod 8, and that integer is the sum of three squares.

(c) Find an example of 2 consecutive positive integers neither of which is the sum of three squares.

- From (b) the only way this can happen is if the two integers are 7 and 0 modulo 8, and the 0-modulo-8 integer is of the form $4^a(8b+7)$. This will be the case whenever $a \geq 2$, so for instance we can take $a = 2$ and $b = 0$ to obtain the integers 111, 112.

---

4. The goal of this problem is to prove the slightly sharper version of Minkowski's theorem for closed sets.

   (a) Suppose S is a closed subset of n-measure 1 inside $[0,1]^n$. Prove that $S = [0,1]^n$. [Hint: Consider the complement of S.]

   - The complement of S inside $[0,1]^n$ is open (by definition).
   - Because measure is additive, we also have $\mu(S) + \mu(S^c) = \mu([0,1]^n) = 1$, so $\mu(S^c) = 1 - 1 = 0$.
   - If S^c were nonempty, select any point P. Since S^c is open, there exists a ball of positive radius around P inside S^c. But this ball would have positive measure, contradicting the fact that $\mu(S^c) = 0$.
   - Therefore, S^c is empty so $S = [0,1]^n$.

   (b) Suppose S is a closed, bounded, measurable set in $\mathbb{R}^n$ whose n-measure is equal to 1. Show that there exist two points x and y in S such that $x - y$ has integer coordinates.

   - As in class, write down the union of translates of S by lattice vectors inside $[0,1]^n$. If any of these translates intersect, then we get the desired points x and y.
   - Otherwise, these translates are disjoint, so the union is a closed subset of $[0,1]^n$ that has measure 1 (since measure is additive). Then by (a) the union equals $[0,1]^n$, which again has two points that differ by integer coordinates (namely, any two vertices of the box).

   (c) Suppose B is a convex closed set in $\mathbb{R}^n$ that is symmetric about the origin and whose n-measure is $\geq 2^n$. Prove that B contains a nonzero point all of whose coordinates are integers.

   - The regular version of Minkowski's theorem applies if the measure is $> 2^n$. If the measure equals 2^n, then $\frac{1}{2}B$ has measure 1, so by (b) it contains points x, y with $x - y \in \mathbb{Z}^n$. Then $2x, 2y \in B$ so $2x, -2y \in B$ by symmetry, so $x - y \in B$ by convexity, as required.

---

5. Suppose that α and β are real numbers and that $N > 1$.

   (a) Find the volume of the region $(x, y, z) \in \mathbb{R}^3$ with $|x| \leq N$, $|\alpha x - y| \leq 1/\sqrt{N}$, $|\beta x - z| \leq 1/\sqrt{N}$.

   - The region is described by the inequalities $-N \leq x \leq N$, $\alpha x - 1/\sqrt{N} \leq y \leq \alpha x + 1/\sqrt{N}$, $\beta x - 1/\sqrt{N} \leq z \leq \beta x + 1/\sqrt{N}$ so its volume is $\int_{-N}^{N} \int_{\alpha x - 1/\sqrt{N}}^{\alpha x + 1/\sqrt{N}} \int_{\beta x - 1/\sqrt{N}}^{\beta x + 1/\sqrt{N}} 1 \, dz \, dy \, dz = 8$.
   - Alternatively, it is a skew box, so its volume is the determinant of the spanning vectors $2N \langle 1, 0, 0 \rangle$, $\frac{2}{\sqrt{N}} \langle \alpha, -1, 0 \rangle$, $\frac{2}{\sqrt{N}} \langle \beta, 0, -1 \rangle$, and this determinant is $2N \cdot (-\frac{2}{\sqrt{N}})^2 = 8$.

   (b) Show there exist integers p, q, r with $1 \leq r \leq N$ such that $|\alpha - p/r|$ and $|\beta - q/r|$ are both at most $\frac{1}{r^{3/2}}$.

   - The region from part (a) is centrally symmetric, convex, closed, and has measure 2^3.
   - Therefore by Minkowski's theorem, it contains a nonzero lattice point (r, p, q), meaning that $|r| \leq N$, $|\alpha p - r| \leq 1/\sqrt{N}$, and $|\beta q - r| \leq 1/\sqrt{N}$. If we had $r = 0$ then the other conditions would force $p = q = 0$, contrary to the assumption that (r, p, q) is nonzero.
   - Now rescaling the triple by -1 if needed to make r positive, we see that $1 \leq r \leq N$ and that $|\alpha - p/r| \leq \frac{1}{r\sqrt{N}}$ and $|\beta - q/r| \leq \frac{1}{r\sqrt{N}}$ as well.
   - Finally since $r \leq N$ we see that $\frac{1}{r\sqrt{N}} \leq \frac{1}{r^{3/2}}$, so the required estimates hold as claimed.

Remark: The idea of (b) is that we can provide simultaneous approximations to the real numbers α and β using a shared denominator r such that the approximation error is small relative to r.

---

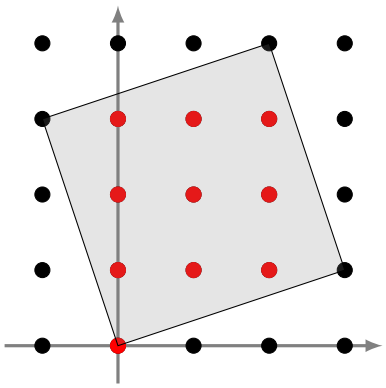
6. The goal of this problem is to give a geometric method for analyzing $\mathbb{Z}[i]/(\beta)$ for a nonzero $\beta \in \mathbb{Z}[i]$.

(a) Show that the ideal (β) forms a sublattice of the Gaussian integer lattice inside $\mathbb{C}$, and compute the area of its fundamental domain. [Hint: It is spanned by β and $i\beta$.]

- Notice that $(\beta) = \{\beta x + i\beta y : x, y \in \mathbb{Z}\}$ so the underlying lattice is spanned by β and $i\beta$.
- These vectors are perpendicular so the fundamental domain is simply a square of side length $|\beta|$, so the area is $|\beta|^2 = N(\beta)$.

(b) Let $\beta = 3 + i$. Draw a fundamental region for $\mathbb{Z}[i]/(\beta)$, and use it to find an explicit list of residue class representatives for $\mathbb{Z}[i]/(\beta)$.

- Here is the resulting fundamental region with the inequivalent points marked in red:



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

(c) Show that the number of residue classes in $\mathbb{Z}[i]/(\beta)$ is equal to the total number of interior points I, plus half of the number of boundary points B, minus one, inside the fundamental domain. [Hint: The boundary points come in pairs, except for the four corners.]

- We are simply counting inequivalent lattice points inside the square spanned by β and $i\beta$.
- Each interior point is not equivalent to any other point in the square. All four of the corner points are equivalent, and all of the boundary points that are not at corners come in pairs (the left edge and right edge, or the top edge and bottom edge).
- Thus, the total number of inequivalent points is equal to $I + (B-4)/2 + 1 = I + B/2 - 1$.

(d) Deduce that the number of distinct residue classes in $\mathbb{Z}[i]$ modulo β is equal to $N(\beta)$. [Hint: Use Pick's theorem to put (a) and (b) together.]

- By (a) the area of the fundamental domain is $N(\beta)$. By (b), the number of residue classes is equal to $I + B/2 - 1$, which by Pick's theorem also equals the area. Thus, the number of residue classes equals $N(\beta)$.

(e) Does this method also work for $\mathcal{O}_{\sqrt{D}}/I$ for a general nonzero ideal I of $\mathcal{O}_{\sqrt{D}}$? [Hint: Yes, with the right way to view I as a lattice.]

- Yes, it does, assuming we use the Minkowski embedding when $D > 0$: as we have already seen, I will form a sublattice whose index is the cardinality of $\mathcal{O}_{\sqrt{D}}/I$, and so picking out the inequivalent points from the fundamental domain will yield unique residue class representatives.
- One can use an affine change of variables to convert to the case of the Gaussian lattice, in which case we can invoke the results above.

---

7. The goal of this problem is to show that $\mathcal{O}_{\sqrt{-19}}$ is a PID that is not Euclidean. If R is an integral domain, we say an element $u \in R$ is a universal side divisor if it is not zero, not a unit, and every $x \in R$ can be written in the form $x = qu + z$ where z is either zero or a unit. Equivalently, u is a universal side divisor when every nonzero residue class modulo u is represented by a unit of R.

   (a) Suppose R is a Euclidean domain that is not a field. If u is a nonzero nonunit of R having minimal norm among nonzero nonunits in R (with respect to the norm function on R), show that u is a universal side divisor.

   - Since R is not a field, it has at least one nonzero element that is not a unit. Then there exists such a u by the well-ordering axiom.
   - Let $x \in R$ and divide x by u: we see that $x = qu + z$ where $z = 0$ or $N(z) < N(u)$. But because u has minimal norm among all nonzero nonunits, and $N(z) < N(u)$, the only possibility is that z is either 0 or a unit. Thus, u satisfies the condition for being a universal side divisor.

   (b) If u is a universal side divisor in $\mathcal{O}_{\sqrt{-19}}$, show that u must divide one of $x-1$, x, $x+1$ for any $x \in R$.

   - By definition, any universal side divisor u must divide $x - z$ for $z = 0$ or z a unit.
   - Since the only units in $\mathcal{O}_{\sqrt{-19}}$ are ± 1, this means u must divide one of $x-1$, x, $x+1$.

   (c) Show that $\mathcal{O}_{\sqrt{-19}}$ has no universal side divisors and conclude that $\mathcal{O}_{\sqrt{-19}}$ is not Euclidean. [Hint: Apply (b) when $x = 2$ and $x = (1+\sqrt{-19})/2$, and compute norms.]

   - Suppose u is a universal side divisor in $\mathcal{O}_{\sqrt{-19}}$. By (b) applied to $x = 2$ we see that u divides 1, 2, or 3, hence has norm dividing 1, 4, or 9.
   - By (b) applied to $x = (1+\sqrt{-19})/2$ we see that u divides $(-1+\sqrt{-19})/2$ or $(1+\sqrt{-19})/2$ or $(3+\sqrt{-19})/2$ hence has norm dividing 5, 5, or 7.
   - But the only elements satisfying both of these conditions are those of norm 1, but that would imply u is a unit, contradiction. Hence $\mathcal{O}_{\sqrt{-19}}$ has no universal side divisors so by (a), $\mathcal{O}_{\sqrt{-19}}$ is not Euclidean.

   (d) Show that $\mathcal{O}_{\sqrt{-19}}$ has trivial class group. Deduce that $\mathcal{O}_{\sqrt{-19}}$ is a PID that is not Euclidean.

   - Since $-19 \equiv 1 \pmod 4$, we have $\Delta = -19$, and so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{2}{\pi}\sqrt{19} \approx 2.7750 < 3$, so the only nontrivial ideals we need to consider are ideals of norm 2.
   - The minimal polynomial of the generator $\omega = \frac{1+\sqrt{-19}}{2}$ is $x^2 - x + 5$.
   - For (2) we see the polynomial is irreducible modulo 2, so (2) is inert and does not yield a nontrivial element of the class group. Hence the class group is trivial, so $\mathcal{O}_{\sqrt{-19}}$ has trivial class group, hence is a PID. By (c), $\mathcal{O}_{\sqrt{-19}}$ is not Euclidean, so it is a PID that is not Euclidean.

---

8. [Challenge] The goal of this problem is to give a proof using Minkowski's theorem of the Diophantine approximation theorem we established using continued fractions: that for any irrational real number α there exist infinitely many rationals p/q with $|\alpha - p/q| < \frac{1}{2}q^{-2}$.

   (a) Suppose $A = \{a_{i,j}\}_{1 \le i,j \le n}$ is a real $n \times n$ matrix whose determinant is not zero. If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are positive real numbers such that $\lambda_1\lambda_2\cdots\lambda_n \ge |\det A|$, prove that there exist integers $x_1, x_2, \ldots, x_n$, not all zero, such that $|a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n| \le \lambda_1$, $|a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n| \le \lambda_2$, ... , and $|a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,n}x_n| \le \lambda_n$.

   - Let Λ be the lattice spanned by the columns of A, whose fundamental domain has volume $|\det A|$ as we discussed in class.
   - Also let B be the convex, centrally-symmetric, closed region in $\mathbb{R}^n$ defined by $|x_i| \le \lambda_i$ for each $1 \le i \le n$. This region is simply a box with side lengths $2\lambda_i$ so its n-measure is $2^n\lambda_1\lambda_2\cdots\lambda_n \ge 2^n|\det A|$.
   - Since the measure of B is $\ge 2^n$ times the volume of the fundamental domain of Λ, we conclude that there is a nonzero element of Λ in B.
   - If this vector is $x_1\langle a_{1,1}, a_{2,1}, \ldots, a_{n,1}\rangle + x_2\langle a_{1,2}, a_{2,1}, \ldots, a_{n,2}\rangle + \cdots + x_n\langle a_{1,n}, a_{2,n}, \ldots, a_{n,n}\rangle$, then the ith component of this sum has absolute value $\le \lambda_i$, and this is exactly the desired condition.

(b) Suppose that a, b, c, d are real numbers such that $ad - bc \neq 0$. Show that there exist integers p, q not both zero such that $|ap + bq| \cdot |cp + dq| \leq \frac{1}{2}|ad - bc|$ and $|ap + bq|, |cp + dq| \leq \sqrt{2|ad - bc|}$. [Hint: Apply (a) to the forms $(ax + by) \pm (cx + dy)$, then use the triangle inequality and the arithmetic-geometric mean inequality.]

- Following the hint, consider the two forms $(a+c)x+(b+d)y$ and $(a+c)x+(b+d)y$, of determinant $2(ad - bc)$.
- Then by (a) with $\lambda_1 = \lambda_2 = \sqrt{2|ad - bc|}$, there exist integers p, q not both zero such that $X = |(ap + bq) + (cp + dq)|$ and $Y = |(ap + bq) - (cp + dq)|$ are at most $\sqrt{2|D|}$.
- By the triangle inequality, we have $|ap + bq| + |cp + dq| \leq \max(X, Y) \leq \sqrt{2|D|}$, so in particular each term is at most that value.
- Finally by AM-GM we have $|ap + bq| \cdot |cp + dq| \leq \left[\frac{|ap + bq| + |cp + dq|}{2}\right]^2 = \frac{1}{2}|ad - bc|$ as required.

(c) Let α be a real number and fix a positive real number t. Show that there exist integers p, q not both zero such that $\left|pq - \alpha q^2\right| \leq \frac{1}{2}$ and with $|tp - \alpha tq| \leq \sqrt{2}$. [Hint: Use (b) with $a = t$, $b = -\alpha t$.]

- We apply (b) with $a = t$, $b = -\alpha t$, $c = 0$, $d = 1/t$ with $ad - bc = 1$: then (b) yields that $|tp - \alpha tq| \leq \sqrt{2}$ and that $|tp - \alpha tq| \cdot |q/t| \leq \frac{1}{2}$ which is equivalent to the desired $\left|pq - \alpha q^2\right| \leq \frac{1}{2}$.

(d) Let α be an irrational real number. Show that there exist infinitely many rational numbers p/q such that $|\alpha - p/q| < \frac{1}{2}q^{-2}$. [Hint: For any finite N, choose t large enough so that $|p - \alpha q| > \sqrt{2}/t$ whenever $q \leq N$.]

- Since α is irrational, for any finite bound N, the minimum value M of $|p - \alpha q|$ among all $q \leq N$ is nonzero, since there is only one value of p that makes the value less than $1/2$ in absolute value.
- Take t large enough such that $\sqrt{2}/t$ is less than M. Applying (c) for this value of t yields that there exists p, q such that $|\alpha - p/q| < \frac{1}{2}q^{-2}$ and $|p - \alpha q| \leq \sqrt{2}/t < M$, but this requires $q > N$ by the above.
- We conclude that there exists such a p/q with $q > N$ for any N, so there are infinitely many such p/q.
