Topics: Congruent numbers, averages, baby Hasse–Weil.

9.1. Recall that $n \in \mathbf{Z}_{\geqslant 1}$ is a *congruent number* if there exists $x \in \mathbf{Q}$ such that $x^2 - n$ and $x^2 + n$ are squares of rational numbers.

(a) Suppose n is a congruent number and let $x \in \mathbf{Q}$ be such that $x^2 - n = u^2$ and $x^2 + n = v^2$ for some $u, v \in \mathbf{Q}$. Let $a = v + u$ and $b = v - u$. Prove that a and b are the legs of a rational right triangle with area n.

(b) Suppose $n \in \mathbf{Z}_{\geqslant 1}$ is the area of a rational right triangle. Let x be one half of the hypotenuse. Prove that $x^2 - n$ and $x^2 + n$ are squares, hence n is a congruent number.

9.2. Let's put together Fermat's Infinite Descent proof that 1 is not a congruent number. Proceed by contradiction: suppose 1 is a congruent number.

(a) Prove that there exists an integer right triangle whose area is a perfect square.

[**Hint**: Start with a rational right triangle (a, b, c) given by the assumption that 1 is congruent.]

(b) Pick a triangle (u, v, w) as in part (a) where the hypotenuse w is minimal.

Prove that $\mathsf{gcd}\,(u, v) = 1$.

(c) Write $u = m^2 - n^2$, $v = 2mn$, $w = m^2 + n^2$, with m, n of opposite parity, $m > n > 0$, and $\mathsf{gcd}\,(m, n) = 1$.

Prove that each of the integers $m, n, m - n, m + n$ is a perfect square.

(d) Write $m = p^2$, $n = q^2$, $m - n = r^2$, $m + n = s^2$.

Given the constraints on m and n, what constraints do you get on r and s?

Use them to prove that m has to be odd.

(e) Set

$$R = \frac{s - r}{2}, \quad S = \frac{s + r}{2}.$$

Show that (R, S, p) gives an integer right triangle with square area and hypotenuse $p < w$, contradicting the minimality of w.

9.3. We explore how the average of a sequence can depend heavily on the ordering of the terms.

The quantity we will study is the number $N(f)$ of real roots of a monic quadratic polynomial with integer coefficients:

$$f(x) = x^2 + bx + c, \qquad b, c \in \mathbf{Z}. \tag{1}$$

We will order such polynomials according to two different height functions, and estimate the average number of roots with respect to each ordering.

(a) Given a polynomial as in (1), define

$$H_1(f) = H_1(b, c) = \mathsf{max}\,\{|b|, |c|\}.$$

For a fixed $X \in \mathbf{R}$, define

$$\mathcal{P}_{1,X} = \{f : \; H_1(f) < X\}.$$

i. Compute the exact values of $\#\mathcal{P}_{1,1}$ and $\#\mathcal{P}_{1,2}$.

ii. Sketch the region corresponding to $\mathcal{P}_{1,X}$ in the $b-c$ plane. On the same graph, identify the regions corresponding to the subsets of $\mathcal{P}_{1,X}$ given by polynomials with 0 real roots; with 1 real root; with 2 real roots.

iii. Find the average number of roots with respect to H_1:

$$N_{1,\mathrm{avg}} = \lim_{X\longrightarrow\infty} \frac{\sum\limits_{f\in\mathcal{P}_{1,X}} N(f)}{\#\mathcal{P}_{1,X}}.$$

You may assume that, for a bounded region R in the plane, the area of R gives a good estimate for the number of points with integral coordinates inside R.

(b) Given a polynomial as in (1), define

$$H_2(f) = H_2(b,c) = \max\left\{|b|, \sqrt{|c|}\right\}.$$

For a fixed $X \in \mathbf{R}$, define

$$\mathcal{P}_{2,X} = \{f :\ H_2(f) < X\}.$$

i. Compute the exact values of $\#\mathcal{P}_{2,1}$ and $\#\mathcal{P}_{2,2}$.

ii. Sketch the region corresponding to $\mathcal{P}_{2,X}$ in the $b-c$ plane. On the same graph, identify the regions corresponding to the subsets of $\mathcal{P}_{2,X}$ given by polynomials with 0 real roots; with 1 real root; with 2 real roots.

iii. Find the average number of roots with respect to H_2:

$$N_{2,\mathrm{avg}} = \lim_{X\longrightarrow\infty} \frac{\sum\limits_{f\in\mathcal{P}_{2,X}} N(f)}{\#\mathcal{P}_{2,X}}.$$

9.4. Let's (almost) prove the genus zero case of the Hasse–Weil bound.

Fix a prime $p > 2$ and a monic polynomial f of degree $n = 1, 2$ with coefficients in $\mathbf{F}_p$ and no multiple roots and consider the curve C defined by the equation $y^2 = f(x)$. Since the genus is 0, the Hasse–Weil bound in this case reduces to $\#C(\mathbf{F}_p) = p + 1$.

We take it for granted that C has one point at infinity when $n = 1$, and two points at infinity when $n = 2$.

(a) For $n = 1$, count the number of solutions in $\mathbf{F}_p$ to an equation of the form $y^2 = x + b$ and verify that $\#C(\mathbf{F}_p) = p + 1$.

(b) For $n = 2$, consider the equation $y^2 = x^2 + ax + b$. Show that the change of variables $x = u - \frac{a}{2}$, $c = b - \frac{a^2}{4}$ gives the equation

$$y^2 - u^2 = c$$

and that $c \neq 0$.

(c) Check that the function $(u, y) \mapsto (y - u, y + u)$ is a bijection $\mathbf{F}_p^2 \longrightarrow \mathbf{F}_p^2$.

(d) Deduce that the points (u, y) on the curve $y^2 - u^2 = c$ are in bijection with the points (s, t) on the curve $st = c$. Check that there are precisely $p - 1$ pairs $(s, t) \in \mathbf{F}_p^2$ satisfying $st = c$, and conclude that $C(\mathbf{F}_p) = p - 1 + 2 = p + 1$ in the case $n = 2$.