

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

9.1. Recall that $n \in \mathbf{Z}_{\geq 1}$ 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 $n \in \mathbf{Z}_{\geq 1}$ 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.

Solution.

- (a) We have

$$a^2 + b^2 = (v + u)^2 + (v - u)^2 = 2v^2 + 2u^2 = 2x^2 + 2n + 2x^2 - 2n = 4x^2 = (2x)^2,$$

so (a, b, x) forms a rational right triangle.

The area is

$$\frac{ab}{2} = \frac{v^2 - u^2}{2} = \frac{2n}{2} = n.$$

- (b) Let (a, b, c) give the rational right triangle with area n , so that $2n = ab$. We set $x = c/2$. We have

$$x^2 - n = \frac{c^2}{4} - n = \frac{a^2 + b^2 - 4n}{4} = \frac{a^2 + b^2 - 2ab}{4} = \left(\frac{a - b}{2}\right)^2,$$

and

$$x^2 + n = \frac{c^2}{4} + n = \frac{a^2 + b^2 + 4n}{4} = \frac{a^2 + b^2 + 2ab}{4} = \left(\frac{a + b}{2}\right)^2. \quad \square$$

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

Solution.

- (a) Take $(a, b, c) \in \mathbf{Q}^3$ such that $a^2 + b^2 = c^2$ and $ab = 2$. Let d be the common denominator of a, b, c , then $(da, db, dc) \in \mathbf{Z}^3$ is an integer right triangle with area d^2 .
- (b) Denote the area of the triangle by $uv/2 = t^2$ with $t \in \mathbf{Z}$.

Let $g = \gcd(u, v)$, then $g \mid w$. So the triple $(u/g, v/g, w/g) \in \mathbf{Z}^3$ gives a triangle with area $uv/(2g^2) = (t/g)^2$.

This area is therefore an integer and the square of a rational number, hence it is a perfect square. By the minimality of w , we must have $w/g = w$ so $g = 1$.

- (c) We have

$$t^2 = \frac{1}{2}uv = mn(m-n)(m+n).$$

Since $\gcd(m, n) = 1$, we also have

$$\gcd(m, m \pm n) = \gcd(n, m \pm n) = \gcd(m - n, m + n) = 1.$$

By unique factorisation into primes, if a product of four pairwise coprime integers is a perfect square, each of the factors is a perfect square.

- (d) We have seen that $\gcd(m+n, m-n) = 1$, so $\gcd(r, s) = 1$. As m and n have opposite parity, $m+n$ and $m-n$ are odd, so r and s are odd. Finally, $m+n > m-n > 0$ so $s > r > 0$.

Since r and s are odd we have $r^2 \equiv s^2 \equiv 1 \pmod{4}$, so

$$2n = s^2 - r^2 \equiv 0 \pmod{4},$$

hence n is even and m is odd.

- (e) We have

$$R^2 + S^2 = \frac{(s-r)^2 + (s+r)^2}{4} = \frac{2s^2 + 2r^2}{4} = \frac{4m}{4} = m = p^2.$$

Since both r and s are odd, R and S are integers.

The area of the triangle is

$$\frac{RS}{2} = \frac{s^2 - r^2}{8} = \frac{n}{4} = \left(\frac{q}{2}\right)^2,$$

and as we have seen in part (d) n is even, so q is even, so $q/2$ is an integer.

Finally,

$$p \leq p^2 = m < m^2 + n^2 = w. \quad \square$$

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:

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

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

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

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 :

$$N_{1,\text{avg}} = \lim_{X \rightarrow \infty} \frac{\sum_{f \in \mathcal{P}_{1,X}} N(f)}{\#\mathcal{P}_{1,X}}.$$

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 :

$$N_{2,\text{avg}} = \lim_{X \rightarrow \infty} \frac{\sum_{f \in \mathcal{P}_{2,X}} N(f)}{\#\mathcal{P}_{2,X}}.$$

Solution.

(a)

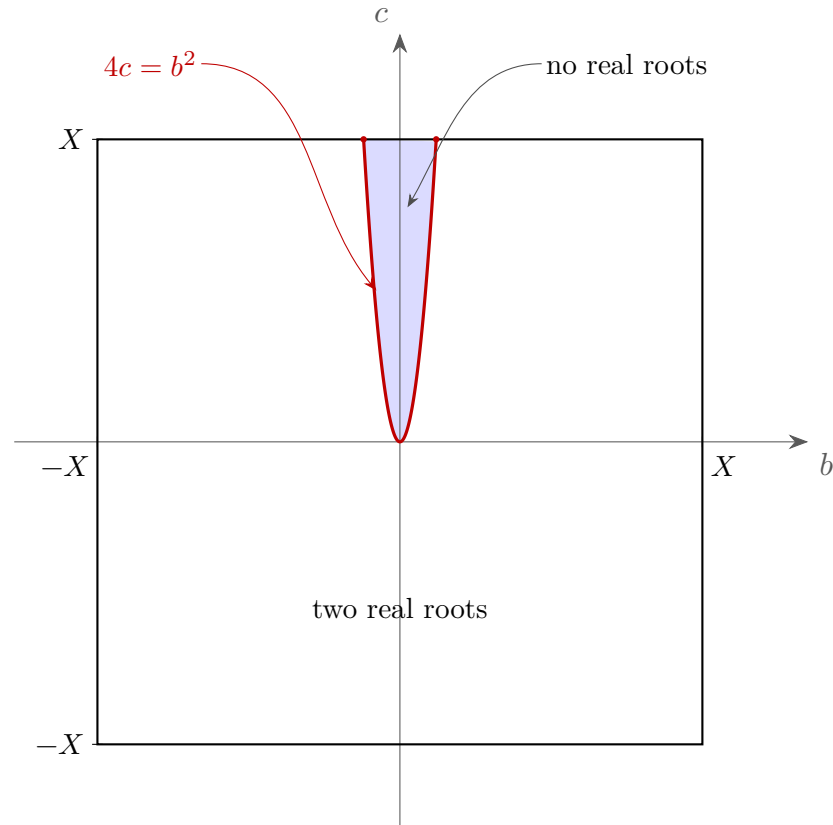
- i. We have

$$\mathcal{P}_{1,1} = \{f : |b| < 1, |c| < 1\} = \{f : b = c = 0\} \quad \text{so} \quad \#\mathcal{P}_{1,1} = 1,$$

and

$$\mathcal{P}_{1,2} = \{f : |b| < 2, |c| < 2\} = \{f : b = -1, 0, 1, c = -1, 0, 1\} \quad \text{so} \quad \#\mathcal{P}_{1,2} = 9.$$

- ii. Here is the sketch:



iii. The area of $\mathcal{P}_{1,X}$ is $A_{\text{tot}} = (2X)^2 = 4X^2$.

The area of the shaded region (where the polynomials have no real roots) is

$$\begin{aligned} A_0 &= \int_{-2\sqrt{X}}^{2\sqrt{X}} \left(X - \frac{b^2}{4} \right) db = 2 \int_0^{2\sqrt{X}} \left(X - \frac{b^2}{4} \right) db \\ &= 2 \left(2X\sqrt{X} - \frac{(2\sqrt{X})^3}{12} \right) = \frac{8}{3} X^{3/2}. \end{aligned}$$

The region where the polynomials have one real root is the red curve, hence its area is $A_1 = 0$.

The region where the polynomials have two real roots has area $A_2 = A_{\text{tot}} - A_1 - A_0$.

Therefore

$$\begin{aligned} N_{1,\text{avg}} &= \lim_{X \rightarrow \infty} \frac{\sum_{f \in \mathcal{P}_{1,X}} N(f)}{\#\mathcal{P}_{1,X}} = \lim_{X \rightarrow \infty} \frac{0 \cdot A_0 + 1 \cdot A_1 + 2 \cdot A_2}{A_{\text{tot}}} \\ &= \lim_{X \rightarrow \infty} \frac{2 \left(4X^2 - \frac{8}{3} X^{3/2} \right)}{4X^2} = \lim_{X \rightarrow \infty} 2 \left(1 - \frac{2}{3X^{1/2}} \right) = 2. \end{aligned}$$

(b)

i. We have

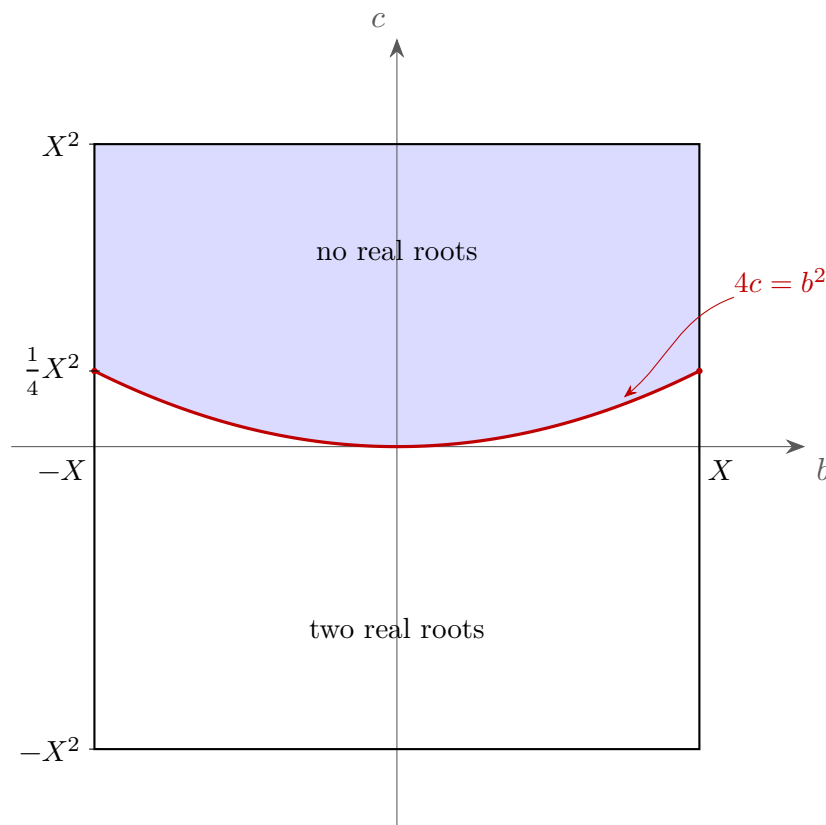
$$\mathcal{P}_{2,1} = \{f : |b| < 1, |c|^{1/2} < 1\} = \{f : b = c = 0\} \quad \text{so} \quad \#\mathcal{P}_{2,1} = 1,$$

and

$$\mathcal{P}_{2,2} = \{f : |b| < 2, |c|^{1/2} < 2\} = \{f : b = -1, 0, 1, c = -3, -2, -1, 0, 1, 2, 3\},$$

so $\#\mathcal{P}_{2,2} = 21$.

ii. Here is the sketch:



iii. The area of $\mathcal{P}_{2,X}$ is $A_{\text{tot}} = (2X^2)(2X) = 4X^3$.

The area of the shaded region (where the polynomials have no real roots) is

$$\begin{aligned} A_0 &= \int_{-X}^X \left(X^2 - \frac{b^2}{4} \right) db = 2 \int_0^X \left(X^2 - \frac{b^2}{4} \right) db \\ &= 2 \left(X^3 - \frac{X^3}{12} \right) = \frac{11}{6} X^3. \end{aligned}$$

The region where the polynomials have one real root is the red curve, hence its area is $A_1 = 0$.

The region where the polynomials have two real roots has area $A_2 = A_{\text{tot}} - A_1 - A_0$.

Therefore

$$\begin{aligned} N_{2,\text{avg}} &= \lim_{X \rightarrow \infty} \frac{\sum_{f \in \mathcal{P}_{2,X}} N(f)}{\#\mathcal{P}_{2,X}} = \lim_{X \rightarrow \infty} \frac{0 \cdot A_0 + 1 \cdot A_1 + 2 \cdot A_2}{A_{\text{tot}}} \\ &= \lim_{X \rightarrow \infty} \frac{2 \left(4X^3 - \frac{11}{6} X^3 \right)}{4X^3} = \lim_{X \rightarrow \infty} \frac{\frac{13}{3} X^3}{4X^3} = \frac{13}{12}. \quad \square \end{aligned}$$

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 $\mathbf{F}_p^2 \rightarrow \mathbf{F}_p^2$.
- (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 $n = 2$.

Solution.

- (a) Suppose (x, y) satisfies $y^2 = x + b$. We have the following possibilities:
- $x + b = 0$, corresponding to a single point $(-b, 0)$;
 - $x + b$ is a quadratic residue r^2 ; there are $(p - 1)/2$ such r , each giving 2 solutions, for a total of $p - 1$ points;
 - $x + b$ is a quadratic non-residue, giving zero solutions.

We conclude that there are $1 + (p - 1)$ points (x, y) on the curve, so together with one point at infinity we have $\#C(\mathbf{F}_p) = p + 1$.

- (b) Algebraic manipulation:

$$y^2 = \left(u - \frac{a}{2}\right)^2 + a\left(u - \frac{a}{2}\right) + b = u^2 - \frac{a^2}{4} + b = u^2 + c.$$

Suppose $0 = c = b - \frac{a^2}{4}$, then $a^2 - 4b = 0$ so the quadratic polynomial $f(x) = x^2 + ax + b$ has a repeated root, contradiction.

- (c) Easy to see that $(s, t) \mapsto ((t - s)/2, (t + s)/2)$ is an inverse function.

Alternatively, note that the given function is a linear transformation with matrix $\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$, and the determinant is $-2 \neq 0$ in $\mathbf{F}_p$.

- (d) To solve $st = c$, write $t = c/s$. The parameter s can now be any nonzero element in $\mathbf{F}_p$, and t is uniquely determined by s . So we get $p - 1$ pairs (s, t) , and therefore $p - 1$ pairs (u, y) , and finally $p - 1$ points (x, y) on C . With the two points at infinity we have $C(\mathbf{F}_p) = p + 1$. $\square$