12. 3/6

12.1. Test 1 was out of 150 points. Scores ≥ 120 are A-range, scores ≥ 100 are B-range, and scores ≥ 80 are C-range. You are welcome to reach out to me if you're worried about how you're doing, and/or deciding whether or not to drop the course.

12.2. A comment on Non-Book Problem 1 from Problem Set 2. Many people tried to apply the well-ordering principle to the set $\mathbf{N}^2$ of ordered pairs of natural numbers. However, the principle only applies to $\mathbf{N}$.

The point is that a priori, it isn't clear what it means for an ordered pair of numbers to be "smallest". In order to do that, we need to measure an ordered pair (x_1, x_2) by a single number. There are a couple of ways to do so. One option that helps with Non–Book Problem 1 is $x_1 x_2$. That is, the well-ordering principle can be applied to the set

$$\{n \in \mathbf{N} \mid n = x_1 x_2 \text{ for some pair } (x_1, x_2) \in \mathbf{N}^2 \text{ that solves } x_1^2 = 2x_2^2\}.$$

12.3. *Lattice-point problems* One of our initial topics was linear Diophantine equations: that is, solving $ax + by = c$ for integers x, y.

The name comes from the fact that $ax + by = c$ determines a line in the (x, y)-plane. If a *lattice point* is a point whose coordinates are integers, then the problem can be restated geometrically as the problem of finding all lattice points on the line.

So next we ask: Given c, which lattice points live on the circle $x^2 + y^2 = c$? Given a, b, c, which lattice points live on the curve $ax^2 + by^2 = c$?

12.4. *A composition law* Apparently, Fermat got interested in integers of the form $x^2 + y^2$ after learning, from Diophantus' *Arithmetica*, that the set of such numbers is stable under multiplication. That is:

Proposition 12.1. *If $M, N \in \mathbf{Z}$ are each a sum of two perfect squares, then MN is a sum of two perfect squares.*

The proof is to stare at the magic identity:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

But how would you guess that this identity is true?

12.5. We will explain the proof in two ways, both anachronistic.

12.5.1. The first way involves linear algebra. Observe that

$$\det \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x^2 + y^2.$$

Next, observe that

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}.$$

Finally, recall that the determinant of a product of matrices is the product of their determinants.

Viewing 2×2 matrices as linear transformations of a 2-dimensional vector space, or plane, we can view this proof as a interpretation of the magic identity via the geometry of the Euclidean plane. But how do you come up with these matrices in the first place?

12.5.2. The second way gives a simpler interpretation of the matrices. Observe that if $z = x + iy$, where $i = \sqrt{-1}$, then the absolute value of z is its magnitude as a vector in the complex plane, which is

$$|z| = x^2 + y^2.$$

Next, observe that

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

as complex numbers. Finally, recall that the absolute value of a product of two complex numbers is the product of their absolute values.

12.6. Note that the magic identity was discovered in ancient times, whereas complex numbers were not accepted until the Renaissance at earliest (*e.g.*, by Cardano), and matrix multiplication was not introduced until the 19th century (by Grassmann).

The best use of abstraction is not to make things more sophisticated, but to make things simpler.

12.7. *More general composition laws* From his book, we can infer that Diophantus, in the 3rd century, knew the magic identity.

Brahmagupta, in the 6th century, discovered the following generalization:

$$(a^2 + nb^2)(c^2 + nd^2) = (ac - nbd)^2 + n(ad + bc)^2. \tag{12.1}$$

Fermat knew this identity as well. It led him to study not just integers of the form $x^2 + y^2$, but of the forms $x^2 + 2y^2$ and $x^2 + 3y^2$.

In the 19th century, Gauss discovered an even more general composition law for integers of the form $Ax^2 + Bxy + Cy^2$. These polynomials are called binary quadratic forms.

In the early 2000s, in his PhD thesis, the Fields Medalist Manjul Bhargava discovered at least thirteen other phenomena that could be called composition laws for other polynomial expressions of higher degree.

12.8. We will stick to the forms that interested Brahmagupta, namely, $x^2 \pm ny^2$ for various $n \in \mathbf{N}$.

Note that it's enough to study the case where n is *squarefree*, meaning it has no perfect-square divisors. For if $n = k^2 n'$, then $x^2 \pm ny^2 = x^2 \pm n'(ky)^2$.

The curve $x^2 \pm ny^2 = c$ is an ellipse when the sign is positive, and a hyperbola when it is negative. There is a huge difference between these cases. We will study the negative case first.

12.9. To motivate this case: First, observe that since n is squarefree, a generalization of Non-Book Problem 1 on Problem Set 2 shows that $\sqrt{n}$ is not rational. The lattice points on the hyperbola

$$x^2 - ny^2 = 1$$

are closely related to the problem of approximating $\sqrt{n}$ by rational numbers. Indeed, rearranging gives

$$\frac{x}{y} = \sqrt{n + \frac{1}{y^2}} = \sqrt{n} + O\left(\frac{1}{y^2}\right),$$

where $O\left(\frac{1}{y^2}\right)$ means an error term that decays quadratically in the size of y.

12.10. The curve $x^2 - ny^2 = 1$ is called Pell's equation. Here is another reason it is interesting: If $(x, y) = (a, b)$ and $(x, y) = (c, d)$ are two points on the curve, then by substituting $-n$ for n in (12.1), we see that

$$(x, y) = (ac + nbd, ad + bc)$$

lives on the curve as well.

In fact, under the operation

$$(a, b) \star (c, d) := (ac + nbd, ad + bc),$$

the points on Pell's curve (for fixed squarefree $n \in \mathbf{N}$) form an infinite group. We will return to this fact later this week.

13. 3/8

13.1. Fix squarefree $n \in \mathbf{N}$. We've discussed the lattice points on the curve

$$x^2 - ny^2 = 1.$$

It always contains the lattice points $(\pm 1, 0)$. Can we find another latttice point when $n = 2$? When $n = 3$? When $n = 5$? Our next goal is to answer this question.

13.2. Recall that after we insert some minus signs, Brahmagupta's identity is

$$(a^2 - nb^2)(c^2 - nd^2) = (ac + nbd)^2 - n(ad + bc)^2. \tag{13.1}$$

We described this as a composition law.

More simply, the set of numbers that take the form $x^2 - ny^2$ for some $x, y \in \mathbf{Z}$ is closed under multiplication.

If we allow ourselves to use $\sqrt{n}$ as well as integers, then we can factor both sides of (13.1). Thus it follows from the simpler identities

$$(a + b\sqrt{n})(c + d\sqrt{n}) = (ac + nbd) + (ad + bc)\sqrt{n},$$
$$(a - b\sqrt{n})(c - d\sqrt{n}) = (ac + nbd) - (ad + bc)\sqrt{n}.$$

13.3. *Norms* That is, the following set (pronounced: "$\mathbf{Z}$-adjoin-$\sqrt{n}$") is also closed under multiplication:

$$\mathbf{Z}[\sqrt{n}] = \{x + y\sqrt{n} \in \mathbf{R} \mid x, y \in \mathbf{Z}\}.$$

Brahmagupta implies that the map $\mathbf{N} : \mathbf{Z}[\sqrt{n}] \to \mathbf{Z}$ defined by

$$\mathbf{N}(x + y\sqrt{n}) = x^2 - ny^2$$

preserves multiplication:

$$\mathbf{N}((a + b\sqrt{n})(c + d\sqrt{n})) = \mathbf{N}(a + b\sqrt{n})\mathbf{N}(c + d\sqrt{n}).$$

It is called the *norm* map.

13.4. We also see that $\mathbf{Z}[\sqrt{n}]$ is closed under addition and subtraction:

$$(a + b\sqrt{n}) \pm (c + d\sqrt{n}) = (a \pm c) + (b \pm d)\sqrt{n}.$$

It can't be closed under division, because it contains 0. What if we exclude 0? Does every nonzero element of $\mathbf{Z}[\sqrt{n}]$ have a multiplicative inverse?

No: because $\mathbf{Z}[\sqrt{n}]$ contains $\mathbf{Z}$, and most nonzero elements of $\mathbf{Z}$ do not have a multiplicative inverse. Indeed, if $a > 1$, then $0 < \frac{1}{a} < 1$, but there are no integers in this interval.

13.5. The funny thing is, $\mathbf{Z}[\sqrt{n}]$ does have elements strictly between 0 and 1.

Lemma 13.1. *Distinct pairs $(x, y) \in \mathbf{Z}^2$ give distinct numbers $x + y\sqrt{n}$ (as long as n is squarefree).*

Theorem 13.2. *For any $M \in \mathbf{N}$, there is a pair $(x, y) \in \mathbf{Z}^2$ such that*

$$|x - y\sqrt{n}| < \frac{1}{M}.$$

In fact, we can simultaneously ensure $|x + y\sqrt{n}| < 3M\sqrt{n}$.

Proof. By the pigeonhole principle. For each $k \in \mathbf{N}$, let

$$\begin{aligned} a_k &= \lceil k\sqrt{n} \rceil, \\ \epsilon_k &= a_k - k\sqrt{n} \in [0, 1). \end{aligned}$$

By the lemma, the numbers $\epsilon_0, \epsilon_1, \ldots, \epsilon_M$ must be pairwise distinct. But there are $M + 1$ of them. So two of them, say ϵ_k and ϵ_ℓ, must differ by a value strictly between 0 and $\frac{1}{M}$. Now, taking $x = a_\ell - a_k$ and $y = \ell - k$ gives

$$|x - y\sqrt{n}| = |\epsilon_\ell - \epsilon_k| < \frac{1}{M}.$$

Note that $y = \ell - k \leq M$. Therefore

$$|x + y\sqrt{n}| \leq |x - y\sqrt{n}| + |2y\sqrt{n}| < \frac{1}{M} + 2M\sqrt{n} \leq 3M\sqrt{n}.$$

□

Corollary 13.3. *There are infinitely many pairs $(x, y) \in \mathbf{Z}^2$ such that*

$$|x^2 - ny^2| < 3\sqrt{n}.$$

Proof. The theorem shows that for any $M \in \mathbf{N}$, we can pick $x, y \in \mathbf{Z}$ such that

$$\begin{aligned} |x - y\sqrt{n}| &< \frac{1}{M}, \\ |x^2 - ny^2| &< \frac{1}{M}(3M\sqrt{n}) = 3\sqrt{n}. \end{aligned}$$

In general, suppose we've found $M = M_i$ and $(x, y) = (x_i, y_i)$ satisfying these inequalities. Pick M_{i+1} so that $\frac{1}{M_{i+1}} < |x_i - y_i\sqrt{n}|$. Then we can find $x_{i+1}, y_{i+1} \in \mathbf{Z}$ such that $M = M_{i+1}$ and $(x, y) = (x_{i+1}, y_{i+1})$ also satisfy the inequalities. But now,

$$|x_{i+1} - y_{i+1}\sqrt{n}| < \frac{1}{M_{i+1}} < |x_i - y_i\sqrt{n}|.$$

So by induction, we get an infinite sequence of pairwise-distinct solutions (x, y) to the inequality in the original statement. □

14. 3/10

14.1. Last time, we showed that for a fixed squarefree $n \in \mathbf{N}$, there are infinitely many lattice points (x, y) such that

$$-3\sqrt{n} < x^2 - ny^2 < 3\sqrt{n}.$$

So by the pigeonhole principle, there is some integer

$$-3\sqrt{n} < N < 3\sqrt{n}$$

such that $x^2 - ny^2 = N$ for infinitely many pairs $(x, y) \in \mathbf{Z}^2$.

Applying the principle again, there is some integer $0 \leq A < N$ such that infinitely many of these pairs also satisfy $x \equiv A \pmod{N}$.

Applying the principle yet again, there is some integer $0 \leq B < N$ such that infinitely many of the latter pairs also satisfy $y \equiv B \pmod{N}$.

So in particular, there are distinct lattice points $(a, b) \neq \pm(u, v)$ such that

$$\begin{aligned} a^2 - nb^2 = u^2 - nv^2 &= N, \\ a \equiv u &\equiv A \pmod{N}, \\ b \equiv v &\equiv B \pmod{N} \end{aligned}$$

simultaneously. Since $\sqrt{n}$ is irrational, $N \neq 0$. Hence $u + v\sqrt{n} \neq 0$.

Lemma 14.1. *In the situation above,*

$$\frac{a - b\sqrt{n}}{u - v\sqrt{n}} \in \mathbf{Z}[\sqrt{n}].$$

Proof. Expand:

$$\frac{a - b\sqrt{n}}{u - v\sqrt{n}} = \frac{(a - b\sqrt{n})(u + v\sqrt{n})}{u^2 - nv^2} = \frac{(au - nbv) + (av - bu)\sqrt{n}}{u^2 - nv^2}.$$

The last denominator is $\pm N$. So we must show that N divides $au - nbv$ and $av - bu$. Indeed, $a \equiv u \pmod{N}$ and $b \equiv v \pmod{N}$ together imply $av \equiv bu \pmod{N}$, and also, $au - nbv \equiv a^2 - nb^2 \equiv 0 \pmod{N}$. □

Theorem 14.2. *For squarefree $n \in \mathbf{N}$, the Pell equation $x^2 - ny^2 = 1$ has a solution $(x, y) \in \mathbf{Z}^2$ distinct from $(\pm 1, 0)$.*

Proof. In the situation above, we can write

$$\frac{a - b\sqrt{n}}{u - v\sqrt{n}} = x - y\sqrt{n}$$

for some $x, y \in \mathbf{Z}$. Therefore,

$$x^2 - ny^2 = \mathbf{N}(x - y\sqrt{n}) = \frac{\mathbf{N}(a - b\sqrt{n})}{\mathbf{N}(u - v\sqrt{n})} = \frac{N}{N} = 1.$$

Finally, $(a, b) \neq \pm(u, v)$ implies $a - b\sqrt{n} \neq \pm(u - v\sqrt{n})$. Thus $(x, y) \neq (\pm 1, 0)$. □

14.2. *The "Pell group"* In particular, the set of elements

$$\left\{ x + y\sqrt{n} \;\middle|\; \begin{array}{l} x, y \in \mathbf{Z}, \\ x^2 - ny^2 = 1 \end{array} \right\} \subseteq \mathbf{Z}[\sqrt{n}]$$

forms an infinite group under multiplication: for, if it contains $x + y\sqrt{n} \neq \pm 1$, then it also contains the powers $(x + y\sqrt{n})^k$ for all $k \in \mathbf{Z}$, and these will be pairwise distinct. Note that in this case, $(x + y\sqrt{n})^{-1} = x - y\sqrt{n}$.

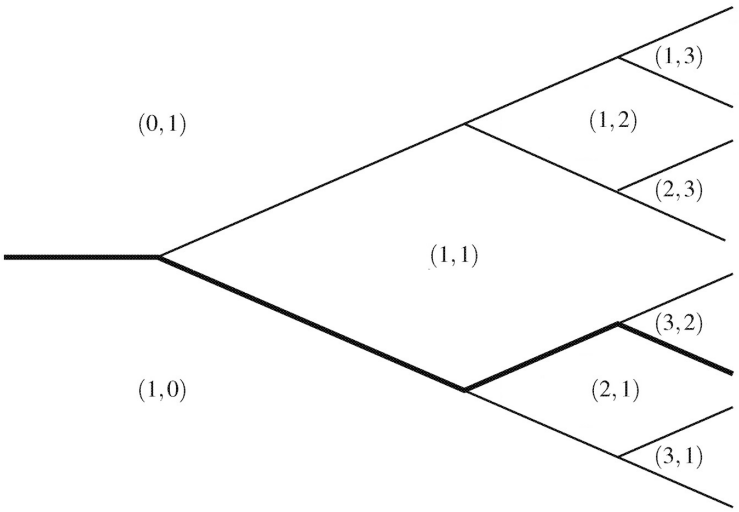
Corollary 14.3. *For squarefree $n \in \mathbf{N}$, the Pell equation $x^2 - ny^2 = 1$ has infinitely many solutions.*

14.3. *The topograph of a quadratic form* We mentioned earlier that $x^2 - ny^2$ is a special case of a broader class of polynomials, the binary quadratic forms $Ax^2 + Bxy + Cy^2$.

John Horton Conway found a beautiful way to visualize the structure among the values of a binary quadratic form on integers x, y. First draw an infinite binary tree in the plane. It divides the plane into regions, which we label by pairs $(x, y) \in \mathbf{Z}^2$. The rules are:

(1) We start with $(0, 1)$ and $(1, 0)$ at the far left.
(2) If a region touches two regions we've labeled (x, y') and (x', y'), then the new region is labeled $(x + x', y + y')$.

Thus:



Now in each region, replace the label (x, y) with the value $Ax^2 + Bxy + Cy^2$. The result is the *map* (in Conway's lingo, *topograph*) of the quadratic form. For example, Stillwell Figure 5.7 is the map of the quadratic form $x^2 - 3y^2$.

Theorem 14.4 (Conway)**.** *There is a unique "river" that divides the negative values from the positive values. Moreover, the values along both "riverbanks" are periodic.*