CHAPTER 31

Diophantine Approximation and Pell's Equation

From "A Friendly introduction to Number Theory" by Silverman

We now return to the problem of finding solutions to Pell's equation

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

As we observed in the last chapter, we should look for solutions among those pairs (x, y) making $\left|x - y\sqrt{D}\right|$ small, since any solution will to Pell's equation satisfy

$$\left|x - y\sqrt{D}\right| = \frac{1}{\left|x + y\sqrt{D}\right|} < \frac{1}{y}.$$

The idea we will use is to take two pairs for which $x^2 - Dy^2$ has the same value and "divide them."

An example will help illustrate what we mean. We'll take $D = 13$. Looking at the table in Chapter 30, we see that the pairs $(x_1, y_1) = (11, 3)$ and $(x_2, y_2) = (119, 33)$ are both solutions to the equation $x^2 - 13y^2 = 4$. We "divide" these two solutions as follows:

$$\begin{aligned}\frac{119 - 33\sqrt{13}}{11 - 3\sqrt{13}} &= \left(\frac{119 - 33\sqrt{13}}{11 - 3\sqrt{13}}\right)\left(\frac{11 + 3\sqrt{13}}{11 + 3\sqrt{13}}\right) \\ &= \frac{22 - 6\sqrt{13}}{4} \\ &= \frac{11}{2} - \frac{3}{2}\sqrt{13}.\end{aligned}$$

Voila! The pair $(11/2, 3/2)$ is a solution to Pell's equation $x^2 - 13y^2 = 1$. Unfortunately, as you may already have noticed, it is not a solution in integers. The difficulty is the appearance of that pesky 2 in the denominator. More precisely, notice that there was a 4 in the denominator coming from the fact that $11^2 - 3^2 \cdot 13 = 4$; and we were only able to cancel 2 out of the denominator.

Maybe if we look for more solutions to $x^2 - 13y^2 = 4$, we'll find one which allows us to cancel the entire 4 in the denominator. Searching for additional solutions, we eventually find (14159, 3927), and using this solution as our (x_2, y_2), we calculate

$$\frac{14159 - 3927\sqrt{13}}{11 - 3\sqrt{13}} = \frac{2596 - 720\sqrt{13}}{4} = 649 - 180\sqrt{13}.$$

Eureka! The Pell equation $x^2 - 13y^2 = 1$ has the solution in integers $(x, y) = (649, 180)$.

Why did the pairs (11, 3) and (14159, 3927) successfully lead to a solution in integers? It turns out that these pairs got rid of the 4 in the denominator because

$$11 \equiv 14159 \pmod 4 \qquad \text{and} \qquad 3 \equiv 3927 \pmod 4.$$

Armed with this crucial observation, we are finally ready to verify Pell's Equation Theorem as stated in Chapter 29. For your convenience, we restate it here.

Pell's Equation Theorem. *Let D be a positive integer which is not a perfect square. Then Pell's equation*

$$x^2 - Dy^2 = 1$$

always has solutions in positive integers. If (x_1, y_1) is the solution with smallest x_1, then every solution (x_k, y_k) can be obtained by taking powers

$$x_k + y_k\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^k \qquad \text{for } k = 1, 2, 3, \ldots.$$

VERIFICATION. Our first goal is to show that Pell's equation has at least one solution. Dirichlet's Diophantine Approximation Theorem (Chapter 29) tells us that there are infinitely many pairs of positive integers (x, y) which satisfy the inequality

$$\left|x - y\sqrt{D}\right| < \frac{1}{y}.$$

Suppose that (x, y) is such a pair. We want to estimate the size of

$$|x^2 - Dy^2| = \left|x - y\sqrt{D}\right| \cdot \left|x + y\sqrt{D}\right|.$$

The first factor on the right is less than $1/y$. What can we say about the second factor?

Using the fact that $\left|x - y\sqrt{D}\right| < 1/y$, we see that x is bounded by

$$x < y\sqrt{D} + 1/y,$$

and so

$$x + y\sqrt{D} < \left(y\sqrt{D} + 1/y\right) + y\sqrt{D} < 2y\sqrt{D} + 1/y < 3y\sqrt{D}.$$

Multiplying both sides of this last inequality by $\left|x - y\sqrt{D}\right|$ gives

$$|x^2 - Dy^2| = \left|x - y\sqrt{D}\right| \cdot 3y\sqrt{D} < (1/y) \cdot \left(3y\sqrt{D}\right) = 3\sqrt{D}.$$

To recapitulate, we have shown that every solution in positive integers (x, y) to the inequality

$$\left|x - y\sqrt{D}\right| < 1/y$$

also satisfies the estimate

$$|x^2 - Dy^2| < 3\sqrt{D}.$$

We're now going to use a variant of the Pigeonhole Principle introduced in the last chapter. Our pigeons will be the the positive integer solutions (x, y) to $\left|x - y\sqrt{D}\right| < 1/y$. Dirichlet's Diophantine Approximation Theorem (Chapter 30) tells us that there are infinitely many pigeons.[†] For pigeonholes we will take the integers

$$-T, -T+1, -T+2, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots, T-2, T-1, T,$$

where T is the largest integer less than $3\sqrt{D}$. We know that if (x, y) is a pigeon, then the quantity $x^2 - Dy^2$ is between $-T$ and T, so we can assign the pigeon (x, y) to the pigeonhole numbered $x^2 - Dy^2$.

[†] Don't worry, you won't be assigned the job of feeding the pigeons, nor will you have to clean out the pigeonholes.

We've now taken infinitely many pigeons and stuffed them into a finite collection of pigeonholes![‡] Clearly there must be some pigeonhole which contains infinitely many pigeons. Say pigeonhole M contains infinitely many pigeons. In mathematical terms, this means that the "Pell-like" equation

$$x^2 - Dy^2 = M$$

has infinitely many solutions in positive integers (x, y). We'll write the list of solutions as

$$(X_1, Y_1), (X_2, Y_2), (X_3, Y_3), (X_4, Y_4), \ldots.$$

Keep firmly in mind that this list continues indefinitely.

Following the path suggested by the example at the beginning of this chapter, we are going to look for two solutions (X_j, Y_j) and (X_k, Y_k) which also satisfy

$$X_j \equiv X_k \pmod{M} \qquad \text{and} \qquad Y_j \equiv Y_k \pmod{M}.$$

We'll find them by once again using the Pigeonhole Principle. This time our pigeons will be the solutions $(X_1, Y_1), (X_2, Y_2), \ldots$, so we have infinitely many pigeons. The pigeonholes will be the pairs

$$(A, B) \qquad \text{with } 0 \le A < M \text{ and } 0 \le B < M,$$

so there are M^2 pigeonholes. We assign each pigeon (X_i, Y_i) to a pigeonhole by reducing the numbers X_i and Y_i modulo M. In other words, the pigeon (X_i, Y_i) is assigned to the pigeonhole (A, B) by choosing A and B to satisfy

$$X_i \equiv A \pmod{M}, \quad Y_i \equiv B \pmod{M}, \quad 0 \le A, B < M.$$

We have again managed to stuff infinitely many pigeons into a finite number of pigeonholes, so again there must be some pigeonhole containing infinitely many pigeons. In particular, we can find two different pigeons (X_j, Y_j) and (X_k, Y_k) nesting in the same hole. Mathematically, we have

[‡] This is a task akin to, but messier than, that of getting infinitely many angels to dance on the head of a pin. Which brings up a question you may care to ponder: "To what extent is the Pigeonhole Principle an Obvious Truth, and to what extent is it an Act of Faith?"

produced two pairs of positive integers (X_j, Y_j) and (X_k, Y_k) with the following properties:

$$\begin{aligned} X_j &\equiv X_k \pmod{M}, & X_j^2 - DY_j^2 &= M, \\ Y_j &\equiv Y_k \pmod{M}, & X_k^2 - DY_k^2 &= M. \end{aligned}$$

As described earlier in this chapter, we now expect to get a solution (x, y) to Pell's equation $x^2 - Dy^2 = 1$ by setting

$$x + y\sqrt{D} = \frac{X_j - Y_j\sqrt{D}}{X_k - Y_k\sqrt{D}} = \frac{(X_jX_k - Y_jY_kD) + (X_jY_k - X_kY_j)\sqrt{D}}{X_k^2 - DY_k^2}.$$

In other words, we claim that the formulas

$$x = \frac{X_jX_k - Y_jY_kD}{M} \qquad \text{and} \qquad y = \frac{X_jY_k - X_kY_j}{M}$$

give a solution to $x^2 - Dy^2 = 1$ in integers.

First we check that (x, y) satisfies Pell's equation.

$$\begin{aligned} x^2 - Dy^2 &= \left(\frac{X_jX_k - Y_jY_kD}{M}\right)^2 - D\left(\frac{X_jY_k - X_kY_j}{M}\right)^2 \\ &= \frac{(X_j^2 - DY_j^2)(X_k^2 - DY_j^2)}{M^2} \\ &= 1. \end{aligned}$$

Second, we must verify that x and y are integers. Using the congruences $X_j \equiv X_k \pmod{M}$ and $Y_j \equiv Y_k \pmod{M}$, we find that the "numerators" of x and y satisfy

$$\begin{aligned} X_jX_k - Y_jY_kD &\equiv X_j^2 - Y_j^2D = M \equiv 0 \pmod{M}, \\ X_jY_k - X_kY_j &\equiv X_jY_j - X_jY_j \equiv 0 \pmod{M}. \end{aligned}$$

Thus, the numerators are divisible by M, so the M's in the denominators can be canceled. This shows that x and y are indeed integers, so we have completed our task of finding an integer solution to Pell's equation $x^2 - Dy^2 = 1$. Of course, if either x or y is negative, we can always replace them by $-x$ or $-y$, thereby finding a solution to Pell's equation in positive integers. This completes the verification of the first half of Pell's Equation Theorem.

For the second half, we let (x_1, y_1) be the solution with smallest x_1, and we need to show that every solution is obtained by taking powers of $x_1 + y_1\sqrt{D}$. As you will see, the proof of this fact is very similar to the proof we gave in Chapter 28 when $D = 2$. We suppose that (u, v) is some solution with $u > x_1$, and we want to find another solution (s, t) satisfying

$$u + v\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)\left(s + t\sqrt{D}\right) \qquad \text{and} \qquad s < u.$$

The new solution (s, t) is determined by setting

$$u + v\sqrt{D} = (x_1s + y_1Dt) + (y_1s + x_1t)\sqrt{D},$$

so we need to solve the simultaneous equations

$$u = x_1s + y_1Dt \qquad \text{and} \qquad v = y_1s + x_1t$$

for s and t. A little bit of algebra gives the solutions

$$s = x_1u - y_1Dv \qquad \text{and} \qquad t = -y_1u + x_1v,$$

where we have used the fact that $x_1^2 - Dy_1^2 = 1$. We are left to check that (s, t) is a solution, that s and t are positive, and that $s < u$.

To see that (s, t) is a solution, we compute

$$\begin{aligned} s^2 - Dt^2 &= (x_1u - y_1Dv)^2 - D(-y_1u + x_1v)^2 \\ &= (x_1^2 - Dy_1)^2(u^2 - Dv^2) \\ &= 1. \end{aligned}$$

Next we observe that

$$u^2 = 1 + Dv^2 > Dv^2$$

and

$$\left(x_1 - y_1\sqrt{D}\right)\left(x_1 + y_1\sqrt{D}\right) = 1 > 0,$$

from which we deduce that

$$u > \sqrt{D}v \qquad \text{and} \qquad x_1 - y_1\sqrt{D} > 0.$$

Using these inequalities, we find that

$$s = x_1u - y_1Dv > x_1\sqrt{D}v - y_1Dv = \left(x_1 - y_1\sqrt{D}\right)\sqrt{D}v > 0,$$

which shows that s is positive.

In order to show that t is also positive, we start with the following chain of reasoning:

$u > x_1$	We assumed this.
$u^2 > x_1^2$	Square both sides.
$(x_1^2 - Dy_1^2)u^2 > x_1^2$	Since we know $x_1^2 - Dy_1^2 = 1$.
$x_1^2(u^2 - 1) > Dy_1^2u^2$	A little algebra.
$Dx_1^2v^2 > Dy_1^2u^2$	Since we know $u^2 - Dv^2 = 1$.
$x_1v > y_1u$	Divide by D and take square roots.

This final inequality immediately implies that

$$t = -y_1u + x_1v > 0.$$

Finally, we observe that

$$u = x_1s + y_1Dt$$

is certainly larger than s, since x_1, s, y_1, D, and t are all positive integers. We have now shown that if (u, v) is a positive integer solution to Pell's equation

$$x^2 - Dy^2 = 1$$

with $u > x_1$, then there is another positive integer solution (s, t) which is determined by the formula

$$u + v\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)\left(s + t\sqrt{D}\right)$$

and which satisfies $s < u$.

Suppose that $s > x_1$. Then we can repeat the procedure, starting with (s, t), to find yet another solution (q, r) with $q < s$. And so on. In this way we will produce a list of solutions

$$(u, v), (u_1, v_1), (u_2, v_2), (u_3, v_3), \ldots$$

with

$$u > u_1 > u_2 > u_3 > \cdots,$$

where successive solutions are related by the formula

$$u_{i+1} + v_{i+1}\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)\left(u_i + v_i\sqrt{D}\right).$$

But the u_i's can't decrease indefinitely, since they are positive integers. Further, the smallest solution is (x_1, y_1), so every $u_i \geq x_1$. Eventually some u_i will equal x_1 and the list will stop. Let's suppose that the list looks like

$$(u, v), (u_1, v_1), (u_2, v_2), (u_3, v_3), \ldots, (u_{k-1}, v_{k-1}), (u_k, v_k) = (x_1, y_1).$$

Then we find that

$$\begin{aligned} u + v\sqrt{D} &= \left(x_1 + y_1\sqrt{D}\right)\left(u_1 + v_1\sqrt{D}\right) \\ &= \left(x_1 + y_1\sqrt{D}\right)^2\left(u_2 + v_2\sqrt{D}\right) \\ &\vdots \\ &= \left(x_1 + y_1\sqrt{D}\right)^k\left(u_k + v_k\sqrt{D}\right) \\ &= \left(x_1 + y_1\sqrt{D}\right)^{k+1} \qquad \text{since } (u_k, v_k) = (x_1, y_1). \end{aligned}$$

This shows that $u + v\sqrt{D}$ is a power of $x_1 + y_1\sqrt{D}$, which completes the verification of Pell's Equation Theorem.

Exercise 31.1. In this chapter we have shown that Pell's equation $x^2 - Dy^2 = 1$ always has a solution in positive integers. This exercise explores what happens if the 1 on the right-hand side is replaced by some other number.
(a) For each $2 \leq D \leq 15$ which is not a perfect square, determine whether or not the equation $x^2 - Dy^2 = -1$ has a solution in positive integers. Can you determine a pattern which will let you predict for which D's it has a solution?
(b) If (x_0, y_0) is a solution to $x^2 - Dy^2 = -1$ in positive integers, show that $(x_0^2 + Dy_0^2, 2x_0y_0)$ is a solution to Pell's equation $x^2 - Dy^2 = 1$.
(c) Find a solution to $x^2 - 41y^2 = -1$, by plugging in $y = 1, 2, 3, \ldots$ until you find a value for which $41y^2 - 1$ is a perfect square. (You won't need to go very far.) Use your answer and (b) to find a solution to Pell's equation $x^2 - 41y^2 = 1$ in positive integers.
(d) If (x_0, y_0) is a solution to the equation $x^2 - Dy^2 = M$, and if (x_1, y_1) is a solution to Pell's equation $x^2 - Dy^2 = 1$, show that $(x_0x_1 + Dy_0y_1, x_0y_1 + y_0x_1)$ is also a solution to the equation $x^2 - Dy^2 = M$. Use this to find 5 different solutions in positive integers to the equation $x^2 - 2y^2 = 7$.