THEOREM (EXISTENCE OF SOLUTIONS TO PELL'S EQUATION): Let D be a positive integer that is not a perfect square. Then the Pell's equation $x^2 - Dy^2 = 1$ has a positive solution.

THEOREM (SOLUTIONS TO PELL'S EQUATION ARE CONVERGENTS): Let D be a positive integer that is not a perfect square. For every positive solution (a, b) to the Pell's equation $x^2 - Dy^2 = 1$, there is some $k \in \mathbb{Z}_{\geq 0}$ such that the ratio $\frac{a}{b}$ is a convergent C_k of the continued fraction of $\sqrt{D}$.

THEOREM (GOOD APPROXIMATIONS ARE CONVERGENTS): Let r be an irrational real number. If p, q are integers with $q > 0$ such that $|r - \frac{p}{q}| < \frac{1}{2q^2}$, then there is some $k \in \mathbb{Z}_{\geq 0}$ such that $\frac{p}{q}$ is a convergent C_k of the continued fraction of r.

(1) Solving Pell's equation completely:
  (a) Given the theorems above, devise a method to find the smallest positive solution to the Pell's equation $x^2 - Dy^2 = 1$.
  (b) Apply your method for $D = 2$, $D = 3$, $D = 10$, and $D = 21$. Compare your results for $D = 2$ and $D = 3$ to what you found last time by trial and error.
  (c) Give a formula for all positive solutions to Pell's equation for $D = 10$ and $D = 21$.

(a) Compute the continued fraction for $\sqrt{D}$, and test whether $p_k^2 - Dq_k^2 = 1$ for the sequence of convergents $C_k = \frac{p_k}{q_k}$. The first one that works is the smallest positive solution of Pell's equation.
(b) For $D = 2$, the convergent $C_1 = \frac{3}{2}$ yields the smallest solution $(3, 2)$.
For $D = 3$, the convergent $C_1 = \frac{2}{1}$ yields the solution $(2, 1)$.
For $D = 10$, the convergent $C_1 = \frac{19}{6}$ yields the solution $(19, 6)$.
For $D = 21$, the convergent $C_5 = \frac{55}{12}$ yields the solution $(55, 12)$.
(c) For $D = 10$, the positive solutions $(x_k, y_k)$are given by the coefficients of $x_k + y_k\sqrt{10} = (19 + 6\sqrt{10})^k$.
For $D = 21$, the positive solutions $(x_k, y_k)$are given by the coefficients of $x_k + y_k\sqrt{21} = (55 + 12\sqrt{21})^k$.

(2) Prove the Theorem (Solutions to Pell's equation are convergents) using the Theorem (Good approximations are convergents).

Suppose that (a, b) is a positive solution to the Pell's equation, so $a^2 - Db^2 = 1$. Dividing through by b^2,

$$\left| \left(\frac{a}{b}\right)^2 - D \right| < \frac{1}{b^2}.$$

Factoring the left-hand side, we get

$$\left| \frac{a}{b} - \sqrt{D} \right| \left| \frac{a}{b} + \sqrt{D} \right| < \frac{1}{b^2}, \quad \text{so} \quad \left| \frac{a}{b} - \sqrt{D} \right| < \frac{1}{b^2 \left| \frac{a}{b} + \sqrt{D} \right|}.$$

We claim that $\frac{a}{b} + \sqrt{D} > 2$ for any solution to Pell's equation. Indeed, $D \geq 2$ implies $\sqrt{D} > 1$ and $a > b$ implies $\frac{a}{b} > 1$ as well. Thus, from the equations above, we have

$$\left|\frac{a}{b} - \sqrt{D}\right| < \frac{1}{2b^2}.$$

By the Theorem (Good approximations are convergents), $\frac{a}{b}$ must be a convergent of $\sqrt{D}$.

(3) Proof of Theorem (Existence of solutions to Pell's equation):

(a) Use Dirichlet's approximation theorem to show that there are infinitely many pairs of integers (x_i, y_i) such that $|x_i^2 - Dy_i^2| < 2\sqrt{D} + 1$.

(b) Show that there is some integer m with $0 < |m| < 2\sqrt{D} + 1$ such that there are infinitely many pairs of integers (x_i, y_i) with $x_i^2 - Dy_i^2 = m$.

(c) Show that there is some integer m with $|m| < 2\sqrt{D} + 1$ and $a, b \in \mathbb{Z}$ such that there are infinitely many pairs of integers (x_i, y_i) with

$$\begin{cases} x_i^2 - Dy_i^2 = m \\ x_i \equiv a \pmod{|m|} \\ y_i \equiv b \pmod{|m|} \end{cases}.$$

(d) Given $i \neq j$ and x_i, x_j, y_i, y_j as in the previous part, show that $\frac{x_j + y_j\sqrt{D}}{x_i + y_i\sqrt{D}}$ is an element of $\mathbb{Z}[\sqrt{D}]$.

(e) Complete the proof of the Theorem.

(a) By Dirichlet's approximation theorem, there are infinitely many p/q such that

$$\left|\frac{p}{q} - \sqrt{D}\right| < \frac{1}{q^2},$$

given by the convergents of the continued fraction of $\sqrt{D}$. Then

$$\left|\left(\frac{p}{q}\right)^2 - D\right| = \left|\frac{p}{q} - \sqrt{D}\right|\left|\frac{p}{q} + \sqrt{D}\right| < \frac{\left|\frac{p}{q} + \sqrt{D}\right|}{q^2},$$

so

$$|p^2 - Dq^2| < \frac{p}{q} + \sqrt{D}.$$

Since $q \geq 1$, we have that $\frac{p}{q} - \sqrt{D} \leq 1$ by Dirichlet, so $\frac{p}{q} + \sqrt{D} < 2\sqrt{D} + 1$. (Note that equality is impossible since $\sqrt{D}$ is irrational.)

For p/q as above, taking $x_i = p$, $y_i = q$, we get infinitely many pairs of integers with $|x_i^2 - Dy_i^2| < 2\sqrt{D} + 1$.

(b) There are finitely many integers m such that $|m| < 2\sqrt{D} + 1$, so by the pigeonhole principle, there must be some m such that there are infinitely many (x_i, y_i) with $x_i^2 - Dy_i^2 = m$.

(c) Take m as in the previous part; this m is nonzero since $\sqrt{D}$ is irrational. For each element in the sequence obtained in the previous part, it corresponds to one element of $\mathbb{Z}_{|m|} \times \mathbb{Z}_{|m|}$ by taking the congruences

$$\begin{cases} x_i \equiv a \pmod{|m|} \\ y_i \equiv b \pmod{|m|} \end{cases}.$$

Since $\mathbb{Z}_{|m|} \times \mathbb{Z}_{|m|}$ is finite, by the pigeonhole principle, there must be some element of $\mathbb{Z}_{|m|} \times \mathbb{Z}_{|m|}$ corresponding to infinitely many elements of the sequence. This gives the statement.

(d) Given $i \neq j$ and x_i, x_j, y_i, y_j as in the previous part, note that

$$N(x_j + y_j\sqrt{D}) = N(x_i + y_i\sqrt{D}) = m.$$

We can write

$$\frac{x_j + y_j\sqrt{D}}{x_i + y_i\sqrt{D}} = \frac{1}{m}(x_j + y_j\sqrt{D})(x_i - y_i\sqrt{D}) = \frac{1}{m}((x_i x_j - y_i y_j D) + (x_j y_i - x_i y_j)\sqrt{D}).$$

We claim that

$$x_i x_j - y_i y_j D \equiv x_j y_i - x_i y_j \equiv 0 \pmod{|m|}.$$

Indeed,

$$\begin{aligned} x_i x_j - y_i y_j D &\equiv a^2 - b^2 D \equiv m \equiv 0 && \pmod{|m|} \\ x_j y_i - x_i y_j &\equiv ab - ab \equiv 0 && \pmod{|m|}. \end{aligned}$$

This implies that the coefficients of $(x_i x_j - y_i y_j D) + (x_j y_i - x_i y_j)\sqrt{D}$ are divisible by m, so the number above is an element of $\mathbb{Z}[\sqrt{D}]$.

(e) In the previous part, we have found an element $\alpha \in \mathbb{Z}[\sqrt{D}]$ such that $\alpha(x_i + y_i\sqrt{D}) = x_j + y_j\sqrt{D}$ and

$$N(x_j + y_j\sqrt{D}) = N(x_i + y_i\sqrt{D}) = m \neq 0.$$

Thus, by the lemma, we much have $N(\alpha) = 1$. This yields the solution we seek.

(4) Prove[1] Theorem (Good approximations are convergents).

Suppose that p/q is not a convergent of r. If $q = q_k$ for some k but $p \neq p_k$, then

$$\left| r - \frac{p}{q_k} \right| \geq \left| \left| \frac{p}{q_k} - \frac{p_k}{q_k} \right| - \left| r - \frac{p_k}{q_k} \right| \right|.$$

Since $\left| \frac{p}{q_k} - \frac{p_k}{q_k} \right| \geq \frac{1}{q_k}$ and $\left| r - \frac{p_k}{q_k} \right| < \frac{1}{q_k^2}$ by Dirichlet approximation Theorem, the difference above is at least $\frac{q_k - 1}{q_k^2} > \frac{1}{2q_k^2}$, contradicting the hypotheses. Thus, we must have $q \neq q_k$ for any k, so $q_{k-1} < q < q_k$ for some k.

By hypothesis,

$$\left| r - \frac{p}{q} \right| < \frac{1}{2q^2} < \frac{1}{2q q_{k-1}}.$$

Following the proof of Problem set #5 problem #4, by replacing k by $k-1$ in steps (a)–(d), we see that

$$|q_{k-1} r - p_{k-1}| \leq |qr - p|.$$

Since $|qr - p| < 1/2q$, by hypothesis, we get

$$\left| r - \frac{p_{k-1}}{q_{k-1}} \right| \leq \frac{1}{2q q_{k-1}}.$$

[1] Hint: If not, we can assume $q_{k-1} < q < q_k$ for some k. In Problem set #5 problem #4, the same proof with $k-1$ in place of k in parts (a)–(d) shows that, under the same hypotheses, $|qr - p| \geq |q_{k-1} r - p_{k-1}|$. Then show that $|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}| < \frac{1}{q q_{k-1}}$.

Then, by the triangle inequality,

$$\left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| \leq \left|r - \frac{p}{q}\right| + \left|r - \frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{2qq_{k-1}} + \frac{1}{2qq_{k-1}} = \frac{1}{qq_{k-1}}.$$

Clearing denominators, this forces $\left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| = 0$. This contradicts the assumption that p/q is not a convergent of r.