Math 4527 (Number Theory 2)

Lecture #8 of 38 $\sim$ February 4, 2021

Pell's Equation (Part 2)

- Pell's Equation and Rational Approximation
- Proofs of Some Results
- Computing Solutions to Pell's Equation

This material represents §6.3.1-6.3.2 from the course notes.

Pell's, I

We continue our study of Pell's equation $x^2 - Dy^2 = r$.

- We can recast much of our discussion in terms of the norm map on $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \,:\, a, b \in \mathbb{Z}\}$, defined as via $N(a + b\sqrt{D}) = a^2 - Db^2$.
- The norm map is always integer-valued and is also multiplicative.
- As we observed, solving $x^2 - Dy^2 = r$ is equivalent to solving $N(x + y\sqrt{D}) = r$.
- We also pointed out last time that an element $\alpha = a + b\sqrt{D}$ is a unit in $\mathbb{Z}[\sqrt{D}]$ if and only its norm $N(\alpha) = a^2 - Db^2$ is 1 or -1.

Pell's E, II

As we will show, $\mathbb{Z}[\sqrt{D}]$ always has a "smallest" nontrivial unit:

Definition

For a fixed positive squarefree D, a fundamental solution (x_1, y_1) to Pell's equation is a pair (x_1, y_1) of positive integers such that $x_1^2 - Dy_1^2 = \pm 1$ and $x_1 + y_1\sqrt{D}$ is minimal.

The fundamental unit of $\mathbb{Z}[\sqrt{D}]$ is $u = x_1 + y_1\sqrt{D}$.

Pell's Eq, III

Examples: By searching for solutions to $x^2 - Dy^2 = \pm 1$ we can generate fundamental units for various small nonsquare D:

D	2	3	5	6	7
Fund. Unit	$1+\sqrt{2}$	$2+\sqrt{3}$	$2+\sqrt{5}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$
Norm	-1	1	-1	1	1
D	8	10	11	12	13
Fund. Unit	$3+\sqrt{8}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$7+2\sqrt{12}$	$18+5\sqrt{13}$
Norm	1	-1	1	1	-1
D	14	15	17	18	19
Fund. Unit	$15+4\sqrt{14}$	$4+\sqrt{15}$	$4+\sqrt{17}$	$17+4\sqrt{18}$	HW #3
Norm	1	1	-1	1	HW #3

Pell's Equ, IV

One of the other key ideas for solving Pell's equation is the observation that if $x^2 - Dy^2$ is small and x, y are positive, then x/y is a good approximation to $\sqrt{D}$.

- To illustrate, suppose we have a solution of $x^2 - Dy^2 = 1$.
- Dividing by y^2 yields $(x/y)^2 - D = 1/y^2$, and now solving for x/y gives $x/y = \sqrt{D + 1/y^2} = \sqrt{D} \cdot \sqrt{1 + 1/(Dy^2)} \approx \sqrt{D} \cdot (1 + 1/(2Dy^2)) = \sqrt{D} + 1/(2y^2\sqrt{D})$ using the linearization $\sqrt{1+z} \approx 1 + z/2$.
- In fact, the linearization is an overestimate since $(1 + z/2)^2 = 1 + z + z^2/4 > 1 + z$.
- Thus, we obtain the inequality $\left| \frac{x}{y} - \sqrt{D} \right| < \frac{1}{2y^2\sqrt{D}}$.

Pell's Equa, II

The point is that if $x^2 - Dy^2 = 1$, then x/y is a good approximation to $\sqrt{D}$: $\left|\frac{x}{y} - \sqrt{D}\right| < \frac{1}{2y^2\sqrt{D}}$.

- In fact, the approximation is extremely good. From our results on continued fractions and rational approximation, we know that if α is irrational and p/q has the property that $|\alpha - p/q| < 1/(2q^2)$, then in fact p/q is a continued fraction convergent to α.
- So, since $\sqrt{D} > 1$, this means any solution to $x^2 - Dy^2 = 1$ must arise as a continued fraction convergent to $\sqrt{D}$.

Pell's Equat, III

We can see quite explicitly that the solutions to $x^2 - 2y^2 = 1$ arise from continued fraction convergents to
$\sqrt{2} = [1, \overline{2}] = [1, 2, 2, 2, \dots]$.

- The first few convergents are 1/1, 3/2, 7/5, 17/12, 41/29, 99/70, ... , which (as ordered pairs) have $x^2 - 2y^2$ respectively equal to -1, 1, -1, 1, -1, 1, ...
- These convergents are precisely the solutions to $x^2 - 2y^2 = \pm 1$ we identified earlier.
- We remark also that the period of the continued fraction expansion here is equal to 1 and the fundamental unit corresponds to the convergent [1].

Pell's Equati, V

Let's try it out for $D = 3$.

- Here, we have $\sqrt{3} = [1, \overline{1, 2}] = [1, 1, 2, 1, 2, \ldots]$ with convergents 1/1, 2/1, 5/3, 7/4, 19/11, 26/15, 71/41, ...
- As ordered pairs, these convergents have $x^2 - 3y^2$ respectively equal to -2, 1, -2, 1, -2, 1, ...
- Here, we can see that we do not obtain any solutions to $x^2 - 3y^2 = -1$ (since in fact there are none as we proved earlier) but we do obtain solutions to $x^2 - 3y^2 = -2$ and $x^2 - 3y^2 = 1$.
- The period of the continued fraction expansion here is equal to 2, while the fundamental unit corresponds to the convergent $[1, 2]$.

Pell's Equatio, VI

Let's try $D = 7$.

- Here, we have $\sqrt{7} = [2, \overline{1, 1, 1, 4}] = [2, 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$ with convergents 2/1, 3/1, 5/2, 8/3, 37/14, 45/17, 82/31, 127/48, 590/223, ...
- As ordered pairs, these convergents have $x^2 - 7y^2$ respectively equal to -3, 2, -3, 1, -3, 2, -3, 1, -3, ...
- Here again we obtain no solutions to $x^2 - 3y^2 = -1$ but we do obtain solutions to $x^2 - 3y^2 = -3$, $x^2 - 3y^2 = 2$, and $x^2 - 3y^2 = 1$.
- The period of the continued fraction expansion here is equal to 4, while the fundamental unit corresponds to the convergent $[2, 1, 1, 1]$.

Pell's Equation, VII

Let's try one more: $D = 13$.

- Here, $\sqrt{13} = [3, \overline{1, 1, 1, 6}] = [3, 1, 1, 1, 1, 6, \dots]$ with convergents 3/1, 4/1, 7/2, 11/3, 18/5, 119/33, 137/38, 256/71, 393/109, 649/180, ...
- As ordered pairs, these convergents have $x^2 - 13y^2$ respectively equal to -4, 3, -3, 4, -1, 4, -3, 3, -4, 1, ...
- Here we obtain solutions to $x^2 - 13y^2 = r$ for $r = -4, -3, -1, 1, 3, 4$.
- The period of the continued fraction expansion here is equal to 4, while the fundamental unit corresponds to the convergent $[3, 1, 1, 1, 1]$.

It appears that the fundamental unit is obtained after one period of the continued fraction expansion, regardless of whether it has norm 1 or -1. Let's prove this!

Pell's Equation C, VIII

Theorem (Pell's Equation, Part 1)

Let D be a positive squarefree integer. Then the following hold:

1. *Let r be an integer with $r^2 < D$. If x and y are positive integers with $x^2 - Dy^2 = r$, then x/y is a continued fraction convergent to $\sqrt{D}$.*
2. *$x^2 - Dy^2 = 1$ always has a nontrivial integer solution.*
3. *The ring $\mathbb{Z}[\sqrt{D}]$ has a well-defined fundamental unit $u = x_1 + y_1\sqrt{D}$. Furthermore, if w is an arbitrary unit in $\mathbb{Z}[\sqrt{D}]$, then $w = \pm u^n$ for some integer n (possibly negative).*
4. *If $u = x_1 + y_1\sqrt{D}$ is the fundamental unit in $\mathbb{Z}[\sqrt{D}]$, then if we define $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$ for nonnegative integers n, then (x_n, y_n) is a solution to $x^2 - Dy^2 = \pm 1$, and these are all of the solutions up to changing the signs of x_n or y_n.*

Pell's Equation Co, IX

Theorem (Pell's Equation, Part 2)

Let $D > 0$ be squarefree, with $\sqrt{D} = [a_0, \ldots, a_n, \alpha_{n+1}]$, and take $p_n/q_n = [a_0, a_1, \ldots, a_n]$ to be the nth convergent. Define the sequences A_n and C_n by setting $A_0 = 0$ and $C_0 = 1$, and for $n \geq 1$ set $A_{n+1} = a_n C_n - A_n$ and $C_{n+1} = (D - A_{n+1}^2)/C_n$.

5. *The continued fraction expansion of $\sqrt{D}$ is periodic and of the form $[a_0, \overline{a_1, a_2, \cdots, a_{k-1}, 2a_0}]$ with $a_0 = \lfloor \sqrt{D} \rfloor$.*
6. *The sequences A_n and C_n are integer-valued, $\alpha_n = (A_n + \sqrt{D})/C_n$, $\quad p_n p_{n-1} - D q_n q_{n-1} = (-1)^n A_{n+1}$, and $p_n^2 - D q_n^2 = (-1)^{n+1} C_{n+1}$.*
7. *With notation as in (5), the fundamental unit of $\mathbb{Z}[\sqrt{D}]$ is $p_{k-1} + q_{k-1}\sqrt{D}$. Its norm is -1 when k is odd and its norm is $+1$ when k is even.*

Pell's Equation Con, X

1. Let r be an integer with $r^2 < D$. If x and y are positive integers with $x^2 - Dy^2 = r$, then x/y is a continued fraction convergent to $\sqrt{D}$.

Proof:

- First suppose $r > 0$. We show $|x/y - \sqrt{D}| < 1/(2y^2)$, which implies x/y is a continued fraction convergent to $\sqrt{D}$.
- Using $\sqrt{1+t} < 1 + t/2$ for $t > 0$ yields $x/y = \sqrt{D}\sqrt{1 + r/(Dy^2)} < \sqrt{D}(1 + r/(2Dy^2))$.
- Thus, $\left|\frac{x}{y} - \sqrt{D}\right| < \frac{r}{2\sqrt{D}y^2} \le \frac{1}{2y^2}$, as claimed.
- If $r < 0$, then $x^2 - Dy^2 = r$ implies $y^2 - (1/D)x^2 = |r|/D$.
- Then since $(|r|/D)^2 < 1/D$, by the argument above (which does not require D to be integral) we see y/x is a continued fraction convergent to $1/\sqrt{D}$, so x/y is a continued fraction convergent to its reciprocal, $1/(1/\sqrt{D}) = \sqrt{D}$.

Pell's Equation Cont, XI

2. The equation $x^2 - Dy^2 = 1$ always has a nontrivial solution in integers (x, y).

Proof:

- If p/q is a continued fraction convergent to $\sqrt{D}$, then p/q is within $1/q^2 \leq 1$ of $\sqrt{D}$, so $|p/q - \sqrt{D}| < 1/q^2$ and $|p/q + \sqrt{D}| < 1 + 2\sqrt{D}$.
- Then $$\left|p^2 - Dq^2\right| = q^2 \, |p/q - \sqrt{D}| \cdot |p/q + \sqrt{D}| < q^2 \cdot (1/q^2) \cdot (1 + 2\sqrt{D}) = 1 + 2\sqrt{D}.$$
- Since $\sqrt{D}$ is irrational, there are an infinite number of convergents but only a finite number of possible values for $p^2 - Dq^2$.
- Therefore, by the pigeonhole principle, there is some r such that $p^2 - Dq^2 = r$ has infinitely many solutions. Choose such an r.

Pell's Equation Conti, XII

2. The equation $x^2 - Dy^2 = 1$ always has a nontrivial solution in integers (x, y).

<u>Proof</u> (continued):

- Select r such that $p^2 - Dq^2 = r$ has infinitely many solutions.
- Then there are only finitely many possible pairs for the reduction of (p, q) modulo r, so again by pigeonhole there are two distinct convergents x/y and s/t such that $x^2 - Dy^2 = s^2 - Dt^2 = r$, $x \equiv s \pmod{r}$, and $y \equiv t \pmod{r}$.
- Now we compute $u = \frac{x+y\sqrt{D}}{s+t\sqrt{D}} = \frac{xs-Dyt}{r} + \frac{-xt+ys}{r}\sqrt{D}$.
- Observe that $xs - Dyt \equiv x^2 - Dy^2 \equiv 0 \pmod{r}$ and $-xt + ys \equiv 0 \pmod{r}$, so in fact $u \in \mathbb{Z}[\sqrt{D}]$.
- But $N(u) = \frac{N(x+y\sqrt{D})}{N(s+t\sqrt{D})} = 1$, so u is a unit in $\mathbb{Z}[\sqrt{D}]$ and

$\left(\frac{xs - Dyt}{r}, \frac{-xt + ys}{r}\right)$ is a nontrivial solution to Pell's equation.

Pell's Equation Contin, XIII

3. The ring $\mathbb{Z}[\sqrt{D}]$ has a well-defined fundamental unit $u = x_1 + y_1\sqrt{D}$. Furthermore, if w is an arbitrary unit in $\mathbb{Z}[\sqrt{D}]$, then $w = \pm u^n$ for some integer n (possibly negative).

Proof:

- The fundamental unit is well-defined by (2), since we are assured of the existence of at least one solution to $x^2 - Dy^2 = \pm 1$. Observe (trivially) that because $u = x_1 + y_1\sqrt{D}$ with x_1, y_1 positive, we have $u > 1$.
- If w is any arbitrary unit, then by scaling by -1 if necessary, we may assume w is positive.
- Then there exists a unique integer n such that $w \in [u^n, u^{n+1})$ since u is a real number greater than 1 and these intervals $[u^n, u^{n+1})$ partition the interval $(0, \infty)$.

Pell's Equation Continu, XIV

3. The ring $\mathbb{Z}[\sqrt{D}]$ has a well-defined fundamental unit $u = x_1 + y_1\sqrt{D}$. Furthermore, if w is an arbitrary unit in $\mathbb{Z}[\sqrt{D}]$, then $w = \pm u^n$ for some integer n (possibly negative).

Proof (continued):

- For $w \in [u^n, u^{n+1})$, we see $w \cdot u^{-n} \in [1, u)$, and $w \cdot u^{-n}$ is also a unit in $\mathbb{Z}[\sqrt{D}]$.
- If this unit $x + y\sqrt{D}$ were not equal to 1, then (possibly after flipping signs on one of its terms) it would yield a positive solution (x, y) to Pell's equation $x^2 - Dy^2 = \pm 1$ such that $x + y\sqrt{D} < u$.
- But this contradicts the minimality of u, so in fact we must have $w \cdot u^{-n} = 1$, whence $w = u^n$.
- Since we chose the sign of w to be positive, the units in $\mathbb{Z}[\sqrt{D}]$ are then of the form $\pm u^n$, as claimed.

Pell's Equation Continue, XV

3. The ring $\mathbb{Z}[\sqrt{D}]$ has a well-defined fundamental unit $u = x_1 + y_1\sqrt{D}$. Furthermore, if w is an arbitrary unit in $\mathbb{Z}[\sqrt{D}]$, then $w = \pm u^n$ for some integer n (possibly negative).

Remarks:

- This result says that the unit group structure of $\mathbb{Z}[\sqrt{D}]$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$: the $\mathbb{Z}/2\mathbb{Z}$ factor represents the $\pm$ sign while the $\mathbb{Z}$ factor represents the power n of the fundamental unit u.
- It is a special case of Dirichlet's unit theorem, which states that the unit group of the ring of algebraic integers in any algebraic number field K is a finitely generated abelian group whose rank is $r = r_1 + r_2 - 1$, where r_1 is the number of real embeddings of K and r_2 is the number of conjugate pairs of complex embeddings.
- Our result is the case $K = \mathbb{Q}(\sqrt{D})$, with $r_1 = 2$ and $r_2 = 0$.

Pell's Equation Continued, XVI

4. If $u = x_1 + y_1\sqrt{D}$ is the fundamental unit in $\mathbb{Z}[\sqrt{D}]$, then if we define $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$ for nonnegative integers n, then (x_n, y_n) is a solution to $x^2 - Dy^2 = \pm 1$, and these are all of the solutions up to changing the signs of x_n or y_n.

Proof:

- This is merely a rewriting of (3) in terms of solutions to $x^2 - Dy^2 = \pm 1$ rather than units in $\mathbb{Z}[\sqrt{D}]$.
- As we already showed, the solutions to $x^2 - Dy^2 = \pm 1$ correspond precisely to units $x + y\sqrt{D}$ in $\mathbb{Z}[\sqrt{D}]$.
- Since the units are $\pm(x_1 + y_1\sqrt{D})^n$ for arbitrary integers, and we can pick the signs of the coordinates using the $\pm$ and selecting n to be positive or negative, the full list of solutions is indeed as claimed.

Pell's Equation Continued F, XVII

5. The continued fraction expansion of $\sqrt{D}$ is periodic and of the form $[a_0, \overline{a_1, a_2, \cdots, a_{k-1}, 2a_0}]$ with $a_0 = \lfloor\sqrt{D}\rfloor$.

Proof:

- Consider instead the continued fraction expansion of $\alpha = a_0 + \sqrt{D}$ where $a_0 = \lfloor\sqrt{D}\rfloor$: we claim that it is $[\overline{2a_0, a_1, a_2, \ldots a_{k-1}}]$ for some positive integer k.
- The zeroth term is $\lfloor\alpha\rfloor = \lfloor a_0 + \sqrt{D}\rfloor = a_0 + \lfloor\sqrt{D}\rfloor = 2a_0$.
- It remains to see that the expansion is purely periodic; by our results, this is equivalent to saying that $\alpha = a_0 + \sqrt{D}$ is reduced. Clearly $\alpha > 1$, and also $-1/\overline{\alpha} = \dfrac{1}{\sqrt{D} - a_0} > 1$ because $0 < \sqrt{D} - a_0 < 1$ by the definition of a_0.
- Therefore, $\alpha = a_0 + \sqrt{D}$ is reduced, so its continued fraction is periodic with even starting term as claimed. The claims about the expansion of $\sqrt{D}$ are then immediate.

Pell's Equation Continued Fr, XVIII

I will skip the proofs of items (6) and (7) today because they are a bit messy (we'll do them next time, though!), so that we will have time to do some examples.

- The main fact to remember from (7) is that we can compute the fundamental unit of $\mathbb{Z}[\sqrt{D}]$ by truncating the continued fraction expansion of $\sqrt{D}$ right before its last term in the repeating part.
- Explicitly: if $\sqrt{D} = [a_0, \overline{a_1, a_2, \ldots, a_{k-1}, 2a_0}]$ and $p_{k-1}/q_{k-1} = [a_0, a_1, \ldots, a_{k-1}]$, then the fundamental unit of $\mathbb{Z}[\sqrt{D}]$ is $p_{k-1} + q_{k-1}\sqrt{D}$.
- The norm of the fundamental unit also dictates whether there is a solution to the negative Pell equation $x^2 - Dy^2 = -1$: if the norm is -1 then there is a solution (odd powers of the fundamental unit) while if the norm is $+1$ then there is no solution.

Pell's Equation Continued Fra, XIX

Now that we have all of these wonderful results, we can fairly easily compute the fundamental unit in $\mathbb{Z}[\sqrt{D}]$.

- All we need to do is find the continued fraction expansion of $\sqrt{D}$ until we hit the periodic part, and then compute the appropriate convergent.
- We then get a complete characterization of the solutions to the Pell equation(s) $x^2 - Dy^2 = \pm 1$ by taking powers of the fundamental unit.

Pell's Equation Continued Frac, XX

Example: Observe that $\sqrt{2} = [1, \overline{2}]$.

1. Find the fundamental unit of $\mathbb{Z}[\sqrt{2}]$ and describe all the units.
2. Find the smallest nontrivial solution to $x^2 - 2y^2 = 1$.
3. Find a solution to $x^2 - 2y^2 = 1$ with $x > 2021$.

Pell's Equation Continued Frac, XX

Example: Observe that $\sqrt{2} = [1, \overline{2}]$.

1. Find the fundamental unit of $\mathbb{Z}[\sqrt{2}]$ and describe all the units.
2. Find the smallest nontrivial solution to $x^2 - 2y^2 = 1$.
3. Find a solution to $x^2 - 2y^2 = 1$ with $x > 2021$.

- The desired convergent is $[1] = 1/1$ so we get the fundamental unit $u = 1 + \sqrt{2}$ — as we computed earlier, but which is also extremely easy to find anyway.
- Thus, the units of $\mathbb{Z}[\sqrt{2}]$ are $\pm(1 + \sqrt{2})^n$ for $n \in \mathbb{Z}$.
- Since the fundamental unit has norm -1, the smallest solution will be the square $(1 + \sqrt{2})^2 = 3 + 2\sqrt{2}$ yielding $(x, y) = (3, 2)$.
- To find a solution with $x > 2021$ we just have to take a big enough even power of the fundamental unit. The smallest one is $(1 + \sqrt{2})^{10} = 3363 + 2378\sqrt{2}$, so we get a solution $(x, y) = (3363, 2378)$.

Pell's Equation Continued Fract, XXI

Example: Observe that $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$.

1. Find the fundamental unit of $\mathbb{Z}[\sqrt{7}]$ and describe all the units.
2. Determine whether or not $x^2 - 7y^2 = -1$ has a solution.
3. Find the smallest two nontrivial solutions to $x^2 - 7y^2 = 1$.

Pell's Equation Continued Fract, XXI

Example: Observe that $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$.

1. Find the fundamental unit of $\mathbb{Z}[\sqrt{7}]$ and describe all the units.
2. Determine whether or not $x^2 - 7y^2 = -1$ has a solution.
3. Find the smallest two nontrivial solutions to $x^2 - 7y^2 = 1$.

- The desired convergent is $C_4 = [2, 1, 1, 1] = 8/3$, and we can indeed verify that $8^2 - 7 \cdot 3^2 = 1$.
- Thus, the fundamental unit is $u = 8 + 3\sqrt{7}$, and the full set of units is $\pm(8 + 3\sqrt{7})^n$ for $n \in \mathbb{Z}$.
- Since 4 is even, the norm of the fundamental unit is $+1$, so there are no solutions to $x^2 - 7y^2 = -1$.
- The smallest two units are $u = 8 + 3\sqrt{7}$ and $u^2 = 127 + 48\sqrt{7}$ yielding the pairs $(x, y) = (8, 3)$ and $(127, 48)$.

Pell's Equation Continued Fracti, XXII

<u>Example</u>: Observe that $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$.

1. Find the fundamental unit of $\mathbb{Z}[\sqrt{13}]$.
2. Determine whether or not $x^2 - 13y^2 = -1$ has a solution.
3. Find the smallest two nontrivial solutions to $x^2 - 13y^2 = 1$.

Pell's Equation Continued Fracti, XXII

Example: Observe that $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$.

1. Find the fundamental unit of $\mathbb{Z}[\sqrt{13}]$.
2. Determine whether or not $x^2 - 13y^2 = -1$ has a solution.
3. Find the smallest two nontrivial solutions to $x^2 - 13y^2 = 1$.

- The desired convergent is $C_5 = [3, 1, 1, 1, 1] = 18/5$, and we can indeed verify that $18^2 - 13 \cdot 5^2 = -1$.
- Thus, the fundamental unit is $u = 18 + 5\sqrt{13}$.
- Since 5 is odd, the norm of the fundamental unit is -1, so there are solutions to $x^2 - 13y^2 = -1$, and the smallest is $(x, y) = (18, 5)$.
- The smallest two units of positive norm are then $u^2 = 649 + 180\sqrt{13}$ and $u^4 = 842401 + 233640\sqrt{13}$ yielding the pairs $(x, y) = (649, 180)$ and $(842401, 233640)$.

Pell's Equation Continued Fractio, XXIII

We have reduced the seemingly quite difficult problem of solving Pell's equation $x^2 - Dy^2 = \pm 1$ to the very approachable problem of computing the continued fraction expansion of $\sqrt{D}$.

- Nonetheless, the method we have been using to find the continued fraction expansion for $\sqrt{D}$ requires a lot of computation, since each step requires us to keep track of the remainder term by rationalizing the resulting square root in the denominator.

Pell's Equation Continued Fraction, XXIV

Next time, I will explain the purpose of the sequences A_n and C_n that show up in parts (6) and (7) of the theorem.

- The point is that these sequences automatically encode the remainder term, because $\alpha_n = (A_n + \sqrt{D})/C_n$.
- The identities in (6) then give us an efficient way to calculate these sequences A_n and C_n recursively, along with the relation $a_n = \lfloor \alpha_n \rfloor = \lfloor (A_n + \sqrt{D})/C_n \rfloor$.
- Once we have the terms a_n from the continued fraction expansion, we can then compute the convergent terms p_n and q_n using the magic box procedure from a few lectures ago.

We can put all of these calculations together into a computational device that is sometimes called the "super magic box". It is quite easy to do by hand even for moderately large D, and is far more efficient than the "naive" numerical approach for computing a continued fraction.

Summary

We proved a bunch of things about the connections between continued fractions and the solutions to Pell's equation.

We did a few examples of computing fundamental units using continued fractions.

Next lecture: The super magic box, more Diophantine equations.