

## Lecture 20

### Rgt kqf le'E qpvlpwgf 'Ht cevkqpu 'S wcf t cvle 'Kt cvkqperkslgu

Review:  $x = [a_0, a_1, \dots]$ ,  $x_0 = x$ ,  $a_0 = x_0$ , write  $x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 \dots}} \Rightarrow a_1 = \frac{1}{x - a_0}$ ,  
 at any point  $x_n = [a_n, a_{n+1}, \dots]$ ,  $x = x_0 = [a_0, a_1, \dots, a_{n-1}, x_n]$ , convergents  
 $\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$ .  $x$  is rational if and only if continued fraction is finite  
 (terminates), and is quadratic irrational (ie., satisfies some quadratic equation)  
 if and only if continued fraction is periodic.

*Continuing proof (from last lecture).* Proving that if  $x$  is a quadratic irrational,  
 then continued fraction is periodic

**Step 0:**

$$x = \frac{a + \sqrt{b}}{c} \Rightarrow \frac{B_0 + \sqrt{d}}{C_0}$$

with  $B_0, C_0, d$  integers,  $d > 0$ ,  $C_0 | d - B_0^2$

**Step 1:** Defined  $B_i, C_i$  by induction.  $x_0 = x$ ,  $a_i = [x_i]$ ,  $x_i = \frac{B_i + \sqrt{d}}{C_i}$  defines  
 $B_i, C_i$  uniquely.  $x_{i+1} = \frac{1}{x_i - a_i} \Rightarrow B_{i+1} = a_i C_i - B_i$ ,  $C_{i+1} = \frac{d - B_{i+1}^2}{C_i}$ , with  
 $B_i, C_i \in \mathbb{Q}$ .

Strategy: show all  $B_i, C_i$  are integers, then show are bounded, therefore repeat.

**Step 2:** By induction show  $B_i, C_i$  are integers and that  $C_i | d - B_i^2$ . For  $i = 0$  it's  
 obvious, as  $B_0, C_0 \in \mathbb{Z}$ ,  $C_0 | d - B_0^2$  by step 0. Easy to see that  $B_{i+1}$  is integer.

$$\begin{aligned} C_{i+1} &= \frac{d - B_{i+1}^2}{C_i} \\ &= \frac{d - (a_i C_i - B_i)^2}{C_i} \\ &= \frac{d - B_i^2 - a_i^2 C_i^2 + 2a_i C_i B_i}{C_i} \\ &= \frac{d - B_i^2}{C_i} - a_i^2 C_i + 2a_i B_i \in \mathbb{Z} \end{aligned}$$

Finally show that  $C_{i+1} | d - B_{i+1}^2$  since  $\frac{d - B_{i+1}^2}{C_{i+1}} = C_i$  is an integer.

**Step 3:** Check that  $x_i = \frac{B_i + \sqrt{d}}{C_i}$  by induction. True for  $i = 0$ ,  $x_0 = \frac{B_0 + \sqrt{d}}{C_0}$ . For

$x_{i+1}$ ,

$$\begin{aligned}
x_{i+1} &= \frac{1}{x_i - a_i} \\
&= \frac{1}{\frac{B_i + \sqrt{d}}{C_i} - a_i} \\
&= \frac{C_i}{\sqrt{d} - (a_i C_i - B_i)} \\
&= \frac{C_i}{\sqrt{d} - B_{i+1}} \\
&= \frac{C_i(\sqrt{d} + B_{i+1})}{d - B_{i+1}^2} \\
&= \frac{\sqrt{d} + B_{i+1}}{C_{i+1}}
\end{aligned}$$

**Step 4:** Need to bound  $B_i, C_i$ . Let  $y_i = \frac{B_i - \sqrt{d}}{C_i}$  be  $\bar{x}_i$ . We have  $x = x_0 = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}$  where  $\{\frac{p_n}{q_n}\}$  are convergents to  $x$ . If we replace  $\sqrt{d}$  by  $-\sqrt{d}$  we get that  $y_0 = \frac{y_n p_{n-1} + p_{n-2}}{y_n q_{n-1} + q_{n-2}}$ . Solve for  $y_n$

$$y_n = \frac{-(q_{n-2} y_0 - p_{n-2})}{q_{n-1} y_0 - p_{n-1}} = -\frac{q_{n-2}}{q_{n-1}} \left( \frac{y_0 - \frac{p_{n-2}}{q_{n-2}}}{y_0 - \frac{p_{n-1}}{q_{n-1}}} \right)$$

Now let  $n \rightarrow \infty$ , we get  $-\frac{q_{n-2}}{q_{n-1}} \left( \frac{y_0 - x_0}{y_0 - x_0} \right)$ , so for sufficiently large  $n$  the expression for  $y_n$  is negative.

Given  $y_n = \frac{B_i - \sqrt{d}}{C_i}$ ,  $x_n - y_n$  is positive,  $x_n - y_n = \frac{2\sqrt{d}}{C_n} > 0$ , then  $C_n > 0$  for large enough  $n$ . Then  $1 \leq C_n \leq C_n C_{n+1} = d - B_{n+1}^2 \leq d$ , so  $C_n$  is bounded for large  $n$  (hence for all  $n$ ). Also,  $B_{n+1}^2 < B_{n+1}^2 + C_n C_{n+1} = d$ , so  $|B_{n+1}| < \sqrt{d}$  for large enough  $n$ , and so  $B_n$  is also bounded.

**Step 5:** There are only finitely many possibilities for  $(B_n, C_n)$ , so there must be

two natural numbers  $n$  and  $n + k$  such that  $(B_n, C_n) = (B_{n+k}, C_{n+k})$ . Then

$$\begin{aligned}
x_n &= \frac{B_n + \sqrt{d}}{C_n} \\
&= \frac{B_{n+k} + \sqrt{d}}{C_{n+k}} \\
&= x_{n+k} \\
\Rightarrow a_n &= \lfloor x_n \rfloor \\
&= \lfloor x_{n+k} \rfloor \\
&= a_{n+k} \\
\Rightarrow B_{n+1} &= a_n C_n - B_n \\
&= a_{n+k} C_{n+k} - B_{n+k} \\
&= B_{n+k+1} \\
\Rightarrow C_{n+1} &= \frac{d - B_{n+1}^2}{C_n} \\
&= \frac{d - B_{n+k+1}^2}{C_{n+k}} \\
&= C_{n+k+1}
\end{aligned}$$

So  $(B_{n+1}, C_{n+1}) = (B_{n+k+1}, C_{n+k+1})$ , and so on, and so the representation  $x_0 = x = [a_0, \dots, a_{n-1}, \overline{a_n, a_{n+1}, \dots, a_{n+k-1}}]$  is periodic.

Next, we want to understand what the continued fraction for  $\sqrt{d}$  looks like for  $d > 0$  not a square. One reason is to solve the Pell-Brahmagupta Equation, which is the diophantine equation  $x^2 - dy^2 = 1$  for  $x, y \in \mathbb{Z}$ . If  $(x, y)$  is a positive solution to the P-B equation, then  $(x + \sqrt{d}y)(x - \sqrt{d}y) = 1$ , so since  $x > \sqrt{d}y$ ,

$$\begin{aligned}
|x - \sqrt{d}y| &= \frac{1}{|x + \sqrt{d}y|} \\
\Rightarrow \left| \sqrt{d} - \frac{x}{y} \right| &= \frac{1}{y(x + \sqrt{d}y)} < \frac{1}{y(2\sqrt{d}y)}
\end{aligned}$$

$\Rightarrow \frac{x}{y}$  is an approximation to  $\sqrt{d}$ , which is at least as good as  $\frac{1}{2\sqrt{d}y^2}$ . If some  $\frac{p}{q}$  approximates irrational  $\alpha$  with error  $\leq \frac{1}{2q^2}$  then it must be a convergent to  $\alpha$  [proved in PSet 9], so all solutions to P-B equation must come from convergents  $\frac{x}{y}$  of  $\sqrt{d}$ . ■

**Theorem 71.** *Let  $x$  be a quadratic irrational, and  $\bar{x}$  be its conjugate (ie., if  $x = \frac{a+b\sqrt{d}}{c}$  with  $a, b, c, d \in \mathbb{Z}$ , then  $\bar{x} = \frac{a-b\sqrt{d}}{c}$ ). The continued fraction of  $x$  is purely periodic (ie.,  $[a_0, a_1, \dots, a_{n-1}]$ ) if and only if  $x > 1$  and  $-1 < \bar{x} < 0$ .*

*Proof - Part 1.* First suppose  $x > 1$  and  $-1 < \bar{x} < 0$ . We know that continued

fraction for  $x$  will repeat at some point, i.e., there's an  $n$ -digit block that repeats and a "start point"  $m$  such that

$$x = [a_0, a_1, \dots, a_{m-1}, \overline{a_m, a_{m+1}, \dots, a_{m+n-1}}]$$

Want to show that we can take  $m = 0$ . We'll do this by downward induction - i.e., by "advancing"  $m$ . We'll show that  $a_{m-1} = a_{m-1+n}$ .

We know that  $a_i \geq 1$  for all  $i$ . So rewrite  $x_{i+1} = \frac{1}{x_i - a_i}$  as  $\frac{1}{x_{i+1}} = x_i - a_i$ . Take conjugate

$$\frac{1}{\overline{x_{i+1}}} = \overline{x_i} - a_i$$

Now by induction, we'll show that  $-1 < \overline{x_i} < 0$ . For  $i = 0$  this is by hypothesis. If we know for  $i$  then  $\overline{x_i} - a_i < -1$ , since  $\overline{x_i} < 0$  and  $a_i > 1$ , and so  $\frac{1}{\overline{x_{i+1}}} < -1$  which forces  $-1 < \overline{x_{i+1}} < 0$ , which completes the induction.

Then, since

$$-a_i - \frac{1}{\overline{x_{i+1}}} = -\overline{x_i} \in (0, 1)$$

we have  $-\frac{1}{\overline{x_{i+1}}} \in (a_i, a_i + 1)$  and  $\lfloor -\frac{1}{\overline{x_{i+1}}} \rfloor = a_i$ . Now we know that  $a_{m+k} = a_{m+k+n}$  for all  $k \geq 0$ .

$$x_m = [a_m, a_{m+1}, \dots] = [a_{m+n}, a_{m+n+1}, \dots] = x_{m+n}$$

so  $\overline{x_m} = \overline{x_{m+n}}$ .

$$a_{m-1} = \left\lfloor -\frac{1}{\overline{x_m}} \right\rfloor = \left\lfloor -\frac{1}{\overline{x_{m+n}}} \right\rfloor = a_{m+n-1}$$

therefore we can take  $m = 0$ , and so  $x$  is purely periodic.  $\square$

*Proof.* Suppose  $x$  is purely periodic,  $x = [\overline{a_0, a_1, \dots, a_{n-1}}]$ . Want to show that  $x > 1$  and  $-1 < \overline{x} < 0$ . For any  $x$ ,  $a_0 = a_n > 1 \Rightarrow x > 1$ . So let's assume that  $n \geq 4$  (can always take larger blocks if not). Now

$$\begin{aligned} x &= [a_0, a_1, \dots, a_{n-1}, x] = \frac{p_{n-1}x + p_{n-2}}{q_{n-1}x + q_{n-2}} \\ \Rightarrow q_{n-1}x^2 + (q_{n-2} - p_{n-1})x - p_{n-2} &= 0 = f(x) \end{aligned}$$

$\overline{x}$  is the other root. We know that  $x > 1$ , so it's enough to show that  $f(x)$  has a root between  $-1$  and  $0$ . Do this by showing that  $f(0)$  and  $f(-1)$  have opposite signs.

$$\begin{aligned} f(0) &= -p_{n-2} < 0 \\ f(-1) &= q_{n-1} - q_{n-2} + p_{n-1} - p_{n-2} \\ &= (a_{n-1} - 1)q_{n-2} + q_{n-3} + (a_{n-1} - 1)p_{n-2} + p_{n-3} > 0 \end{aligned}$$

■

MIT OpenCourseWare  
<http://ocw.mit.edu>

18.781 Theory of Numbers  
Spring 2012

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.