

# 104B Problem Set 7

Rino Sanchez

March 13, 2003

## 11.2, # 13, 19

13. Let  $a/b = [a_0, \dots, a_n, a_n, \dots, a_0] = p_{2n+1}/q_{2n+1}$ . Show that  $p_{2n+1} = p_n^2 + p_{n-1}^2$  and  $q_{2n+1} = p_n q_n + q_{n-1} p_{n-1}$ .

It's far easier to use matrix methods for this. If we split the product just right and use the formulas given in lecture for  $p_k$  and  $q_k$  as entries of matrices, then the equations get spit out fairly easily (the question marks mean that we don't care about those terms of the matrix).

$$\begin{aligned} \begin{pmatrix} p_{2n+1} & p_{2n} \\ q_{2n+1} & q_{2n} \end{pmatrix} &= \begin{bmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \end{bmatrix} \begin{bmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} \end{bmatrix} \\ &= \begin{pmatrix} p_n^2 + p_{n-1}^2 & ? \\ p_n q_n + q_{n-1} p_{n-1} & ? \end{pmatrix} \end{aligned}$$

19. The result of Exercise 11 can be used to prove the important theorem that a prime  $p \equiv 1 \pmod{4}$  is representable as a sum of two squares. This proof due to H.J. Smith is outlined in the following exercises.

(a) Let  $S$  be the set of simple continued fraction expansions of the fractions  $p/q$ ,  $2 \leq q \leq \frac{p-1}{2}$ . If  $[a_0, a_1, a_2, \dots, a_k] \in S$ , then show that the reversed fraction  $[a_k, a_{k-1}, \dots, a_1, a_0]$  is also in  $S$ .

Luckily, we have a formula for  $[a_k, a_{k-1}, \dots, a_1, a_0]$  in terms of the convergents  $C_i = p_i/q_i$  of  $[a_0, \dots, a_k] = p/q$ , given by  $[a_k, a_{k-1}, \dots, a_1, a_0] = p_k/p_{k-1} = p/p_{k-1}$ . What we would like to show is that  $2 \leq p_{k-1} \leq \frac{p-1}{2}$ , which would imply that  $p/p_{k-1} \in S$ . Since  $p/q \in S$ , by definition we have  $2 \leq q \leq \frac{p-1}{2}$ . Using the  $q \leq \frac{p-1}{2}$  part, we can multiply by  $2/q$  to arrive at  $p/q \geq 2 + 1/q > 2$ , which implies that  $a_0 \geq 2$ , and as  $p_i$  is an increasing sequence and  $p_0 = a_0 \geq 2$ , we must have  $p_i \geq 2$  for all  $i$ . This proves that  $p_{k-1} \geq 2$ , half of our desired inequality. For the right side,  $p_{k-1} \leq \frac{p-1}{2}$ , we can isolate  $p$  to see that we want to prove  $p \geq 2p_{k-1} + 1$ . We note that a continued fraction expansion cannot end in 1, because  $[a, 1] = [a + 1]$ , and therefore  $a_k \geq 2$ . Now we can simply apply our inductive formulas to finish the proof

$$p = p_k = a_k p_{k-1} + p_{k-2} \geq 2p_{k-1} + p_{k-2} \geq 2p_{k-1} + 1$$

(b) Let  $f : S \rightarrow S$  be the function defined by  $f([a_0, a_1, \dots, a_k]) = [a_k, \dots, a_0]$ . Show that  $f \circ f$  (the composition of  $f$  with itself) is the identity and that  $f$  leaves an element  $x$  of  $S$  fixed, that is,  $f(x) = x$  for some  $x$ .

It is clear that  $f \circ f$  is the identity function on  $S$ , but to prove that  $f$  leaves an element  $x$  of  $S$  fixed, we have to count the number of elements in  $S$ . If  $S$  has an even number of elements, say  $2k$ , then  $f$  can simply switch between the two elements in  $k$  distinct pairs in  $S$ , but if  $S$  has an odd number of elements, say  $2k + 1$ , then there are at most  $k$  pairs that are switched by  $f$  and one extra element that must be fixed by  $f$ . Since  $p = 1 + 4k$  is a fixed prime, the condition for  $p/q \in S$  depends only on  $q$  (i.e.  $2 \leq q \leq \frac{p-1}{2}$ ), then the number of possible  $q$  is  $\frac{p-1}{2} - 1 = 2k - 1$ , so  $S$  has an odd number of elements as desired.

(c) Suppose  $f(x) = x$ . Show that  $x$  is a symmetric continued fraction. Explain why  $x$  must have an even number of terms. Conclude that  $p$  is representable as a sum of two squares.

If we can prove that  $x$  has an even number of terms, then we can simply apply problem 13 to write  $p$  as a sum of two squares, namely  $p = p_n^2 + p_{n-1}^2$  if  $p/q = [a_0, \dots, a_n, a_n, \dots, a_0]$ . Now we assume that

$x = [a_0, \dots, a_k, \dots, a_0]$ , an odd number of terms. It is easier to apply the matrix methods covered in lecture.

$$\begin{aligned} \begin{pmatrix} p_{2k} & p_{2k-1} \\ q_{2k} & q_{2k-1} \end{pmatrix} &= \left[ \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \right] \left[ \begin{pmatrix} a_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \right] \\ &= \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} \cdot \begin{pmatrix} p_{k-1} & q_{k-1} \\ p_{k-2} & q_{k-2} \end{pmatrix} \\ &= \begin{pmatrix} p_{k-1}(p_k + p_{k-2}) & ? \\ ? & ? \end{pmatrix} \end{aligned}$$

This proves that  $p = p_{2k} = p_{k-1}(p_k + p_{k-2})$ , which a nontrivial factorization of  $p$  (all  $p_i$  are positive integers), contradiction our assumption that  $p$  was prime. Hence, the continued fraction expansion of  $x$  has an even number of terms as desired.

(d) For  $p = 13$  and  $p = 29$ , compute  $S$ ,  $x$  and the corresponding representation of  $p$  as a sum of two squares.

Let  $p = 13$ . Then the set  $S = \{13/2, 13/3, \dots, 13/6\}$ , and we need to compute the continued fraction expansions of all these fractions to find the fixed point of the function  $f$  defined above. In this case, we have  $13/5 = [2, 1, 1, 2]$ , so  $k = 1$ ,  $p_1 = 3$ ,  $p_0 = 2$ , and  $p = 13 = 3^2 + 2^2$ .

Let  $p = 29$ . Then the set  $S = \{29/2, 29/3, \dots, 29/14\}$ , and if you compute the continued fractions, we find that  $29/12 = [2, 2, 2, 2]$  is the one we need. Then  $k = 1$ ,  $p_1 = 5$ ,  $p_0 = 2$ , and  $p = 29 = 5^2 + 2^2$ .

### 11.3, # 11

11. Using Algorithm 11.3.5, find the first three terms of the continued fraction expansion of  $\sqrt[3]{2}$ .

Let  $f(x) = x^3 - 2$ , which only has one real positive root, namely  $\sqrt[3]{2}$  (the other two roots are not real). Then  $a_0 = 1$ ,  $g(x) = (x+1)^3 - 2$ , and  $f_1(x) = -x^3((1+1/x)^3 - 2) = 2x^3 - (x+1)^3 = x^3 - 3x^2 - 3x - 1$ . From the plot of  $f_1$ , we can tell that  $a_1 = 3$ , so  $g(x) = f_1(x+3)$ , and  $f_2(x) = -x^3((3+1/x)^3 - 3(3+1/x)^2 - 3(3+1/x) - 1)$ . From the plot of  $f_2$ , we can tell that  $a_2 = 1$ . This gives us  $\sqrt[3]{2} = [1, 3, 1, \dots]$ .

### 11.4, # 4, 6, 9

4. Evaluate the following continued fractions.

(a)  $[3, 2, 1, 3, 2, 1, \dots]$ : Let  $x = [3, 2, 1, 3, 2, 1, \dots]$ . Then  $x = [3, 2, 1, x]$ , so we compute

$$x = [3, 2, 1, x] = 3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{x}}} = 3 + \frac{1}{2 + \frac{x}{x+1}} = 3 + \frac{x+1}{3x+2} = \frac{10x+7}{3x+2}$$

Then we can see that  $x(3x+2) = 10x+7$ , which gives  $3x^2 - 8x - 7 = 0$  with roots  $\frac{8 \pm 2\sqrt{37}}{6} = \frac{4 \pm \sqrt{37}}{3}$ . Since  $x > 0$ , we must have  $x = \frac{4 + \sqrt{37}}{3}$ .

(b)  $[1, 2, 2, 3, 2, 3, 2, 3, \dots]$ : Let  $x = [1, 2, 2, 3, 2, 3, 2, 3, \dots]$  and  $y = [2, 3, 2, 3, \dots]$ . Then  $x = [1, 2, y]$ , so we start by finding  $y$ .

$$y = [2, 3, y] = 2 + \frac{1}{3 + \frac{1}{y}} = 2 + \frac{y}{3y+1} = \frac{7y+2}{3y+1}$$

This means that  $y(3y+1) = 7y+2$ , so  $3y^2 - 6y - 2 = 0$ , and so  $y = \frac{6 \pm 2\sqrt{15}}{6} = \frac{3 \pm \sqrt{15}}{3}$ . As  $y > 0$ , we must have  $y = \frac{3 + \sqrt{15}}{3}$ . Now we finally calculate  $x$

$$x = [1, 2, y] = 1 + \frac{1}{2 + \frac{1}{y}} = 1 + \frac{y}{2y+1} = \frac{3y+1}{2y+1} = \frac{4 + \sqrt{15}}{\frac{6+2\sqrt{15}}{3} + 1} = \frac{6 + \sqrt{15}}{7}$$

6. Prove that every eventually periodic continued fraction is a quadratic irrational.

Let  $x = [a_0, a_1, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+n}}]$  be an eventually periodic continued fraction. Let  $y$  be the repeating part  $[\overline{a_k, \dots, a_{k+n}}]$ . Then let  $p_i/q_i$  be the convergents of  $y$ , and now we can expand using our inductive formulas for  $p_i$  and  $q_i$

$$y = [\overline{a_k, \dots, a_{k+n}}] = [a_k, \dots, a_{k+n}, y] = \frac{yp_n + p_{n-1}}{yq_n + q_{n-1}}$$

Therefore,  $y(yq_n + q_{n-1}) = yp_n + p_{n-1}$ , and  $y$  is a root of  $q_n y^2 + (q_{n-1} - p_n)y - p_{n-1} = 0$  and is then a quadratic irrational (it has an infinite continued fraction so it must be irrational). Hence,  $y$  must be of the form  $\frac{a+\sqrt{n}}{b}$  with  $a, b$  rational. Since  $x = [a_0, a_1, \dots, a_{k-1}, y]$  and all the  $a_i$  are integers, one can easily see that  $x$  is also of the form  $\frac{a+\sqrt{n}}{b}$ , because for any integer  $c$ ,

$$\left[ c, \frac{a + \sqrt{n}}{b} \right] = c + \frac{b}{a + \sqrt{n}} = \frac{b + ac + c\sqrt{n}}{a + \sqrt{n}}$$

Rationalizing the denominator, we once again get a number of the form  $\frac{a'+\sqrt{n}}{b'}$ . You can then apply an induction argument to finish the proof.

9. Verify that the first complete quotient  $x_1$  in the expansion of  $\sqrt{n}$  satisfies  $-1 < \overline{x_1} < 0$ .

If following the algorithm defined in Theorem 11.4.1 for the first two steps, we see that  $A_0 = 0$ ,  $B_0 = 1$ ,  $A_1 = a_0$ , and  $B_1 = n - a_0^2$ , so  $x_1 = \frac{a_0 - \sqrt{n}}{n - a_0^2}$  and

$$\overline{x_1} = \frac{a_0 - \sqrt{n}}{n - a_0^2} = \frac{a_0 - \sqrt{n}}{(\sqrt{n} - a_0)(\sqrt{n} + a_0)} = \frac{-1}{\sqrt{n} + a_0} < 0$$

As  $a_0 = \lfloor \sqrt{n} \rfloor$ , we have  $\sqrt{n} - a_0 < 1$ , or  $a_0 - \sqrt{n} > -1$ , and since  $n - a_0^2 \geq 1$ , we have  $\overline{x_1} = \frac{a_0 - \sqrt{n}}{n - a_0^2} > -1$ .

### 11.5, # 1

1. Show that the continued fraction expansion of  $a_0 + \sqrt{n}$  with  $a_0 = \lfloor \sqrt{n} \rfloor$  is purely periodic.

We first refer to Example 11.5.5, which says that if  $\sqrt{n} = [a_0, \overline{a_1, a_2, \dots, a_k}]$ , then  $a_k = 2a_0$ . Now, it's clear that the expansion of  $a_0 + \sqrt{n}$  is

$$[2a_0, \overline{a_1, a_2, \dots, 2a_0}] = [2a_0, a_1, a_2, \dots, a_{k-1}, 2a_0, a_1, a_2, \dots] = [2a_0, a_1, a_2, \dots, a_{k-1}]$$