Math 115 Fall, 2011

Professor K. A. Ribet

Assignment due November 22, 2011

1. Suppose that $\langle a_0, a_1, \ldots, a_n\rangle$ is the simple continued fraction representation of a rational number. (Recall that our conventions dictate that a_n be at least 2.) Define the numbers h_n and k_n as usual. Establish the formula

$$\frac{k_n}{k_{n-1}} = \langle a_n, a_{n-1}, \ldots, a_2, a_1\rangle.$$

(Hint: it seems helpful to recall the recursive formula that defines k_i in terms of a_i and previous ks.)

This seems to go easily by induction. If $n = 1$, the formula is correct because $\langle a_1\rangle = a_1$ and because $k_0 = 1$, $k_1 = a_1$. Assume that n is at least 2 and that the result is true with $n - 1$ in place of n. We have

$$\langle a_n, a_{n-1}, \ldots, a_2, a_1\rangle = a_n + \frac{1}{\langle a_{n-1}, \ldots, a_2, a_1\rangle} = a_n + \frac{k_{n-2}}{k_{n-1}} = \frac{k_n}{k_{n-1}},$$

where the last step comes from the recursive formula alluded to by the statement of the problem.

2. Suppose that p is an odd prime number and that u is the square root of -1 mod p that satisfies $1 \le u \le (p-1)/2$. Take u/p to be the rational number of part (1). In other words, write

$$\frac{u}{p} = \langle a_0, a_1, \ldots, a_n\rangle.$$

Show that $k_n = p$ and that $h_n = u$. Using the formula $h_n k_{n-1} - k_n h_{n-1} = (-1)^{n-1}$, show that n is even and that $k_{n-1} = u$.

Since $\langle a_0, a_1, \ldots, a_n\rangle = u/p$, and since this fraction is in lowest terms (because u is not divisible by p), we do have $h_n = u$ and $k_n = p$. The formula $h_n k_{n-1} - k_n h_{n-1} = (-1)^{n-1}$ thus reads $uk_{n-1} - ph_{n-1} = (-1)^{n-1}$. It gives in particular the mod p congruence $uk_{n-1} \equiv (-1)^{n-1}$. Multiplying by u, we get $k_{n-1} \equiv (-1)^n u$. This means, in particular, that $k_{n-1} \equiv \pm u$ We have $p = k_n \ge a_n k_{n-1}$ and also that a_n is at least 2 (by our convention that the continued fraction expansion of a rational number does not end in 1). Hence $k_{n-1} < p/2$. Because we have, by assumption, the inequality $u < p/2$, we cannot have $k_{n-1} \equiv -u$, which would give $k_{n-1} = p - u > p/2$. Hence we are forced to conclude that k_{n-1} is congruent to u mod p and thus is in fact equal to u since both u and k_{n-1} are positive integers that are less than p. Recalling the congruence $k_{n-1} \equiv (-1)^n u$, we conclude that n is even.

3. Combining (1) and (2), show that

$$p/u = \langle a_n, a_{n-1}, \ldots, a_2, a_1 \rangle.$$

Conclude that the strings $(a_n, a_{n-1}, \ldots, a_2, a_1)$ and $(a_1, \ldots, a_n)$ are identical.

The expression $\langle a_n, a_{n-1}, \ldots, a_2, a_1 \rangle$ has been shown to be k_n/k_{n-1}, but in our situation we have seen that $k_n = p$ and $k_{n-1} = u$. Hence we do have $p/u = \langle a_n, a_{n-1}, \ldots, a_2, a_1 \rangle$. Now $u/p = \langle a_0, a_1, \ldots, a_n \rangle = a_0 + 1/\langle a_1, \ldots, a_n \rangle$, but $a_0 = 0$ since u/p is between 0 and 1. Hence $p/u = \langle a_1, \ldots, a_n \rangle$, which gives a second continued fraction expansion for p/u. There are, in fact, two different continued fraction expansions for a rational number (Theorem 7.2 on page 329). However, these expansions differ only in the trivial way that is explained at the beginning of §7.2. It follows from the discussion of §7.2 that two continued fraction representations of a rational number that have the same length must in fact be identical. In other words, the "strings" described by the problem are the same.