

March 16, 2006

Physics 681-481; CS 483: Assignment #5

(please hand in after the lecture, Thursday, April 6th, in three weeks)

The two questions that follow illustrate the mathematics of the final (post-quantum-computational) stage of Shor's period finding procedure, as described on pages 17 and 18 of Chapter 3 of the lecture notes. The detective work you are asked to carry out makes use of the theorem, cited in the lecture notes, that if j and r have no common factors, and x is an estimate for the fraction j/r that differs from it by less than $1/2r^2$, then j/r will appear as one of the partial sums in the continued fraction expansion of x .

1. Suppose you know that the integer r is less than 100 and that 11490 is within $\frac{1}{2}$ of an integral multiple of $2^{14}/r$. What is r ?

2. Suppose you know that the integer r is less than 100 and that 11343 and 13653 are both within $\frac{1}{2}$ of integral multiples of $2^{14}/r$. What is r ?

These numbers are small enough to find with an exhaustive computer search, but you would learn nothing from this, and should answer them by using continued fractions, with no technological aids other than a (nonprogrammable) calculator. Since $2^{14} = 128^2 > 100^2$, in either question the fraction j/r for some integer j will necessarily be¹ one of the partial sums² of the continued fraction expansion of $y/2^{14}$, where y is one of the cited 5-digit integers. The partial sum with the largest denominator less than 100 is the one you are looking for. Once you have found the answer you can easily check that it is correct.

The continued fraction expansion of a number x between 0 and 1 is

$$x = \frac{1}{a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}} \quad (1)$$

with positive integers a_0, a_1, a_2, \dots . Evidently a_0 is the integral part of $1/x$. Let x_1 be the fractional part of $1/x$. Then

$$x_1 = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}} \quad (2)$$

¹ Theorem 184, page 153, Hardy and Wright, *An Introduction to the Theory of Numbers*, 4th Edition, Oxford, 1965.

² Defined below.

so a_1 is the integral part of $1/x_1$. Letting x_2 be the fractional part of $1/x_1$ one can continue this iterative procedure to extract a_2 as the integral part of $1/x_2$, and so on.

By the partial sums of the continued fraction (1), one means

$$\frac{1}{a_0}, \quad \frac{1}{a_0 + \frac{1}{a_1}}, \quad \frac{1}{a_0 + \frac{1}{a_1 + \frac{1}{a_2}}}, \quad \text{etc.} \quad (3)$$

I used an unprogrammed pocket calculator to solve these numerical puzzles. All you need to do is to keep subtracting the integral part from the display and inverting what remains. Your essay should describe the numbers a_0, a_1, a_2, \dots in the continued fraction expansions you generated and what partial sums you looked at to provide yourself with the information needed to extract the values of r in Questions 1 and 2.

If you find the arithmetical labor of computing successive partial sums onerous (I didn't), feel free to use the (famous but not entirely obvious) recursion relation for the numerators p and denominators q of the partial sums: $p_n = a_n p_{n-1} + p_{n-2}$, and $q_n = a_n q_{n-1} + q_{n-2}$, with $p_0 = 1, q_0 = a_0, p_1 = a_1, q_1 = 1 + a_0 a_1$.