

# Math 4440

## Mission 6

Melanie Nun, Colin Sidey, Cameron Smith,  
Bharadwaj Thirumal

October 17, 2016

### 3.12 Continued Fractions

Long decimals are cumbersome and prone to loss of significance or rounding error. It is beneficial, then, to have a method to approximate or even solve such numbers by rational numbers. Continued fractions are a convenient way to do this.

The simplest way to approximate a decimal with a rational number is to take the nearest integer. This is inaccurate but quick and simple and provides a basis for continued fractions.

Let  $[x]$  be the largest integer  $[x] \leq x$ . Then a decimal (for example,  $\sqrt{5} = 2.23606798$ ) can be roughly approximated by  $[\sqrt{5}] = 2$ . The remainder is then  $.23606798$ .

To get a better approximation, approximate the remainder by  $\frac{1}{.23606798} = 4.236067977 \Rightarrow [\frac{1}{.23606798}] = 4$ . Then  $\sqrt{5} \approx 2 + \frac{1}{4}$ .

For a better approximation, continue:  $[\frac{1}{4.236067977-4}] = [4.236067977] = 4$ .

We can see that in the case of  $\sqrt{5}$ , this pattern of remainder  $[\frac{1}{4.236067977-4}] = [4.236067977] = 4$  will continue indefinitely.

We write the solution as  $\sqrt{5} \approx 2 + \frac{1}{4 + \frac{1}{4 + \frac{1}{4 + \dots}}}$ .

Converting these approximations to a rational number is easy:

$$\begin{aligned}\sqrt{5} &\approx 2 + \frac{1}{4} = \frac{9}{4} \\ &\approx 2 + \frac{1}{4 + \frac{1}{4}} = \frac{38}{17} \\ &\approx 2 + \frac{1}{4 + \frac{1}{4 + \frac{1}{4}}} = \frac{161}{72}\end{aligned}$$

The approximations get increasingly better:

$$\begin{aligned}|\sqrt{5} - \frac{9}{4}| &= .01393202 \\ |\sqrt{5} - \frac{38}{17}| &= .0007738599\end{aligned}$$

$$|\sqrt{5} - \frac{161}{72}| = .00000431336$$

$\sqrt{5}$  is an irrational number - its continued fraction will go on indefinitely. Continued fractions for a rational number will be finite. For example, examine  $\frac{25}{7} = 3.5714286$

$$\begin{aligned} 3.5714286 &\approx 3 + \frac{1}{1} \\ &\approx 3 + \frac{1}{1 + \frac{1}{1}} \\ &\approx 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}} \end{aligned}$$

Simplifying the last fraction gives  $\frac{25}{7}$ , the number we used to get our decimal.

Any arbitrary number  $x$  can be approximated this way: the generalization is as follows. Let  $a_0 = [x]$ ,  $x_0 = x$ ,  $x_{i+1} = \frac{1}{x_i - a_i}$  and  $a_{i+1} = [x_{i+1}]$ . Then we have

$$\frac{p_n}{q_n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\dots + \frac{1}{a_n}}}}}$$

Continue until  $x_i = a_i$  or until approximation reaches sufficient accuracy. It can be shown that each successive approximation is better than the last, i.e.:  $|x - \frac{p_{n+1}}{q_{n+1}}| < |x - \frac{p_n}{q_n}|$

There is an important theorem to help us understand the size of approximations needed.

**Theorem 1.** For  $r, s \in \mathbb{Z}$ , if  $|x - \frac{r}{s}| < \frac{1}{2s^2}$ , then  $\frac{r}{s} = \frac{p_i}{q_i}$  for some  $i$ .

This theorem is significant because we can find an  $r$  for any  $s$  so that  $\frac{1}{2s^2}$  is small enough for our purposes - i.e., we can find a rational number approximation for an irrational number as accurate as we choose. However, the approximation will never be perfect  $\forall s \in \mathbb{Z}$ ,  $\frac{1}{2s^2} > 0$ . This is as we expect, because irrational numbers by definition will never be equal to a rational number.

## 6.2.1 Low Exponent Attacks

The choice of  $d$  in the RSA cryptosystem can compromise the security of the system. Once a potential attacker has found  $d$ , it's relatively simple to find  $p$  and  $q$ . The first thing we want to do is pick a  $d$  value that is sufficiently large as to make a brute force search for  $d$  infeasible. However, there is another way to exploit a poor choice of  $d$ . In a theorem by M. Wiener, we see that if a small value of  $d$  is chosen, the value of  $d$  can be calculated quickly.

**Theorem 2.** Let  $p, q$  be primes with  $q < p < 2q$  and  $pq = n$ . Let  $d > 1$  and  $e < \phi(n)$  such that  $ed \equiv 1 \pmod{\phi(n)}$ . If  $d < \frac{n^{\frac{1}{3}}}{3}$  then  $d$  can be computed quickly.

The proof of this theorem draws on a series of inequalities and the properties of continued fractions and their approximations. By working through the details of the proof we get the inequality:

$$0 < \frac{k}{d} - \frac{e}{n} < \frac{1}{3d^2}$$

Here we see that the difference between the fractions  $\frac{k}{d}$  and  $\frac{e}{n}$  must be less than  $\frac{1}{3d^2}$ . If  $d$  is small, the difference between those fractions need not be very small, but if  $d$  is very large, then the difference between those fractions must be very small.

Recall from earlier the result: For  $r, s \in \mathbb{Z}$ , if  $|x - \frac{r}{s}| < \frac{1}{2s^2}$ , then  $\frac{r}{s} = \frac{p_i}{q_i}$  for some  $i$ . This will be the basis for an attack. Note that,  $|x - \frac{k}{d}| < \frac{1}{2s^2}$  and  $x = \frac{e}{n}$ . Since we know  $e$  and  $n$ , we can use continued fractions to approximate a value for  $\frac{k}{d}$ . To perform the attack, Eve will compute the first approximation for  $\frac{e}{n}$  and return values  $A = k$  and  $B = d$ . Now, since

$$ed = 1 + \phi(n)k$$

$$ed - 1 = \phi(n)k$$

$$\frac{ed - 1}{k} = \phi(n)$$

By using  $A$  and  $B$  to calculate  $C = \frac{ed-1}{k}$ , we check if  $C$  is an integer because  $\phi(n)$  must be an integer. If  $C$  isn't an integer then we refine our approximation and find new values for  $A$  and  $B$ . Otherwise we continue and try to find roots. Take  $x^2 - (n - C + 1)x + n = x^2 - (n - \phi(n) + 1)x + n = (x - p)(x - q)$ . If we calculate the values of  $(x - p)$  and  $(x - q)$  and rerun numbers with high decimal accuracy, then we know we've found roots; otherwise we start over and calculate new continued fraction values for  $A$  and  $B$ .

We will now demonstrate this technique with an example. Take  $q = 127$  and  $p = 163$  (Note that  $q < p < 2q$ ). So we have  $n = 20701$  and  $\phi(n) = 20412$ . Now we chose  $e$ , let's take  $e = 8165$  and we note that  $\gcd(e, \phi(n)) = 1$ .

Our first step here is to calculate the continued fractions of  $\frac{e}{n} = \frac{8165}{20701}$ . Using Wolfram Alpha to calculate, we get the continued fractions  $[0; 2, 1, 1, 6, 1, 1, 2, 1, 4, 2, 3, 2]$ . We now calculate our  $A, B$ , and  $C$ .

We start with  $0 + \frac{1}{2}$ . Here we have  $A = 1, B = 2$ . We know that  $d$  must be odd so we move on to our next approximation.

$$0 + \frac{1}{2 + \frac{1}{1}} = \frac{1}{3}$$

So we have  $A = 1$  and  $B = 3$ .  $C = (8165 * 3 - 1) * \frac{1}{1} = 24494$ . We then try and find roots for  $x^2 - (20701 - 24494 + 1)x + 20701 = x^2 + 3792x + 20701$ . It's clear that this will have no real roots so we continue by refining our  $A$  and  $B$ .

$$0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1}}} = \frac{2}{5}$$

Here  $A = 2$  and  $B = 5$ .  $C = (8165 * 5 - 1) * \frac{1}{2} = 20412$ . Now we try to find roots for  $x^2 - (20701 - 20412 + 1)x + 20701 = x^2 - 290x + 20701$ . Calculating these roots we find  $x = 127$  and  $x = 163$  which have no decimal uncertainty so we know we've found our  $p$  and  $q$  and we note that these are the exact  $p$  and  $q$  we picked for the example.

## Algorithms

In order to factor  $n = 160523347$ , we needed to combine the two algorithms we wrote. To do this, we put a call to the Attempted Factorization Phase after finding each  $p_i$  and  $q_i$  in the Continued Fraction algorithm to check if  $C$  is an integer. Once we verified it with the example on page 171, we proceeded with the problem. The entire program is attached. When  $(p_5, q_5) = (14, 37)$  was checked in the Attempted Factorization Phase, it was discovered that 13001 and 12347 are the factors of  $n$ .

## Credits

Melanie: Continued Fractions

Colin: Low Exponent Attacks

Bharadwaj: Code for Continued Fractions

Cameron: Code for Attempted Factorization Phase