15.10 Continued Fraction Method for Factorisation

11. januar 2018

Question 2.

For a real number $x \in \mathbb{R}$ the partial quotients are defined, setting $x_0 = x$,

$$a_n = \lfloor x_n \rfloor,$$

$$x_{n+1} = \frac{1}{x_n - a_n}.$$

No further partial quotients are defined if $a_n = x_n$.

Assume $x = \sqrt{N}$ for positive integer N. If N is a square number, $a_0 = x_0$ as $x_0 = \sqrt{N}$ is an integer. So assume N is not square, then $\sqrt{N}$ is irrational and has an infinite set of of partial quotients. We now show

$$x_n = \frac{r_n + \sqrt{N}}{s_n}, \quad r_n, s_n \in \mathbb{Z}$$

with $s_n | (r_n^2 - N)$.

$$x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\sqrt{N} - a_0} = \frac{a_0 + \sqrt{N}}{N - a_0^2}$$

which gives $r_1 = a_0$ and $s_1 = N - a_0^2$. Clearly, $s_1 | (a_0^2 - N)$.

Assuming $x_n = \frac{r_n+\sqrt{N}}{s_n}$ for a given $n \in \mathbb{N}$, and r_n, s_n as above, we get

$$\begin{aligned}
x_{n+1} &= \frac{1}{x_n - a_n} \\
&= \frac{1}{\frac{r_n+\sqrt{N}}{s_n} - a_n} \\
&= \frac{s_n}{(r_n - s_n a_n) + \sqrt{N}} \\
&= \frac{s_n(-(r_n - s_n a_n) + \sqrt{N})}{N - (r_n - s_n a_n)^2} \\
&= \frac{s_n(s_n a_n - r_n + \sqrt{N})}{(N - r_n^2) - s_n^2 a_n^2 + 2 r_n s_n a_n} \\
&= \frac{s_n a_n - r_n + \sqrt{N}}{2 r_n a_n - q_n - s_n a_n^2}
\end{aligned}$$

where $q_n \in \mathbb{Z}$ is such that $q_n s_n = r_n^2 - N$ according to the induction hypothesis. This completes the proof by induction, with

$$r_{n+1} = s_n a_n - r_n \tag{1}$$

and

$$s_{n+1} = 2 r_n a_n - q_n - s_n a_n^2 \tag{2}$$

since

$$\begin{aligned}
r_{n+1}^2 - N &= (s_n a_n - r_n)^2 - N \\
&= s_n^2 a_n^2 + r_n^2 - 2 s_n a_n r_n - N \\
&= s_n^2 a_n^2 - 2 s_n a_n r_n + q_n s_n \\
&= s_n(s_n a_n^2 - 2 s_n a_n r_n + q_n) \\
&= -s_n s_{n+1}
\end{aligned}$$

so indeed, $s_{n+1} | (r_{n+1}^2 - N)$. Furthermore, we note that $q_{n+1} = -s_n$.

Using this insight the partial quotients, a_n, can be found purely by integer division,

$$a_n s_n = (r_n + a_0) + d$$

where d is an integer such that $0 \leq d < s_n$, and $a_0 = \left\lfloor \sqrt{N} \right\rfloor$ as before. The integers s_n, r_n are found using eq. (1) and (2).

Observations on the partial quotients:

They seem to repeat themselves in a palindrome pattern.

r and s approach $\sqrt{N}$ and $2\sqrt{N}$ respectively from below as N increases.

Question 3.

From considering the values of N for which a solution to the negative Pell's equation are found using convergents, it is apparent that non of these are divisible by 3. Being divisible by 3 is in fact a condition on N that ensures the negative Pell's equation is insoluble.

This is a special case of a more general condition. Assume p is a prime such that $a^2 \not\equiv -1$ for all $a \in \mathbb{N}$. If $p|N$, then

$$x^2 - Ny^2 \equiv x^2 \pmod{p}$$

and it is clear that there are no solutions to the negative Pell's equation for N. 3 is such a prime for which -1 is not a square congruence class, as is 7 and 11.

Avoiding integer overflow with support up to 10^{15}. Assume $N \leq 10^{10}$, and $x, y \leq 10^{15}$. Then

$$|x^2 - Ny^2| \leq 10^{40}. \tag{3}$$

Let $\{p_1, \ldots, p_k\}$ be primes such that

$$P = \prod_{i=1}^{k} p_i > 10^{40} + 1. \tag{4}$$

If

$$x^2 - Ny^2 \equiv \pm 1 \pmod{p_i}$$

for $i = 1, \ldots, k$, then $p_i | x^2 - Ny^2 \mp 1$. This implies $P|(x^2 - Ny^2 \mp 1)$. Then

$$x^2 - Ny^2 \mp 1 = 0$$

since otherwise

$$P \leq x^2 - Ny^2 \mp 1$$

which is in contradiction with (3) and (**??**).

Computing Pell's equation for all primes in such a set of primes as the above, will ensure that a solution has actually been found while avoiding integer overflow can be obtained by choosing the primes $< \sqrt{10^{15}}$.

Question 4.

$$\begin{aligned} x^2 &\equiv y^2 \pmod{N} \\ \iff N&|(x+y)(x-y) \end{aligned}$$

so for any prime factor $p|N$ we have $p|(x+y)$ or $p|(x-y)$. Using the Euclidean algorithm we can efficiently find factors of N by considering

$$\gcd(N, x+y)$$

$$\gcd(N, x-y)$$

If we assume N is odd and $N = ab$ for non-trivial factors $a, b \in N$, with $a \leq b$, then a, b must be odd and we can define integers,

$$x = a + \frac{b-a}{2}$$

$$y = \frac{b-a}{2}.$$

With these definitions, $a = x - y$, $b = x + y$, and

$$N = ab = (x-y)(x+y) = x^2 - y^2.$$

This proves that our assumptions on N imply that there exists x, y with $x^2 \equiv y^2 \pmod{N}$.

Question 5.