must have a denominator larger than c_i). Another property is analogous to the fact that the decimal (or base-b) digits of a real number x repeat if and only if x is rational. In the continued fraction expansion of x, we saw that the sequence of integers a_i terminates if and only if x is rational. It can be shown that the a_i become a repeating sequence if and only if x is a quadratic irrationality, i.e., of the form $x_1 + x_2\sqrt{n}$ with x_1 and x_2 rational and n not a perfect square. This is known as Lagrange's theorem.

Example 1. If we start expanding $\sqrt{3}$ as a continued fraction, we obtain

$$\sqrt{3} = 1 + \frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{1+}\,\frac{1}{2+}\cdots.$$

At this point we might conjecture that the a_i's alternate between 1 and 2. To prove this, let x equal the infinite continued fraction on the right with alternating 1's and 2's. Then clearly $x = 1 + \frac{1}{1+(1/(1+x))}$, as we see by replacing x on the right by its definition as a continued fraction. Simplifying the rational expression on the right and multiplying both sides of the equation by $2+x$ gives: $2x + x^2 = 3 + 2x$, i.e., $x = \sqrt{3}$.

Proposition V.4.2. *Let $x > 1$ be a real number whose continued fraction expansion has convergents b_i/c_i. Then for all i: $|b_i^2 - x^2c_i^2| < 2x$.*

Proof. Since x is between b_i/c_i and b_{i+1}/c_{i+1}, and since the absolute value of the difference between these successive convergents is $1/c_ic_{i+1}$ (by Proposition V.4.1(c)), we have

$$|b_i^2 - x^2c_i^2| = c_i^2\left|x - \frac{b_i}{c_i}\right|\left|x + \frac{b_i}{c_i}\right| < c_i^2\frac{1}{c_ic_{i+1}}\left(x + \left(x + \frac{1}{c_ic_{i+1}}\right)\right).$$

Hence,

$$\begin{aligned}|b_i^2 - x^2c_i^2| - 2x &< 2x\left(-1 + \frac{c_i}{c_{i+1}} + \frac{1}{2xc_{i+1}^2}\right) < 2x\left(-1 + \frac{c_i}{c_{i+1}} + \frac{1}{c_{i+1}}\right)\\ &< 2x\left(-1 + \frac{c_{i+1}}{c_{i+1}}\right) = 0.\end{aligned}$$

This proves the proposition.

Proposition V.4.3. *Let n be a positive integer which is not a perfect square. Let b_i/c_i be the convergents in the continued fraction expansion of $\sqrt{n}$. Then the residue of b_i^2 modulo n which is smallest in absolute value (i.e., between $-n/2$ and $n/2$) is less than $2\sqrt{n}$.*

Proof. Apply Proposition V.4.2 with $x = \sqrt{n}$. Then $b_i^2 \equiv b_i^2 - nc_i^2$ *mod* n, and the latter integer is less than $2\sqrt{n}$ in absolute value.

Proposition V.4.3 is the key to the continued fraction algorithm. It says that we can find a sequence of b_i's whose squares have small residues by taking the numerators of the convergents in the continued fraction expansion of $\sqrt{n}$. Note that we do not have to find the actual convergent: only the numerator b_i is needed, and that is needed only modulo n. Thus, the fact that the numerator and denominator of the convergents soon become