method of finding integers b between 1 and n such that the least absolute residue $b^2 \ mod \ n$ is a product of small primes. This is most likely to occur if the absolute value of $b^2 \ mod \ n$ is small. In this section we describe a method (originally due to Legendre) for finding many b such that $|b^2 \ mod \ n| < 2\sqrt{n}$. This method uses "continued fractions," so we shall start with a brief introduction to the continued fraction representation of a real number. Our account will describe only those features which will be needed here; the reader interested in a more thorough treatment of continued fractions should consult, for example, Davenport's classic and readable book (see the references at the end of the section).

Continued fractions. Given a real number x, we construct its continued fraction expansion as follows. Let $a_0 = [x]$ be the greatest integer not greater than x, and set $x_0 = x - a_0$; let $a_1 = [1/x_0]$, and set $x_1 = 1/x_0 - a_1$; and for $i > 1$, let $a_i = [1/x_{i-1}]$, and set $x_i = 1/x_{i-1} - a_i$. If/when you find that $1/x_{i-1}$ is an integer, you have $x_i = 0$, and the process stops. It is not hard to see that the process terminates if and only if x is rational (because in that case the x_i are rational numbers with decreasing denominators). Because of the construction of $a_0, a_1, \ldots, a_i$, for each i you can write

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{a_i + x_i}}},$$

which is usually written in a more compact notation as follows:

$$x = a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\,\frac{1}{a_3+}\cdots\frac{1}{a_i + x_i}.$$

Suppose that x is an *irrational* real number. If we carry out the above expansion to the i-th term and then delete x_i, we obtain a rational number b_i/c_i, called the i-th *convergent* of the continued fraction for x:

$$\frac{b_i}{c_i} = a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\,\frac{1}{a_3+}\cdots\frac{1}{a_{i-1}+}\,\frac{1}{a_i}.$$

Proposition V.4.1. *In the above notation, one has:*

(a) $\frac{b_0}{c_0} = \frac{a_0}{1}$; $\frac{b_1}{c_1} = \frac{a_0a_1+1}{a_1}$; $\frac{b_i}{c_i} = \frac{a_ib_{i-1}+b_{i-2}}{a_ic_{i-1}+c_{i-2}}$ *for* $i \geq 2$;

(b) *the fractions on the right in part (a) are in lowest terms, i.e., if* $b_i = a_ib_{i-1} + b_{i-2}$ *and* $c_i = a_ic_{i-1} + c_{i-2}$, *then* $g.c.d.(b_i, c_i) = 1$;

(c) $b_ic_{i-1} - b_{i-1}c_i = (-1)^{i-1}$ *for* $i \geq 1$.

Proof. We define the sequences $\{b_i\}$ and $\{c_i\}$ by the relations in (a), and prove by induction that then b_i/c_i is the i-th convergent. We will prove this without assuming that the a_i are integers, i.e., we will prove that for any real numbers a_i the ratio b_i/c_i with b_i and c_i defined by the formulas in (a) is equal to $a_0 + \frac{1}{a_1+}\cdots\frac{1}{a_i}$. It is trivial to check the beginning of the induction ($i = 0, 1, 2$). We now suppose that the claim is true through the