very large does not worry us. We never need to work with integers larger than n^2 (when we multiply integers modulo n).

We now describe in sequence how the continued fraction algorithm works. All we do is use the factor-base method in §3, except with Proposition V.4.3 replacing random choice of the b_i's.

Continued fraction factoring algorithm. Let n be the integer to be factored. All computations below will be done modulo n, i.e., products and sums of integers will be reduced modulo n to their least nonnegative residue (or least absolute residue in step (3)). First set $b_{-1} = 1$, $b_0 = a_0 = [\sqrt{n}\,]$, and $x_0 = \sqrt{n} - a_0$. Compute $b_0^2 \ mod\ n$ (which will be $b_0^2 - n$). Next, for $i = 1, 2, \ldots$ successively:

1. Set $a_i = [1/x_{i-1}]$ and then $x_i = 1/x_{i-1} - a_i$.
2. Set $b_i = a_i b_{i-1} + b_{i-2}$ (reduced modulo n).
3. Compute $b_i^2 \ mod\ n$. After doing this for several i, look at the numbers in step 3 which factor into $\pm$ a product of small primes. Take your factor base B to consist of -1, the primes which occur in more than one of the $b_i^2 \ mod\ n$ (or which occur to an even power in just one $b_i^2 \ mod\ n$). Then list all of the numbers $b_i^2 \ mod\ n$ which are B-numbers, along with the corresponding vectors $\vec{\epsilon}_i$ of zeros and ones. If possible, find a subset whose vectors sum to zero. Set $b = \prod b_i$ (working modulo n and taking the product over the subset for which $\sum \vec{\epsilon}_i = 0$). Set $c = \prod p_j^{\gamma_j}$, where p_j are the elements of B (except for -1) and $\gamma_j = \frac{1}{2}\sum \alpha_{ij}$ (with the sum taken over the same subset of i; see §3). If $b \not\equiv \pm c \ mod\ n$, then $g.c.d.(b+c, n)$ is a nontrivial factor of n. If $b \equiv \pm c \ mod\ n$, then look for another subset of i such that $\sum \vec{\epsilon}_i = 0$. If it is not possible to find any subset of i such that $\sum \vec{\epsilon}_i = 0$, then you must continue computing more a_i, b_i, and $b_i^2 \ mod\ n$, enlarging your factor base B if necessary.

Remark. In order to be able to compute $c = \prod p_j^{\gamma_j}$, it is efficient if for each B-number $b_i^2 \ mod\ n$ we record the vector $\vec{\alpha}_i = \{\ldots, \alpha_{ij}, \ldots\}_j$ rather than $\vec{\epsilon}_i$, which is simply $\vec{\alpha}_i$ reduced modulo 2.

Example 2. Use the above algorithm to factor 9073.

Solution. We first make a list of successive a_i's and b_i's (where b_i is the least nonnegative residue modulo n of $a_i b_{i-1} + b_{i-2}$), along with the corresponding least absolute residue modulo n of b_i^2:

i	0	1	2	3	4
a_i	95	3	1	26	2
b_i	95	286	381	1119	2619
$b_i^2 \ mod\ n$	-48	139	-7	87	-27

Looking at the last line of the table, we see that it is reasonable to set $B = \{-1, 2, 3, 7\}$. Then $b_i^2 \ mod\ n$ is a B-number for $i = 0, 2, 4$. The corresponding vectors $\vec{\alpha}_i$ are, respectively, $\{1, 4, 1, 0\}$, $\{1, 0, 0, 1\}$, and $\{1, 0, 3, 0\}$. The sum of the first and third is zero modulo 2. So let us choose $b = 95 \cdot 2619 \equiv 3834 \ mod\ 9073$, and $c = 2^2 \cdot 3^2 = 36$. Thus, $3834^2 \equiv 36^2 \ mod\ 9073$.