n is a product of two integers which are close to one another. This method, called "Fermat factorization," is based on the fact that n is then equal to a difference of two squares, one of which is very small.

Proposition V.3.1. *Let n be a positive odd integer. There is a 1-to-1 correspondence between factorizations of n in the form $n = ab$, where $a \geq b > 0$, and representations of n in the form $t^2 - s^2$, where s and t are nonnegative integers. The correspondence is given by the equations*

$$t = \frac{a+b}{2}, \qquad s = \frac{a-b}{2}; \qquad\qquad a = t + s, \qquad b = t - s.$$

Proof. Given such a factorization, we can write $n = ab = ((a+b)/2)^2 - ((a-b)/2)^2$, so we obtain the representation as a difference of two squares. Conversely, given $n = t^2 - s^2$ we can factor the right side as $(t+s)(t-s)$. The equations in the proposition explicitly give the 1-to-1 correspondence between the two ways of writing n.

If $n = ab$ with a and b close together, then $s = (a-b)/2$ is small, and so t is only slightly larger than $\sqrt{n}$. In that case, we can find a and b by trying all values for t starting with $[\sqrt{n}] + 1$, until we find one for which $t^2 - n = s^2$ is a perfect square.

In what follows, we shall assume that n is never a perfect square, so as not to have to worry about trivial exceptions to the procedures and assertions.

Example 1. Factor 200819.

Solution. We have $[\sqrt{200819}] + 1 = 449$. Now $449^2 - 200819 = 782$, which is not a perfect square. Next, we try $t = 450$: $450^2 - 200819 = 1681 = 41^2$. Thus, $200819 = 450^2 - 41^2 = (450+41)(450-41) = 491 \cdot 409$.

Notice that if the a and b are not close together for any factorization $n = ab$, then the Fermat factorization method will eventually find a and b, but only after trying a large number of $t = [\sqrt{n}] + 1, [\sqrt{n}] + 2, \ldots$. There is a generalization of Fermat factorization that often works better in such a situation. We choose a small k, successively set $t = [\sqrt{kn}] + 1, [\sqrt{kn}] + 2$, etc., until we obtain a t for which $t^2 - kn = s^2$ is a perfect square. Then $(t+s)(t-s) = kn$, and so $t + s$ has a nontrivial common factor with n which can be found by computing $g.c.d.(t+s, n)$.

Example 2. Factor 141467.

Solution. If we try to use Fermat factorization, setting $t = 377, 378, \ldots$, after a while we tire of trying different t's. However, if we try $t = [\sqrt{3n}] + 1 = 652, \ldots$ we soon find that $655^2 - 3 \cdot 141467 = 68^2$, at which point we compute $g.c.d.(655 + 68, 141467) = 241$. We conclude that $141467 = 241 \cdot 587$. The reason why generalized Fermat factorization worked with $k = 3$ is that there is a factorization $n = ab$ with b close to $3a$. With $k = 3$ we need to try only four t's, whereas with simple Fermat factorization (i.e., $k = 1$) it would have taken thirty-eight t's.

Factor bases. There is a generalization of the idea behind Fermat factorization which leads to a much more efficient factoring method. Namely,