we use the fact that any time we are able to obtain a congruence of the form $t^2 \equiv s^2 \ mod\ n$ with $t \not\equiv \pm s \ mod\ n$, we immediately find a factor of n by computing $g.c.d.(t+s, n)$ (or $g.c.d.(t-s, n)$). This is because we have $n|t^2 - s^2 = (t+s)(t-s)$, while n does not divide $t+s$ or $t-s$; thus $g.c.d.(t+s, n)$ must be a proper factor a of n, and then $b = n/a$ divides $g.c.d.(t-s, n)$.

Example 4. Suppose we want to factor 4633, and happen to notice that 118^2 leaves a remainder of $25 = 5^2$ modulo 4633. Then we find that $g.c.d.(118+5, 4633) = 41$, $g.c.d.(118-5, 4633) = 113$, and $4633 = 41 \cdot 113$. A skeptic might wonder how in Example 4 we ever came upon a number such as 118 whose square has least positive residue also a perfect square. Would a random selection of various b soon yield one for which the least positive residue of $b^2 \ mod\ n$ is a perfect square? That is very unlikely if n is large, so it is necessary to generalize this method in a way that allows much greater flexibility in choosing the b's for which we consider $b^2 \ mod\ n$. The idea is to choose several b_i's which have the property that $b_i^2 \ mod\ n$ is a product of small prime powers, and such that some subset of them, when multiplied together, give a b whose square is congruent to a perfect square modulo n. We now give the details.

By the "least absolute residue" of a number a modulo n we mean the integer in the interval from $-n/2$ to $n/2$ to which a is congruent. We shall denote this $a \ mod\ n$.

Definition. A *factor base* is a set $B = \{p_1, p_2, \ldots, p_h\}$ of distinct primes, except that p_1 may be the integer -1. We say that the square of an integer b is a *B-number* (for a given n) if the least absolute residue $b^2 \ mod\ n$ can be written as a product of numbers from B.

Example 5. For $n = 4633$ and $B = \{-1, 2, 3\}$, the squares of the three integers 67, 68 and 69 are B-numbers, because $67^2 \equiv -144 \ mod\ 4633$, $68^2 \equiv -9 \ mod\ 4633$, and $69^2 \equiv 128 \ mod\ 4633$.

Let $\mathbf{F}_2^h$ denote the vector space over the field of two elements which consists of h-tuples of zeros and ones. Given n and a factor base B containing h numbers, we show how to correspond a vector $\vec{\epsilon} \in \mathbf{F}_2^h$ to every B-number. Namely, we write $b^2 \ mod\ n$ in the form $\prod_{j=1}^h p_j^{\alpha_j}$ and set the j-th component ϵ_j equal to $\alpha_j \ mod\ 2$, i.e., $\epsilon_j = 0$ if α_j is even, and $\epsilon_j = 1$ if α_j is odd.

Example 6. In the situation of Example 5, the vector corresponding to 67 is $\{1, 0, 0\}$, the vector corresponding to 68 is $\{1, 0, 0\}$, and the vector corresponding to 69 is $\{0, 1, 0\}$.

Suppose that we have some set of B-numbers $b_i^2 \ mod\ n$ such that the corresponding vectors $\vec{\epsilon}_i = \{\epsilon_{i1}, \ldots, \epsilon_{ih}\}$ add up to the zero vector in $\mathbf{F}_2^h$. Then the product of the least absolute residues of b_i^2 is equal to a product of *even* powers of all of the p_j in B. That is, if for each i we let a_i denote the least absolute residue of $b_i^2 \ mod\ n$ and we write $a_i = \prod_{j=1}^h p_j^{\alpha_{ij}}$, we obtain