$$\prod a_i = \prod_{j=1}^{h} p_j^{\sum_i \alpha_{ij}},$$

with the exponent of each p_j an even number on the right. Then the right hand side is the square of $\prod_j p_j^{\gamma_j}$ with $\gamma_j = \frac{1}{2}\sum_i \alpha_{ij}$. Thus, if we set $b = \prod_i b_i \ mod\ n$ (least positive residue) and $c = \prod_j p_j^{\gamma_j}\ mod\ n$ (least positive residue), we obtain two numbers b and c, constructed in quite different ways (one as a product of b_i's and the other as a product of p_j's) whose squares are congruent modulo n.

It may happen that $b \equiv \pm c\ mod\ n$, in which case we are out of luck, and we must start again with another collection of B-numbers whose corresponding vectors sum to zero. This will happen, for example, if we foolishly choose b_i less than $\sqrt{n/2}$, in which case all of the vectors are zero-vectors, and we end up with a trivial congruence.

But for more randomly chosen b_i, because n is composite we would expect that b and c would happen to be congruent (up to ± 1) modulo n at most 50% of the time. This is because any square modulo n has $2^r \geq 4$ square roots if n has r different prime factors (see Exercise 7 of § I.3); thus a random square root of b^2 has only a $2/2^r \leq \frac{1}{2}$ chance of being either b or $-b$. And as soon as we have b and c with $b^2 \equiv c^2\ mod\ n$ but $b \not\equiv \pm c\ mod\ n$ we can immediately find a nontrivial factor $g.c.d.(b+c, n)$, as we saw before. Thus, if we go through the above procedure for finding b and c until we find a pair that gives us a nontrivial factor of n, we see that there is at most a 2^{-k} probability that this will take more than k tries.

In practice, how do we choose our factor base B and our b_i? One method is to start with B consisting of the first h primes (or the first $h-1$ primes together with $p_1 = -1$) and choose random b_i's until we find several whose squares are B-numbers. Another method is to start by choosing some b_i's for which $b_i^2\ mod\ n$ (least absolute residue) is small in absolute value (for example, take b_i close to $\sqrt{kn}$ for small multiples kn; another way will be explained in §4). Then choose B to consist of a small set of small primes (and usually $p_1 = -1$) so that several of the $b_i^2\ mod\ n$ can be expressed in terms of the numbers in B.

Example 7. In the situation of Examples 5–6, we actually chose 67 and 68 because they are close to $\sqrt{4633}$. After finding that $67^2 \equiv -144\ mod\ 4633$ and $68^2 \equiv -9\ mod\ 4633$, we saw that we can choose $B = \{-1, 2, 3\}$. As we saw before, the vectors corresponding to $b_1 = 67$ and $b_2 = 68$ are $\{1, 0, 0\}$ and $\{1, 0, 0\}$, which add up to the zero vector. We compute $b = 67 \cdot 68\ mod\ 4633 = -77$ and $c = 2^{\gamma_2} \cdot 3^{\gamma_3}$ (we can ignore the power of -1 in c), i.e., $c = 36$. Fortunately, $-77 \not\equiv \pm 36\ mod\ 4633$, and so we find a factor by computing $g.c.d.(-77 + 36, 4633) = 41$.

When can we be sure that we have enough b_i to find a sum of $\vec{\epsilon}_i$ which is the zero vector? In other words, given a collection of vectors in $\mathbf{F}_2^h$, when can we be sure of being able to find a subset of them which sums to zero? To ask for this is to ask for the collection of vectors to be *linearly*