dependent over the field $\mathbf{F}_2$. According to basic linear algebra (which applies just as well over the field $\mathbf{F}_2$ as over the real numbers), this is guaranteed to occur as soon as we have $h+1$ vectors. Thus, at worst we'll have to generate $h+1$ different B-numbers in order to find our first example of $(\prod_i b_i)^2 \equiv (\prod_j p_j^{\gamma_j})^2$ *mod* n. (Example 7 shows that we may very well obtain linearly dependent vectors sooner; in that case $h=3$, and we were able to stop after finding two B-numbers.) If h is large, we might not be able to notice by inspection a subset of vectors which sums to zero; in that case, we must write the vectors as rows in a matrix and use the row-reduction technique of linear algebra to find a linearly dependent set of rows.

Example 8. Let $n = 4633$. Find the smallest factor-base B such that the squares of 68, 69 and 96 are B-numbers, and then factor 4633.

Solution. As we saw before, 68^2 *mod* n and 69^2 *mod* n are products of -1, 2, and 3; since 96^2 *mod* $n = -50$, the least absolute residues of all three squares can be written in terms of the factor-base $B = \{-1, 2, 3, 5\}$. We already computed the vectors $\epsilon_1 = \{1,0,0,0\}$ and $\epsilon_2 = \{0,1,0,0\}$ corresponding to 68 and 69, respectively. Since $96^2 \equiv -50$ *mod* 4633, we have $\epsilon_3 = \{1,1,0,0\}$. Since the sum of these vectors is zero, we can take $b = 68\cdot 69\cdot 96 \equiv 1031$ *mod* 4633 and $c = 2^4\cdot 3\cdot 5 = 240$. Then we obtain $g.c.d.(240+1031, 4633) = 41$.

Examples 7 and 8 indicate how one might proceed systematically to find several b_i such that the least absolute residue b_i^2 *mod* n is a product of small primes. The likelihood that b_i^2 *mod* n is a product of small primes is greater if this residue is small in absolute value. Thus, we might successively try integers b_i close to $\sqrt{kn}$ for small integers k. For example, we might choose $[\sqrt{kn}]$ and $[\sqrt{kn}]+1$ for $k = 1, 2, \ldots$.

Example 9. Let us factor $n = 1829$ by taking for b_i all integers of the form $[\sqrt{1829k}]$ and $[\sqrt{1829k}]+1$, $k = 1, 2, \ldots$, such that b_i^2 *mod* n is a product of primes less than 20. For such b_i we write b_i^2 *mod* $n = \prod_j p_j^{\alpha_{ij}}$ and tabulate the α_{ij}. After taking $k = 1, 2, 3, 4$, we have the following table, in which the number at the top of the j-th column is p_j and the entry in the i-th row beneath p_j is the power of p_j which occurs in b_i^2 *mod* n:

b_i	-1	2	3	5	7	11	13
42	1	–	–	1	–	–	1
43	–	2	–	1	–	–	–
61	–	–	2	–	1	–	–
74	1	–	–	–	–	1	–
85	1	–	–	–	1	–	1
86	–	4	–	1	–	–	–

We now look for a subset of rows whose entries sum to an even number in each column. We see at a glance that the 2nd and 6th rows sum to the even row – 6 – 2 – – – . This leads to the congruence $(b_2\cdot b_6)^2 \equiv (2^{6/2}\cdot 5^{2/2})^2$ *mod* n, i.e., $(43\cdot 86)^2 \equiv 40^2$ *mod* 1829. But since