

Example in Washington/Trapp, page 189-191.

Factorization of $n = 3837523$ using the remainders of some squares $(\text{mod } n)$. Note, in the book there is a 7th column for the prime 17, which is all zeros and so we can safely delete it and we only consider the seven primes 2, 3, 5, 7, 11, 13, 19 to factor the remainders. The following matrix gives the exponent vectors for the remainders of the selected squares $(\text{mod } n)$. The integers, whose squares we compute, are in the first column. They are all of the form $[\sqrt{in} + j]$ as discussed in the book and i, j are listed in column 2, 3.

$$F := \left(\begin{array}{cc|cccccccc|c} n = 3837523 & i & j & 2 & 3 & 5 & 7 & 11 & 13 & 19 & \text{remainder} \\ \hline 9398^2 & 23 & 4 & 0 & 0 & 5 & 0 & 0 & 0 & 1 & 59375 \\ 19095^2 & 95 & 2 & 2 & 0 & 1 & 0 & 1 & 1 & 1 & 54340 \\ 1964^2 & 1 & 6 & 0 & 2 & 0 & 0 & 0 & 3 & 0 & 19773 \\ 17078^2 & 76 & 1 & 6 & 2 & 0 & 0 & 1 & 0 & 0 & 6336 \\ 8077^2 & 17 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 38 \\ 3397^2 & 3 & 4 & 5 & 0 & 1 & 0 & 0 & 2 & 0 & 27040 \\ 14262^2 & 53 & 1 & 0 & 0 & 2 & 2 & 0 & 1 & 0 & 15925 \end{array} \right)$$

So for example $9398^2 \pmod{n} = 59375 = 2^0 \cdot 3^0 \cdot 5^5 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot 19^1$. To find a product of the remainders, which is a square, we look compute the following matrix $A := F \pmod{2}$ by replacing an even number in an exponent vector by 0 and an odd number in an exponent vector by 1:

$$A := \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

A basis for left nullspace of A is given by the following three vectors of the matrix N using standard row reduction: (note the last column of A is the sum of the first and the forth column of A).

$$N := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Taking the sum of the corresponding exponent vectors in F .

$$\begin{array}{ccccccc} 2 & 3 & 5 & 7 & 11 & 13 & 19 \\ \hline 6 & 0 & 6 & 0 & 0 & 2 & 2 \\ 8 & 4 & 6 & 0 & 2 & 4 & 2 \\ 0 & 2 & 2 & 2 & 0 & 4 & 0 \end{array}$$

and dividing the entries by 2 to get the exponent vector of a square root we get:

2	3	5	7	11	13	19
3	0	3	0	0	1	1
4	2	3	0	1	2	1
0	1	1	1	0	2	0

This tells us using the first vector of N and the corresponding numbers 9398, 8077 and 3397:

$$(9398 \cdot 8077 \cdot 3397)^2 \equiv (2^3 \cdot 3^0 \cdot 5^3 \cdot 7^0 \cdot 11^0 \cdot 13^1 \cdot 19^1)^2 \pmod{n}$$

Note that on the left hand side $X := 9398 \cdot 8077 \cdot 3397 \pmod{n} = 3590523$ and on the right hand side $Y := 2^3 \cdot 3^0 \cdot 5^3 \cdot 7^0 \cdot 11^0 \cdot 13^1 \cdot 19^1 \pmod{n} = 247000$. So we get:

$$3590523^2 \equiv 247000^2 \pmod{n}$$

and we can test $\gcd(X - Y, n)$. It is n .

Applying this recipe to the second vector of N , the left hand side is

$$9398 \cdot 19095 \cdot 1964 \cdot 17078 \pmod{n} = 2230387$$

and the right hand side gives

$$635778000 \pmod{n} = 2586705,$$

so we get

$$2230387^2 \equiv 2586705^2 \pmod{n}$$

and $\gcd(2230387 - 2586705, n) = 1093$.