Thisisanexampleofthequadraticsieveinwhichweattempttofactorise$n = 87463$

> $with(numtheory)$:

> $n := 500657$;

$$n := 500657 \tag{1}$$

> $t := \mathrm{trunc}(evalf(\mathrm{sqrt}(n)))$;

$$t := 707 \tag{2}$$

>

We begin by establishing our factor base B which is the first six primes p such that (n/p) = 1 (i.e. the first 6 primes p for which n is a quadratic residue mod p).

> $a := 2$: i $:= 0$: while i < 7 do if $legendre(n, a) = 1$ then $print(a)$; $i := i + 1$; end if; $a := nextprime(a)$: end do:

$$\begin{gathered} 2 \\ 11 \\ 13 \\ 19 \\ 23 \\ 29 \\ 31 \end{gathered} \tag{3}$$

> $y := x \to (x + 707)^2 - 500657$;

$$y := x \mapsto (x + 707)^2 - 500657 \tag{4}$$

Hence B = {2, 11, 13, 19, 23, 29, 31}

We now search for numbers for which the factorisation into primes of y(x) is 'B smooth' (i.e. it only contains elements from the set B)

> for x from -100 to 200 do if $\max(ifactors(y(x))) \le 31$ then $print(x, y(x), ifactor(y(x)))$; end if; end do;

$$-97, -128557, -(11)(13)(29)(31)$$

$$-82, -110032, -(2)^4(13)(23)^2$$

$$-31, -43681, -(11)^2(19)^2$$

$$-12, -17632, -(2)^5(19)(29)$$

$$-10, -14848, -(2)^9(29)$$

$$-4, -6448, -(2)^4(13)(31)$$

$$2, 2024, (2)^3(11)(23)$$

$$4, 4864, (2)^8(19)$$

$$46, 66352, (2)^4 (11) (13) (29)$$

$$48, 69368, (2)^3 (13) (23) (29)$$

$$58, 84568, (2)^3 (11) (31)^2$$

$$61, 89167, (13) (19)^3$$

$$102, 153824, (2)^5 (11) (19) (23)$$

$$140, 216752, (2)^4 (19) (23) (31)$$

$$178, 282568, (2)^3 (11) (13)^2 (19) \tag{5}$$

>

We convert the exponents of the factors into a matrix A and then form B which is the same matrix modulo 2. Column 1 of A indicates if y(x) is negative while the second column is the exponents of 2 etc.

B = {-1, 2, 11, 13, 19, 23, 29, 31}

> $A := matrix(15, 8, [1, 0, 1, 1, 0, 0, 1, 1,\ 1, 4, 0, 1, 0, 2, 0, 0,\ 1, 0, 2, 0, 2, 0, 0, 0,\ 1, 5, 0, 0, 1, 0, 1, 0,\ 1, 9, 0, 0, 0, 0, 1, 0,\ 1$

$$A := \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 4 & 0 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 2 & 0 & 2 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 9 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 4 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 8 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 4 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 3 & 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 \\ 0 & 5 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \end{bmatrix} \tag{6}$$

> $B := map(x \rightarrow x \mod 2, op(A));$

$$B := \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \tag{7}$$

We note that row 7 + row 9 + row 10 of B is 0 mod 2.

Row 2 corresponds to x = 2 and row 9 corresponds to x = 46 and row 10 corresponds to x = 48. and so x + t are 709, 753 and 755 respectively. u is the product of these modulo n

>

$$59406 \tag{8}$$

> $u := 625 \cdot 676 \cdot 711 \cdot 768 \mod 500657;$

$$u := 31115 \tag{9}$$

B = {-1, 2, 11, 13, 19, 23, 29, 31}
The numbers used to form v are highlighted in red above and we add the columns and then divide by 2.
–¿ column for -1, sum = (1+1)/2 = 1
–¿ column for 2, sum = (4+8)/2 = 6
–¿ column for 11, sum = (2)/2 = 1
–¿ column for 13, sum = (1+1)/2 = 1
–¿ column for 19, sum = (2+1+3)/2 = 3
–¿ column for 23, sum = (2)/2 = 1
> $v := -1 \cdot 2^6 \cdot 11 \cdot 13 \cdot 19^3 \cdot 23 \mod 500657;$

$$v := 102724 \tag{10}$$

> $u^2 \mod 500657;$

$$373244 \tag{11}$$

> $v^2 \mod 500657;$

$$373244 \tag{12}$$

If we have done our calculations correct we would expect to find that uˆ2 congruent to vˆ2 mod n which we do. We now attempt to find a factor of n by finding the greatest common divisor of u-v and n

> $\gcd(u - v, n);$

$$101 \tag{13}$$

We claim that 101 is a factor of n and confirm this below

> $ifactor(500657);$

$$(101)\,(4957) \tag{14}$$

If we do not find a non-trivial factor this way (i.e. the gcd is 1) then we need to choose a different set f linearly dependent rows and repeat until we find a solution

>

>