

Quadratic Residue Examples

QS1. The Quadratic Residue Sieve Program (QRSP) tests $x = 0, \pm 1, \pm 2, \dots, \pm L$.

If the prime factorization of $q(x)$ involves the 'primes' in the factor base \mathcal{S} , the QRSP computes

- $a = (x + m)$ and
- the $(0,1)$ -vector \underline{e} which gives the exponent modulo 2 in the prime factorization of $q(x)$.

Example : $n = 4601$, $m = \lfloor \sqrt{n} \rfloor = 67$. $\mathcal{S} = \{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23\}$; $L = 10$.

The QRSP finds 13 values of x for which the prime factorization of $q(x)$ involves only 'primes' in \mathcal{S} .

i	x_i	$q(x_i)$	Factorization of $q(x_i)$	a_i	\underline{e}_i (modulo 2)
1	-10	-1352	$-2^3 \times 13^2$	57	(1,1,0,0,0,0,0,0,0)
2	-8	-1120	$-2^5 \times 5 \times 7$	59	(1,1,0,1,1,0,0,0,0)
3	-7	-1001	$-7 \times 11 \times 13$	60	(1,0,0,0,1,1,1,0,0)
4	-6	-880	$-2^4 \times 5 \times 11$	61	(1,0,0,1,0,1,0,0,0)
5	-1	-245	-5×7^2	66	(1,0,0,1,0,0,0,0,0)
6	0	-112	$-2^4 \times 7$	67	(1,0,0,0,1,0,0,0,0)
7	1	23	23	68	(0,0,0,0,0,0,0,0,1)
8	2	160	$2^5 \times 5$	69	(0,1,0,1,0,0,0,0,0)
9	3	299	13×23	70	(0,0,0,0,0,0,1,0,0)
10	4	440	$2^3 \times 5 \times 11$	71	(0,1,0,1,0,1,0,0,0)
11	6	728	$2^3 \times 7 \times 13$	73	(0,1,0,0,1,0,1,0,0)
12	7	875	$5^3 \times 7$	74	(0,0,0,1,1,0,0,0,0)
13	8	1024	2^{10}	75	(0,0,0,0,0,0,0,0,0)

For example, when $i = 3$, $x = -7$, then

$$q(x_3) = (-7 + 67)^2 - 4601 = -1001 = -7 \times 11 \times 13$$

$$a_3 = (-7 + 67) = 60$$

Since the exponents of 7, 11 and 13 are odd (modulo 2)

$$\underline{e}_2 = (1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$$

QS2. Search for subsets of i -indices for which the sum of the \underline{e}_i -vectors is the 0-vector.

In the example, there are at least two sets

$$\mathcal{T}_1 = \{13\} \quad \mathcal{T}_2 = \{2, 6, 8\}$$

QS3. For each such subset \mathcal{T} , the product of the $q(x_i)$ values is a perfect square.

$$\mathcal{T}_1 = \{13\} \quad q_{\mathcal{T}_1} = 2^{10}$$

$$\mathcal{T}_2 = \{2, 6, 8\} \quad q_{\mathcal{T}_2} = 2^{14} \times 5^2 \times 7^2$$

QS4. For each such subset \mathcal{T} , compute the product of the $\{a_i\}$ modulo 4601.

$$\mathcal{T}_1 = \{13\} \quad a_{\mathcal{T}_1} = 75$$

$$\mathcal{T}_2 = \{2, 6, 8\} \quad a_{\mathcal{T}_2} = 59 \times 67 \times 69 = 272757 = 1298 \pmod{4601}$$

QS5. Since the sum of the \mathbf{e}_i -vectors is equal to the 0 vector modulo 2, $q_{\mathcal{T}_j} = a_{\mathcal{T}_j}^2 \pmod{n}$. A factor of n can be found if $\sqrt{q_{\mathcal{T}_j}} \pm a_{\mathcal{T}_j} \neq 0 \pmod{4601}$.

$$\begin{aligned}
 \mathcal{T}_1 &= \{13\} \\
 \sqrt{q_{\mathcal{T}_1}} \pmod{4601} &= 2^5 = 32 \\
 a_{\mathcal{T}_1} \pmod{4601} &= 75 \\
 75 \pm 32 &= 107, 43 \neq 0 \pmod{4601} \\
 \gcd\{43, 4601\} &= 43 \quad \gcd\{107, 4601\} = 107 \\
 \mathcal{T}_2 &= \{2, 6, 8\} \\
 \sqrt{q_{\mathcal{T}_2}} \pmod{4601} &= 2^7 \times 5 \times 7 = 4480 \\
 a_{\mathcal{T}_2} \pmod{4601} &= 1298 \\
 4480 \pm 1298 &= 7788, 3182 \neq 0 \pmod{4601} \\
 \gcd\{4480 - 1298, 4601\} &= 43 \quad \gcd\{4480 + 1298, 4601\} = 107
 \end{aligned}$$

n = 14167 m = 119				
S = {-1, 2, 3, 13, 37, 53, 59, 61, 71, 79, 89}				
i	x _i	q _i	a _i	e(x) (mod 2)
1	0	-6 = -2 × 3	119	(1,1,1,0,0,0,0,0,0,0)
2	-1	-243 = -3 ⁵	118	(1,0,1,0,0,0,0,0,0,0)
3	2	474 = 2 × 3 × 79	121	(0,1,1,0,0,0,0,0,0,1)
4	-3	-711 = -3 ² × 79	116	(1,0,0,0,0,0,0,0,0,1)
5	4	962 = 2 × 13 × 37	123	(0,1,0,1,1,0,0,0,0,0)
6	6	1458 = 2 × 3 ⁶	125	(0,1,0,0,0,0,0,0,0,0)
7	-8	-1846 = -2 × 13 × 71	111	(1,1,0,1,0,0,0,0,1,0)
8	-9	-2067 = -3 × 13 × 53	110	(1,0,1,1,0,1,0,0,0,0)
9	17	4329 = 3 ² × 13 × 37	136	(0,0,0,1,1,0,0,0,0,0)
10	-17	-3763 = -53 × 71	102	(1,0,0,0,0,1,0,0,1,0)
11	18	4602 = 2 × 3 × 13 × 59	137	(0,1,1,1,0,0,1,0,0,0)
12	-20	-4366 = -2 × 37 × 59	99	(1,1,0,0,1,0,1,0,0,0)
13	-21	-4563 = -3 ³ × 13 ²	98	(1,0,1,0,0,0,0,0,0,0)
14	-22	-4758 = -2 × 3 × 13 × 61	97	(1,1,1,1,0,0,0,1,0,0)
15	28	7442 = 2 × 61 ²	147	(0,1,0,0,0,0,0,0,0,0)
16	-33	-6771 = -3 × 37 × 61	86	(1,0,1,0,1,0,0,1,0,0)
17	-34	-6942 = -2 × 3 × 13 × 89	85	(1,1,1,1,0,0,0,0,0,1)
18	39	10797 = 3 × 59 × 61	158	(0,0,1,0,0,0,1,1,0,0)
19	44	12402 = 2 × 3 ² × 13 × 53	163	(0,1,0,1,0,1,0,0,0,0)
20	-48	-9126 = -2 × 3 ³ × 13 ²	71	(1,1,1,0,0,0,0,0,0,0)

n = 14167 m = 119		
S = {-1, 2, 3, 13, 37, 53, 59, 61, 71, 79, 89}		
T	√b _T (modulo n)	a _T (modulo n)
{0, 2, -3}	2 × 3 ² × 79 = 1422	119 × 121 × 116 = 12745
{-1, -21}	3 ⁴ × 13 = 1053	118 × 98 = 11564

$$a = 11564 \quad b = 1053 \quad |a - b| = 10511 \quad a + b = 12617$$

$$\gcd\{10511, 14167\} = 457 \quad \gcd\{12617, 14167\} = 31$$

$$a = 12745 \quad b = 1422 \quad |a - b| = 11323 \quad a + b = 14167$$

$$\gcd\{11323, 14167\} = 1 \quad \gcd\{14167, 14167\} = 1$$