The common known parameters of the signature scheme are the BVMT defining the used FNAA (Table I), the prime value p, and the quadratic non-residue μ used as the structural coefficient in the BVMT. The size of the prime p is to be set equal to 256- to 512- bit. Besides the value p should have the structure $p=eq$, where e is a small even number (for example, having the size 2- to 16- bit) and q is a prime having large size. One can easily generate the value p such that $\mu=2$ is a quadratic non-residue modulo p.

TABLE I. The Used BVMT

∘	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	μe_0	e_3	μe_2
e_2	e_2	e_3	e_0	e_1
e_3	e_3	μe_2	e_1	μe_0

Table 1
The BVMT setting the 4-dimensional FNAA (μ, $\lambda \neq 0$).

·	e_0	e_1	e_2	e_3
e_0	μe_0	0	0	μe_3
e_1	0	λe_1	λe_2	0
e_2	μe_2	0	0	μe_1
e_3	0	λe_3	λe_0	0

$e_0^i(1,0,0,0)$

Usually the multiplication operation of two vectors A and $B=\sum_{j=0}^{m-1} b_j \mathbf{e}_j$ is defined in the following equation:

$$A \circ B = \sum_{i}^{m-1}\sum_{j}^{m-1} a_i b_j (\mathbf{e}_i \circ \mathbf{e}_j).$$

$A = [1,2,3,4]$

$= 1\cdot e_0 + 2\cdot e_1 + 3\cdot e_2 + 4e_3$

$B = [0,3,4,2]$ $\quad m=4$

$q=5$ or $q=7$

$A = \sum_{i=1}^{m} a_i \cdot e_i \qquad B = \sum_{i=1}^{m} b_i \cdot e_i$

$A = a_0\cdot e_0 + a_1\cdot e_1 + a_2\cdot e_2 + a_3\cdot e_3 \qquad B = b_0\cdot e_0 + b_1\cdot e_1 + b_2\cdot e_2 + b_3\cdot e_3$

$$A \circ B = \left(\sum_{i=0}^{m-1} a_i\cdot e_i\right) \circ \left(\sum_{j=0}^{m-1} b_j\cdot e_j\right) = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} (a_i\cdot b_j)(e_i \circ e_j)$$

$$= (a_0b_0)(e_0\circ e_0) + (a_0b_1)(e_0\circ e_1) + (a_0b_2)(e_0\circ e_2) + (a_0b_3)(e_0\circ e_3) +$$

$$(a_1b_0)(e_1\circ e_0) + (a_1b_1)(e_1\circ e_1) + (a_1b_2)(e_1\circ e_2) + (a_1b_3)(e_1\circ e_3) +$$

$$(a_2b_0)(e_2\circ e_0) + (a_2b_1)(e_2\circ e_1) + (a_2b_2)(e_2\circ e_2) + (a_2b_3)(e_2\circ e_3) +$$

$$(a_3b_0)(e_3\circ e_0) + (a_3b_1)(e_3\circ e_1) + (a_3b_2)(e_3\circ e_2) + (a_3b_3)(e_3\circ e_3)$$

$$= (a_0\cdot b_0)(e_0\circ e_0) + (a_0b_3)(e_0\circ e_3) + (a_1b_1)(e_1\circ e_1) + (a_1b_2)(e_1\circ e_2) +$$
$$(a_2b_0)(e_2\circ e_0) + (a_2b_3)(e_2\circ e_3) + (a_3b_1)(e_3\circ e_1) + (a_3b_2)(e_3\circ e_2)$$

$$= (a_0\cdot b_0)\mu e_0 + (a_0b_3)\mu e_3 + (a_1b_1)\lambda e_1 + (a_1b_2)\lambda e_2 +$$
$$(a_2b_0)\mu e_2 + (a_2b_3)\mu e_1 + (a_3b_1)\lambda e_3 + (a_3b_2)\lambda e_0$$

$A = [1, 2, 3, 4] = 1 \cdot e_0 + 2 \cdot e_1 + 3 \cdot e_2 + 4 e_3$

$B = [0, 3, 4, 2] = 0 \cdot e_0 + 3 \cdot e_1 + 4 e_2 + 2 e_3$

$$A \circ B$$

$$= (a_0 \cdot b_0)\, \mu e_0 + (a_0 b_3)\, \mu e_3 + (a_1 b_1)\, \lambda e_1 + (a_1 b_2)\, \lambda e_2 +$$
$$(a_2 b_0)\, \mu e_2 + (a_2 b_3)\, \mu e_1 + (a_3 b_1) \lambda e_3 + (a_3 b_2)\, \lambda e_0$$

$$= (1 \cdot 0)\, \mu e_0 + (1 \cdot 2)\, \mu e_3 + (2 \cdot 3)\, \lambda e_1 + (2 \cdot 4)\, \lambda e_2 +$$
$$(3 \cdot 0)\, \mu e_2 + (3 \cdot 2)\, \mu e_1 + (4 \cdot 3) \lambda e_3 + (4 \cdot 4)\, \lambda e_0$$

$$= 2\mu e_3 + 6\lambda e_1 + 8\lambda e_2 + 6\mu e_1 + 12\lambda e_3 + 16\lambda e_0$$
$$= (2\mu + 12\lambda) e_3 + (6\mu + 6\lambda) e_1 + (8\lambda) e_2 + (16\lambda) e_0$$

assume $\mu, \lambda = 1$

$$A \circ B = 16 e_0 + 12 e_1 + 8 e_2 + 14 e_3 = [16, 12, 8, 14]$$

$$\lambda_B = \sum_{j=0}^{n-1} \mu_j b_j = \mu_0 b_0 + \mu_1 b_1 + \mu_2 b_2 + \mu_3 b_3$$
$$= [b_0, b_1, b_2, b_3]$$

$\langle i, j, k \rangle$

$e_i = (1, 0, 0) \qquad e_j = (0, 1, 0)$

$e_i * e_j = \mu_i \cdot e_j \qquad e_i \circ e_j = \mu_j \cdot e_i$

HDLP basis generation

$N=(n_0,n_1,n_2,n_3)$. Using Table 1one can reduce the vector Eq. (4) to the system of four linear equations and get the following formula describing the set of p^2 different values $L_N=(l_0, l_1, l_2, l_3)$:

$$L_N = \left(d,\ h,\ \frac{n_1(1-\lambda h)}{\mu n_3},\ \frac{n_0(1-\mu d)}{\lambda n_2}\right),\ d,h = 0,\ 1,\ \ldots,p-1. \tag{5}$$

The solutions of the vector equation

$$NX = N \tag{6}$$

defines all local right-sided units R_N corresponding to the vector N. Using Table 1 one can reduce the vector Eq. (4) to the system of four linear equations and get the formula describing the set of p^2 values $R_N=(r_0,r_1,r_2,r_3)$:

$$R_N = \left(d,\ h,\ \frac{n_0(1-\mu d)}{\lambda n_3},\ \frac{n_1(1-\lambda h)}{\mu n_2}\right),\ d,h = 0,\ 1,\ \ldots,p-1. \tag{7}$$

Intersection of the sets (5) and (6) includes p local two-sided units relating to the vector N which are described by the formula:

$$E'_N = \left(d,\ \frac{\lambda n_1 - \mu n_0 + \mu^2 n_0 d}{\lambda^2 n_1},\ \frac{n_0(1-\mu d)}{\lambda n_3},\ \frac{n_0(1-\mu d)}{\lambda n_2}\right), \tag{8}$$
$$d = 0,\ 1,\ \ldots,p-1.$$

The majority of the local units corresponding to some non-invertible vector N are invertible vectors. Actually, each of the sets (5) and (7) contains p^2-p invertible vectors and p non-invertible ones. The set (8) contains $p-1$ invertible vectors and only one non-invertible vector which can be computed using the following formula:

$$E''_N = \left(\frac{n_0}{\lambda n_1+\mu n_0},\ \frac{n_1}{\lambda n_1+\mu n_0},\ \frac{n_2}{\lambda n_1+\mu n_0},\ \frac{n_3}{\lambda n_1+\mu n_0}\right). \tag{9}$$

The last value represents the unit of the cyclic group generated by different powers of the vector N. The value E''_N can be also computed using the formula:

$$E''_N = N^{\omega}. \tag{10}$$

where ω is the local order of the vector N. However the computation on the base of the formula (9) has about 300 times lower computational complexity. The order ω is equal to $p-1$ or to one of the divisors of the value $p-1$.

PQC Signature scheme used

4. Proposed candidates for post-quantum signature scheme

4.1. Signature schemes on the 4-dimensional FNAA

Suppose the owner of the public key (Y,Z,T) wishes to compute signature to the electronic document M. This can be performed using the following three digital signature schemes based on the proposed form of the HDLP.

4.1.1. Signature generation algorithm A

The first signature scheme (based on the first proposed form of the HDLP) has been designed using the Schnorr digital signature protocol [16] as the prototype. The first proposed signature scheme is described as follows.

1 Select at random an integer $k < q$ and compute the vector $V = J \circ N^k \circ U$.
2 Compute the first signature element $v = F_h(M, V)$, where M is document to be signed F_h is the used hash function satisfying the collision-resistance requirement.
3 Compute the second signature element s: $s = k + xv \bmod q$.

OUTPUT: the signature (v, s) to the document M.

4.1.2. Signature verification algorithm A

Verification of the signature (v, s) to the document M is to be performed as follows:

1 Compute the vector V': $V'=Z^s T Y^{-v}$.
2 Compute the hash value v' from the document M to which the vector V' is concatenated: $v' = F_h(M, V')$.
3 If $v' = v$, then the signature is accepted as genuine. Otherwise the signature is rejected.

Proof of the correctness of the signature scheme is as follows:

$$\begin{aligned} V' &= \left(G \circ R'_N \circ N \circ G^{-1}\right)^s \circ (T) \circ \\ &\circ \left(Q \circ N^x \circ L'_N \circ Q^{-1}\right)^{-v} = G \circ \left(R'_N \circ N\right)^s \circ G^{-1} \circ \\ &\circ \left(G \circ E''_N \circ Q^{-1}\right) \circ Q \circ \left(N^x \circ L'_N\right)^{-v} \circ Q^{-1} = \\ &= G \circ R'_N \circ N^s \circ N^{-vx} \circ L'_N \circ Q^{-1} = \\ &= J \circ N^{k+vx} \circ N^{-vx} \circ U = J \circ N^k \circ U \Rightarrow \\ &\Rightarrow V' = V \Rightarrow v' = v. \end{aligned}$$

$$L'_N = \left(d, \lambda^{-1} - \mu\lambda^{-1}d, \frac{a_1}{a_3}d, \frac{a_0(1-\mu d)}{\lambda a_2}\right), d = 0, 1, .., p-1 \quad (22)$$

For the right-sided units one can easily derive the formula:

$$R'_N = \left(d, \lambda^{-1} - \mu\lambda^{-1}d, \quad \frac{a_0(1-\mu d)}{\lambda a_3}, \quad \frac{a_1}{a_2}d\right), \; d = 0, \; 1, \; ..., p-1. \quad (23)$$

Selection of random values d and computation in line with the formulas (22) and (23) gives random units L'_N and R'_N.

Procedure for generating the public key is as follows:

1 Generate a non-invertible vector N of order q and two random invertible vectors Q and G of order q, which satisfy the conditions $Q \circ N \neq N \circ Q$, $G \circ N \neq N \circ G$, and $Q \circ G \neq G \circ Q$.
2 Generate at random the local left-sided unit L'_N (using the formula (22)) and local left-sided unit R'_N (using the formula (23)).
3 Generate a random non-negative integer $x < q$ and compute the vector $Y = Q \circ N^x \circ L'_N \circ Q^{-1}$.
4 Compute the vector $Z = GR'_N NG^{-1}$.
5 Using the formula (9) calculate the local two-sided unit E''_N of the vector N.
6 Compute the vector $T = G \circ E''_N \circ Q^{-1}$.

OUTPUT: the public key in the form the triple of the non-invertible vectors (Y, Z, T).

public key generation: Y, Z, T

2 random invertible vectors: Q, G

$Q = [q_0, q_1, q_2, q_3]$; $q_0 \cdot q_1 \neq q_2 \cdot q_3$

$G = [g_0, g_1, g_2, g_3]$; $g_0 \cdot g_1 \neq g_2 \cdot g_3$

$Q = [1, 2, 3, 4]$ $G = [0, 1, 2, 3]$

1 non-invertible vector: N

$N = [n_0, n_1, n_2, n_3]$; $n_0 \cdot n_1 = n_2 \cdot n_3$

$N = [2, 3, 1, 6]$

$$Q \circ N = \begin{aligned} &(a_0 b_0)(e_0 \circ e_0) + (a_0 b_1)(e_0 \circ e_1) + (a_0 b_2)(e_0 \circ e_2) + (a_0 b_3)(e_0 \circ e_3) + \\ &(a_1 b_0)(e_1 \circ e_0) + (a_1 b_1)(e_1 \circ e_1) + (a_1 b_2)(e_1 \circ e_2) + (a_1 b_3)(e_1 \circ e_3) + \\ &(a_2 b_0)(e_2 \circ e_0) + (a_2 b_1)(e_2 \circ e_1) + (a_2 b_2)(e_2 \circ e_2) + (a_2 b_3)(e_2 \circ e_3) + \\ &(a_3 b_0)(e_3 \circ e_0) + (a_3 b_1)(e_3 \circ e_1) + (a_3 b_2)(e_3 \circ e_2) + (a_3 b_3)(e_3 \circ e_3) \end{aligned}$$

$$= \begin{aligned} &(a_0 b_0) m_0 e_0 + (a_0 b_1) m_0 e_1 + (a_0 b_2) m_0 e_2 + (a_0 b_3) m_0 e_3 + \\ &(a_1 b_0) m_1 e_0 + (a_1 b_1) m_1 e_1 + (a_1 b_2) m_1 e_2 + (a_1 b_3) m_1 e_3 + \\ &(a_2 b_0) m_2 e_0 + (a_2 b_1) m_2 e_1 + (a_2 b_2) m_2 e_2 + (a_2 b_3) m_2 e_3 + \\ &(a_3 b_0) m_3 e_0 + (a_3 b_1) m_3 e_1 + (a_3 b_2) m_3 e_2 + (a_3 b_3) m_3 e_3 \end{aligned}$$

$N \circ Q =$ Same results as above, just changes the orientation of a_n and b_n.

i = 0 1 2 3

base_a : 'e_0', 'e_1', 'e_2', 'e_3' df.at[base_b, base_a]

base_b : 0, 1, 2, 3

```
if type(df.at[base_b[j], base_a[i]]) = str
        product.append('*', df.at[base_b[j], base_a[i]])

elif type(df.at[base_b[j], base_a[i]]) = int
        product * df.at[base_b[j], base_a[i]])
```

Quanternion

- noncommutative division algebra

$i^2 = j^2 = K^2 = i \cdot j \cdot K = -1$

The set of quaternions is denoted $\mathbb{H}$ and can be written as a linear combination:

$\mathbb{H} = a \cdot 1 + b \cdot i + c \cdot j + d \cdot K$ (a, b, c, d must be explicit real numbers)

Can be represented using complex 2×2 matrices

$$\mathbb{H} = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$$

if $a \cdot b = c \cdot d$ set $a=1, b=2, c=2, d=1$

$$\mathbb{H} = \begin{bmatrix} 1+i2 & 2+i1 \\ -2+i1 & 1-i2 \end{bmatrix} \rightarrow |\mathbb{H}| = (1+i2)(1-i2) - (2+i1)(-2+i1)$$

$$= 1 - i2 + i2 - i^2 2 - (-4 + i2 - i2 + i^2) = 1 - (-1) \cdot 2 - (-4 + (-1)) = 1 + 2 + 5 = 8$$

if $a \cdot b \neq c \cdot d$ set $a=1, b=2, c=3, d=4$

$$\mathbb{H} = \begin{bmatrix} 1+i2 & 3+i4 \\ -3+i4 & 1-i2 \end{bmatrix} \rightarrow |\mathbb{H}| = (1+i2)(1-i2) - (3+i4)(-3+i4)$$

$$= 1 - i2 + i2 - i^2 2 - (-9 + i12 - i12 + i^2 16) = 1 + 2 - (-9 - 16) = 3 + 25 = 28$$

base vector multiplication table for quaternions

	1	i	j	K
1	1	i	j	K
i	i	-1	K	$-j$
j	j	$-K$	-1	i
K	K	j	$-i$	-1

basis_1 $\circ$ basis_2

Quaternion formation and conjugate

$$a = a_1 + a_2 \cdot i + a_3 \cdot j + a_4 \cdot k \qquad \bar{a} = a_1 - a_2 \cdot i - a_3 j - a_4 \cdot k$$

Sum of two quaternions

$$a + b = (a_1 + b_1) + (a_2 + b_2) i + (a_3 + b_3) j + (a_4 + b_4) k$$

Product of two quaternions

$$\begin{aligned} a \cdot b = {} & (a_1 \cdot b_1 - a_2 \cdot b_2 - a_3 \cdot b_3 - a_4 \cdot b_4) + (a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_4 - a_4 \cdot b_3) i + \\ & (a_1 \cdot b_3 - a_2 \cdot b_4 + a_3 \cdot b_1 + a_4 \cdot b_2) j + (a_1 \cdot b_4 + a_2 \cdot b_3 - a_3 \cdot b_2 + a_4 \cdot b_1) k \end{aligned}$$

1 Generate a non-invertible vector N of order q and two random invertible vectors Q and G of order q, which satisfy the conditions $Q \circ N \neq N \circ Q$, $G \circ N \neq N \circ G$, and $Q \circ G \neq G \circ Q$.
2 Generate at random the local left-sided unit L'_N (using the formula (22)) and local left-sided unit R'_N (using the formula (23)).
3 Generate a random non-negative integer $x < q$ and compute the vector $Y = Q \circ N^x \circ L'_N \circ Q^{-1}$.
4 Compute the vector $Z = GR'_N NG^{-1}$.
5 Using the formula (9) calculate the local two-sided unit E''_N of the vector N.
6 Compute the vector $T = G \circ E''_N \circ Q^{-1}$.

OUTPUT: the public key in the form the triple of the non-invertible vectors (Y, Z, T).

Except the elements of the public key and integer q, all other values used in the described algorithm are secret. However, only the integer x and the triple of vectors (N,J,U), where $J = G \circ R'_N$ and $U = L'_N \circ Q^{-1}$, represent the private key that is needed to compute digital signatures.

$N=(n_0,n_1,n_2,n_3)$. Using Table 1 one can reduce the vector Eq. (4) to the system of four linear equations and get the following formula describing the set of p^2 different values $L_N = (l_0, l_1, l_2, l_3)$:

$$L_N = \left(d,\ h,\ \frac{n_1(1-\lambda h)}{\mu n_3},\ \frac{n_0(1-\mu d)}{\lambda n_2}\right),\ d,h = 0,\ 1,\ \ldots, p-1. \tag{5}$$

The solutions of the vector equation

$$NX = N \tag{6}$$

defines all local right-sided units R_N corresponding to the vector N. Using Table 1 one can reduce the vector Eq. (4) to the system of four linear equations and get the formula describing the set of p^2 values $R_N=(r_0,r_1,r_2,r_3)$:

$$R_N = \left(d,\ h,\ \frac{n_0(1-\mu d)}{\lambda n_3},\ \frac{n_1(1-\lambda h)}{\mu n_2}\right),\ d,h = 0,\ 1,\ \ldots, p-1. \tag{7}$$

Intersection of the sets (5) and (6) includes p local two-sided units relating to the vector N which are described by the formula:

$$E'_N = \left(d,\ \frac{\lambda n_1 - \mu n_0 + \mu^2 n_0 d}{\lambda^2 n_1},\ \frac{n_0(1-\mu d)}{\lambda n_3},\ \frac{n_0(1-\mu d)}{\lambda n_2}\right), \tag{8}$$

$d = 0,\ 1,\ \ldots, p-1.$

The majority of the local units corresponding to some non-invertible vector N are invertible vectors. Actually, each of the sets (5) and (7) contains $p^2 - p$ invertible vectors and p non-invertible ones. The set (8) contains $p - 1$ invertible vectors and only one non-invertible vector which can be computed using the following formula:

$$E''_N = \left(\frac{n_0}{\lambda n_1 + \mu n_0},\ \frac{n_1}{\lambda n_1 + \mu n_0},\ \frac{n_2}{\lambda n_1 + \mu n_0},\ \frac{n_3}{\lambda n_1 + \mu n_0}\right). \tag{9}$$

$$L'_N = \left(d, \lambda^{-1} - \mu\lambda^{-1}d, \frac{a_1}{a_3}d, \frac{a_0(1-\mu d)}{\lambda a_2}\right), d = 0, 1, .., p-1 \tag{22}$$

For the right-sided units one can easily derive the formula:

$$R'_N = \left(d, \lambda^{-1} - \mu\lambda^{-1}d,\ \frac{a_0(1-\mu d)}{\lambda a_3},\ \frac{a_1}{a_2}d\right),\ d = 0,\ 1,\ \ldots, p-1. \tag{23}$$

$A = a_0 + a_1 i + a_2 j + a_3 k$

$p = 2q+1$

Q, G invertible vectors

$a_0 \cdot a_1 \neq a_2 \cdot a_3$

N non-invertible vector

$a_0 \cdot a_1 = a_2 \cdot a_3$

A, N, Ln, q

B, N, Rn, q

A, B, E'', q

$q = 7$ $\quad Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$p = 2q + 1 = 15 \bmod 7 = 1$

$\langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 0\} \rightarrow$ p generates the cyclic group

$$V' = \left(G \circ R'_N \circ N \circ G^{-1}\right)^s \circ (T) \circ$$
$$\circ \left(Q \circ N^x \circ L'_N \circ Q^{-1}\right)^{-v} = G \circ (R'_N \circ N)^s \circ G^{-1} \circ$$
$$\circ \left(G \circ E''_N \circ Q^{-1}\right) \circ Q \circ (N^x \circ L'_N)^{-v} \circ Q^{-1} =$$
$$= G \circ R'_N \circ N^s \circ N^{-vx} \circ L'_N \circ Q^{-1} =$$
$$= J \circ N^{k+vx} \circ N^{-vx} \circ U = J \circ N^k \circ U \Rightarrow$$
$$\Rightarrow V' = V \Rightarrow v' = v.$$

$$\frac{1}{\lambda} - \frac{n \cdot d}{\lambda} = h$$

$$L_N = \left(d, h, \frac{n_1(1-\lambda h)}{\mu n_3}, \frac{n_0(1-\mu d)}{\lambda n_2}\right), \; d, h = 0, \; 1, \; \ldots, p-1.$$

$$L'_N = \left(d, \lambda^{-1} - \mu\lambda^{-1}d, \frac{a_1}{a_3}d, \frac{a_0(1-\mu d)}{\lambda a_2}\right), d = 0, 1, .., p-1$$

In the case L_N has independent variables d and h that contain values from 0 to p-1, there can be a total of p^2 vector combinations.
Given that our prime number $q = 7$, and $p = 2 \cdot q + 1 = 15$, then we should expect to have 225 quaternion vectors of L_N and at least one of those vectors should match L'_N as this would contain the same independent variable d, giving 15 different combinations of L'_N.
If vectors L_N and L'_N contain the same d value and match, then we've found the right HDLP pair to use for the Public Key generation.
The same applies to R_N and R'_N

L R
A∘B

$$3 \cdot 2 = 6 \cdot 1$$

$p = 13 \qquad d, h = 0, 1, \cdots 14$

$n_0 = N[0]$

$n_1 = N[1]$

$\frac{1}{\lambda} - \frac{\mu d}{\lambda}$

for h in range 13

  for d in range 13

$$L_N = \left(d, h, \frac{n_1(1-\lambda h)}{\mu n_3}, \frac{n_0(1-\mu d)}{\lambda n_2}\right) \mod 7$$

$$L_{N\_dash} = \left(d, \lambda^{-1} - \mu \cdot \lambda^{-1} \cdot d, \frac{n_1}{n_3} \cdot d, \frac{n_0(1-\mu d)}{\lambda n_2}\right) \mod 7$$

$$R_N = \left(d, h, \frac{n_0(1-\mu d)}{\lambda n_3}, \frac{n_1(1-\lambda h)}{\mu n_2}\right) \mod 7$$

$$R_{N\_dash} = \left(d, \frac{1-\mu d}{\lambda}, \frac{n_0(1-\mu d)}{\lambda n_3}, \frac{n_1}{n_2} d\right) \mod 7$$

if quart. L_N == quart. L_{N_dash}

  print(d)

check for non-invertible E''_N

$$E\_double = \left(\frac{n_0}{\lambda n_1 + \mu n_0}, \frac{n_1}{\lambda n_1 + \mu n_0}, \frac{n_2}{\lambda n_1 + \mu n_0}, \frac{n_3}{\lambda n_1 + \mu n_0}\right) \mod 7$$

E_double_q = quart. E_double

for d in range p

$$E\_prime = \left(d, \frac{\lambda n_1 - \mu n_0 + \mu^2 \cdot n_0 \cdot d}{\lambda^2 \cdot n_1}, \frac{n_0(1-\mu d)}{\lambda n_3}, \frac{n_0(1-\mu d)}{\lambda \cdot n_2}\right) \mod 7$$

E_prime_q = quart. E_prime

if (E_{prime_q} = E_double_q)

  print(d)