Reed-Solomon Encoding and Decoding

Set the parameters here.

In[1]:=
```
m = 8; n = 14; p = 17; e = Floor[(n - m) / 2]
```

Out[1]= 3

Construct the code matrix for `RS (m, n, p)`.

In[2]:=
```
(code = Table[PowerMod[j, i, p], {i, 0, m - 1}, {j, 0, n - 1}]) // MatrixForm
```

Out[2]//MatrixForm=

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 0 & 1 & 4 & 9 & 16 & 8 & 2 & 15 & 13 & 13 & 15 & 2 & 8 & 16 \\ 0 & 1 & 8 & 10 & 13 & 6 & 12 & 3 & 2 & 15 & 14 & 5 & 11 & 4 \\ 0 & 1 & 16 & 13 & 1 & 13 & 4 & 4 & 16 & 16 & 4 & 4 & 13 & 1 \\ 0 & 1 & 15 & 5 & 4 & 14 & 7 & 11 & 9 & 8 & 6 & 10 & 3 & 13 \\ 0 & 1 & 13 & 15 & 16 & 2 & 8 & 9 & 4 & 4 & 9 & 8 & 2 & 16 \\ 0 & 1 & 9 & 11 & 13 & 10 & 14 & 12 & 15 & 2 & 5 & 3 & 7 & 4 \end{pmatrix}$$

Select a random message vector.

In[3]:=
```
mess = RandomInteger[{0, p - 1}, m]
```

Out[3]= {1, 12, 0, 9, 16, 5, 5, 15}

Encode the message.

In[4]:=
```
enc = Mod[mess.code, p]
```
Out[4]=
```
{1, 12, 16, 5, 1, 9, 3, 14, 15, 12, 2, 3, 4, 6}
```

Put errors in at most $e = (n - m) / 2$ random places.

In[5]:=
```
recv = Mod[enc + Sum[UnitVector[n, RandomInteger[{1, n}]] * RandomInteger[{0, p - 1}], {e}],
```
Out[5]=
```
{1, 12, 16, 5, 1, 9, 3, 9, 15, 12, 6, 3, 4, 6}
```

In[6]:=
```
Mod[recv - enc, p]
```
Out[6]=
```
{0, 0, 0, 0, 0, 0, 0, 12, 0, 0, 4, 0, 0, 0}
```

Error locator polynomial $E(x)$ of degree e with undetermined coefficients

In[7]:=
```
eund = x^e + Sum[u[i] x^i, {i, 0, e - 1}]
```
Out[7]= $x^3 + u[0] + x\, u[1] + x^2\, u[2]$

Key polynomial $Q(x)$ of degree less than $m + e$ with undetermined coefficients

In[8]:=
```
qund = Sum[v[i] x^i, {i, 0, m + e - 1}]
```
Out[8]= $v[0] + x\, v[1] + x^2\, v[2] + x^3\, v[3] + x^4\, v[4] + x^5\, v[5] + x^6\, v[6] + x^7\, v[7] + x^8\, v[8] + x^9\, v[9] + x^{10}\, v[10]$

Table of values $r[i]\, E(i) - Q(i)$. We will solve for these to be zero.

In[9]:=
```
(eqns = Table[Expand[recv[[i + 1]] (eund /. x → i) - (qund /. x → i), Modulus → p], {i, 0, n - 1}
 TableForm
```

Out[9]//TableForm=
```
u[0] + 16 v[0]
12 + 12 u[0] + 12 u[1] + 12 u[2] + 16 v[0] + 16 v[1] + 16 v[2] + 16 v[3] + 16 v[4] + 16 v[5] + 16 v[6] +
9 + 16 u[0] + 15 u[1] + 13 u[2] + 16 v[0] + 15 v[1] + 13 v[2] + 9 v[3] + v[4] + 2 v[5] + 4 v[6] + 8 v[7]
16 + 5 u[0] + 15 u[1] + 11 u[2] + 16 v[0] + 14 v[1] + 8 v[2] + 7 v[3] + 4 v[4] + 12 v[5] + 2 v[6] + 6 v[7
13 + u[0] + 4 u[1] + 16 u[2] + 16 v[0] + 13 v[1] + v[2] + 4 v[3] + 16 v[4] + 13 v[5] + v[6] + 4 v[7] + 16
3 + 9 u[0] + 11 u[1] + 4 u[2] + 16 v[0] + 12 v[1] + 9 v[2] + 11 v[3] + 4 v[4] + 3 v[5] + 15 v[6] + 7 v[7]
2 + 3 u[0] + u[1] + 6 u[2] + 16 v[0] + 11 v[1] + 15 v[2] + 5 v[3] + 13 v[4] + 10 v[5] + 9 v[6] + 3 v[7] +
10 + 9 u[0] + 12 u[1] + 16 u[2] + 16 v[0] + 10 v[1] + 2 v[2] + 14 v[3] + 13 v[4] + 6 v[5] + 8 v[6] + 5 v[
13 + 15 u[0] + u[1] + 8 u[2] + 16 v[0] + 9 v[1] + 4 v[2] + 15 v[3] + v[4] + 8 v[5] + 13 v[6] + 2 v[7] + 1
10 + 12 u[0] + 6 u[1] + 3 u[2] + 16 v[0] + 8 v[1] + 4 v[2] + 2 v[3] + v[4] + 9 v[5] + 13 v[6] + 15 v[7] +
16 + 6 u[0] + 9 u[1] + 5 u[2] + 16 v[0] + 7 v[1] + 2 v[2] + 3 v[3] + 13 v[4] + 11 v[5] + 8 v[6] + 12 v[7]
15 + 3 u[0] + 16 u[1] + 6 u[2] + 16 v[0] + 6 v[1] + 15 v[2] + 12 v[3] + 13 v[4] + 7 v[5] + 9 v[6] + 14 v[
10 + 4 u[0] + 14 u[1] + 15 u[2] + 16 v[0] + 5 v[1] + 9 v[2] + 6 v[3] + 4 v[4] + 14 v[5] + 15 v[6] + 10 v[
7 + 6 u[0] + 10 u[1] + 11 u[2] + 16 v[0] + 4 v[1] + v[2] + 13 v[3] + 16 v[4] + 4 v[5] + v[6] + 13 v[7] +
```

Extract matrix of coefficients of the equations we need to solve

In[10]:=
```
vars = Join[Table[u[i], {i, 0, e - 1}], Table[v[i], {i, 0, m + e - 1}]]
```

Out[10]=
```
{u[0], u[1], u[2], v[0], v[1], v[2], v[3], v[4], v[5], v[6], v[7], v[8], v[9], v[10]}
```

In[11]:=
```
(mat = Table[Coefficient[eqns[[i]], vars[[j]]], {i, 1, n}, {j, 1, m + 2 e}]) // MatrixForm
```

Out[11]//MatrixForm=

$$\begin{pmatrix} 1 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 12 & 12 & 12 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\ 16 & 15 & 13 & 16 & 15 & 13 & 9 & 1 & 2 & 4 & 8 & 16 & 15 & 13 \\ 5 & 15 & 11 & 16 & 14 & 8 & 7 & 4 & 12 & 2 & 6 & 1 & 3 & 9 \\ 1 & 4 & 16 & 16 & 13 & 1 & 4 & 16 & 13 & 1 & 4 & 16 & 13 & 1 \\ 9 & 11 & 4 & 16 & 12 & 9 & 11 & 4 & 3 & 15 & 7 & 1 & 5 & 8 \\ 3 & 1 & 6 & 16 & 11 & 15 & 5 & 13 & 10 & 9 & 3 & 1 & 6 & 2 \\ 9 & 12 & 16 & 16 & 10 & 2 & 14 & 13 & 6 & 8 & 5 & 1 & 7 & 15 \\ 15 & 1 & 8 & 16 & 9 & 4 & 15 & 1 & 8 & 13 & 2 & 16 & 9 & 4 \\ 12 & 6 & 3 & 16 & 8 & 4 & 2 & 1 & 9 & 13 & 15 & 16 & 8 & 4 \\ 6 & 9 & 5 & 16 & 7 & 2 & 3 & 13 & 11 & 8 & 12 & 1 & 10 & 15 \\ 3 & 16 & 6 & 16 & 6 & 15 & 12 & 13 & 7 & 9 & 14 & 1 & 11 & 2 \\ 4 & 14 & 15 & 16 & 5 & 9 & 6 & 4 & 14 & 15 & 10 & 1 & 12 & 8 \\ 6 & 10 & 11 & 16 & 4 & 1 & 13 & 16 & 4 & 1 & 13 & 16 & 4 & 1 \end{pmatrix}$$

Constant terms of the equations we need to solve

In[12]:=
```
b = Mod[-eqns /. {u[_] :> 0, v[_] :> 0}, p]
```

Out[12]= {0, 5, 8, 1, 4, 14, 15, 7, 4, 7, 1, 2, 7, 10}

Solve for the coefficients `u[i]` and `v[i]`.

In[13]:=
```
uv = LinearSolve[mat, b, Modulus → p]
```

Out[13]= {5, 2, 11, 5, 11, 1, 8, 8, 3, 16, 3, 5, 0, 15}

Plug them back in to find the polynomials `E (x), Q (x)`.

In[14]:=
```
ex = eund /. u[i_] :> uv[[i + 1]]
```

Out[14]= $5 + 2x + 11x^2 + x^3$

In[15]:=
```
qx = qund /. v[i_] :> uv[[i + 1 + e]]
```

Out[15]= $5 + 11x + x^2 + 8x^3 + 8x^4 + 3x^5 + 16x^6 + 3x^7 + 5x^8 + 15x^{10}$

Divide $Q(x)/E(x)$ with coefficients mod p.

In[16]:=
```
Together[qx / ex, Modulus → p]
```

Out[16]= $1 + 12x + 9x^3 + 16x^4 + 5x^5 + 5x^6 + 15x^7$

Compare with the original message.

In[17]:=
```
mess
```

Out[17]= {1, 12, 0, 9, 16, 5, 5, 15}