Public Key Cryptography

Lecture 8

The Discrete Logarithm Problem

Index

1. Silver-Pohlig-Hellman algorithm

2. Berlekamp's algorithm

Algorithms for the Discrete Logarithm Problem

Generic algorithms (work in any cyclic group):

- Brute-Force Search
- Shanks' Baby-Step-Giant-Step Method
- Pollard's Rho Method (1978)
- Silver-Pohlig-Hellman Method (1978)

Non-generic algorithms (work only in specific groups, in particular in $(\mathbb{Z}_p^*, \cdot)$):

- The Index Calculus Method

All known methods for computing discrete logarithms are exponential-time algorithms.

Silver-Pohlig-Hellman algorithm

- Silver-Pohlig-Hellman (1978)
- computes discrete logarithms in F_q, that is, given a generator g of F_q^* and $y \in F_q^*$, determines $x = \log_g y \in \{0, \ldots, q-2\}$
- it works well if $q-1$ has only small prime factors

Precalculations:

1. Write $q - 1 = \prod_{i=1}^{t} p_i^{c_i}$ for some distinct primes p_i.
2. For each prime $p | q-1$, we compute the p-th roots of unity

$$\alpha_{p,j} = g^{j(q-1)/p}$$

for each $j = 0, \ldots, p-1$.

3. We make a look-up table with the values $\alpha_{p,j}$ that will be used to compute the discrete logarithm of any $y \in F_q^*$.

The Silver-Pohlig-Hellman algorithm (cont.)

The algorithm:

- The value of the discrete logarithm $x = \log_g y$ will be determined modulo $p_i^{c_i}$ for each i and then the results will be combined by the Chinese Remainder Theorem to obtain $x \mod q-1$.
- In what follows fix $p = p_i$ and $c = c_i$. We write:

$$x = x_0 + x_1 p + \cdots + x_{c-1} p^{c-1} \pmod{p^c},$$

  where $0 \leq x_j < p$, and we determine the x_j's.
- In order to determine x_0 we compute

$$y^{(q-1)/p} = g^{x(q-1)/p} = g^{x_0(q-1)/p} = \alpha_{p,x_0} \,,$$

  which is a p-th root of unity. Compare $y^{(q-1)/p}$ with the precalculated values $\alpha_{p,j}$ for $0 \leq j < p$ and set x_0 to be the value j for which $y^{(q-1)/p} = \alpha_{p,j}$.

The Silver-Pohlig-Hellman algorithm (cont.)

- In order to find x_1 we replace y by $y_1 = yg^{-x_0}$. Then

$$\log_g y_1 = x - x_0 = x_1 p + \cdots + x_{c-1} p^{c-1} \pmod{p^c}.$$

  Then we have

$$\begin{aligned} y_1^{(q-1)/p^2} &= g^{(x-x_0)(q-1)/p^2} = g^{(x_1+x_2p+\cdots+x_{c-1}p^{c-2})(q-1)/p} \\ &= g^{x_1(q-1)/p} = \alpha_{p,x_1}. \end{aligned}$$

  Compare $y_1^{(q-1)/p^2}$ with the precalculated values $\alpha_{p,j}$ for $0 \le j < p$ and set x_1 to be the value j for which $y_1^{(q-1)/p^2} = \alpha_{p,j}$.
- We proceed inductively to find all the x_j's. For each $i = 1, \ldots, c-1$ set

$$y_i = yg^{-(x_0+x_1p+\cdots+x_{i-1}p^{i-1})}.$$

  Then

$$\log_g y_i = x_i p^i + \cdots + x_{c-1} p^{c-1} \pmod{p^c}.$$

The Silver-Pohlig-Hellman algorithm (cont.)

Then we have

$$\begin{aligned} y_i^{(q-1)/p^{i+1}} &= g^{(x_i + x_{i+1}p + \cdots + x_{c-i-1}p^{c-i-1})(q-1)/p} \\ &= g^{x_i(q-1)/p} = \alpha_{p,x_i} \, . \end{aligned}$$

Then we set x_i to be the value j for which $y_i^{(q-1)/p^{i+1}} = \alpha_{p,j}$.

- When we are done we have $x \bmod p^c$.
- After doing this for each $p|q-1$, we use the Chinese Remainder Theorem to get $x \bmod q-1$.

Proposition

The complexity of the Silver-Pohlig-Hellman algorithm is $O(p_k^{1/2}(\log q)^2)$ where p_k is the largest prime factor of $q-1$.

The Silver-Pohlig-Hellman algorithm - example

Example. Consider the field F_q, where $q = 37$, and the generator $g = 2$ of F_{37}^*. Let us compute $\log_g y$, where $y = 28$.

Precalculations:

1. We write $q - 1 = 36 = 2^2 \cdot 3^2$.
2. For each prime $p | q - 1$ we compute the p-th roots of unity

$$\alpha_{p,j} = g^{j(q-1)/p}, \quad j = 0, \dots, p-1.$$

$$\begin{cases} \alpha_{2,0} = 1 \\ \alpha_{2,1} = 2^{36/2} = 2^{18} = -1 \pmod{37} \end{cases}$$

For $p = 2$, always $\alpha_{2,0} = 1$ and $\alpha_{2,1} = -1$.

$$\begin{cases} \alpha_{3,0} = 1 \\ \alpha_{3,1} = 2^{36/3} = 2^{12} = 26 \pmod{37} \\ \alpha_{3,2} = 2^{2 \cdot 36/3} = 2^{24} = 10 \pmod{37} \end{cases}$$

3. We get the following look-up table:

$j\backslash p$	2	3
0	1	1
1	-1	26
2		10

The algorithm:

- First we take $p = 2$ and determine

$$x = x_0 + 2x_1 \pmod{4}.$$

We compute

$$y^{(q-1)/p} = 28^{18} = 1 \pmod{37}$$

whence we conclude that $x_0 = 0$. Next, we compute

$$y^{(q-1)/p^2} = 28^{9} = -1 \pmod{37}$$

whence we conclude that $x_1 = 1$. Thus $x = 2 \pmod{4}$.

The Silver-Pohlig-Hellman algorithm - example (cont.)

- Now we take $p = 3$ and determine

$$x = x_0 + 3x_1 \pmod{9}.$$

We compute

$$y^{(q-1)/p} = 28^{12} = 26 \pmod{37}$$

whence we conclude that $x_0 = 1$. Next, we have

$$y_1 = yg^{-x_0} = 28/2 = 14$$

and compute

$$y_1^{(q-1)/p^2} = 14^4 = 10 \pmod{37}$$

whence we conclude that $x_1 = 2$. Thus $x = 7 \pmod{9}$.

- Finally we solve the system of congruences

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 7 \pmod{9} \end{cases}$$

We get the solution $x = 34 \pmod{36}$.

- Therefore, $\log_2 28 = 34$ in F_{37}^*.

Berlekamp's algorithm

Throughout p is a prime and K is a field.

Definition

Let $f = a_0 + a_1 X + \cdots + a_n X^n, g \in K[X]$. We define:

- The *formal derivative*: $f' = a_1 + 2a_2 X + \cdots + na_n X^{n-1}$.
- The *composition* $f \circ g = a_0 + a_1 g + \cdots + a_n g^n$.

Theorem

Let $f \in K[X]$ be such that $\gcd(f, f') = 1$. Then f is square-free (that is, it is not divisible by the square of any polynomial in $K[X]$).

Theorem

Let $f \in \mathbb{Z}_p[X]$.
(i) $f' = 0 \Leftrightarrow \exists g \in \mathbb{Z}_p[X]$: $f = g \circ X^p$.
(ii) $f^p = f \circ X^p$.

Berlekamp's algorithm (cont.)

Problem

Write a given monic polynomial $f \in \mathbb{Z}_p[X]$ in the form $f = f_1^{e_1} \cdot f_2^{e_2} \cdot \dots \cdot f_r^{e_r}$ for some distinct monic irreducible $f_1, \dots, f_r \in \mathbb{Z}_p[X]$.

Cases of our problem

Denoting $d = gcd(f, f')$, we have the following cases:

- **Case 1.** $d = 1$. Then f is square-free.
- **Case 2.** $d = f$. Then $f' = 0$, so $f = g \circ X^p$ for $g \in \mathbb{Z}_p[X]$.
- **Case 3.** $1 \neq d \neq f$. Then d is a non-trivial factor of f.

New problem

Consider a monic polynomial $f \in \mathbb{Z}_p[X]$ with $deg(f) = n \geq 1$ and $gcd(f, f') = 1$ (square-free) and determine its factorization $f = f_1 f_2 \dots f_r$ into distinct monic irreducible polynomials.

Berlekamp's algorithm (cont.)

Berlekamp's Algorithm

- Input: a monic polynomial $f \in \mathbb{Z}_p[X]$ with $deg(f) = n \geq 1$ and $gcd(f, f') = 1$.
- Output: the distinct monic irreducible factors of f.
- Algorithm:
  1. Write the matrix $Q = (q_{ik}) \in M_n(\mathbb{Z}_p)$ whose entries are given by the equalities:

  $$X^{pk} = \sum_{i=0}^{n-1} q_{ik} X^i \ (mod\ f),$$

  for every $k \in \{0, \ldots, n-1\}$.

Berlekamp's Algorithm (cont.)

2. $V = \mathbb{Z}_p[X]/(f)$ is a vector space over $\mathbb{Z}_p$, a basis being $B = (1, X, \dots, X^{n-1})$.
Let $\varphi : V \to V$, $\varphi(h) = h^p - h \pmod{f}$. Then φ is a linear map and $[\varphi]_B = Q - I_n$.
Determine

$$r = dim\, Ker\, \varphi = n - rank(Q - I_n),$$

that gives the number of distinct monic irreducible factors of f. If $r = 1$, then f is irreducible. Otherwise go to Step 3.
3. Determine a basis $(h_1, \dots, h_r)$ of $Ker\, \varphi \leq V \cong \mathbb{Z}_p^n$. We may see φ as $\psi : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ and determine a basis $(v_1, \dots, v_r)$ of $Ker\, \psi$.
Then we get the basis $(h_1, \dots, h_r)$ of $Ker\, \varphi$ by considering $h_1 = \sum_{i=0}^{n-1} a_i X^i$, where $a_0, \dots, a_{n-1}$ are the coordinates of v_1 in the canonical basis of $\mathbb{Z}_p^n$ etc.

Berlekamp's Algorithm (cont.)

4. A factor (not necessarily non-trivial!) of f is given by $gcd(f, h_1 - s)$ for some $s \in \mathbb{Z}_p$. If the use of h_1 does not succeed in finding the r irreducible factors of f, then consider $h_2 = \sum_{i=0}^{n-1} a_i X^i$, where $a_0, \ldots, a_{n-1}$ are the coordinates of v_2 etc. until getting all the irreducible factors of f.

Remarks. (i) Berlekamp's algorithm works, with some adaptation, for polynomials over any finite field F_q and not only over $\mathbb{Z}_p$. It is efficient for q small.
(ii) By using Berlekamp's algorithm one can also decide if a polynomial is irreducible.

Example 1. Let us use Berlekamp's algorithm to factorize

$$g = X^{16} + X^{12} + X^8 + X^6 + 1 \in \mathbb{Z}_2[X] .$$

We have

$$g' = 16X^{15} + 12X^{11} + 8X^7 + 6X^5 = 0 ,$$

hence $gcd(g, g') = g$. In fact we have

$$g = f \circ X^2 = f^2 ,$$

where

$$f = X^8 + X^6 + X^4 + X^3 + 1 .$$

Now $f' = 8X^7 + 6X^5 + 4X^3 + 3X^2 = X^2$ and $gcd(f, f') = 1$, hence f is square-free.
We determine the matrix $Q = (q_{ik}) \in M_8(\mathbb{Z}_2)$, where the q_{ik}'s are given by

$$X^{2k} = \sum_{i=0}^{7} q_{ik} X^i \pmod{f} , \quad k = 0, \dots , 7 .$$

Berlekamp's algorithm - examples (cont.)

Consider the $\mathbb{Z}_2$-vector space

$$V = \mathbb{Z}_2[X]/(f) = \{a_0 + a_1 X + \cdots + a_7 X^7 \mid a_0, \ldots, a_7 \in \mathbb{Z}_2\}.$$

One of its bases is the list of vectors $B = (1, X, \ldots, X^7)$.
For $k \in \{0, \ldots, 7\}$, q_{ik} are the coordinates of the vector X^{2k} in the basis B. Note that $1, X^2, X^4, X^6$ belong to B, and we have:

$$\begin{aligned}
1 &= 1 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4 + 0 \cdot X^5 + 0 \cdot X^6 + 0 \cdot X^7 \\
X^2 &= 0 \cdot 1 + 0 \cdot X + 1 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4 + 0 \cdot X^5 + 0 \cdot X^6 + 0 \cdot X^7 \\
X^4 &= 0 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 1 \cdot X^4 + 0 \cdot X^5 + 0 \cdot X^6 + 0 \cdot X^7 \\
X^6 &= 0 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4 + 0 \cdot X^5 + 1 \cdot X^6 + 0 \cdot X^7
\end{aligned}$$

The next powers are obtained by computing $X^{2k} \bmod f$ (we do not explicitly write zeros anymore):

$$\begin{aligned}
X^8 &= 1 + X^3 + X^4 + X^6 \\
X^{10} &= 1 + X^2 + X^3 + X^4 + X^5 \\
X^{12} &= X^2 + X^4 + X^5 + X^6 + X^7 \\
X^{14} &= 1 + X + X^3 + X^4 + X^5
\end{aligned}$$

Berlekamp's algorithm - examples (cont.)

The same results as above can be obtained by using successively the identity $f = 0 \ (mod \ f)$:

$$\begin{cases} X^8 & = -X^6 - X^4 - X^3 - 1 \\ & = 1 + X^3 + X^4 + X^6; \\ X^{10} & = X^8 + X^6 + X^5 + X^2 \\ & = (X^6 + X^4 + X^3 + 1) + X^6 + X^5 + X^2 \\ & = 1 + X^2 + X^3 + X^4 + X^5; \\ X^{12} & = X^2 + X^4 + X^5 + X^6 + X^7; \\ X^{14} & = X^9 + X^8 + X^7 + X^6 + X^4 \\ & = (X^7 + X^5 + X^4 + X) \\ & +(X^6 + X^4 + X^3 + 1) + X^7 + X^6 + X^4 \\ & = 1 + X + X^3 + X^4 + X^5. \end{cases}$$

Berlekamp's algorithm - examples (cont.)

Hence we get the matrix

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Let $\varphi : V \to V$, $\varphi(h) = h^2 - h \pmod f$. Then φ is a linear map and $[\varphi]_B = Q - I_8$. Then

$$r = dim\, Ker\, \varphi = n - rank(Q - I_8)$$

is the number of irreducible factors of f.
In order to compute r, one can apply elementary operations to compute $rank(Q - I_8)$ from an echelon form of $Q - I_8$. This step is optional, since we obtain again this information by determining a basis of $Ker\, \varphi$ later on.

Berlekamp's algorithm - examples (cont.)

$$Q - I_8 = \begin{pmatrix} 0&0&0&0&1&1&0&1\\ 0&1&0&0&0&0&0&1\\ 0&1&1&0&0&1&1&0\\ 0&0&0&1&1&1&0&1\\ 0&0&1&0&0&1&1&1\\ 0&0&0&0&0&0&1&1\\ 0&0&0&1&1&0&0&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \sim \begin{pmatrix} 0&0&0&0&1&1&0&1\\ 0&1&0&0&0&0&0&1\\ 0&0&1&0&0&1&1&1\\ 0&0&0&1&1&1&0&1\\ 0&0&1&0&0&1&1&1\\ 0&0&0&0&0&0&1&1\\ 0&0&0&1&1&0&0&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 0&0&0&0&1&1&0&1\\ 0&1&0&0&0&0&0&1\\ 0&0&1&0&0&1&1&1\\ 0&0&0&1&1&1&0&1\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&1\\ 0&0&0&1&1&0&0&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \sim \begin{pmatrix} 0&0&0&0&1&1&0&1\\ 0&1&0&0&0&0&0&1\\ 0&0&1&0&0&1&1&1\\ 0&0&0&1&1&1&0&1\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&1\\ 0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&1&1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 0&0&0&0&1&1&0&1\\ 0&1&0&0&0&0&0&1\\ 0&0&1&0&0&1&1&1\\ 0&0&0&1&1&1&0&1\\ 0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&1&1\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \sim \begin{pmatrix} 0&0&0&0&1&1&0&1\\ 0&1&0&0&0&0&0&1\\ 0&0&1&0&0&1&1&1\\ 0&0&0&1&1&1&0&1\\ 0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&1&1\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix}.$$

We get $rank(Q - I_8) = 6$ (the number of non-zero rows from an echelon form of the matrix). Hence f has $r = 2$ irreducible factors.

Since $dim\, V = deg(f) = 8$, we have $V \cong \mathbb{Z}_2^8$. Now we identify φ with $\psi : \mathbb{Z}_2^8 \to \mathbb{Z}_2^8$ and determine a basis of

$$Ker\, \psi = \{a \in \mathbb{Z}_2^8 \mid \psi(a) = 0\}.$$

Hence

$$Ker\, \psi = \{a = (a_0, \ldots, a_7) \in \mathbb{Z}_2^8 \mid (Q - I_8)[a] = [0]\}\,.$$

We get the system:

$$\begin{cases} a_4 + a_5 + a_7 = 0 \\ a_1 + a_7 = 0 \\ a_1 + a_2 + a_5 + a_6 = 0 \\ a_3 + a_4 + a_5 + a_7 = 0 \\ a_2 + a_5 + a_6 + a_7 = 0 \\ a_6 + a_7 = 0 \\ a_3 + a_4 = 0 \\ a_6 + a_7 = 0 \end{cases}$$

that has the solution:

$$a_1 = a_2 = a_5 = a_6 = a_7,\, a_3 = a_4 = 0,\, a_0, a_7 \in \mathbb{Z}_2\,.$$

$$Ker\,\psi = \{(a_0, a_7, a_7, 0, 0, a_7, a_7, a_7) \mid a_0, a_7 \in \mathbb{Z}_2\}$$
$$=< (1,0,0,0,0,0,0,0), (0,1,1,0,0,1,1,1) > .$$

Thus we have a basis of $Ker\,\psi$, consisting of the two generators. The associated polynomials (forming a basis of $Ker\,\varphi$) are:

$$\begin{cases} h_1 = 1 \\ h_2 = X + X^2 + X^5 + X^6 + X^7 \end{cases}$$

To obtain a non-trivial factor we compute

$$gcd(f, h_2) = X^6 + X^5 + X^4 + X + 1$$

(or $gcd(f, h_2 - 1) = X^2 + X + 1$).
Therefore,

$$f = (X^2 + X + 1)(X^6 + X^5 + X^4 + X + 1)$$

is the factorization of f (we already know that f has 2 irreducible factors). It follows that:

$$g = f^2 = (X^2 + X + 1)^2 (X^6 + X^5 + X^4 + X + 1)^2 .$$

Example 2. Let us use Berlekamp's algorithm to factorize

$$g = X^8 + 2X^7 + X^6 + X^5 + 2X^3 \in \mathbb{Z}_3[X] .$$

We have $g = X^3 \cdot f$, where

$$f = X^5 + 2X^4 + X^3 + X^2 + 2 \in \mathbb{Z}_3[X] .$$

Then

$$f' = 5X^4 + 8X^3 + 3X^2 + 2X = -X^4 - X^3 - X$$

and $gcd(f, f') = 1$, hence f is square-free.
We determine the matrix $Q = (q_{ik}) \in M_5(\mathbb{Z}_3)$, where the q_{ik}'s are given by

$$X^{3k} = \sum_{i=0}^{4} q_{ik} X^i \pmod{f}, \quad k = 0, \ldots, 4 .$$

Berlekamp's algorithm - examples (cont.)

Consider the $\mathbb{Z}_3$-vector space

$$V = \mathbb{Z}_3[X]/(f) = \{a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 \mid a_0, \dots, a_4 \in \mathbb{Z}_3\}.$$

One of its bases is the list of vectors $B = (1, X, \dots, X^4)$.
For $k \in \{0, \dots, 4\}$, q_{ik} are the coordinates of the vector X^{3k} in the basis B. Note that $1, X^3$ belong to B, and we have:

$$\begin{aligned} 1 &= 1 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4 \\ X^3 &= 0 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 1 \cdot X^3 + 0 \cdot X^4 \end{aligned}$$

The next powers are obtained by computing $X^{3k} \bmod f$ (we do not explicitly write zeros anymore):

$$\begin{aligned} X^6 &= 1 + X - X^2 + X^3 \\ X^9 &= X \\ X^{12} &= X^4 \end{aligned}$$

The same results as above can be obtained by using successively the identity $f = 0 \ (mod\ f)$:

$$\begin{cases} X^5 & = -2X^4 - X^3 - X^2 - 2 = X^4 - X^3 - X^2 + 1; \\ X^6 & = X^5 - X^4 - X^3 + X \\ & = (X^4 - X^3 - X^2 + 1) - X^4 - X^3 + X \\ & = -2X^3 - X^2 + X + 1 \\ & = 1 + X - X^2 + X^3; \\ X^9 & = X^6 - X^5 + X^4 + X^3 \\ & = (X^3 - X^2 + X + 1) - (X^4 - X^3 - X^2 + 1) + X^4 + X^3 = X; \\ X^{12} & = X^4. \end{cases}$$

Hence we get the matrix $Q = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

Berlekamp's algorithm - examples (cont.)

Let $\varphi : V \to V$, $\varphi(h) = h^3 - h \pmod{f}$. Then φ is a linear map and $[\varphi]_B = Q - I_5$. Then

$$r = dim\, Ker\, \varphi = n - rank(Q - I_5)$$

is the number of irreducible factors of f.

In order to compute r, one can compute $rank(Q - I_5)$ from an echelon form of $Q - I_5$. This step is optional, since we obtain again this information by determining a basis of $Ker\, \varphi$ later on.

$$Q - I_5 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We get $rank(Q - I_5) = 2$ (the number of non-zero rows from an echelon form of the matrix). Hence f has $r = 3$ irreducible factors.

Berlekamp's algorithm - examples (cont.)

Since $dim\, V = deg(f) = 5$, we have $V \cong \mathbb{Z}_3^5$. Now we identify φ with $\psi : \mathbb{Z}_3^5 \to \mathbb{Z}_3^5$ and determine a basis of

$$Ker\, \psi = \{a \in \mathbb{Z}_3^5 \mid \psi(a) = 0\}.$$

Hence

$$Ker\, \psi = \{a = (a_0, \ldots, a_4) \in \mathbb{Z}_3^5 \mid (Q - I_5)[a] = [0]\}\,.$$

We get the system:

$$\begin{cases} a_2 = 0 \\ -a_1 + a_2 + a_3 = 0 \\ a_2 = 0 \\ a_1 + a_2 - a_3 = 0 \end{cases}$$

that has the solution:

$$a_1 = a_3, a_2 = 0, a_0, a_3, a_4 \in \mathbb{Z}_3\,.$$

Berlekamp's algorithm - examples (cont.)

$$Ker\,\psi = \{(a_0, a_3, 0, a_3, a_4) \mid a_0, a_3, a_4 \in \mathbb{Z}_3\} =$$

$$=< (1,0,0,0,0), (0,1,0,1,0), (0,0,0,0,1) >=< v_1, v_2, v_3 > \ .$$

A basis of $Ker\,\psi$ is (v_1, v_2, v_3).
The associated polynomials (forming a basis of $Ker\,\varphi$) are:

$$\begin{cases} h_1 = 1 \\ h_2 = X + X^3 \\ h_3 = X^4 \end{cases}$$

We compute $gcd(f, h_2 - s)$, where $s \in \mathbb{Z}_3$. We have $gcd(f, h_2) = X^2 + 1$, $gcd(f, h_2 - 1) = X + 1$. The third factor is obtained by dividing f by the two factors already determined. Therefore,

$$f = (X+1)(X^2+1)(X^2+X-1)\,,$$

hence

$$g = X^3(X+1)(X^2+1)(X^2+X-1)\,.$$

Selective Bibliography

- R. Lidl, G. Pilz, *Applied Abstract Algebra*, Springer, 1998.
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. [http://www.cacr.math.uwaterloo.ca/hac]