Gerasimos C. Meletiou
Explicit form for the discrete logarithm over the field $\mathbb{GF}(p, k)$


Persistent URL: [http://dml.cz/dmlcz/107463](http://dml.cz/dmlcz/107463)

**Terms of use:**

© Masaryk University, 1993

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use.*

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
EXPLICIT FORM FOR THE DISCRETE LOGARITHM OVER THE FIELD $GF(p,k)$

Gerasimos C. Meletiou

Abstract. For a generator of the multiplicative group of the field $GF(p,k)$, the discrete logarithm of an element $b$ of the field to the base $a$, $b \neq 0$ is that integer $z : 1 \leq z \leq p^k - 1$, $b = a^z$. The $p$-ary digits which represent $z$ can be described with extremely simple polynomial forms.

1. Introduction

The present note addresses the Discrete Logarithm problem ([1], [3], [4], [6]). The problem amounts to finding a quick method (efficient algorithm) for the computation of an integer $z$ satisfying the equation:

$$a^z = b.$$ 

for $b \in GF(p,k)$, given a generator $a$ of the multiplicative group of the field $GF(p,k)$. The main practical interest in the problem stems from cryptography ([1], [2], [3], [4], [6]).

In the case that $a$ and $z$ are known the computation of $b$ can be done rapidly (Discrete Exponential Function [4], [7, p. 399]). However, computing $z$ from $a$ and $b$, that is, computing logarithms over $GF(p,k)$, does not appear to admit a fast algorithm. ([1], [3], [4]).

The integer $z$ in (1) is computed modulo $p^k - 1$. In the case $k = 1$, $a$ and $b$ can be regarded as integers from $\{1, 2, \ldots, p-1\}$ and $z$ as an integer from $\{1, \ldots, p-2\}$. The following polynomial formula has been found ([6]).

$$z \equiv \sum_{i=1}^{p-2} (1 - a^i)^{-1} b^i \pmod{p}.$$ 

The mere existence of such a formula in terms of powers of $b$ is due to the fact that in a finite field every function from the field to itself can be expressed as a


Key words and phrases: discrete logarithm, finite fields, cryptography.

Received December 10, 1991.
polynomial. Although (2) is of no computational use, still, it is of mathematical interest.

The generalization of (2) to the field $GF(p, k)$, $k > 1$ is the purpose of this correspondence. Integer $z$ in (1) is going to be computed modulo $q - 1$, $q = p^k$. Therefore it can be assumed $1 \leq z \leq q - 1$ and

\begin{equation}
(3) \quad z = \sum_{m=0}^{k-1} d_m p^m,
\end{equation}

where $0 \leq d_m \leq p - 1$. We use the numeric system with $p$ as a basis, the $d_m$s are $p$-digits. In the case $p = 2$ the $d_m$s are binary digits (that is bits).

For $k = 1$ one has $z = d_0$.

It remains to find explicit formulas for the $d_m$s. Since $0 \leq d_m \leq q - 1$ $d_m$ can be regarded as an element of $GF(p, k)$. The $d_m$s are uniquely determined in (3); they are functions of $b$ provided that $a$ is a generator of the multiplicative group of $GF(p, k)$. Then

\begin{equation}
(4) \quad d_m = \sum_{i=1}^{q-2} b^i/(1 - a^i)^m, \quad m = 0, 1, \ldots, k - 1.
\end{equation}

Trivially, (4) is a generalization of (2).

For $p = 2$ (4) becomes

\begin{equation}
(5) \quad d_m = \sum_{i=1}^{q-2} b^i/(1 + a^i)^m, \quad m = 0, 1, \ldots, k_1, d_i \in \{0, 1\}.
\end{equation}

Therefore in any finite field the discrete logarithm function can be expressed with $k$ polynomials with $q - 2$ different coefficients. Surprisingly enough, the formulas for the coefficients are very simple.

**II. Main Calculations**

Equation (4) has to be shown. For $m = 0$ it becomes:

\begin{equation}
(6) \quad d_0 = \sum_{i=1}^{q-2} b^i(1 - a^i)^{-1}.
\end{equation}

For the proof Lagrangian Interpolation is going to be used. According to (3) $d_0$ is the rightmost $p$-digit of $z$, thus $d_0 \equiv z \pmod{p}$. The characteristic of the field is $p$. It follows:

\begin{equation}
(7) \quad d_0 = 1 \cdot \delta(b, a) + 2 \cdot \delta(b, a^2) + \cdots + (q - 1) \cdot \delta(b, a^{q-1})
\end{equation}

where $\delta(b, a^j)$ is defined as

\[\delta(b, a^j) = \begin{cases} 1 & b = a^j \\ 0 & b \neq a^j \end{cases}.\]
Further

\[(8) \quad \delta(b, a^j) = 1 - (b - a^j)^{q-1} = 1 - \sum_{i=0}^{q-1} b^i (-a^j)^{q-1-i} \cdot \binom{q-1}{i}.\]

However, since \(q = p^k\) one concludes:

\[(9) \quad \binom{q-1}{i} = \frac{(p^k-1)(p^k-2) \cdots (p^k-i)}{i!} \equiv (-1)^i \pmod p.\]

In the case \(p \neq 2\) the value of \((-1)^{q-1}\) is 1.
In the case \(p = 2\), \((-1)^{q-1} = -1 \equiv 1 \pmod 2\). Thus (8) implies:

\[\delta(b, a^j) = -\sum_{i=1}^{q-1} b^i a^{-ij}.\]

Therefore

\[(10) \quad d_0 = \sum_{j=1}^{q-1} j \left( -\sum_{i=1}^{q-1} b^i a^{-ij} \right) = \sum_{i=1}^{q-1} b^i \left( -\sum_{j=1}^{q-1} j \cdot a^{-ij} \right).\]

The sum \(-\sum_{j=1}^{q-1} j \cdot a^{-ij}\) becomes 0 for \(i = q - 1\), since \(a^{q-1} = 1\), and it becomes

\[-\frac{a^{-i}}{1 - a^{-i}} = (1 - a^i)^{-1}\]

in the case \(i \neq q - 1\). Equality (6) is therefore true.

The above proof for (6) is similar to the proof given by Well's in [6, p. 846] generalized to the field \(GF(p, k)\). It becomes clear because of the observation at the end of [6] which states that in the field with \(q = p^k\) elements the matrix \(M(a) = (a^j)\), \(0 \leq i, j \leq q - 2\) satisfies \(M(a)^{-1} = -M(a^{-1})\). Also it is a good idea to be mentioned that \(M(a)\) is a discrete Fourier transform over \(GF(p, k)\) ([5]).

It suffices formulas for the \(d_s\)s to be derived, \(1 \leq s \leq k - 1\). Since \(z \cdot p^k \equiv z(\mod q - 1)\) it is true:

\[(11) \quad a^{z \cdot p^k} = b \quad \text{or} \quad (a^{v^s})^{p^{k-s} \cdot z} = b.\]

The transformation \(x \mapsto x^{p^s}\) is an automorphism of the field. Therefore \(a^{v^s}\) is a generator of the multiplicative group.

According to (3) \(p^{k-s} \cdot z\) equals to

\[\sum_{m=0}^{s-1} d_m p^{k+m-s} + \sum_{m=s}^{k-1} d_m p^{k+m-s}.\]

The powers of \(p\) are for \(m \geq s\)

\[(12) \quad p^{k+m-s} = p^k \cdot p^{m-s} \equiv p^{m-s}(\mod q - 1).\]
Therefore

\[(13) \quad p^{k-s}z \equiv v(\text{mod } q - 1), \]

where

\[(14) \quad v = \sum_{m=s}^{k-1} d_m p^{m-s} + \sum_{m=0}^{s-1} d_m p^{k+m-s}. \]

It follows from (14) that $0 \leq v \leq q - 1$. Equation (14) is just the representation of $v$ with $p$-ary digits. The rightmost $p$-digit is the coefficient of $p^0$ that is $d_s$.

Equation (11) can be written as:

\[(15) \quad (a^{p^s})^v = b. \]

The integer $v$ is the discrete logarithm of $b$ to the basis $a^{p^s}$. From (6) it is concluded

\[(16) \quad d_s = \sum b^i (1 - a^{p^i})^{-1} = \sum b^i (1 - a^i)^{-p^s}. \]

The last equation in (16) is true since $x \mapsto x^{p^s}$ is a field automorphism. The proof is complete.

References