MATHEMATICS OF COMPUTATION
Volume 67, Number 224, October 1998, Pages 1679–1689
S 0025-5718(98)00969-7

AN ALGORITHM FOR EVALUATION OF DISCRETE LOGARITHMS IN SOME NONPRIME FINITE FIELDS

IGOR A. SEMAEV

ABSTRACT. In this paper we propose an algorithm for evaluation of logarithms in the finite fields F_{p^n}, where the number $p^n - 1$ has a small primitive factor r. The heuristic estimate of the complexity of the algorithm is equal to $\exp((c + o(1))(\log p\, r \log^2 r)^{1/3})$, where n grows to ∞, and p is limited by a polynomial in n. The evaluation of logarithms is founded on a new congruence of the kind of D. Coppersmith, $C(x)^k \equiv D(x)$, which has a great deal of solutions—pairs of polynomials $C(x), D(x)$ of small degrees.

INTRODUCTION

Let α be a fixed primitive element of the finite field F_q. The discrete logarithm problem in the finite field consists in an effective solution of the equation

$$\alpha^x = \beta \tag{1}$$

with respect to x, with a known $\beta \in F_q$. Breaking a number of systems of public cryptography comes to evaluation of discrete logarithms [1]. There is a vast literature on this subject. We note only those works which are important for our considerations. For recent developments and other references see [7]. A method for solving equation (1) whose complexity is proportional to $sr^{1/2}$, where s is the number of prime divisors of $q - 1$ and r is the largest prime divisor of $q - 1$, is proposed in Pohlig and Hellman [2]. In 1979 Adleman [3] proposed an algorithm for evaluation of logarithms for the case when q is a prime number; its running time is estimated by the value

$$\exp((c + o(1))(\log q \log\log q)^{1/2}) \tag{2}$$

with $q \to \infty$. Later this method was adapted to fields of characteristic 2, i.e., for $q = 2^n$ [4]. The estimate (2) is equally valid in the case when $q = p^n$ and the number p is bounded by a polynomial in n as $n \to \infty$. The growth of the value (2) as $q \to \infty$ is of subexponential character, i.e., the Adleman method is substantially superior to the method of the work [2]. We describe briefly the Adleman algorithm for the case of the field F_{2^n}. Let $P(x)$ be a primitive polynomial of degree n over F_2. At the first stage we find logarithms of the field F_{2^n} whose elements modulo $P(x)$ are polynomials of degree at most b (b is a parameter of the method). To this end, we try to express the residues $x^m \bmod P(x)$ as products of irreducible polynomials of

Received by the editor March 30, 1993 and, in revised form, August 30, 1995.
1991 *Mathematics Subject Classification.* Primary 11T71, 11Y16, 94A60.
Key words and phrases. Cryptography, discrete logarithms, finite fields.

degree at most b with random integer m. Each factorization of this kind produces a linear equation $\bmod 2^n - 1$ with respect to unknown logarithms. We must produce a sufficient number of such equations and then solve this set of equations. In order to find a logarithm of a fixed element $B(x) \bmod P(x)$ of the field F_{2^n}, one has to obtain at least one factorization of a residue of the type $B(x)x^m \bmod P(x)$ into the product of polynomials of degree at most b. Unlike the method of Pohlig-Hellman, the Adleman algorithm is not deterministic, and the estimation of its complexity is the expected value of a random variable, the running time of the method.

In 1984 an article of Coppersmith [5] in which an algorithm for evaluation of logarithms in the fields F_{2^n} was proposed, was published in IEEE Transactions on Information Theory. The asymptotic running time of the Coppersmith algorithm equals

$$\exp((c + o(1))(n \log^2 n)^{1/3}) \tag{3}$$

as $n \to \infty$. It is obvious that with $q = 2^n$ and $n \to \infty$ the function under the exponential in (2) increases much faster than that in the estimate of Coppersmith. This means that Coppersmith's method is much more efficient than the Adleman algorithm.

We review the Coppersmith algorithm. It differs from Adleman's method in more efficient production of linear relations between logarithms of elements of the field F_{2^n}, with irreducible polynomials of low degrees being their inverse images in the ring $F_2[x]$. In this case the author substantially uses the fact that the field F_{2^n} has nontrivial automorphisms. Let $P(x) = x^n + Q(x)$ be an irreducible polynomial over F_2 of degree n, with $Q(x)$ being some polynomial of degree at most $n^{2/3}$. Let $q_j(x)$, $1 \le j \le N_b$, be irreducible polynomials of degree at most $b = c_1(n \log^2 n)^{1/3}$ with c_1 a constant and log a natural logarithm. At the first stage we must find logarithms of the elements of F_{2^n} that are the residues $q_j(x)$, $1 \le j \le N_b$. Let us take the integer d approximately equal to $c_2(n^2 \log n)^{1/3}$, where c_2 is a constant. It is shown in the Coppersmith article that there exist 2^{2d+1} pairs of polynomials $C(x), D(x)$ of degree at most $(nd)^{1/2}$ that satisfy the congruence

$$C(x)^k \equiv D(x) \pmod{P(x)}, \tag{4}$$

with k being a suitable power 2. If the polynomials $C(x), D(x)$ are factorized in the product of irreducible polynomials $q_j(x)$, $1 \le j \le N_b$, then one obtains a linear equation modulo $2^n - 1$ for logarithms of the elements of the field F_{2^n} that are the residues $q_j(x) (\bmod P(x))$. We look through suitable pairs of polynomials $C(x), D(x)$ until we have a system of linear equations that is sufficient for the evaluation of logarithms of the elements $q_j(x) (\bmod P(x))$. This system may be solved, for example, using the Gauss method.

Let $\mathcal{P}(b, d)$ be the probability of the fact that a random polynomial of degree at most d is factorized in the product of irreducible polynomials of degree at most b. One has to bear in mind two relations in order to make a selection of optimal parameters and produce an asymptotic estimation of the algorithm. First, one should have a sufficient number of pairs of polynomials $C(x), D(x)$ of degree at most $(nd)^{1/2}$ that satisfy the congruence (4) for producing a sufficient number of linear relations. Thus

$$2^{2d+1} \sim (2^{b+1}/b\mathcal{P}^2(b, (nd)^{1/2}). \tag{5}$$

Second, one should minimize the complexity of this stage. To this end, the complexity of producing linear relations and the complexity of solving this system must

be the same. Thus,

$$2^{b+1}/b\mathcal{P}^2(b,(nd)^{1/2}) \sim (2^{b+1}/b)^3. \tag{6}$$

Relations (5) and (6) allow us to calculate the constants c_1 and c_2. In this way we will find the complexity of evaluating logarithms of irreducible polynomials of lower degrees which is expressed by (3) with $c = 1.52$.

Coppersmith showed further how to calculate the logarithms of a random element of the field. His method consists in a successive expression of an unknown logarithm in terms of logarithms of polynomials of lesser degrees. Solutions of bounded degrees of the congruence (4) are also used in this method. The parameters of this procedure are chosen in such a way that its complexity should be of the kind (3) with $c < 1$. Thus the congruence (4) with many solutions—pairs of polynomials $C(x), D(x)$ of bounded degrees—is the central element of the Coppersmith method.

Is it possible to find an algorithm similar to Coppersmith's for the field F_{2^n} in other finite fields F_{p^n}? Prime fields do not have nontrivial automorphisms. Let us review more thoroughly the congruence (4) in the case of the field F_{p^n}:

$$(x^h A(x) + B(x))^k \equiv -x^{hk-n}Q(x)A(x^k) + B(x^k) (\mathrm{mod}\, P(x)). \tag{7}$$

In this congruence h, k are the parameters of the method and the degree of the polynomials $A(x)$ and $B(x)$ is bounded by d. The number k is a power of the characteristic p; we assume that the value p also grows as $n \to \infty$. Then, generally speaking, the residue modulo $P(x)$ of the polynomial on the right side of (7) behaves as a random polynomial reduced modulo $P(x)$. Due to this fact, the use of the congruence (7) for producing linear relations does not make sense. However, if p grows very slowly in comparison with n, then the evaluation of logarithms in the field F_{p^n} using the Coppersmith method is somewhat more rapid that the evaluation by the Adleman method.

In this paper we propose two new congruences of the kind of Coppersmith's (4). These congruences are used for evaluation of logarithms in the finite fields F_{p^n}, where $r = 2n + 1$ is a prime number and the multiplicative order of p modulo r equals $2n$ or n (n is odd), or the number $p^n - 1$ has a small primitive factor r. The asymptotic running time for these fields is similar to that of Coppersmith and equals

$$\exp((c + o(1))(\log p\, r \log^2 r)^{1/3}), \tag{8}$$

where the value of p is bounded by a polynomial in n as $n \to \infty$.

1.

Let us consider the case of the field F_{p^n}, where $r = 2n + 1$ is a prime and the multiplicative order of p modulo r equals $2n$ or n (n is odd). Under these conditions we describe a new method for obtaining linear relations, which is different from the Coppersmith method.

Let θ be a root of the polynomial $(x^r - 1)/(x - 1)$ over F_p. This polynomial is irreducible if the prime p is a primitive root of unity modulo r. The elements $\theta, \theta^2, \ldots, \theta^{2n}$ form a normal basis of the field $F_{p^{2n}}$ over F_p. It is obvious that the traces in F_{p^n} of the elements of this basis form a normal basis of the field F_{p^n} over F_p. Thus,

$$\eta_i = \theta^i + \theta^{-i}, \qquad 1 \le i \le n, \tag{9}$$

are linearly independent over F_p and are connected by the relations $\eta_i = \eta_1^{p^{\nu_i}}$, where $p^{\nu_i} \equiv i (\mathrm{mod}\, r)$. Suppose that the order of p modulo r equals n, and n is odd. Then the elements (9) also form a normal basis of the field F_{p^n} over F_p, for which we have the relations $\eta_i = \eta_1^{p^{\nu_i}}$, where $p^{\nu_i} \equiv i$ or $-i (\mathrm{mod}\, r)$.

In any case, $F_{p^n} = F_p(\eta_1)$. Let $P_1(x)$ denote an irreducible polynomial of degree n over F_p, where the element η_1 is a root. From the form of the elements of the basis (9) we have the following relations:

$$\eta_1^2 = \eta_2 + 2,$$
$$\eta_i \eta_1 = \eta_{i-1} + \eta_{i+1}, \qquad 2 \le i \le n-1,$$
$$\eta_n \eta_1 = \eta_n + \eta_{n-1}.$$

Hence it is clear that $\eta_i = \psi_i(\eta_1)$, $1 \le i \le n-1$, where $\eta_i(x)$ is a polynomial of degree i. The polynomials $\psi_i(x)$ satisfy the recurrence relation

$$\psi_{i+1}(x) = x\psi_i(x) - \psi_{i-1}(x) \tag{10}$$

with the initial conditions $\psi_1(x) = x$, $\psi_0(x) = 2$. The polynomials $\psi_i(x)$, $1 \le i \le n-1$, are all the roots of $P_1(x)$ modulo $P_1(x)$. It is easy to check from the form of these roots (9) that modulo $P_1(x)$ the sequence of polynomials

$$\psi_i(x), \qquad i = 0, 1, \ldots,$$

is periodic with period $r = 2n+1$. In this case the following congruence holds:

$$\psi_{n+i+1}(x) \equiv \psi_{n-i}(x) \ (\mathrm{mod}\, P_1(x)). \tag{11}$$

Lemma 1. *For $1 \le i \le n$ the following identity is true:*

$$\psi_{n-i}(x) \equiv (\psi_i(x) - \psi_{i-1}(x) + \cdots + (-1)^i)\psi_n(x) \ (\mathrm{mod}\, P_1(x)). \tag{12}$$

Proof. It follows from (10) that

$$\psi_{n+1}(x) = x\psi_n(x) - \psi_{n-1}(x) \ (\mathrm{mod}\, P_1(x)),$$

and from (11) we have

$$\psi_{n+1}(x) \equiv \psi_n(x) \ (\mathrm{mod}\, P_1(x)).$$

Therefore,

$$\psi_{n-1}(x) \equiv (x-1)\psi_n(x) \equiv (\psi_1(x) - 1)\psi_n(x) \ (\mathrm{mod}\, P_1(x)).$$

Thus, the identity (12) is valid for $i = 1$. Suppose that the assertion is valid for $1 \le i < k$. We shall prove it for $i = k$. We have the congruences:

$$\begin{aligned}
\psi_{n-k}(x) &\equiv \psi_1(x)\psi_{n-k+1}(x) - \psi_{n-k+2}(x) \\
&\equiv (\psi_1(x)(\psi_{k-1}(x) - \psi_{k-2}(x) + \cdots + (-1)^{k-1}) \\
&\qquad - (\psi_{k-2}(x) - \psi_{k-3}(x) + \cdots + (-1)^{k-2}))\psi_n(x) \\
&\equiv (\psi_k(x) + \psi_{k-2}(x) - \psi_{k-1}(x) - \psi_{k-3}(x) + \cdots \\
&\qquad + (-1)^{k-2}(\psi_2(x) + 2) + (-1)^{k-1}\psi_1(x) \\
&\qquad - \psi_{k-2}(x) + \psi_{k-3}(x) - \cdots - (-1)^{k-2})\psi_n(x) \\
&\equiv (\psi_k(x) - \psi_{k-1}(x) + \cdots + (-1)^k)\psi_n(x) \ (\mathrm{mod}\, P_1(x)).
\end{aligned}$$

The lemma is proved. □

Now let $\varphi_0 = 1$ and

$$\varphi_i = \psi_i(x) - \psi_{i-1}(x) + \cdots + (-1)^i, \qquad 1 \le i \le n.$$

Then the congruence of Lemma 1 holds:

$$\psi_{n-i}(x) \equiv \varphi_i(x)\psi_n(x), \qquad 0 \le i \le n,$$

where $\varphi_i(x)$ is a polynomial of degree i.

We consider the action of the group of automorphisms of the field F_{p^n} on the elements of the normal basis (9). If $p^{\nu_i} \equiv i$ or $-i \pmod r$, $1 \le i \le n$, then

$$(\psi_k(x))^{p^{\nu_i}} \equiv \psi_{ki}(x) \pmod{P_1(x)}.$$

Theorem 1. *Suppose that the inequalities $n/(s+1) \le d < n/(s-1)$ and the congruences $k = p^{\nu_s} \equiv s$ or $-s \pmod r$ and $l = p^{\nu_n} \equiv n$ or $-n \pmod r$ hold for the numbers $1 \le s, d \le n$. Then the congruence*

$$C(x)^k \equiv x^l D(x) \pmod{P_1(x)} \tag{13}$$

has at least $(p^{m+1}-1)/(p-1)$ solutions which are pairs of polynomials $C(x), D(x)$ of degree at most d, where $m = [d - n/s + d/s]$. We do not distinguish between those pairs of polynomials that can be obtained from each other by multiplication by a constant from F_p^*.

Proof. It is easy to check that if the inequalities $d - m \le i \le d$ are valid, then under the conditions of the theorem the inequalities

$$n - d \le si \le n + d + 1$$

hold. Therefore, if $d - m \le i \le d$ and $si = n - k_i$ or $n + k_i + 1$, then the congruences

$$(\psi_i(x))^{p^{\nu_s}} \equiv \psi_{si}(x) \equiv \psi_n(x)\varphi_{k_i}(x) \pmod{P_1(x)},$$

where $k_i \le d$, are true. We multiply this congruence by $c_i \in F_p$ and sum up over i in the interval $[d - m, d]$. Considering that

$$\psi_n(x) \equiv x^l \pmod{P_1(x)},$$

we have the congruence

$$\left(\sum_{i=d-m}^{d} c_i\psi_i(x)\right)^{p^{\nu_s}} \equiv x^l \sum_{i=d-m}^{d} c_i\varphi_{k_i}(x),$$

where on the left side in parentheses and on the right side for the second factor we have the polynomials of degree at most d. Thus, we obtain at least $(p^{m+1}-1)/(p-1)$ desired solutions of the congruence (13). The theorem is proved. □

The use of the solutions of the congruence (13) for evaluation of logarithms in the fields is similar to that in the method of Coppersmith. The analysis of the complexity is also similar, and so we will discuss this briefly. The algorithm has two parameters b and d. These are the limits of the degrees of the irreducible polynomials whose logarithms are calculated at the first stage and the degrees of the polynomials $C(x), D(x)$, solutions of the congruence (13). Let

$$d = c_1(n^2 \log n)^{1/3}, \qquad b = c_2(n \log^2 n)^{1/3},$$

where c_1, c_2 are some values independent of n. Let the relations $d = [n/s]$ and $n/(s+1) \le d < n/(s-1)$ be valid; then one can use the result of Theorem 1. Thus,

the congruence (13) has at least $(p^{m+1}-1)/(p-1)$, $m=[d-n/s+d/s]$, solutions—pairs of polynomials of degrees at most d. It is evident from the conditions for s that one can believe that $s=c_1^{-1}(n/\log n)^{1/3}$ and $m=c_1^2(n\log^2 n)^{1/3}$. The following two relations are similar to (5) and (6):

$$p^m \sim p^{b+1}/b\mathcal{P}(b,d)^2, \tag{14}$$

$$p^{b+1}/b\mathcal{P}(b,d)^2 \sim (p^{b+1}/b)^{\omega}. \tag{15}$$

The value of ω is determined by the method of solution of the corresponding system of linear equations. Suppose that $\omega=3$. In the paper [4] one can find the asymptotic value of the number of binary polynomials of degrees at most d, all irreducible factors of which are of degrees at most b. If the numbers d and b satisfy the relations $d^{\varepsilon}\le b\le d^{1-\varepsilon}$, then it may be assumed from the above that

$$\mathcal{P}(b,d)=\exp(-(1+o(1))db^{-1}\log db^{-1}).$$

When these polynomials are taken modulo p, the same result is true if the value of p is bounded by a polynomial in d. The proof of this proposition coincides with the proof given in the paper by Odlyzko, with the exception of minor details.

From (14) and (15) we obtain two relations for c_1 and c_2, once the parameters b and d are expressed in terms of n. We find $c_2=(4\omega/9(\omega-1)^2\log^2 p)^{1/3}$. Thus, the complexity of the evaluation of the logarithms of polynomials of small degrees is estimated by the value

$$\exp((c+o(1))(\log p\, n\log^2 n)^{1/3}),$$

where $c=(4\omega/9(\omega-1)^2)^{1/3}$, $n\to\infty$, and the prime p is bounded by a polynomial in n. The complexity of the evaluation of the logarithm of a random polynomial does not exceed the value (8).

For example, we review the evaluation of logarithms in the field of order 2^{23}. We note that $2\cdot 23+1=47$ is a prime, and the multiplicative order of 2 modulo 47 is equal to 23. We will produce a system of linear equations with respect to logarithms of those elements of the field that modulo $P_1(x)$ are irreducible polynomials of degrees at most $b=4$. Let

$$\begin{aligned}
t_1 &= \log(x)=1,\\
t_2 &= \log(x+1),\\
t_3 &= \log(x^2+x+1),\\
t_4 &= \log(x^3+x+1),\\
t_5 &= \log(x^3+x^2+1),\\
t_6 &= \log(x^4+x^3+x^2+x+1),\\
t_7 &= \log(x^4+x^3+1),\\
t_8 &= \log(x^4+x+1).
\end{aligned}$$

Let $d=10$ and $s=3$; then $2^{19}\equiv 3 \pmod{47}$, and we can produce the congruence (13) where $k=2^{19}$, $l=2^{22}$ and

$$\begin{aligned}
C(x) &= c_0\psi_6+c_1\psi_7+c_2\psi_8+c_3\psi_9+c_4\psi_{10},\\
D(x) &= c_0\varphi_5+c_1\varphi_2+c_2\varphi_0+c_3\varphi_3+c_4\varphi_6,
\end{aligned}$$

where

$$\begin{aligned}
\psi_6 &= x^6 + x^2, & \varphi_5 &= x^5 + x^4 + x^2 + x + 1,\\
\psi_7 &= x^7 + x^5 + x, & \varphi_2 &= x^2 + x + 1,\\
\psi_8 &= x^8, & \varphi_0 &= 1,\\
\psi_9 &= x^9 + x^7 + x^5 + x, & \varphi_3 &= x^3 + x^2 + 1,\\
\psi_{10} &= x^{10} + x^6 + x^2, & \varphi_6 &= x^6 + x^5 + x^4 + x + 1.
\end{aligned}$$

Then, we define the pairs of polynomials $C(x), D(x)$ all irreducible factors of which are of degrees at most 4. In order to produce these pairs, one should look through all the values of c_i, $i = 0, 4$. For example,

$$\begin{gathered}
c_0 = 0, \quad c_1 = 1, \quad c_2 = c_3 = c_4 = 0,\\
C(x) = \psi_7 = x^7 + x^5 + x = x(x^3 + x^2 + 1)^2,\\
D(x) = \varphi_2 = x^2 + x + 1,\\
C(x)^{2^{19}} \equiv x^{2^{22}} D(x) \text{ implies } 2^{19}(t_1 + 2t_5) = 2^{22}t_1 + t_3.
\end{gathered}$$

Similarly,

$$\begin{aligned}
2^{22}t_1 &= 2^{22}t_1,\\
2^{19}(2t_1 + 2t_5) &= 2^{22}t_1 + t_1 + 2t_2 + t_3,\\
2^{19}(t_1 + t_2 + t_3 + t_7) &= 2^{22}t_1 + t_1 + t_2,\\
2^{19}(t_1 + t_2 + 2t_5) &= 2^{22}t_1 + t_3 + t_4,\\
2^{19}(t_1 + 2t_2 + 2t_4) &= 2^{22}t_1 + t_5,\\
2^{19}(t_1 + 2t_2 + t_3 + t_7) &= 2^{22}t_1 + t_1 + t_2 + t_4,\\
9 \cdot 2^{19}t_1 &= 2^{22}t_1 + t_1 + 2t_2,\\
2^{19}(t_1 + t_6 + t_8) &= 2^{22}t_1 + 2t_1 + t_2,\\
2^{19}(8t_1 + t_2) &= 2^{22}t_1 + t_4,\\
2^{19}(2t_1 + t_2 + t_3 + t_7) &= 2^{22}t_1 + 2t_1 + 3t_2,\\
10 \cdot 2^{19}t_1 &= 2^{22}t_1 + 2t_1 + 4t_2,\\
2^{19}(t_1 + t_2 + t_6 + t_8) &= 2^{22}t_1 + 2t_1 + t_2 + t_4,\\
2^{19}(2t_1 + 2t_2 + 2t_4) &= 2^{22}t_1 + t_1 + 2t_2 + t_5,\\
2^{19}(8t_1 + 2t_2) &= 2^{22}t_1 + 2t_4,\\
2^{19}(9t_1 + t_2) &= 2^{22}t_1 + t_1 + 2t_2 + t_4,\\
2^{19}(t_1 + 3t_2 + 2t_4) &= 2^{22}t_1 + t_4 + t_5,\\
2^{19}(2t_1 + t_6 + t_8) &= 2^{22}t_1 + 3t_1 + 3t_2,\\
2^{19}(8t_1 + t_3) &= 2^{22}t_1 + t_3 + t_7.
\end{aligned}$$

After some calculation we have

$$\begin{aligned} t_2 &= 4\,456\,447,\\ t_3 &= 4\,194\,559,\\ t_4 &= 8\,142\,847,\\ t_5 &= 4\,196\,351,\\ t_6 + t_8 &= 4\,194\,335,\\ t_7 &= 3\,931\,920. \end{aligned}$$

It happens that t_6 and t_8 are not determined individually, since they occur in the combination $t_6 + t_8$. We attribute this phenomenon to some fine properties of the sequence $\psi_i(x)$ modulo $q_1(x) = x^4 + x^3 + x^2 + x + 1$ and $q_2(x) = x^4 + x + 1$. Let θ_j be a root of the polynomial $U^2 + x_j U + 1$, where x_j is a root of $q_j(x)$. Then

$$\theta_j^i + \theta_j^{-i} = \psi_i(x) \pmod{q_j(x)}.$$

Since $\theta_j^{17} = 1$, $j = 1, 2$, in analogy with (11) we have

$$\psi_{9+i}(x) \equiv \psi_{8-i}(x) \pmod{q_j(x)}.$$

Thus $\psi_{9+i} + \psi_{8-i}$ is divisible by both q_1 and q_2. The only combinations of $\psi_6, \psi_7, \ldots,$ ψ_{10} divisible by q_1 or q_2 are linear combinations of $\psi_9 + \psi_8$ and $\psi_{10} + \psi_7$; therefore, if t_8 appears, so does t_6, and vice versa.

Generally speaking, let T_q be the period of a root of the polynomial $U^2 + xU + 1$, where x is a root of the irreducible polynomial $q(x)$ of degree $s \le b$. Then T_q divides $p^s - 1$ or $p^s + 1$. In our example $p = 2$, $s = 4$ and $T_{q_j} = 17$. Consequently,

$$\psi_{T_q - i}(x) \equiv \psi_i(x) \pmod{q(x)}.$$

The product of the polynomials q such that $T_q = T$, divides $\psi_{T-i} - \psi_i$. Hence their logarithms occur together on the left side of the relations produced from (13), where

$$C(x) = \sum c_i(\psi_{T-i} - \psi_i).$$

The sum is over all i such that $d - m \le T - i$, $i \le d$. It can disrupt the expected frequency of the relations. However, it becomes highly improbable as p grows to ∞ no more slowly than d.

2.

In this section we study the case of the fields F_{p^n} where $p^n - 1$ has a small factor r that does not divide numbers $p^s - 1$, $s < n$.

Let r denote a factor of $p^n - 1$ that satisfies the following condition: there is an element $\xi \in F_q$ such that $\xi^r = 1$ and $F_p(\xi) = F_q$. By Zsigmond's theorem there is a prime number r that satisfies the above condition, except for $p = 2$ and $n = 6$. We would like to find the least r of this kind. Let $P_2(x)$ be an irreducible polynomial over F_p with ξ as a root. The values d and b are the parameters of the algorithm. Suppose that $d = c_1(r^2 \log r)^{1/3}$ and $b = c_2(r^2 \log r)^{1/3}$, where c_1 and c_2 are independent of the value of r.

Let u denote the residue mod r of a power of the characteristic p, that is, $u \equiv p^s \pmod r$. Let $0 \le h_i, k_i \le d$, $1 \le i \le T_u$ be all the pairs of the least nonnegative

residues modulo r that satisfy the congruence $h_i u \equiv k_i \pmod r$. Then for $a_i \in F_p$, $1 \le i \le T_u$, we have the following congruence:

$$C(x)^{p^s} \equiv D(x) \pmod{P_2(x)}, \tag{16}$$

where $C(x) = \sum_{i=1}^{T_u} a_i x^{h_i}$, $D(x) = \sum_{i=1}^{T_u} a_i x^{k_i}$ are polynomials of degrees at most d. The congruence (16) is similar to the congruences (4), (13). We shall use solutions of this congruence for the logarithms of the elements of the field F_q that are irreducible polynomials of degrees at most b modulo $P_2(x)$. The number of the pairs of polynomials $C(x), D(x)$ of degrees at most d—solutions of the congruence (16)—is at least $(p^{T_u} - 1)/(p - 1)$. The following theorem was proved in the work [6] by the author.

Theorem 2. *Let $d/(r^2 \log\log r)^{1/3} \to \infty$. Then $T_u = \frac{d^2}{r}(1 + o(1))$ for almost all residues u modulo r.*

We find the complexity of the evaluation of the logarithms of irreducible polynomials of small degrees. The following relations are similar to (14), (15):

$$(p^{d^2/r} - 1)/(p - 1) \sim p^{b+1}/b\mathcal{P}(d, b)^2,$$
$$p^{b+1}/b\mathcal{P}(d, b)^2 \sim (p^{b+1}/b)^w.$$

Simple calculations show that the complexity of this stage of the algorithm does not exceed

$$\exp((c + o(1))(\log p\, r \log^2 r)^{1/3}), \tag{17}$$

where $c = (4\omega^4/9(\omega - 1)^2)^{1/3}$.

The value (17) is also an estimate of the complexity of the evaluation of logarithms in the subfields of the field F_{p^n}. We shall show that in some cases one can evaluate the logarithms with complexity less than (17). Let r be a factor of $p^n - 1$ for which one can find an element $\xi \in F_{p^n}$ such that $\xi^r = 1$ and $F_{p^n} = F_p(\xi)$.

Lemma. *Let $F_p(\xi + \xi^{-1}) = F_{p^{n_1}}$. Then $n_1 = n$ or $n_1 = n/2$.*

Proof. Let $\xi^i + \xi^{-i} = \eta_i$. The element η_1 is a root of an irreducible polynomial $P_3(x)$ over F_p of degree n_1. Consider the equality

$$\eta_1^{p^s} = \eta_1 \quad \text{or} \quad (\xi + \xi^{-1})^{p^s} = \xi + \xi^{-1}$$

for some $s < n$. After evident transformations we have $\xi^{p^s+1} = 1$. Hence $p^s \equiv -1 \pmod r$. By assumption, n is the least number that satisfies the congruence $p^n \equiv 1 \pmod r$. Therefore, n divides $2s$. Thus, n_1 is equal to n or $n/2$. The lemma is proved. □

We note that the identity $\eta_i\eta_1 = \eta_{i+1} + \eta_{i-1}$ holds. Hence the element η_i can be represented as a polynomial in η_1 of degree i. Thus $\eta_i = \psi_i(\eta_1)$. Suppose that for numbers s, h, k we have the congruence $hp^s \equiv k \pmod r$. Then we have the identity:

$$\psi_h(\eta_1)^{p^s} = \psi_k(\eta_1)$$

or the congruence

$$\psi_h(x)^{p^s} \equiv \psi_k(x) \pmod{P_3(x)}. \tag{18}$$

Moreover, the congruence (18) remains valid if $hp^s \equiv -k \pmod r$. Let h_i, k_i, $1 \le i \le T'_u$, be all the pairs of numbers that satisfy the conditions

$$0 \le h_i, |k_i| \le d, \qquad h_i u \equiv k_i \pmod r.$$

Let u be a residue modulo r of some power of p, that is, $u \equiv p^s \pmod r$. We introduce the following notation:

$$C(x) = \sum_{i=1}^{T'_u} a_i \psi_{h_i}(x), \quad D(x) = \sum_{i=1}^{T'_u} a_i \psi_{|k_i|}(x), \qquad a_i \in F_p.$$

The polynomials $C(x), D(x)$ are of degrees at most d, and they satisfy the congruence

$$C(x)^{p^s} \equiv D(x) \pmod{P_3(x)}. \tag{19}$$

The number of pairs of polynomials $C(x), D(x)$ of degrees at most d that satisfy (19) is at least

$$(p^{T'_u} - 1)/(p-1).$$

By Theorem 2, $T'_u = \frac{2d^2}{r}(1+o(1))$ for almost all u as $r \to \infty$ and $d/(r^2 \log\log r)^{1/3} \to \infty$.

The solutions of the congruence (19) of bounded degrees are used for the evaluation of logarithms in the field $F_{p^{n_1}}$, like the solutions of (16) are used for this in the field F_{p^n}. It is easy to show that the complexity of evaluation of logarithms in this field is at most

$$\exp((c+o(1))(\log p\, r \log^2 r)^{1/3}),$$

where $c = (2\omega^4/9(\omega-1)^2)^{1/3}$.

We compare the algorithms of Sections 1 and 2. A. N. Lebedev noticed that the congruence (13) can be extended to the case of the field $F_{p^{n_1}}$, which we discuss in Section 2. However, in this case we have $r > 2n+1$, and the congruence $p^{\nu_s} \equiv \pm s \pmod r$ may have no solution for ν_s, where s is the optimal value of the parameter of our algorithm.

Consider the field F_{p^n}, where $2n+1 = r$ is a prime, and the multiplicative order of p modulo r is equal to $2n$ or n (n is odd). Then r is a primitive prime factor of $p^{2n}-1$ or p^n-1. Thus, if ξ is a primitive root of unity of degree r, then $\eta = \xi + \xi^{-1}$ generates F_{p^n} over F_p. Therefore, we can use the argument of Section 2 to produce a system of linear equations. For instance, we can find a nontrivial $u \equiv p^s \pmod r$, such that the number T_u of solutions of the congruence $hu \equiv k \pmod r$, where $0 < h, |k| \le d$, is the greatest. It should be noted that for almost all residues u we have $T'_u \sim m$, where $r, d \to \infty$, as in the assertion of Theorem 2. Therefore, the two methods give the same estimate for the complexity of the evaluation of logarithms in the field F_{p^n}.

It should be noted that all asymptotic estimates produced in this paper are based on the assumption that the polynomials $C(x)$ and $D(x)$ in the congruences (13), (16) are random and independent from the point of view of factorization in the product of polynomials of small degrees. This fact should be verified by a theory or by an experiment.

Thanks to an anonymous referee for his criticisms and to an anonymous editor of my English.

References

1. W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory, **IT-22** (1976), 644–654. MR **55:**10141
2. S. Pohlig and M. Hellman, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Trans. Inform. Theory **IT-24** (1978) 106–110. MR **58:**4617
3. L. Adleman, *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, 20th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, New York, 1979, pp. 55–60. MR **82a:**68004
4. A. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, Advances in Cryptology, Springer, Berlin and New York, 1985, pp. 224–314. MR **87g:**11022
5. D. Coppersmith, *Fast evaluation of logarithms in fields of characteristic two*, IEEE Trans. Inform. Theory **IT-30** (1984), 587–594. MR **85h:**65041
6. I. A. Semaev, *The number of small solutions of a linear homogeneous congruence*, Mat. Zametki **50** (1991), 102–197; English transl. in Math. Notes, **50** (1991). MR **93c:**11001
7. O. Schirokauer, D. Weber and T. Denny, *Discrete logarithms: the effectiveness of the index calculus method*, Algorithmic number theory, Lecture notes in computer science; vol. 1122, Springer, Berlin and New York, 1996, pp. 337–361.

43-2 Profsoyuznaya Street, Apartment #723, 117420 Moscow, Russia