MATHEMATICS OF COMPUTATION
Volume 71, Number 237, Pages 363–377
S 0025-5718(00)01308-9
Article electronically published on October 17, 2000

SPECIAL PRIME NUMBERS AND DISCRETE LOGS IN FINITE PRIME FIELDS

IGOR A. SEMAEV

Abstract. A set A of primes p involving numbers such as $ab^t + c$, where $|a|, |b|, |c| = O(1)$ and $t \to \infty$, is defined. An algorithm for computing discrete logs in the finite field of order p with $p \in A$ is suggested. Its heuristic expected running time is $L_p[\frac{1}{3}; (\frac{32}{9})^{1/3}]$ for $(\frac{32}{9})^{1/3} = 1.526\cdots$, where $L_p[\alpha;\beta] = \exp((\beta + o(1)) \ln^{\alpha} p (\ln\ln p)^{1-\alpha})$ as $p \to \infty$, $0 < \alpha < 1$, and $0 < \beta$. At present, the most efficient algorithm for computing discrete logs in the finite field of order p for general p is Schirokauer's adaptation of the Number Field Sieve. Its heuristic expected running time is $L_p[\frac{1}{3}; (\frac{64}{9})^{1/3}]$ for $(\frac{64}{9})^{1/3} = 1.9229\cdots$. Using $p \in A$ rather than general p does not enhance the performance of Schirokauer's algorithm. The definition of the set A and the algorithm suggested in this paper are based on a more general congruence than that of the Number Field Sieve. The congruence is related to the resultant of integer polynomials. We also give a number of useful identities for resultants that allow us to specify this congruence for some p.

Let F_p be a finite field of prime order p, and $a \in F_p$ its primitive element. The discrete log problem in F_p is as follows: given a nonzero $b \in F_p$, find the residue $y(\bmod\ p-1)$ for y such that $a^y = b$ in F_p.

The security of several cryptographic systems depends on the difficulty of computing discrete logs [1, 2]. The best known algorithm for computing discrete logs in F_p with an arbitrary prime p is that suggested by Schirokauer in [3]. Its heuristic expected running time is $L[\frac{1}{3}; (\frac{64}{9})^{1/3}]$ for $(\frac{64}{9})^{1/3} = 1.9229\cdots$. Here, as usual,

$$L[\alpha;\beta] = L_p[\alpha;\beta] = \exp((\beta + o(1)) \ln^{\alpha} p \ln\ln^{1-\alpha} p)$$

as $p \to \infty$, $0 < \alpha < 1$, and $0 < \beta$. This method is an adaptation of the popular Number Field Sieve algorithm (NFS), which has been used previously for factorization. It comes from the Gaussian integers method derived in [4] for computing discrete logs in F_p. The NFS algorithm is based on the congruence

$$f(m) \equiv 0(\bmod\ p), \tag{1}$$

where $f(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$ and $m \in \mathbb{Z}$. The main parameter of the method is $k = \deg f(x)$; the other parameters, such as m and the coefficients of $f(x)$, are bounded by $p^{1/k}$ in absolute value. There exists p for which the coefficients of $f(x)$ are no larger than $p^{o(1/k)}$ in absolute value. For example, let $ab^t + c \equiv 0(\bmod\ p)$ for $|a|, |b|, |c| = O(1)$ as $t \to \infty$. Then we have (1) with $f(x) = ax^k + cb^{t_0}$, and $m = b^{(t+t_0)/k}$, where $t \equiv -t_0(\bmod\ k)$ and $0 \le t_0 < k$.

Received by the editor July 16, 1998 and, in revised form, April 3, 2000.
2000 *Mathematics Subject Classification.* Primary 11Y16, 94A60.
Key words and phrases. Cryptography, discrete logarithms, Number Field Sieve.

If $k = o(\sqrt{\ln p})$, then p is as required. Such p are called special prime numbers in [5]. K. McCurley offers a \$100 reward for breaking the Diffie-Hellman scheme with the prime $p = 2 \cdot 739 \cdot q + 1$, where $q = (7^{149} - 1)/6$ [6]. This requires solving the discrete log problem in F_p. The algorithms for solving the discrete log problem in F_p suggested by Gordon [5] and Schirokauer [3] give no advantage to special primes over general primes. There is yet another algorithm in Gordon's work designed specifically for special p, but its expected running time is $L_p[\frac{2}{5}; 1,004]$. In other words, it is asymptotically slower than the algorithms for general p. In [7] McCurley's challenging problem was solved.

In this paper, we define a set A of primes p that includes numbers of the form $ab^t + c$ or their prime factors. We suggest an algorithm for solving the discrete log problem in F_p for $p \in A$ in heuristic expected running time $L_p[\frac{1}{3}; (\frac{32}{9})^{1/3}]$, $(\frac{32}{9})^{1/3} = 1.526\cdots$.

The definition of the set A and the algorithm are based on a more general congruence than (1), namely,

$$\text{Res}(f, g) \equiv 0 (\text{mod } p), \tag{2}$$

where Res is the resultant of the polynomials

$$f(x) = a_0 x^{n_1} + \cdots + a_{n_1-1} x + a_{n_1} \quad \text{and} \quad g(x) = b_0 x^{n_2} + \cdots + b_{n_2-1} x + b_{n_2}$$

over $\mathbb{Z}$. By definition [8]

$$\text{Res}(f, g) = a_0^{n_2} b_0^{n_1} \prod_{\alpha,\beta} (\alpha - \beta) = a_0^{n_2} \prod_{\alpha} g(\alpha) = (-1)^{n_2 n_1} b_0^{n_1} \prod_{\beta} f(\beta),$$

where α and β range over the roots of $f(x)$ and $g(x)$, respectively, with multiplicities taken into account. Obviously, (1) is the special case of (2) corresponding to $\deg g(x) = 1$.

Let $|f| = \max_i |a_i|$ and $|g| = \max_j |b_j|$. Consider the set A' of the primes p for which congruence (2) is valid. The degrees of the polynomials are related to the coefficients as

$$\begin{gathered} \ln^\delta p \le k = n_1 + n_2 \le ((3/2)^{1/3} + o(1))(\ln p / \ln\ln p)^{1/3}, \\ n_2 = o(n_1), \qquad |f| \le p^{o(1/k)}, \quad |g| \approx p^{1/k} \end{gathered} \tag{3}$$

for any fixed positive $\delta < 1/3$. For two positive real-valued functions $a(x)$ and $b(x)$ we write $a(x) \approx b(x)$ if $\ln a(x) / \ln b(x) \to 1$ as $x \to \infty$. We estimate the complexity of the discrete log problem in F_p with $p \in A'$ by $\approx p^{2/k^2}$ operations. In the set A, we include those primes $p \in A'$ for which $k = ((3/2)^{1/3} + o(1))(\ln p / \ln\ln p)^{1/3}$ in (3). It is easy to see that $p^{2/k^2} \approx L_p[\frac{1}{3}; (\frac{32}{9})^{1/3}]$ for $p \in A$. The algorithm has two parts. The first is computing the discrete logs to some base; this only must be done once for a given p and requires $\approx p^{2/k^2}$ operations. The second finds the logarithm of an individual $b \in F_p$. It is asymptotically faster and takes $\approx p^{(1+\sqrt{2})/2k^2}$ for $(1 + \sqrt{2})/2 = 1.914\cdots$. We believe that our algorithm would solve McCurley's challenging problem faster than those suggested in [3, 5, 7].

Let A_X be a set of primes $p < X$ from A. The definition suggests that $|A_X| \ge X^\varepsilon$ for any $\varepsilon = \varepsilon(X)$ such that $\varepsilon(X) \to 0$ as $X \to \infty$. Note that recognizing $p \in A$ requires generally more calculations than solving the discrete log problem in F_p. We note also that the prime numbers $p, p \to \infty$, such as $ab^t + c$ or their big prime factors, are in the set A for $\ln(\max\{|a|, |b|, |c|\}) = o(\ln^{1/3} p \ln\ln^{2/3} p)$.

We stress that our method differs from those of [3, 5]. Indeed, evaluating an individual logarithm by the methods of [3, 5] involves finding an integer l such that

$$a^l b \equiv q_1 q_2 \cdots q_r (\mathrm{mod}\ p)$$

for prime integers $q_i \le p^{1/k}$. Next the logarithm of each q_i must be evaluated. For this purpose, authors of [3, 5] sieve the values of polynomials $f(x) = f_{q_i}(x)$ dependent on q_i for which (1) holds. The advantage of our method is that congruence (2) or (1) does not depend on q_i (see Section 5). This allows us to apply relations (3) or use a polynomial $f(x)$ with small coefficients. In other words, we make extensive use of the structure of special primes.

This author has already used congruence (2) for factoring purposes [9]; similar but more special results are obtained in [10]. Section 7 contains some useful identities for resultants derived in [9].

The author is grateful to MacCentre, Moscow, for technical assistance in preparation of this paper and to Olga Sipacheva for her transformations of my English prose.

1. Algebraic numbers

In this section, we recall some results from algebraic number theory that are used in what follows. We assume that the polynomials $f(x)$ and $g(x)$ in (2) are irreducible over $\mathbb{Q}$. Let α and β be roots of $f(x)$ and $g(x)$, respectively. Then $K_1 = \mathbb{Q}(\alpha)$ and $K_2 = \mathbb{Q}(\beta)$ are fields of algebraic numbers of degrees n_1 and n_2. Let $\mathcal{O}_i$ be the ring of integers in K_i. Generally, α and β are not integers over $\mathbb{Q}$. But $\alpha_1 = a_0\alpha$, $\beta_1 = b_0\beta$ are integers. They are roots of the polynomials

$$f_1(x) = x^{n_1} + a_1 x^{n_1-1} + \cdots + a_0^{n_1-1} a_{n_1},$$
$$g_1(x) = x^{n_2} + b_1 x^{n_2-1} + \cdots + b_0^{n_2-1} b_{n_2},$$

respectively.

Proposition 1. *Let* $\gcd(a_0, a_{n_1}) = 1$*, and let* $\mathfrak{R}$ *denote the ideal that is the* gcd *of the ideals* $\alpha_1\mathcal{O}_1$ *and* $a_0\mathcal{O}_1$ *in* $\mathcal{O}_1$*. Then*

$$\mathrm{Norm}\ \mathfrak{R} = |a_0|^{n_1-1}.$$

Proposition 1 is proved in [9]. Put

$$h(x) = c_0 x^k + c_1 x^{k-1} + \cdots + c_k \in \mathbb{Z}[x].$$

Proposition 2. *Let* $\gcd(a_0, a_{n_1}) = 1$ *and* $\mathfrak{R}_1 = (a_0\mathcal{O}_1)\mathfrak{R}^{-1}$*. Then* $h(\alpha)\mathcal{O}_1 = \mathfrak{Q}\mathfrak{R}_1^{-k}$*, where* $\mathfrak{Q}$ *is an integer ideal in* K_1 *with*

$$\mathrm{Norm}\,\mathfrak{Q} = |a_0^k \,\mathrm{Norm}\, h(\alpha)| \le (k+1)^{n_1}(n_1+1)^{k/2}|f|^k|h|^{n_1}.$$

Proof. We have

$$h(\alpha) = (c_0\alpha_1^k + c_1 a_0 \alpha_1^{k-1} + \cdots + c_k a_0^k)/a_0^k.$$

The numerator of this fraction belongs to $\mathcal{O}_1$ and equals 0 modulo $\mathfrak{R}^k$. Therefore,

$$h(\alpha)\mathcal{O}_1 = (\mathfrak{R}a_0^{-1})^k\mathfrak{Q} = \mathfrak{R}_1^{-k}\mathfrak{Q},$$

where $\mathfrak{Q} = (c_0\alpha_1^k + c_1 a_0\alpha_1^{k-1} + \cdots + c_k a_0^k)\mathcal{O}_1\mathfrak{R}^{-k}$ is an integer ideal. Since $\mathrm{Norm}\,\mathfrak{R}_1 = a_0$, we have $\mathrm{Norm}\,\mathfrak{Q} = |a_0^k \,\mathrm{Norm}\, h(\alpha)|$. Let us find an upper bound for

$|\operatorname{Norm} h(\alpha)|$. By definition,

$$|\operatorname{Norm} h(\alpha)| = \prod_{\alpha} |c_0\alpha^k + c_1\alpha^{k-1} + \cdots + c_k| \le \prod_{\alpha}((k+1)|h| \max\{1, |\alpha|^k\}),$$

where α ranges over the set of roots of $f(x)$. By Landau's inequality

$$|a_0| \prod_{\alpha} \max\{1, |\alpha|\} \le (n_1 + 1)^{1/2}|f|.$$

Hence

$$\begin{aligned} |\operatorname{Norm} h(\alpha)| &\le ((k+1)|h|)^{n_1} \left(|a_0| \prod_{\alpha} \max\{1, |\alpha|\}\right)^k /|a_0|^k \\ &= ((k+1)|h|)^{n_1}(n_1+1)^{k/2}|f|^k/|a_0|^k. \end{aligned}$$

This completes the proof of Proposition 2.

The ring $\mathbb{Z}[\alpha_1]$ is a subring of $\mathcal{O}_1$. If a prime rational q does not divide the index of $\mathbb{Z}[\alpha_1]$ in $\mathcal{O}_1$, then the decomposition of $q\mathcal{O}_1$ in $\mathcal{O}_1$ is given by the following well-known statement [5, p. 127].

Proposition 3. *If q does not divide $[\mathcal{O}_1 \colon \mathbb{Z}[\alpha_1]]$ and*

$$f_1(x) = \prod_i h_i^{e_i}(x) \tag{4}$$

over $F_q[x]$, where $h_i(x)$ are different irreducible polynomials in $F_q[x]$, then $q\mathcal{O}_1 = \prod_i \mathfrak{Q}_i^{e_i}$ for different prime ideals $\mathfrak{Q}_i \subset \mathcal{O}_1$ such that $\mathfrak{Q}_i = \gcd(h_i(\alpha_1)\mathcal{O}_1, q\mathcal{O}_1)$ and $\operatorname{Norm} \mathfrak{Q}_i = q^{\deg h_i(x)}$.

Following [5] we say that a prime ideal of $\mathcal{O}_1$ or $\mathcal{O}_2$ of degree 1 is bad if its norm divides the index $a_0[\mathcal{O}_1 : \mathbb{Z}[\alpha_1]]$ or $b_0[\mathcal{O}_2 \colon \mathbb{Z}[\beta_1]]$, respectively. All other prime ideals of degree 1 are called good.

In [5], prime integers dividing the index are recognized via the following theorem of Dedekind. Suppose that $f_1(x)$ has factorization (4) in the ring $F_q[x]$. Then the primes q divides the index if and only if there exists a j such that $e_j \ge 2$ and $h_j(x)$ divides $(f_1(x) - \prod_i h_i^{e_i}(x))/q$ in $F_q[x]$.

The following proposition slightly generalizes Proposition 2 of [5].

Proposition 4. *If $\gcd(a_0, a_{n_1}) = 1$ and $c, d \neq 0$ are coprime integers such that*

$$c^{n_1} f(d/c) = a_0 d^{n_1} + a_1 c d^{n_1 - 1} + \cdots + a_{n_1} c^{n_1}$$

is coprime to $a_0[\mathcal{O}_1 \colon \mathbb{Z}[\alpha_1]]$, then

$$(c\alpha - d)\mathcal{O}_1 = \mathfrak{Q}_1^{l_1}\mathfrak{Q}_2^{l_2} \cdots \mathfrak{Q}_s^{l_s}\mathfrak{R}_1^{-1},$$

where $\mathfrak{Q}_i$, $i = [1, s]$, are different good prime ideals of $\mathcal{O}_1$, and $\operatorname{Norm} \mathfrak{Q}_i = q_i$ for different q_i. Moreover,

$$c^{n_1} f(d/c) = \prod_i q_i^{l_i}$$

is the prime factorization of $c^{n_1} f(d/c)$.

Consider congruence (2). We assume that p does not divide the Δ_f, Δ_g-discriminants of the polynomials $f(x)$ and $g(x)$ and their leading coefficients a_0 and b_0. Therefore, p does not divide the discriminants of the polynomials $f_1(x)$ and $g_1(x)$. Thus p does not divide $a_0[\mathcal{O}_1 \colon \mathbb{Z}[\alpha_1]]$ and $b_0[\mathcal{O}_2 \colon \mathbb{Z}[\beta_1]]$.

Let $h(x) \in F_p[x]$ be an irreducible polynomial of degree $t \geq 1$ that is a common factor of the polynomials $f(x)$ and $g(x)$ modulo p. Then $h_1(x) = a_0^t h(x/a_0)$ is an irreducible factor of $f_1(x)$ in $F_p[x]$. Similarly, $h_2(x) = b_0^t h(x/b_0)$ is an irreducible factor of $g_1(x)$ in $F_p[x]$. By Proposition 3,

$$\mathfrak{P}_1 = \gcd(h_1(\alpha_1)\mathcal{O}_1, p\mathcal{O}_1) \quad \text{and} \quad \mathfrak{P}_2 = \gcd(h_2(\beta_1)\mathcal{O}_2, p\mathcal{O}_2),$$

are prime ideals of $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively. Therefore, $\mathrm{Norm}(\mathfrak{P}_i) = p^t$. Thus $\mathcal{O}_i/\mathfrak{P}_i \cong F_{p^t}$. Generally, $\alpha \notin \mathcal{O}_1$ and $\beta \notin \mathcal{O}_2$. Put

$$\mathcal{O}_1' = \bigcup_{j=0}^{\infty} a_0^{-j}\mathcal{O}_1, \quad \mathcal{O}_2' = \bigcup_{j=0}^{\infty} b_0^{-j}\mathcal{O}_2.$$

Since p does not divide $a_0 b_0$, the ideal $\mathfrak{P}_i' = \mathfrak{P}_i\mathcal{O}_i'$ is a prime ideal in $\mathcal{O}_i'$. Consider

$$\varphi_i \colon \mathcal{O}_i' \to \mathcal{O}_i'/\mathfrak{P}_i' \cong F_{p^t}, \quad i = 1, 2.$$

Let $\overline{\xi}$ denote the image of $\xi \in \mathcal{O}_i'$ under φ_i. We can assume that $\overline{\alpha} = \overline{\beta}$.

Let $\mathcal{U}_i$ be the group of units of $\mathcal{O}_i$, and $\mathcal{U}_i^* \subseteq \mathcal{U}_i$ the group of roots of unity. Let $n_i = r_{i1} + 2r_{i2}$, where r_{i1} is the number of real embeddings of K_i, and $2r_{i2}$ is the number of its complex embeddings. Consider the well-known map $K_i \to \mathbb{R}^{r_i}$, where $r_i = r_{i1} + r_{i2}$, defined by

$$\xi \in K_i \to l_i(\xi) = (2^{\nu_{i1}} \in \ln|\sigma_{i1}(\xi)|, \ldots, 2^{\nu_{ir_i}} \ln|\sigma_{ir_i}(\xi)|),$$

where

$$\nu_{ij} = \begin{cases} 1 \text{ if } \sigma_{ij} \text{ is a complex embedding,} \\ 0 \text{ if } \sigma_{ij} \text{ is a real embedding.} \end{cases}$$

The image of $\mathcal{U}_i$ under this map is a lattice of dimension $r_i - 1$ in $\mathbb{R}^{r_i}$. The map $\xi \in \mathcal{U}_i \to l_i(\xi)$ is a homomorphism with kernel $\mathcal{U}_i^*$. We define a map

$$l \colon \mathcal{U}_1 \times \mathcal{U}_2 \to \mathbb{R}^{r_1 + r_2}$$

by $l(\xi_1, \xi_2) = (l_1(\xi_1), l_2(\xi_2))$, $\xi_i \in \mathcal{U}_i$. Obviously, $l(\mathcal{U}_1 \times \mathcal{U}_2)$ is a lattice of dimension $r_1 + r_2 - 2$. We denote it by $\mathcal{L}(f, g)$. Thus any $t \geq r_1 + r_2 - 1$ pairs of units $(\xi_{1j}, \xi_{2j}) \in \mathcal{U}_1 \times \mathcal{U}_2$, where $j \in [1, t]$, are related by

$$\prod_{j=1}^{t} \xi_{1j}^{z_j} = \prod_{j=1}^{t} \xi_{2j}^{z_j} = 1,$$

where z_j with $j \in [1, t]$ are integers not all zero. For $\xi \in \mathbb{R}^n$, we denote by $|\xi|$ its Euclidean length. In [11], the following theorem is proved.

Theorem 1. *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$, and λ a positive number such that $\lambda \leq \min_{\xi \in \mathcal{L} - 0} |\xi| = \lambda(\mathcal{L})$, and let $\xi_i \in \mathcal{L}$, with $i \in [1, t]$, be vectors such that $|\xi_i| \leq M$. Suppose that there exist integers z_j with $j \in [1, t]$ such that not all of them are zero and $\sum_{j=1}^{t} z_j \xi_j = 0$. Then there exist such integers z_j with the properties that $|z_j| \leq ((2n+3)M/\lambda)^n$ and their evaluating requires no more than $O(n^{5+\varepsilon}(\ln M/\lambda)^{1+\varepsilon})$ binary operations for any $\varepsilon > 0$.*

If $\mathcal{L} = \mathcal{L}(f, g)$ and $n_1 \geq n_2$, then, by Lemma 1 of [5], we have $\lambda(\mathcal{L}) \geq 1/10n_1^2$. It is easy to see that $|\mathcal{U}_i^*| = O(n_i \ln\ln n_i)$.

2. Description of the algorithm

In this section we give a brief description of our algorithm. The details will be discussed later on. We suppose that all assumptions made in Section 1 concerning the polynomials $f(x)$ and $g(x)$ in (2) hold. The algorithm parameters k, B, and L are related by $B \approx L \approx p^{1/k^2}$, where $k = n_1 + n_2$ obeys estimates (3).

Our method is based on the efficient solution of the principal ideal problem for the good ideals in $\mathcal{O}_i$ whose norms are bounded by B. In other words, we determine positive integers u and v and, for the ideas $\mathfrak{A} \subset \mathcal{O}_1$ and $\mathfrak{B} \subset \mathcal{O}_2$ specified above, algebraic integers $\gamma_{\mathfrak{A}} \in \mathcal{O}_1$ and $\delta_{\mathfrak{B}} \in \mathcal{O}_2$ such that

$$\mathfrak{A}^v = \gamma_{\mathfrak{A}} \mathcal{O}_1, \tag{5}$$

$$\mathfrak{B}^u = \delta_{\mathfrak{B}} \mathcal{O}_2. \tag{6}$$

The numbers $\gamma_{\mathfrak{A}}$ and $\delta_{\mathfrak{B}}$ are calculated approximately; more precisely, we evaluate the vectors $l_1(\gamma_{\mathfrak{A}})$ and $l_2(\delta_{\mathfrak{B}})$ with an accuracy of $\approx B^{1/2}$ binary digits.

2.1. We sieve through pairs c, d of small integers ($|c|, |d| \leq L$) to find coprime c and d for which

$$a_0 \operatorname{Norm}(c\alpha - d) = c^{n_1} f(d/c) \tag{7}$$

and

$$b_0 \operatorname{Norm}(c\beta - d) = c^{n_2} g(d/c) \tag{8}$$

are both smooth with respect to B (or B-smooth), i.e., do not have prime factors larger than B. If integers (7) and (8) are coprime to $a_0[\mathcal{O}_1 \colon \mathbb{Z}[\alpha_1]]$ and $b_0[\mathcal{O}_2 \colon \mathbb{Z}[\beta_1]]$, respectively, then Proposition 4 gives the decompositions

$$(c\alpha - d)\mathcal{O}_1 = \prod_{\mathfrak{A}} \mathfrak{A}^{l_{cd\mathfrak{A}}} \mathfrak{R}_1^{-1}, \qquad (c\beta - d)\mathcal{O}_2 = \prod_{\mathfrak{B}} \mathfrak{B}^{m_{cd\mathfrak{B}}} \mathfrak{R}_2^{-1},$$

where $\mathfrak{A} \subset \mathcal{O}_1$ and $\mathfrak{B} \subset \mathcal{O}_2$ are good ideals with $\operatorname{Norm} \mathfrak{A}, \operatorname{Norm} \mathfrak{B} \leq B$ and

$$\mathfrak{R}_1 = (a_0\mathcal{O}_1)/\gcd(a_0\mathcal{O}_1, \alpha_1\mathcal{O}_1) \subset \mathcal{O}_1, \qquad \mathfrak{R}_2 = (b_0\mathcal{O}_2)/\gcd(b_0\mathcal{O}_2, \beta_1\mathcal{O}_2) \subset \mathcal{O}_2.$$

Note that $\mathfrak{R}_1$ and $\mathfrak{R}_2$ can be eliminated by considering decompositions of the ideals $\frac{(c\alpha - d)}{(c_1\alpha - d_1)}\mathcal{O}_1$ and $\frac{(c\beta - d)}{(c_1\beta - d_1)}\mathcal{O}_2$ for some c_1 and d_1 but this makes the formulas more complicated. For simplicity, we assume that $a_0 = b_0 = 1$. Then the decompositions specified above can be represented as

$$(c\alpha - d)\mathcal{O}_1 = \prod_{\mathfrak{A}} \mathfrak{A}^{l_{cd\mathfrak{A}}} \tag{9}$$

and

$$(c\beta - d)\mathcal{O}_2 = \prod_{\mathfrak{B}} \mathfrak{B}^{m_{cd\mathfrak{B}}}. \tag{10}$$

2.2. Let us raise both relations to the power uv. Relations (5) and (6) imply that

$$(c\alpha - d)^{uv} \prod_{\mathfrak{A}} \gamma_{\mathfrak{A}}^{-ul_{cd\mathfrak{A}}} = \xi_{cd} \tag{11}$$

and

$$(c\beta - d)^{uv} \prod_{\mathfrak{B}} \delta_{\mathfrak{B}}^{-vm_{cd\mathfrak{B}}} = \eta_{cd} \tag{12}$$

are units in $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively. To those coprime pairs c, d for which the integers (7) and (8) are smooth, we assign the pairs $(\xi_{cd}, \eta_{cd}) \in \mathcal{U}_1 \times \mathcal{U}_2$ of units. We can obtain $\approx B$ such pairs of units. Indeed, by condition (3),

$$|c^{n_1} f(d/c)| \leq\approx L^{n_1}|f| \approx p^{1/k}, \qquad |c^{n_2} g(d/c)| \leq\approx L^{n_2}|g| \approx p^{1/k}.$$

The results of [12] imply that the probability $\mathcal{P}$ of the smoothness of both integers (7) and (8) equals $\approx \exp(-2k \ln k)$. Since $L^2\mathcal{P} \geq\approx B$ under the assumptions made above, we obtain $\approx B$ pairs of the required form. Every $s \leq n_1 + n_2$ pairs give two multiplicative relations

$$\prod_{cd} \xi_{cd}^{y_{cd}} = 1, \qquad \prod_{cd} \eta_{cd}^{y_{cd}} = 1. \tag{13}$$

2.3. Relations (11), (12), and (13) imply that

$$\prod_{cd}(c\alpha - d)^{uvy_{cd}} \prod_{\mathfrak{A}} \gamma_{\mathfrak{A}}^{-uy_{cd}l_{cd\mathfrak{A}}} = 1 \quad \text{and} \quad \prod_{cd}(c\beta - d)^{uvy_{cd}} \prod_{\mathfrak{B}} \delta_{\mathfrak{B}}^{-vy_{cd}m_{cd\mathfrak{B}}} = 1.$$

Let $x_{\mathfrak{A}}$ and $x_{\mathfrak{B}}$ denote the logarithms of $\overline{\gamma}_{\mathfrak{A}}, \overline{\delta}_{\mathfrak{B}} \in F_{p^t}$. The relations given above yield the convergence

$$\sum_{\mathfrak{A}} u \left(\sum_{cd} y_{cd} l_{cd\mathfrak{A}} \right) x_{\mathfrak{A}} - \sum_{\mathfrak{B}} v \left(\sum_{cd} y_{cd} m_{cd\mathfrak{B}} \right) x_{\mathfrak{B}} \equiv 0 \pmod{p^t - 1}. \tag{14}$$

2.4. Let $S = (l_{cd\mathfrak{A}})$ and $R = (m_{cd\mathfrak{B}})$ be matrices whose rows are indicated by the pairs c, d for which the integers (7) and (8) are B-smooth and coprime to the indices, and columns are indexed by the good ideals $\mathfrak{A}$ and $\mathfrak{B}$. Then the left-hand side of (14) equals the product of the row $(y_{cd})_{cd}$ and the matrix $(uS, -vR)$. Thus each relation (13) gives one row $(y_{cd})_{cd}$ and congruence (14). These rows form a matrix Y. We have a system of congruences with matrix $T = Y(uS, -vR)$. This matrix is a product of two sparse integer matrices. Consider $x_{\mathfrak{A}_0} = 1$ for some $\mathfrak{A}_0$. The system can be reduced to one system with matrix Y and to another system with matrix $(uS, -vR)$. All the fundamental solutions of the first system can be written at once, since the matrix Y is of a very special form. We solve the other system modulo $p-1$ by applying the Wiedemann algorithm [13] and thereby obtain $x_{\mathfrak{A}} \equiv z(\mathfrak{A}, \mathfrak{A}_0) x_{\mathfrak{A}_0} (\operatorname{mod} p - 1)$ and $x_{\mathfrak{B}} \equiv z(\mathfrak{B}, \mathfrak{A}_0) x_{\mathfrak{A}_0} (\operatorname{mod} p - 1)$.

We have to solve the following problems:

1. Evaluate the terms of relations (5) and (6), i.e., solve the principal ideal problem.
2. Evaluate the terms of (13) for pairs of units (11), (12), i.e., find multiplicative relations between the units.
3. Express the unknown individual logarithm in F_p via $x_{\mathfrak{A}}, x_{\mathfrak{B}} (\operatorname{mod} p - 1)$ and estimate the running time of the entire algorithm.

These problems are solved successively in Sections 3–5.

3. The principal ideal problem

In this section, we evaluate the terms of (5) and (6). Let $B_1 = B^{1/2}$.

3.1. We sieve pairs c, d of small integers ($|c|, |d| \leq L^{1/2}$) to find coprime pairs for which $\operatorname{Norm}(c\alpha - d) = c^{n_1} f(d/c)$ is smooth with respect to B_1 and coprime to $[\mathcal{O}_1 \colon \mathbb{Z}[\alpha]]$. Recall that we assume that $a_0 = 1$. For such c, d, we have

$$(c\alpha - d)\mathcal{O}_1 = \prod_{\mathfrak{A}} \mathfrak{A}^{v_{cd\mathfrak{A}}}, \tag{15}$$

where $\mathfrak{A} \subset \mathcal{O}_1$ are good ideals with $\operatorname{Norm} \mathfrak{A} \leq B_1$. Let s_1 be the number of such ideals. Then $s_1 \approx B_1$. By (3),

$$|\operatorname{Norm}(c\alpha - d)| \leq\approx L^{n_1/2} |f| \approx p^{1/2k}.$$

According to [12], the probability $\mathcal{P}_1$ of smoothness of $\operatorname{Norm}(c\alpha - d)$ is $\approx \exp(-k \ln k)$. Since $L\mathcal{P}_1 \geq\approx B_1$, we obtain $\approx B_1 \approx s_1$ pairs c, d. Consider the sparse integer $(\approx B_1) \times s_1$ matrix $V = (v_{cd\mathfrak{A}})_{cd\mathfrak{A}}$. We can treat V as a square $s_1 \times s_1$ matrix. Using Wiedemann's coordinate recurrence method [13], we determine the characteristic polynomial of V:

$$\lambda(x) = x^{s_1} + \lambda_1 x^{s_1 - 1} + \cdots + \lambda_{s_1},$$

where $v = |\det V| = |(-1)^{s_1} \lambda_{s_1}|$. It is easy to see that $|\lambda_i| \leq \exp(\approx s_1)$. If $v = 0$, we can slightly change V by using several new decompositions of the form (15). Thus, we can restrict ourselves to the case $v \neq 0$.

3.2. Let Λ_0 be the $s_1 \times r_1$ matrix whose rows are the vectors $l_1(c\alpha - d) \in \mathbb{R}^{r_1}$, where c, d range over all pairs used in (15). Each coordinate of $l_1(c\alpha - d)$ is determined with an accuracy of $\approx B_1$ binary digits. Let V' be a square $s_1 \times s_1$ matrix such that $V'V = vE$ for the identity matrix E. We evaluate $\Lambda_1 = V' \Lambda_0$ by

$$\Lambda_1 = -\operatorname{sgn}(\lambda_{s_1})(V^{s_1 - 1} + \lambda_1 V^{s_1 - 2} + \cdots + \lambda_{s_1 - 1} E)\Lambda_0$$

according to Horner's method. So Λ_1 is the $s_1 \times r_1$ matrix with rows $l_1(\gamma_{\mathfrak{A}})$, where each $\gamma_{\mathfrak{A}}$ is defined by $\mathfrak{A}^v = \gamma_{\mathfrak{A}} \mathcal{O}_1$ and $\mathfrak{A}$ ranges over all good ideals $\mathfrak{A}$ with $\operatorname{Norm} \mathfrak{A} \leq B_1$. Since V is sparse and $|\lambda_i| \leq \exp(\approx s_1)$, the entries of Λ_1 are determined with an accuracy of $\approx B_1$ binary digits.

3.3. Let $\mathfrak{A}'$ be a good ideal with $\operatorname{Norm} \mathfrak{A}' = q$, where $B_1 < q \leq B$. Let α_q be a root of the polynomial $f(x) (\operatorname{mod} q)$ such that $\mathfrak{A}' = \gcd((\alpha - \alpha_q)\mathcal{O}_1, q\mathcal{O}_1)$. We sieve pairs of small integers c, d such that $|c|, |d| \leq L$ and $c\alpha_q \equiv d (\operatorname{mod} q)$ to find a coprime pair c, d for which

$$\operatorname{Norm}(c\alpha - d)/q = c^{n_1} f(d/c)/q$$

is a B_1-smooth integer coprime to $[\mathcal{O}_1 : \mathbb{Z}[\alpha]]$. For such c and d we have

$$(c\alpha - d)\mathcal{O}_1 = \mathfrak{A}' \prod_{\mathfrak{A}} \mathfrak{A}^{v(\mathfrak{A}', \mathfrak{A})}, \tag{16}$$

where $\mathfrak{A}$ are good ideals with $\operatorname{Norm} \mathfrak{A} \leq B_1$. Let s be the number of good ideals $\mathfrak{A} \subset \mathcal{O}_1$ with $\operatorname{Norm} \mathfrak{A} \leq B$.

3.4. Let Δ be the $(s-s_1)\times r_1$ matrix with rows $l_1(c\alpha-d)$ determined by (16) for each good ideal $\mathfrak{A}'$ such that $B_1 < \operatorname{Norm}\mathfrak{A}' \le B$. The coordinates of these rows are determined with an accuracy of $\approx B_1$ binary digits. Let us define the $(s-s_1)\times r_1$ matrix Λ_2 by

$$\Lambda_2 = v\Delta - V_1\Lambda_1, \tag{17}$$

where V_1 is the $(s-s_1)\times s_1$ matrix whose rows are $(v(\mathfrak{A}',\mathfrak{A}))_{\mathfrak{A}}$ in (16). The rows of the matrix Λ_2 are $l_1(\gamma_{\mathfrak{A}})$ for good ideals $\mathfrak{A}'$ such that $B_1 < \operatorname{Norm}\mathfrak{A}' \le B$. Their coordinates are determined within $\approx B_1$ binary digits. This gives (5). Relations (6) are obtained similarly.

It is easy to see that decompositions (15) and (16) can be derived with the use of the sieving procedure described in Section 2.

The application of relations (5) requires $\approx B_1$ bits of storage space for each vector $l_1(\gamma_{\mathfrak{A}})$, i.e., $\approx BB_1 = B^{3/2}$ bits in total. To reduce the storage requirement, we store only the matrix Λ_1 and all decompositions of the form (16) used; in other words, we only store the vector $(v(\mathfrak{A}',\mathfrak{A}))_{\mathfrak{A}}$ and pair c, d for each ideal $\mathfrak{A}'$. This requires $\approx B$ bits. The storage space necessary for the application of (6) is determined similarly.

4. Multiplicative relations between units

In this section, we evaluate the terms of (13). To apply Theorem 1, we have to specify the vectors $(l_1(\xi_{cd}), l_2(\eta_{cd})) \in \mathcal{L}(f,g)$ corresponding to the pairs of units ξ_{cd}, η_{cd} defined by (11), (12). In addition, we must estimate their Euclidean lengths. Let us do this for $l_1(\xi_{cd})$. By (11), we have

$$l_1(\xi_{cd}) = uvl_1(c\alpha-d) - u\sum_{\mathfrak{A}} l_{cd\mathfrak{A}} l_1(\gamma_{\mathfrak{A}}). \tag{18}$$

Since the vector $(l_{cd\mathfrak{A}})_{\mathfrak{A}}$ is sparse, we can easily evaluate all $l_1(\gamma_{\mathfrak{A}})$ in (17) with the use of the stored matrix Λ_1 and the corresponding decompositions of the form (16).

First, we estimate the Euclidean length of $l_1(c\alpha-d)$ for c, d with $|c|, |d| \le L$. We have

$$|l_1(c\alpha-d)| \le \sum_{i=1}^{n_1} |\ln|c\alpha^{(i)}-d||,$$

where $\alpha^{(i)}$ are the roots of the polynomial $f(x)$. Since $|c\alpha^{(i)}-d| \le 2L\max\{1,|\alpha^{(i)}|\}$ and by the Landau inequality

$$\max\{1,|\alpha^{(i)}|\} \le \prod_{i=1}^{n_1}\max\{1,|\alpha^{(i)}|\} \le (n_1+1)^{1/2}|f|,$$

we have $|c\alpha^{(i)}-d| \le 2L(n_1+1)^{1/2}|f| = O(p^{1/k})$. Hence $\ln|c\alpha^{(i)}-d| \le c_1(\ln p)/k$ for some $c_1 > 0$. On the other hand, $|\sum_{i=1}^{n_1}\ln|c\alpha^{(i)}-d|| = |\ln|\operatorname{Norm}(c\alpha-d)|| = O((\ln p)/k)$. Therefore,

$$|l_1(c\alpha-d)| \le \left|\sum_{i=1}^{n_1}\ln|c\alpha^{(i)}-d|\right| = O(\ln p).$$

Now, we estimate the Euclidean lengths of the rows of Λ_1. We have $\Lambda_1 = V'\Lambda_0$ for some integer matrix V' such that $V'V = vE$ (see Section 3). By Hadamard's inequality, the entries of V' are bounded by $\exp(\approx B_1)$. Thus the Euclidean lengths of the rows of Λ_1 are also bounded by $\exp(\approx B_1)$. Since $v = \exp(\approx B_1)$, (17) implies that the Euclidean lengths of the rows of Λ_2 are bounded by the same value $\exp(\approx B_1)$. Thus, by (18) $|l_1(\xi_{cd})| \leq \exp(\approx B_1)$. Similarly, $|l_2(\eta_{cd})| \leq \exp(\approx B_1)$.

Using the algorithm suggested by this author in [11], we obtain the terms of the relation $\sum_{cd} y_{cd} l(\xi_{cd}, \eta_{cd}) = 0$ in $\mathcal{L}(f, g)$ for integers y_{cd}, i.e., of the relations

$$\sum_{cd} y_{cd} l_1(\xi_{cd}) = 0, \qquad \sum_{cd} y_{cd} l_2(\eta_{cd}) = 0.$$

Now, the sought relations of the form (13) are obtained from Theorem 1 by multiplying the integer y_{cd} by some factors of $|\mathcal{U}_1^*|$ or $|\mathcal{U}_2^*|$, if necessary.

5. The individual logarithm

In this section we express the unknown logarithm $y(\operatorname{mod} p - 1)$ via the $x_{\mathfrak{A}}, x_{\mathfrak{B}}(\operatorname{mod} p - 1)$ values found in Section 2. We assume that the integer a is bounded by $p^{1/k}$ in absolute value; this is so under the assumption of the generalized Riemann hypothesis [15].

5.1. We search through random integers $l \in [1, p - 1]$ until we find one for which

$$a^l b \equiv q_1 q_2 \cdots q_r (\operatorname{mod} p), \tag{19}$$

where q_i are rational primes $\leq p^{1/k}$; the fulfillment of (19) is verified by the elliptic curve factoring method [14]. For $i \in [0, r]$ let x_i be the logarithm of the residue q_i modulo p (we assume that $q_0 = a$). To find $y(\operatorname{mod} p - 1)$, we must relate x_i to $x_{\mathfrak{A}}$ and $x_{\mathfrak{B}}$.

5.2. For each $i \in [0, r]$ we find an integer c bounded by $L^{1/2}$ in absolute value for which the ideal $\mathfrak{Q}_c = (q_i + cg(\alpha))\mathcal{O}_1$ has the decomposition

$$\mathfrak{Q}_c = \prod_{\mathfrak{A}} \mathfrak{A}^{l_{t\mathfrak{A}}}, \tag{20}$$

where $\mathfrak{A}$ are prime ideals with $\operatorname{Norm} \mathfrak{A} \leq p^{1/k}$ coprime to $[\mathcal{O}_1 \colon \mathbb{Z}[\alpha]]$. To obtain (20), we evaluate $\operatorname{Norm} \mathfrak{Q}_c$, which is coprime to $[\mathcal{O}_1 \colon \mathbb{Z}[\alpha]]$, and find its prime factors $\leq p^{1/k}$ by the elliptic curve factoring method. If the decomposition obtained is complete, then the degrees of the prime ideals on the right-hand side of (20) equal 1 with probability tending to 1. Indeed, let $\mathfrak{Q}_c$ be a product of first-degree prime ideals in $\mathcal{O}_1$ whose norms are $\leq p^{1/k}$ and exponents in $\mathfrak{Q}_c$ equal 1. This is so if $\operatorname{Norm} \mathfrak{Q}_c$ is a $p^{1/k}$-smooth square-free integer. The probability that a $p^{1/k}$-smooth integer bounded by $\approx p$ in absolute value is square-free tends to 1 as $p \to \infty$; this readily follows from the considerations of [12].

Proposition 2 implies that

$$\operatorname{Norm} \mathfrak{Q}_c = |\operatorname{Norm}(q_i + cg(\alpha))| \leq (n_2 + 1)^{n_1} (n_1 + 1)^{n_2/2} |f|^{n_2} |q_i + cg(x)|^{n_1} \approx p.$$

So the probability of the event under consideration is $\approx \exp(-k \ln k)$. Under conditions (3), $L^{1/2} \geq\approx \exp(-k \ln k)$, which implies (20).

5.3. Take a positive real $\nu < 1$. Our immediate goal is to construct a reduction of a good ideal $\mathfrak{A}' \subset \mathcal{O}$ with $\operatorname{Norm} \mathfrak{A}' = q$, where $B < q \leq p^{1/k}$. In other words, we want to find a relation between this ideal and ideals with norms $\leq q^{\nu}$ in $\mathcal{O}_i$, $i = 1, 2$. The ideal $\mathfrak{A}'$ is the gcd of the ideals $(\alpha - \alpha_q)\mathcal{O}_1$ and $q\mathcal{O}_1$ for some root α_q of the polynomial $f(x)$ modulo q. Let $\mathcal{L}_q(\alpha_q)$ be the lattice of pairs of integers (c, d) such that $c\alpha_q \equiv d (\operatorname{mod} q)$.

We look for a coprime pair $(c, d) \in \mathcal{L}_q(\alpha_q)$ such that $|c|, |d| \leq Lq^{1/2}$ and the integers

$$\operatorname{Norm}(c\alpha - d)/q \equiv c^{n_1} f(d/c)/q \quad \text{and} \quad \operatorname{Norm}(c\beta - d) \equiv c^{n_2} g(d/c)$$

are q^{ν}-smooth and coprime to the indices $[\mathcal{O}_1 \colon \mathbb{Z}[\alpha]]$ and $[\mathcal{O}_2 \colon \mathbb{Z}[\beta]]$, respectively. To find it, we apply the elliptic curve factoring method for each such pair. For the pair c, d obtained, we have the decompositions

$$(c\alpha - d)\mathcal{O}_1 = \mathfrak{A}' \prod_{\mathfrak{A}} \mathfrak{A}^{l(\mathfrak{A}', \mathfrak{A})}, \tag{21}$$

$$(c\beta - d)\mathcal{O}_2 = \prod_{\mathfrak{B}} \mathfrak{B}^{m(\mathfrak{A}', \mathfrak{B})}, \tag{22}$$

where $l(\mathfrak{A}', \mathfrak{A}), m(\mathfrak{A}', \mathfrak{B}) \in \mathbb{N}$ and $\mathfrak{A} \subset \mathcal{O}_1, \mathfrak{B} \subset \mathcal{O}_2$ are good ideals with norms $\leq q^{\nu}$. We have the estimate

$$|\operatorname{Norm}(c\alpha - d)| = |c^{n_1} f(d/c)| \leq (n_1 + 1)|f|(Lq^{1/2})^{n_1} \approx p^{1/k} q^{n_1/2}.$$

Similarly,

$$|\operatorname{Norm}(c\beta - d)| = |c^{n_2} g(d/c)| \leq (n_2 + 1)|g|(Lq^{1/2})^{n_2} \approx p^{1/k} q^{n_2/2}.$$

We assume that the probability of q^{ν}-smoothness of $\operatorname{Norm}(c\alpha - d)$ and $\operatorname{Norm}(c\beta - d)$ for a random pair $c, d \in \mathcal{L}_q(\alpha_q)$ with $|c|, |d| \leq Lq^{1/2}$ equals the probability of the occurrence of two q^{ν}-smooth naturals in $[1, \approx p^{1/k} q^{n_1/2}]$ and $[1, \approx p^{1/k} q^{n_2/2}]$, respectively. This probability is $\approx \exp(-u \ln u)$, where

$$u = \frac{k}{2\nu} + \frac{2 \ln p}{k\nu \ln q}.$$

We have $u = \frac{k}{2\nu}(1 + o(1))$ if $p^{1/m} < q \leq p^{1/k}$, where $m = k^{3/2}$, and $u \leq \frac{5k}{2\nu}$ if $B < q \leq p^{1/m}$.

It is easy to see that, for a random $a (\operatorname{mod} q)$, the lattice $\mathcal{L}_q(a)$ has a basis of vectors whose coordinates are bounded by $O(q^{1/2} \ln \ln q)$ with probability tending to 1 as $q \to \infty$. So with probability tending to 1, the number of vectors in $\mathcal{L}_q(a)$ with coordinates bounded by $Lq^{1/2}$ is $\approx L^2$.

For $5/8 \leq \nu < 1$ we have $L^2 \geq\approx \exp(u \ln u)$. Thus, we can find the desired pair and the corresponding decompositions (21) and (22) by searching through a set of pairs $(c, d) \in \mathcal{L}_q(\alpha_q)$ bounded by $Lq^{1/2}$ in absolute value.

A good ideal $\mathfrak{B}' \subset \mathcal{O}_2$ with $\operatorname{Norm} \mathfrak{B}' = q$, where $B < q \leq p^{1/k}$, is reduced similarly.

5.4. For each prime rational q_i, $i \in [1, r]$, on the right-hand side of (19) and $q_0 = a$, we proceed as follows.

Applying the reduction constructed above to each ideal $\mathfrak{A}'$ with $\operatorname{Norm} \mathfrak{A}' = q > B$ on the right-hand side of (20), yields decompositions of the form (21) and (22), where $\operatorname{Norm} \mathfrak{A}$, $\operatorname{Norm} \mathfrak{B} \leq q^{\nu}$. Applying the same reduction to each of the ideals $\mathfrak{A}$ and $\mathfrak{B}$ obtained yields decompositions of the forms (21) and (22) with $\operatorname{Norm}\mathfrak{A}$, $\operatorname{Norm}\mathfrak{B} \le q^{\nu^2}$, etc. Each step gives $O(k)$ new ideals. Thus, after $\exp(O(\ln\ln^2 p))$ steps, we obtain

$$(q_i + c_i g(\alpha)) \prod_{cd} (c\alpha - d)^{z_{icd}} \mathcal{O}_1 = \prod_{\mathfrak{A}} \mathfrak{A}^{l'_{i\mathfrak{A}}}, \tag{23}$$

$$\prod_{cd} (c\beta - d)^{z_{icd}} \mathcal{O}_2 = \prod_{\mathfrak{B}} \mathfrak{B}^{m'_{i\mathfrak{B}}}, \tag{24}$$

where $\mathfrak{A} \subset \mathcal{O}_1$ and $\mathfrak{B} \subset \mathcal{O}_2$ are good ideals with $\operatorname{Norm}\mathfrak{A}$, $\operatorname{Norm}\mathfrak{B} \le B$. Note that the number of nonzero $l'_{i\mathfrak{A}}$ and $m'_{i\mathfrak{B}}$ is bounded by $\exp(O(\ln\ln^2 p))$.The same value bounds the Euclidean lengths of the vectors $(l'_{i\mathfrak{A}})_{\mathfrak{A}}$, $(m'_{i\mathfrak{B}})_{\mathfrak{B}}$, and $(z_{icd})_{cd}$.

5.5. Raising the relations (23) and (24) to the power uv and applying (5) and (6) we see that

$$(q_i + c_i g(\alpha))^{uv} \prod_{cd} (c\alpha - d)^{uvz_{icd}} \prod_{\mathfrak{A}} \gamma_{\mathfrak{A}}^{-ul'_{i\mathfrak{A}}} = \xi_i, \tag{25}$$

and

$$\prod_{cd} (c\beta - d)^{uvz_{icd}} \prod_{\mathfrak{B}} \delta_{\mathfrak{B}}^{-vm'_{i\mathfrak{B}}} = \eta_i \tag{26}$$

are units in $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively. We evaluate the vectors $l_1(\xi_i)$ and $l_2(\eta_i)$ and hence the vector $l(\xi_i, \eta_i) \in \mathcal{L}(f, g)$ with the use of the vectors $l_1(q_i + c_i g(\alpha))$, $l_1(c\alpha - d)$, $l_1(\gamma_{\mathfrak{A}})$, $l_2(c\beta - d)$, and $l_2(\delta_{\mathfrak{B}})$ taken within $\approx B_1$ binary digits. Therefore, $l(\xi_i, \eta_i)$ is determined with the same accuracy. By the method used in Section 4, we derive the integer relation

$$\sum_{cd} y_{cd} l(\xi_{cd}, \eta_{cd}) + y_i l(\xi_i, \eta_i) = 0, \tag{27}$$

where $l(\xi_i, \eta_i)$ is the vector obtained above and ξ_{cd} and η_{cd} satisfy (11) and (12). This gives the relations

$$\xi_i^{y_i} \prod_{cd} \xi_{cd}^{y_{cd}} = 1 \quad \text{and} \quad \eta_i^{y_i} \prod_{cd} \eta_{cd}^{y_{cd}} = 1. \tag{28}$$

Applying the algorithm given by Theorem 1 to evaluate (27) and determining its complexity requires estimating the Euclidean length of the vector $l(\xi_i, \eta_i)$. In Section 3 we showed that $|l_1(c\alpha - d)| = O(\ln p)$. Similarly, we can show that $|l_1(q_i + c_i g(\alpha))| = O(\ln p)$. Thus (25) and (26) imply that $|l_1(\xi_i)| \le \exp(\approx B_1)$, because $u, v \le \exp(\approx B_1)$. Similarly, $|l_2(\eta_i)| \le \exp(\approx B_1)$; so $|l(\xi_i, \eta_i)| \le \exp(\approx B_1)$.

5.6. Relations (25), (26), and (28) together with (11) and (12) and the observation that $\overline{q_i + c_i g(\alpha)} = q_i$ in F_{p^t} give the following multiplicative relation in the finite field F_{p^t}:

$$q_i^{uvy_i} \prod_{\mathfrak{A}} \overline{\gamma}_{\mathfrak{A}}^{(uy_i l'_{i\mathfrak{A}} + u\sum_{cd} y_{cd} l_{cd\mathfrak{A}})} = \prod_{\mathfrak{B}} \overline{\delta}_{\mathfrak{B}}^{(vy_i m'_{i\mathfrak{B}} + v\sum_{cd} y_{cd} m_{cd\mathfrak{B}})}.$$

Therefore,

$$\begin{aligned}uvy_ix_i + u\sum_{\mathfrak{A}}(y_il'_{i\mathfrak{A}} + \sum_{cd} y_{cd}l_{cd\mathfrak{A}})x_{\mathfrak{A}} \\ = v\sum_{\mathfrak{B}}(y_im'_{i\mathfrak{B}} + \sum_{cd} y_{cd}m_{cd\mathfrak{B}})x_{\mathfrak{B}} (\operatorname{mod} p^t - 1).\end{aligned}$$

5.7. Consider this congruence modulo $p-1$. If $\gcd(uvy_i, p-1) = 1$, then x_i is determined by the $x_{\mathfrak{A}}$ and $x_{\mathfrak{B}}$ values, which have been found in Section 2. Suppose that $\gcd(uvy_i, p-1) = l$. Then we have l alternatives for x_i. For large l we repeat some procedures of our algorithm. Let $e(K_j)$ be the exponent of the class group of K_j for $j = 1, 2$. Then $e(K_1)$ divides v and $e(K_2)$ divides u with a high probability. If $\gcd(e(K_j), p-1)$ is large, then the running time of the algorithm may exceed the expected value, but the probability of this event is small. For example, if $\deg g(x) = 1$ and $|f|$ is small, then $e(K_2) = 1$ and $e(K_1)$ is also small. This happens when $ab^t + c \equiv 0(\operatorname{mod} p)$, $|a|, |b|, |c| = O(1)$ and $t \to \infty$.

6. Runtime analysis

We estimate the running time of the algorithm. The sieving and solution of the sparse linear system by Widemann's algorithm require $\approx L^2 \approx B^2 \approx p^{2/k^2}$ operations. To specify (5) and (6), we must find the characteristic polynomial of an $s_1 \times s_1$ sparse integer matrix, where $s_1 \approx B^{1/2}$. This requires $\approx B^{3/2}$ operations. Determining the $s_1 \times r_1$ matrix Λ_1 by Horner's method and the $(s - s_1) \times r_1$ matrix Λ_2 by (17) requires $\approx B_1^3 = B^{3/2}$ operations. We also have to derive $\approx B$ relations of the form (13) by this author's method (see Section 4). By Theorem 1, this requires no more than $\approx BB_1^{1+\varepsilon} = B^{3/2+\varepsilon/2}$ operations for an arbitrary $\varepsilon > 0$.

Now, we estimate the complexity of the calculations performed in Section 5. The probability of obtaining decomposition (19) or (20) is $\approx \exp(-k \ln k)$. The application of the elliptic curve method requires $\approx \exp((2 \ln p^{1/k} \ln \ln p^{1/k})^{1/2})$ operations [14]. Thus, to construct (19) or (20), we must perform

$$\approx \exp(k \ln k + (2 \ln p^{1/k} \ln \ln p^{1/k})^{1/2})$$

operations. It is easy to see that this value does not exceed $\approx p^{\sigma/k^2}$, where $\sigma = (1 + 2\sqrt{2})/2 = 1.91\cdots$ and $k \leq ((3/2)^{1/3} + o(1))(\ln p/ \ln \ln p)^{1/3}$.

Let us estimate the complexity of the reduction. If $p^{1/m} < q \leq p^{1/k}$ and $m = k^{3/2}$, then the probability of obtaining decompositions (21) and (22) is $\approx \exp(-\frac{k}{2\nu} \ln k)$. The application of the elliptic curve method requires

$$\approx \exp((2 \ln p^{1/k} \ln \ln p^{1/k})^{1/2})$$

operations. Thus, if $1/2 \leq \nu < 1$ the complexity of constructing (21) and (22) does not exceed $\approx p^{\sigma/k^2}$ operations. If $B < q \leq p^{1/m}$, then the probability of obtaining decompositions (21) and (22) is at least $\approx \exp(-\frac{5k}{2\nu} \ln k)$. The application of the elliptic curve method requires

$$\approx \exp((2 \ln p^{1/m} \ln \ln p^{1/m})^{1/2}) \approx p^{o(1/k^2)}$$

operations. Thus, if $\frac{5}{4\sigma} \leq \nu < 1$, the total complexity of the reduction step is at most $\approx p^{\sigma/k^2}$. The number of reduction steps is $\exp(O(\ln \ln^2 p))$. Therefore, we can calculate an individual logarithm in $\approx p^{\sigma/k^2}$ operations. For

$$k = ((3/2)^{1/3} + o(1))(\ln p / \ln\ln p)^{1/3},$$

we have $p^{\sigma/k^2} \approx L_p[\frac{1}{3}; \frac{1+2\sqrt{2}}{(18)^{1/3}}]$; $\frac{1+2\sqrt{2}}{(18)^{1/3}} = 1.4608\cdots$.

7. Some identities for resultants

The following theorems are proved in [9].

For a natural m, let $\Phi_m(x)$ be the mth cyclotomic polynomial over $\mathbb{Q}$. By definition, $\Phi_m(x) = \prod_i (x - \xi_m^i)$ over $i \in [1, m]$ such that $\gcd(i, m) = 1$ and ξ_m is a primitive mth-order root of unity. Let $\Phi_m(x, y)$ be the form of degree $\phi(m)$ corresponding to the polynomial $\Phi_m(x)$ (ϕ is the Euler function).

Theorem 2. *Suppose that m, n, s, and l are positive integers,* $\gcd(m, n) = 1$, *a and b are nonzero integers, $s = s_0 + ls_1$, $\delta = (-1)^l$ if $n = 1$ and $m = 1, 2$, and $\delta = 1$ otherwise. Then the following identity is valid:*

$$\Phi_{mn}(a^s, b) = \delta \operatorname{Res}(\Phi_m(a^{s_0}x^l, b), \Phi_n(x, a^{s_1})).$$

This identity with $m = n = 1$ was applied by many authors to factor integers of the form $a^s - b$. Theorem 2 implies the identity

$$\Phi_{mn}(a) = \delta \operatorname{Res}(\Phi_m(x), \Phi_n(x, a)),$$

where $\gcd(m, n) = 1$ and a is a nonzero integer. This identity can be used for factoring purposes or for calculating discrete logs modulo algebraic factors of $a^{mn} - 1$.

Let a_i and b_j, where $i, j \in [0, 2]$, be integers. Put

$$A = a_2b_1 - a_1b_2, \quad B = a_0b_2 - a_2b_0, \quad C = a_1b_0 - a_0b_1.$$

Theorem 3. *The resultant of the polynomials*

$$f(x) = a_0x^n + a_1x^k + a_2 \quad \text{and} \quad g(x) = b_0x^n + b_1x^k + b_2,$$

where $a_0, b_0 \neq 0$, $1 \leq k < n$, and $\gcd(n, k) = 1$, *equals*

$$\operatorname{Res}(f, g) = (-1)^{(n+1)(k+1)}(B^n - C^{n-k}A^k).$$

This theorem can be used for factoring purposes or for calculating discrete logs modulo integers of the form $B^n - A^k$, where A and B grow as $n \to \infty$.

Theorem 4. *For integers $a_0 \neq 0, a_2$, and b_j, where $j \in [0, n]$ and $b_0 \neq 0$, the resultant of the polynomials*

$$f(x) = a_0x^2 + a_2, \qquad g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$$

equals

$$\begin{aligned}\operatorname{Res}(f, g) = (a_0^m b_n - a_0^{m-1}a_2b_{n-2} + \cdots (-1)^m a_2^m b_0)^2 \\ + a_0a_2(a_0^{m-1}b_{n-1} - a_0^{m-2}a_2b_{n-3} + \cdots (-1)^{m-1}a_2^{m-1}b_1)^2\end{aligned}$$

for $n = 2m$ and

$$\begin{aligned}\operatorname{Res}(f, g) = a_0(a_0^m b_n - a_0^{m-1}a_2b_{n-2} + \cdots (-1)^m a_2^m b_1)^2 \\ + a_2(a_0^m b_{n-1} - a_0^{m-1}a_2b_{n-3} + \cdots (-1)^m a_2^m b_0)^2\end{aligned}$$

for $n = 2m + 1$.

This theorem can be used for factoring purposes or for calculating discrete logs modulo integers close to sums of two squares, i.e., having the form $rA^2 + sB^2$ with small r and s.

References

1. W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, **22** (1976), 644–654. MR **55:**10141
2. T. El Gamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, **31** (1985), 469–472. MR **86j:**94045
3. O. Schirokauer, *Discrete logarithms and local units*, Philosophical Transactions of the Royal Society of London (A), **345** (1993), 409–423. MR **95c:**11156
4. D. Coppersmith, A. M. Odlyzko, and R. Schroeppel, *Discrete logarithms in $GF(p)$*, Algorithmica, **1** (1986), 1–15. MR **87g:**11167
5. D. Gordon, *Discrete logarithms in $GF(p)$ using the number field sieve*, SIAM Journal of Discrete Mathematics, **6** (1993), 124–138. MR **94d:**11104
6. K. McCurley, *The discrete logarithm problem*, Cryptology and computational number theory (C. Pomerance, ed.), Proceedings of Symposia in Applied Mathematics, Amer. Math. Soc., Providence, RI, 1990, vol. 42, pp. 49–74. MR **92d:**11133
7. D. Weber and T. Denny, *The solution of McCurley's discrete log challenge*. Advances in cryptology–CRYPTO '98, Lecture Notes in Computer Science, vol. 1462, Springer-Verlag, Berlin, 1998, pp. 458–471. MR **99i:**94057
8. B. L. van der Waerden, *Algebra* 1, Achte Auflage der Modern Algebra, Springer-Verlag, Berlin, 1971. MR **41:**8186
9. I. A. Semaev, *A generalization of the number field sieve*, Probabilistic methods in Discrete Mathematics (Petrozavodsk, 1996), VSP, Utrecht, 1997, pp. 45–63. MR **99j:**11146
10. M. Elkenbracht-Huising, *A multiple polynomial general number field sieve*, Algorithmic Number Theory, Proceedings of ANTS-2, Lecture Notes in Computer Science, vol. 1122, Springer-Verlag, New York, 1996, pp. 99–114.
11. I. A. Semaev, *Evaluation of linear relations between vectors of a lattice in Euclidean space*, Algorithmic Number Theory, Proceedings of ANTS-3, Lecture Notes in Computer Science, vol. 1423, Springer-Verlag, New York, 1998, pp. 311–323.
12. E. R. Canfield, P. Erdos, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, Journal of Number Theory, **17** (1983), 1–28. MR **85j:**11012
13. D. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Transactions on Information Theory, **32** (1986), 54–62. MR **87g:**11166
14. H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Annals of Mathematics, **126** (1987), 649–673. MR **89g:**11125
15. V. Shoup, *Searching for primitive roots in finite fields*, Mathematics of Computation, **58** (1992), 369–380. MR **92e:**11140

Profsoyuznaya ul. 43, korp. 2, kv. 723, 117420 Moscow, Russia
E-mail address: `semaev@box.ru`