Constructing Nonresidues in Finite Fields and the Extended Riemann Hypothesis

February 1, 1990

Johannes Buchmann	Victor Shoup
Univerität des Saarlandes	University of Toronto
Saarbrücken, Germany	Toronto, Canada

Abstract. We describe a new deterministic algorithm for the problem of constructing k-th power nonresidues in finite fields $\mathrm{GF}(p^n)$, where p is prime and k is a prime divisor of $p^n - 1$. We prove under the assumption of the Extended Riemann Hypothesis (ERH), that for fixed n and $p \to \infty$, our algorithm runs in polynomial time. Unlike previous algorithms for this problem, this polynomial time bound holds even if k is very large. More generally, assuming the ERH, in time $(\log p)^{O(n)}$ we can construct a set of elements that generates $\mathrm{GF}(p^n)^*$.

1 Introduction

Consider the following problem: given a finite field $\mathrm{GF}(p^n)$, where p is prime, and a prime divisor k of $p^n - 1$, construct a k-th power nonresidue in $\mathrm{GF}(p^n)$, i.e. an element that is not a perfect k-th power of any other element in $\mathrm{GF}(p^n)$.

The problem of constructing nonresidues lies at the heart of many deterministic algorithms for fundamental problems in finite fields. For example, the problem of constructing an irreducible polynomial of given degree over a finite field can be reduced in deterministic polynomial time to the problem of constructing nonresidues (see [20]). Furthermore, many deterministic algorithms for various special cases of the problem of factoring polynomials over finite fields can be viewed as deterministic reductions to the problem of constructing nonresidues (see [1, 5, 24, 18, 19, 12]).

We are therefore interested in the deterministic complexity of constructing nonresidues. The problem of *testing* whether a given α in $\mathrm{GF}(p^n)$ is a k-th power nonresidue has a trivial solution: just test if $\alpha^{(p^n-1)/k} \neq 1$. If probabilistic algorithms are allowed, then the problem of constructing nonresidues also has a trivial solution: just choose α in $\mathrm{GF}(p^n)$ at random and test whether it is a k-th power nonresidue. However, the deterministic complexity of constructing nonresidues is currently unknown, even under the assumption of the Extended Riemann Hypothesis (ERH). We shall show that for any *fixed* value of n, this problem can be solved in deterministic polynomial time assuming the ERH.

We prove the following theorem.

(1.1) Theorem *Assume the ERH. There is a deterministic algorithm that takes as input a prime p and positive integer n, and outputs a model of the finite field $GF(p^n)$ together with a subset S of elements in this model with the property that S generates the multiplicative group $GF(p^n)^*$ of nonzero elements. Furthermore, there exist constants c and d such that the algorithm runs in time $(c \log p)^{dn}$.*

Since isomorphisms between finite fields can be computed in deterministic polynomial time (as was proved in [15] without any hypothesis), we can construct a generating set in any given model of $\mathrm{GF}(p^n)$ in time $(\log p)^{O(n)}$ assuming the ERH. Since a generating set always contains a k-th power nonresidue, we can construct nonresidues within the same time bound.

Previous Work

There is a deterministic algorithm that will construct a generating set for $\mathrm{GF}(p^n)^*$ in time $p \cdot n^{O(1)}$ (see [22] and [23]), so for small p the problem of constructing nonresidues can be solved in deterministic polynomial time unconditionally.

Assuming the ERH, the algorithm of Huang [12] as generalized by Evdokimov [11] allows us to deterministically construct a k-th power nonresidue in $\mathrm{GF}(p^n)$ in time $k^A \cdot (n \log p)^{O(1)}$ for some positive constant A, where currently the best-known value for A appears to be at least 2. So for small k the problem of constructing nonresidues can be solved in deterministic polynomial time assuming the ERH.

Ankeny's Theorem [2] as sharpened in [3] states that, assuming the ERH, the set of positive integers less than $2(\log p)^2$ generates $\mathrm{GF}(p)^*$. This result has been generalized to $n = 2$ in [22] where it is shown, assuming the ERH, that in deterministic polynomial time a model $\mathrm{GF}(p)(\alpha)$ of $\mathrm{GF}(p^2)$ can be constructed with the property that the set

$$S = \{a_1 + a_2\alpha : |a_i| = O((\log p)^B)\},$$

for a certain positive constant B, generates $\mathrm{GF}(p^2)^*$. Thus, for $n = 1$ and $n = 2$, the problem of constructing nonresidues in $\mathrm{GF}(p^n)$ can be solved in deterministic polynomial time assuming the ERH.

¿From these results, one might conjecture that assuming the ERH we can efficiently construct a basis $\omega_1, \ldots, \omega_n$ for $\mathrm{GF}(p^n)$ over $\mathrm{GF}(p)$ such that the set

$$S = \{a_1\omega_1 + \cdots + a_n\omega_n : |a_i| = O((\log p)^C)\},$$

for some positive constant C, generates $\mathrm{GF}(p^n)^*$. The truth of such a conjecture would immediately imply our Theorem 1.1 with a very simple algorithm. However, we are currently unable to prove such a conjecture, and the algorithm we describe requires some quite elaborate computations in algebraic number fields.

Furthermore, although with the ERH it is possible for $n = 1$ and $n = 2$ to construct in time $(\log p)^{O(1)}$ a set S that not only generates $\mathrm{GF}(p^n)^*$ but in fact contains a primitive root [25, 22], we are currently unable to prove the analogous result for arbitrary n.

We mention also the recent result of Perel'muter and Shparlinsky [16] which states that for fixed n and for any $\alpha \in \mathrm{GF}(p^n)$ of degree n over $\mathrm{GF}(p)$, there exists $t = O(p^{1/2+\epsilon})$ such that $\alpha + t$ is a primitive root for $\mathrm{GF}(p^n)$. It is natural to ask whether we can take $t = (\log p)^{O(1)}$ assuming ERH. An affirmative answer would certainly improve on the results presented here.

Applications

We mention three applications of our main result. In these applications, n is a *fixed* positive integer, and we assume the ERH.

1. *Taking k-th roots in GF(p^n).* Combining our theorem with the algorithms in [1], [12] and [17], we can take k-th roots in $\mathrm{GF}(p^n)$ in deterministic time $\sqrt{k}$ times a polynomial in the input size.

2. *Factoring polynomials over GF(p).* Combining our theorem with techniques in [21], [5] and [6], we can factor polynomials over $\mathrm{GF}(p)$ in deterministic time $\sqrt{k}$ times a polynomial in the input size, where k is the largest prime dividing $\Phi_n(p)$ and Φ_n is the n-th cyclotomic polynomial.

3. *Constructing primitive roots in GF(p^n).* Our theorem implies that given the prime factorization of $p^n - 1$, we can construct a primitive root for $\mathrm{GF}(p^n)$ in deterministic polynomial time.

Previous to this work, these statements had been proven only for the special cases $n = 1$ and $n = 2$.

2 The Algorithm

For integer q, ζ_q denotes a complex primitive q-th root of unity. If R and S are rings (commutative, and containing 1) such that R is a free S-algebra with a basis $\omega_1, \ldots, \omega_n$, then by a *multiplication table* for this basis we mean a collection of n^3 elements $a_{ij}^k \in S$ such that

$$\omega_i \omega_j = \sum_k a_{ij}^k \omega_k.$$

By a *model* for the finite field $\mathrm{GF}(p^n)$, we shall mean a multiplication table for some basis of $\mathrm{GF}(p^n)$ over $\mathrm{GF}(p)$. This definition of a model for $\mathrm{GF}(p^n)$ is equivalent (up to polynomial time computation) in all respects to the more concrete definition of a model as an irreducible polynomial of degree n (see [15]).

Here is a high level description of our algorithm. The input consists of a prime p and a positive integer n. The output is a model of $\mathrm{GF}(p^n)$ together with a set S in this model that generates $\mathrm{GF}(p^n)^*$.

We will assume that $1 < n < \log p$. We can make this assumption, since if $n = 1$, Ankeny's theorem applies, and if $n \geq \log p$, then $p \leq e^n$, and so the algorithms described in [22, 23] will run in the desired time. In particular, we are assuming that $p \nmid n$. Assuming the ERH, we will show that the algorithm below in general runs in time $(n \log p)^{O(n)}$ whenever $p \nmid n$, which is $(\log p)^{O(n)}$ when $n < \log p$.

(2.1) Algorithm

1. Compute the least prime q such that $q \equiv 1 \pmod{n}$, and p remains prime in the ring $\mathcal{O}$ of integers of the subfield $K \subset \mathbf{Q}(\zeta_q)$ of degree n over $\mathbf{Q}$.

2. Compute a $\mathbf{Z}$-basis for the ring $\mathcal{O}$, along with a corresponding multiplication table. Compute the reduction mod p of the multiplication table. This gives a multiplication table for $\mathcal{O}/p\mathcal{O}$ over $\mathbf{Z}/p\mathbf{Z}$ which serves as our model for $\mathrm{GF}(p^n)$.

3. Compute a set $S_0 \subset \mathcal{O}/p\mathcal{O}$ that contains the reduction mod p of a set of generators of the multiplicative group $\mathcal{O}^*$ of units in $\mathcal{O}$.

4. Let
$$B = C_1 \cdot \left[\Delta^{1/2}(\log \Delta)^{n-1}(\log \Delta + n \log p)\right]^2,$$
where $\Delta = q^{n-1}$ and C_1 is an absolute, effectively computable constant described below. Compute a set $S_1 \subset \mathcal{O}/p\mathcal{O}$ such that for each prime $r \leq B$, S_1 contains the reduction mod p of a full set of pairwise nonassociate elements in $\mathcal{O}$ whose norm in absolute value is r.

5. Put $S = S_0 \cup S_1$. This is a generating set for $(\mathcal{O}/p\mathcal{O})^*$.

In [4], it is shown that the least q satisfying the condition in Step 1 is bounded by $O(n^4(\log(np))^2)$, assuming the ERH. Furthermore, this condition can easily be checked in time $(n \cdot \log q \cdot \log p)^{O(1)}$.

Once q has been determined in Step 1, for computational purposes it is probably best to use the normal basis $\zeta_q, \ldots, \zeta_q^{q-1}$ for the field extension $\mathbf{Q}(\zeta_q)/\mathbf{Q}$. Then we can easily compute the element $\eta = T_{\mathbf{Q}(\zeta_q)/K}(\zeta_q)$ in time $q^{O(1)}$ which has the property that $K = \mathbf{Q}(\eta)$. Moreover, in Step 2 of our algorithm, the set consisting of the elements η^σ for $\sigma \in G(K/\mathbf{Q})$ is a $\mathbf{Z}$-basis for $\mathcal{O}$. The entries in the corresponding multiplication table are rational integers bounded by $q^{O(1)}$ in absolute value. This basis and multiplication table can be easily computed in time $q^{O(1)}$. ¿From the conductor/discriminant formula, one sees that $\Delta = q^{n-1}$ is the absolute value of the discriminant of K.

The details of implementing Steps 3 and 4 are given in the following section.

To show that the set S constructed by our algorithm is indeed a generating set, we will make use of the following analog of Ankeny's theorem for number fields.

(2.2) Theorem *Assume ERH. Let K be an arbitrary number field with ring of integers $\mathcal{O}$, class number h, and discriminant of absolute value Δ. Let M be and arbitrary proper ideal in $\mathcal{O}$, and $\alpha \mapsto \overline{\alpha}$ be the natural map from $\mathcal{O}$ to $\mathcal{O}/M$. The group $(\mathcal{O}/M)^*$ is generated by the set of all $\overline{\alpha}$ with $\alpha \in \mathcal{O}$ prime to M such that the norm of α in absolute value is 1 or is a prime $\leq C_2(h \log(\Delta N(M)))^2$. Here, C_2 is an absolute, effectively computable constant.*

Proof. We will make use of the ray class group mod M (in the wide sense) and the associated group of Dirichlet characters.

Let A and B be ideals in $\mathcal{O}$ prime to M. We say that $A \sim B \pmod M$ if there exist $\alpha, \beta \in \mathcal{O}$ such that $\alpha A = \beta B$ and $\alpha \equiv \beta \equiv 1 \pmod M$. The relation $\sim$ is an equivalence relation and the set $\mathcal{K}$ of equivalence classes forms a finite abelian group called the ray class group mod M. Denote by $\mathcal{K}_1$ be the subgroup of $\mathcal{K}$ consisting of those equivalence classes containing principal ideals. It is known that $[\mathcal{K} : \mathcal{K}_1] = h$.

Let G be the multiplicative group $(\mathcal{O}/M)^*$, and let $H = \overline{\mathcal{O}^*}$, which is a subgroup of G. Consider the map $\rho : \mathcal{K}_1 \to G/H$ defined by $\rho([\alpha\mathcal{O}]) = \overline{\alpha}H$. One can easily establish that the map ρ is well-defined, and is in fact a group isomorphism. It follows that if we have set $T \subset \mathcal{O}$ such that the set $\{[\alpha\mathcal{O}] : \alpha \in T\}$ generates $\mathcal{K}_1$, then $\overline{\mathcal{O}^*} \cup \overline{T}$ generates G. It will thus suffice to show that the set of all first degree principal prime ideals whose norm does not exceed the stated bound generates $\mathcal{K}_1$.

A character on the group $\mathcal{K}$ is called a Dirichlet character mod M. It is convenient to view such a character χ as a function on the ideals of $\mathcal{O}$, defining $\chi(A)$ to be zero when A is not prime to M. The collection of characters on $\mathcal{K}$ forms a group with $\#\mathcal{K}$ elements.

We shall make use of the character sum estimates derived in [14]. Let $\hat{k}(u; x, y)$ be the inverse Mellin transform given in (2.1) of [14]. $\hat{k}$ is defined for $y > x > 1$ and $u > 0$; it is positive when $x^2 < u < y^2$, and zero otherwise. We will fix a value of x (determined below), and set $y = ex$. For prime ideal P, let $w(P) = \log N(P) N(P)^{-1} \hat{k}(N(P); x, y)$. Finally, let $I(\chi) = \sum_P \chi(P) w(P)$, where the sum extends over all first degree prime ideals whose norm is between x^2 and y^2.

The following character sum estimates can be easily extracted from the proof of Theorem 1.2 in [14]. Assuming the ERH, we have

$$I(\chi) = \begin{cases} 1 + O(x^{-1}\log(\Delta N(M))) & \text{if } \chi \text{ is trivial,} \\ O(x^{-1}\log(\Delta N(M))) & \text{otherwise.} \end{cases}$$

The implied constants are absolute and effectively computable.

For a subgroup $\mathcal{H}$ of $\mathcal{K}$, let $S(\mathcal{H}) = \sum_{[P]\in\mathcal{H}} w(P)$ where the sum is over all first degree prime ideals P such that $x^2 < N(P) < y^2$, $(P, M) = 1$, and $[P] \in \mathcal{H}$.

We have

$$\sum_{\chi(\mathcal{H})=1} \chi(A) = \begin{cases} [\mathcal{K} : \mathcal{H}] & \text{if } A \in \mathcal{H}, \\ 0 & \text{otherwise,} \end{cases}$$

where the sum extends over the $[\mathcal{K} : \mathcal{H}]$ characters that are trivial on $\mathcal{H}$. Assuming the ERH, it follows that

$$\begin{aligned} S(\mathcal{H}) &= \frac{1}{[\mathcal{K} : \mathcal{H}]} \sum_P w(P) \sum_{\chi(\mathcal{H})=1} \chi(P) \\ &= \frac{1}{[\mathcal{K} : \mathcal{H}]} \sum_{\chi(\mathcal{H})=1} I(\chi) \\ &= \frac{1}{[\mathcal{K} : \mathcal{H}]} + O(x^{-1}\log(\Delta N(M))) \end{aligned}$$

Now suppose that $\mathcal{H}$ is a subgroup of index $d > 1$ in $\mathcal{K}_1$. Then we have

$$\begin{aligned} S(\mathcal{K}_1) - S(\mathcal{H}) &= \frac{d-1}{dh} + O(x^{-1}\log(\Delta N(M))) \\ &\geq \frac{1}{2h} + O(x^{-1}\log(\Delta N(M))). \end{aligned}$$

Therefore, for an appropriately chosen absolute constant C, if we take $x = Ch\log(\Delta N(M))$, this last quantity will be positive, implying the existence of a first degree prime ideal of norm $< y^2$ that lies in $\mathcal{K}_1$ but not in $\mathcal{H}$. Since this holds for any proper subgroup $\mathcal{H}$ of $\mathcal{K}_1$, the theorem is proved. $\square$

¿From Siegel's theorem, $h = O(\Delta^{1/2}(\log \Delta)^{n-1})$, where the implied constant is absolute and effectively computable. It is then clear that there exists an absolute, effectively computable constant C_1 such that with B defined as in Step 4 of Algorithm 2.1, the set S constructed by that algorithm is a generating set for $(\mathcal{O}/p\mathcal{O})^*$.

We should point out that there is no need to explicitly compute the bound B in Step 4 if we are just looking for a k-th power nonresidue for a given k. In this case, only the running time, and not the correctness, of our algorithm depends on the ERH.

3 Constructing Units and Principal Ideals

In this section, we consider the following general situation. We are given an algebraic number field K of of degree n and absolute discriminant Δ. The field is given in terms of the multiplication table for some $\mathbf{Z}$-basis $\omega_1, \ldots, \omega_n$ of the ring of integers $\mathcal{O}$. The entries in the multiplication table are bounded by $(n\Delta)^{O(n)}$. We are also given a prime number p that is inert in K and a bound $B > 0$. Those data are input for all the algorithms described here.

We want to solve the following problems.

1. Find $\mathbf{Z}$-bases for all the degree one prime ideals of norm $\leq B$.

2. Find a generating system mod p for the group of units, i.e. for some system of generators $\varepsilon_1, \ldots, \varepsilon_k$ with representation $\varepsilon_j = \sum_i e_{ij}\omega_i$, we want the values e_{ij} mod p.

3. Find generators mod p for all the ideals found in the first step that are principal, i.e. if α is such a generator with $\alpha = \sum_i a_i\omega_i$, we want the values a_i mod p.

The first problem can be solved by means of linear algebra and polynomial factorization algorithms over finite fields in time $B^{3/2}(n \log B \log \Delta)^{O(1)}$ (see [9]).

The last two problems can be solved by means of the generalized reduction theory that was introduced in [7], [8] and [10]. In those papers algorithms for solving those problems were presented and analyzed for fixed degree n of K. In our context it is, however, necessary to make the dependence of the running time on n explicit. Extending the results that were previously known we are able to prove the following statement:

(3.1) Theorem *Problems (2) and (3) can be solved in time*

$$(n \log \Delta)^{O(n)}(\log p)^{O(1)}(\Delta^{1/2} + B).$$

In the remainder of this section we sketch a proof of this theorem. First, we briefly review the main results from the generalized reduction theory.

For $1 \leq i \leq n$, let $\alpha \mapsto \alpha^{(i)}$ be the i-th embedding of K into $\mathbf{C}$. We assume that the first r embeddings are real, and that the remaining $2s$ embeddings are complex with the i-th and $(i+s)$-th embedding being conjugate for $r+1 \leq i \leq r+s$. Thus, $n = r+2s$. The *Minkowski map* sends α in K to $\underline{\alpha} = (\alpha^{(1)}, \ldots, \alpha^{(r)}, \Re\alpha^{(r+1)}, \Im\alpha^{(r+1)}, \ldots, \Re\alpha^{(r+s)}, \Im\alpha^{(r+s)})$ in $\mathbf{R}^n$.

A fractional ideal A of K is called reduced if $1 \in A$ and there are no nonzero $\alpha \in A$ with $|\alpha^{(i)}| < 1$ for $1 \leq i \leq n$. Let A and A' be two ideals belonging to the same ideal class, so that we can write $A' = (1/\alpha)A$ with $\alpha \in A$ (since $1 \in A'$). These two reduced ideals are called *neighbors* if there are no nonzero $\beta \in A$ with $|\beta^{(i)}| < \max\{1, |\alpha^{(i)}|\}$ for $1 \leq i \leq n$. It was shown in [7] that in the graph corresponding to this neighbor relation, there is a path connecting two reduced ideals if and only if they belong to the same ideal class.

Suppose we perform a depth-first search of all vertices in this graph reachable from the vertex $\mathcal{O}$, which we take as the start vertex. This procedure will partition the edges in this connected component of the graph into *tree edges* and *back edges* in the usual way. Suppose also that an edge from A to A' with $A' = (1/\alpha)A$ is labeled with the number α.

A generating system for the units is found as follows. If we have a labeled path

$$A_0 \overset{\alpha_1}{\rightarrow} A_1 \overset{\alpha_2}{\rightarrow} \cdots \overset{\alpha_k}{\rightarrow} A_k \overset{\alpha_{k+1}}{\rightarrow} A_0,$$

where the first k edges are tree edges and the last one is a back edge, it follows that $A_0 = (\alpha_1 \cdots \alpha_{k+1})A_0$, and hence $\alpha_1 \cdots \alpha_{k+1}$ is a unit. It can be shown that all such so-called *boundary units* generate the group of units in $\mathcal{O}$.

Testing if a given ideal A is principal, and finding a generator if it is, can be be done as follows. If $\alpha \in A$ is such that $\underline{\alpha}$ is a shortest non-zero vector in the corresponding lattice $\underline{A}$, then $A' = (1/\alpha)A$ is reduced. If A is principal then A' is reduced and principal, and so A' must be one of the vertices in the depth-first search tree. If β is the product of the numbers labeling the edges on the path in the tree from $\mathcal{O}$ to A', then $A' = (1/\beta)\mathcal{O}$ and hence $A = (\alpha/\beta)\mathcal{O}$.

The preceding paragraphs describe in broad terms the algorithm for solving problems (2) and (3). We now consider the implementation and complexity of this algorithm.

It is known that the number of reduced principal ideals in K is $(n \log \Delta)^{O(n)}\Delta^{1/2}$ and the number of neighbors of any of each reduced ideal is $(n \log \Delta)^{O(n)}$ [8]. Moreover, the determination of all neighbors of a reduced ideal A can be affected by solving $(n \log \Delta)^{O(n)}$ integer programming problems in the lattice $\underline{A}$. Those integer programming problems consist of deciding whether for some numbers $\alpha_1, \ldots, \alpha_n \in A$ there exists a nonzero $\alpha \in A$ with $|\alpha^{(i)}| < |\alpha_i^{(i)}|$ for $1 \leq i \leq n$. In all those problems we have $\alpha_i^{(i)} = (n\Delta)^{O(n)}$. Therefore we have $\left||\beta^{(i)}| - |\gamma^{(i)}|\right| = 1/(n\Delta)^{O(n)}$ for $1 \leq i \leq n$ and for any two numbers $\beta, \gamma \in A$ that occur in the computation. The integer programming problems can thus be transformed into equivalent problems in n-dimensional integer lattices which can be represented by $(n \log \Delta)^{O(1)}$ bits. By a theorem of Kannan [13] each of those problems can be solved in time $n^{O(n)}(\log \Delta)^{O(1)}$. Hence the computation of all neighbors of A takes time $(n \log \Delta)^{O(n)}$.

In the depth-first search tree, each reduced principal ideal is represented in terms of the uniquely defined $n \times n$ integer transformation matrix in Hermite normal form with respect to the integral basis. Those matrices are of binary length $(n \log \Delta)^{O(1)}$. They are stored in a balanced tree so that searching for a given reduced ideal among those already found can be done quickly. Hence, the computation of all neighbors can be done in time $(n \log \Delta)^{O(n)}$.

Along with each reduced ideal A, we want to store the product β of the numbers α labeling the edges from the root to this ideal. Although individually each such α can be represented using $(n \log \Delta)^{O(1)}$ bits, their product will not in general have such a small representation. We can avoid this problem by passing directly to the field $\mathcal{O}/p\mathcal{O}$: writing $\beta = p^e\gamma$, where $e \in \mathbf{Z}$ and γ prime to p, we only need to store the reduction modulo p of γ. We will denote this quantity by γ_A.

As we are performing the depth-first search, we can construct the mod p reductions of the boundary units as we discover back edges. If $A \overset{\alpha}{\rightarrow} A'$ is a back-edge, then we compute the mod p reduction of the corresponding boundary unit as $\delta\gamma_A/\gamma_{A'}$, where δ is the mod p reduction of the part of α that is prime to p.

Putting all of this together, the computation of all reduced principal ideals in K along with the mod p reductions of the boundary units takes time

$$(n \log \Delta)^{O(n)} \Delta^{1/2} (\log p)^{O(1)}.$$

One we have computed all of the above information, along with $\mathbf{Z}$-bases for those degree one prime ideals of norm bounded by B, we can easily test each of these ideals for principality and find generators using the method outlined earlier. For each such ideal A, we need to find a shortest vector in $\underline{A}$. Using arguments similar to those above and applying Kannan's algorithm, this takes time $(n \log \Delta)^{O(n)}$. We obtain in this way a reduced ideal $A' = (1/\alpha)A$. We can quickly search for A' among the reduced principal ideals, and if it is found, we also find a generator for A', and hence for A itself.

We conclude that generators mod p for all principal degree one prime ideals of norm below B can be found in time

$$(n \log \Delta)^{O(n)} (\log p)^{O(1)} B$$

once problems (1) and (2) have been solved.

References

[1] L. M. Adleman, K. Manders, and G. L. Miller. On taking roots in finite fields. In *18th Annual Symposium on Foundations of Computer Science*, pages 175–178, 1977.

[2] N. C. Ankeny. The least quadratic nonresidue. *Ann. of Math.*, 55:65–72, 1952.

[3] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55:355–380, 1990.

[4] E. Bach and J. Shallit. Factoring with cyclotomic polynomials. *Math. Comp.*, 52(185):201–219, 1989.

[5] E. Bach and J. von zur Gathen. Deterministic factorization of polynomials over special finite fields. Technical Report 799, Computer Sciences Department, University of Wisconsin–Madison, 1988.

[6] E. Bach, J. von zur Gathen, and H. W. Lenstra. Preprint, 1989.

[7] J. Buchmann. On the computation of units and class numbers by a generalization of Lagrange's algorithm. *J. Number Theory*, 26:8–30, 1987.

[8] J. Buchmann. On the period length of the generalized Lagrange algorithm. *J. Number Theory*, 26:31–37, 1987.

[9] J. Buchmann and H. W. Lenstra. Computing maximal orders and decomposing primes in number fields. Preprint.

[10] J. Buchmann and H. C. Williams. On principal ideal testing in algebraic number fields. *J. Symbolic Computation*, 4:11–19, 1987.

[11] S. A. Evdokimov. Factoring a solvable polynomial over a finite field and Generalized Riemann Hypothesis. *Zapiski Nauchn. Semin. Leningr. Otdel. Matem. Inst. Acad. Sci. USSR*, 176:104–117, 1989. In Russian.

[12] M. A. Huang. Riemann hypothesis and finding roots over finite fields. In *17th Annual ACM Symposium on Theory of Computing*, pages 121–130, 1985.

[13] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *15th Annual ACM Symposium on Theory of Computing*, pages 193–206, 1983.

[14] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Inv. math.*, 54:271–296, 1979.

[15] H. W. Lenstra. Finding isomorphisms between finite fields. *Math. Comp.*, 56, 1991. To appear.

[16] G. I. Perel'muter and I. E. Shparlinsky. On the distribution of primitive roots in finite fields. *Uspechi Matem. Nauk*, 45:185–186, 1990. In Russian.

[17] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Trans. Inf. Theory*, 24:106–110, 1978.

[18] L. Rónyai. Factoring polynomials over finite fields. *J. Algorithms*, 9:391–400, 1988.

[19] L. Rónyai. Galois groups and factoring polynomials over finite fields. In *30th Annual Symposium on Foundations of Computer Science*, pages 99–104, 1989.

[20] V. Shoup. Removing randomness from computational number theory (phd thesis). Technical Report 865, Computer Sciences Department, University of Wisconsin–Madison, 1989.

[21] V. Shoup. A theorem on factoring polynomials over finite fields. Technical Report 866, Computer Sciences Department, University of Wisconsin–Madison, 1989. To appear in *Inform. Process. Lett.* as "Smoothness and factoring polynomials over finite fields".

[22] V. Shoup. Searching for primitive roots in finite fields. In *22nd Annual ACM Symposium on Theory of Computing*, pages 546–554, 1990. To appear, *Math. Comp.*

[23] S. A. Stepanov and I. E. Shparlinskiy. On construction of primitive elements and primitive normal bases for finite fields. In *Proc. Colloq. on Comp. Number Theory*, Hungary, 1990.

[24] J. von zur Gathen. Factoring polynomials and primitive elements for special primes. *Theoret. Comput. Sci.*, 52:77–89, 1987.

[25] Y. Wang. On the least primitive root of a prime. *Scientia Sinica*, 10(1):1–14, 1961.