MATHEMATICS OF COMPUTATION
Volume 71, Number 239, Pages 1219–1230
S 0025-5718(01)01352-7
Article electronically published on October 4, 2001

SMOOTH IDEALS IN HYPERELLIPTIC FUNCTION FIELDS

ANDREAS ENGE AND ANDREAS STEIN

ABSTRACT. Recently, several algorithms have been suggested for solving the discrete logarithm problem in the Jacobians of high-genus hyperelliptic curves over finite fields. Some of them have a provable subexponential running time and are using the fact that smooth reduced ideals are sufficiently dense. We explicitly show how these density results can be derived. All proofs are purely combinatorial and do not exploit analytic properties of generating functions.

1. MOTIVATION

The security of the key distribution protocol presented in [DH76] is based on the discrete logarithm problem in the multiplicative group of a finite prime field. This problem can be solved by index calculus methods which create a data base from randomly chosen field elements. Whenever such a field element is smooth, i.e., given as a product of "small" elements, it is added to the data base, and once enough data is collected, the discrete logarithm problem is solved by linear algebra. Elements of the finite fields most popular for implementations, namely, prime fields and fields of characteristic 2, can be represented by integers, respectively univariate polynomials, over $\mathbb{F}_2$. Consequently, the distribution of smooth numbers and polynomials has received considerable attention in the literature, and it could be shown that the discrete logarithm problem in the corresponding finite fields can be solved in subexponential time. Similar attacks exist for the factorization problem, which underlies the commercially most employed public key cryptosystem, described in [RSA78]. We see that *smoothness* of integers and polynomials is an essential concept in cryptography.

To avoid subexponential algorithms it has been suggested to base cryptosystems on the discrete logarithm problem in abelian varieties over finite fields. Specifically, cryptosystems based on the arithmetic in the Jacobians of elliptic and hyperelliptic curves are investigated in the literature (see [Kob87, Mil86] and [Kob89, SSW96]). However, in [ADH94] the authors present an attack which is similar in structure to the algorithm for finite fields and conjecture a subexponential running time for Jacobians of high genus hyperelliptic curves. Hereby, they assume that the ideal class group of the hyperelliptic curve is generated by a subexponential number of prime ideals of small degree. Furthermore, the success of the algorithm depends on the distribution of smooth principal divisors and appears difficult to analyze rigorously. The attack in [ADH94] is formulated for curves over finite prime fields;

Received by the editor January 30, 2000 and, in revised form, October 3, 2000.
2000 *Mathematics Subject Classification.* Primary 11R58, 11Y16, 11R44, 14H40, 68Q25.
Key words and phrases. Distribution of prime ideals, smooth ideal, hyperelliptic function field, subexponential algorithm.

a generalization to arbitrary finite fields is provided by [Bau98]. In [MST99], a provable subexponential method for high-genus hyperelliptic curves defined over fields of odd characteristic is described. In particular, the authors show that the ideal class group of such hyperelliptic curves is generated by the prime ideals of degree at most $\lceil 2\log_q(4g-2)\rceil$ where q denotes the size of the finite field and g the genus of the hyperelliptic curve. These results are generalized to hyperelliptic curves over arbitrary finite fields in [Eng99], and a different algorithm with better running time under reasonable assumptions is described in [EG00]. The algorithms have a provable subexponential running time for hyperelliptic curves of large genus and use the fact that smooth reduced ideals are sufficiently dense. In this contribution, we explicitly show how these density results can be derived. Specifically, we provide effective lower bounds on the number of smooth semireduced divisors as needed in the subexponential methods in [MST99, Eng99, EG00]. All proofs are purely combinatorial and do not exploit analytic properties of generating functions.

We now proceed as follows. In Section 2, we introduce the basic terminology of hyperelliptic function fields and discuss the splitting behavior of prime ideals. In Section 3 we derive bounds on the number of splitting prime polynomials of fixed degree which are essential for the rest of the paper. Section 4 is devoted to the effective lower bounds on the number of smooth semireduced divisors. The influence of these bounds on the subexponential algorithms in [MST99, Eng99, EG00] is discussed in Section 5.

2. Hyperelliptic function fields

Let $K = \mathbb{F}_q$ be the finite field with q elements. Suppose that

$$H = Y^2 + hY - f \in K[X, Y]$$

with $h \in K[X]$ of degree at most g and $f \in K[X]$ monic of degree $2g+1$ or $2g+2$ is irreducible. If the affine curve corresponding to H has no singularities, then its smooth projective model is called a *hyperelliptic curve* of genus g.

The ring of polynomial functions on H, the *coordinate ring* of H, is given by $K[H] := K[X,Y]/(H)$; its *function field* $K(H)$, which is defined as the field of fractions of $K[H]$, is a quadratic extension of $K(X)$. $K[H]$ is the integral closure of $K[X]$ in $K(H)$.

The prime ideals of $K[X]$ are exactly those prime ideals $\mathfrak{p}$ which are generated by a monic irreducible polynomial p. If $\mathfrak{P}$ is a prime ideal of $K[H]$ above $\mathfrak{p}$, then its degree is defined by

$$\deg \mathfrak{P} = [K[H]/\mathfrak{P} : K[X]/\mathfrak{p}] = \left[K[H]/\mathfrak{P} : \mathbb{F}_{q^{\deg p}}\right].$$

Three cases can be distinguished (cf. [Art24]):

1. $Y^2 + hY - f \equiv 0 \pmod{p}$ has two solutions b and $-b-h$ in $K[X]/\mathfrak{p}$. Then there are two prime ideals in $K[H]$ which lie over $\mathfrak{p}$, given by $\mathfrak{P} = (p, b-Y)$ and $\overline{\mathfrak{P}} = (p, -b-h-Y)$, so that $\mathfrak{p}K[H] = \mathfrak{P}\overline{\mathfrak{P}}$. Their degrees are $\deg p$, and p, $\mathfrak{p}$, $\mathfrak{P}$ and $\overline{\mathfrak{P}}$ are called *splitting*.
2. There is one (double) solution b to the equation in $K[X]/\mathfrak{p}$, corresponding to a unique prime ideal $\mathfrak{P} = (p, b-Y)$ over $\mathfrak{p}$, so that $\mathfrak{p}K[H] = \mathfrak{P}^2$. The degree of $\mathfrak{P}$ is $\deg p$, and p, $\mathfrak{p}$ and $\mathfrak{P}$ are called *ramified*.
3. There is no solution to the congruence in $K[X]/\mathfrak{p}$, and $\mathfrak{P} = \mathfrak{p}K[H]$ is the only prime ideal above $\mathfrak{p}$ in $K[H]$. The degree of $\mathfrak{P}$ is $2\deg p$, and p, $\mathfrak{p}$ and $\mathfrak{P}$ are called *inert*.

Let $\mathfrak{A}$ be an ideal of $K[H]$. Then $\mathfrak{A}$ admits a unique decomposition into finitely many prime ideals

$$\mathfrak{A} = \prod_i \mathfrak{P}_i^{e_i}.$$

If $\mathfrak{A}$ is *primitive* or *semireduced*, i.e., has no principal factor, then we clearly have the following properties:

1. None of the $\mathfrak{P}_i$'s is inert, since inert prime ideals are principal.
2. If $\mathfrak{P}_i$ is splitting, then $\overline{\mathfrak{P}_i}$ does not occur in the factorization since $\mathfrak{P}_i\overline{\mathfrak{P}_i} = (p_i)$ is principal.
3. If $\mathfrak{P}_i$ is ramified, then $e_i = 1$, since $\mathfrak{P}_i^2 = (p_i)$ is principal.

The uniqueness of the prime ideal decomposition yields that these conditions are not only necessary, but also sufficient.

We define $\deg \mathfrak{A}$ by $\sum_i e_i \deg \mathfrak{P}_i$. A semireduced ideal is called *reduced* if its degree is at most g. Any semireduced ideal can be uniquely represented in the form $\mathfrak{A} = (a, b - Y)$ with a, $b \in K[X]$, a monic, $\deg b < \deg a$ and $a \mid b^2 + hb - f$. The decomposition of $\mathfrak{A}$ into prime ideals can be determined as follows: Write $a = \prod_i p_i^{e_i}$ with monic irreducible polynomials p_i. Then none of the p_i's is inert since b is a solution of H modulo p_i. Let $b \equiv b_i \pmod{p_i}$ with $\deg b_i < \deg p_i$, and $\mathfrak{P}_i = (p_i, b_i - Y)$. Then $\mathfrak{A} = \prod_i \mathfrak{P}_i^{e_i}$. Furthermore, $\deg \mathfrak{A} = \sum_i e_i \deg \mathfrak{P}_i = \sum_i e_i \deg p_i = \deg a$.

The ideal theory presented above describes the affine part of the hyperelliptic curve: Each prime ideal of $K[H]$ corresponds to a closed affine point on H and gives rise to a valuation on $K(H)$. Depending on the splitting behavior of the "infinite" valuation on $K[X]$, given by the negative degree, we distinguish two cases: The infinite valuation may be splitting, i.e., the hyperelliptic curve has two distinct points at infinity, or it may be ramified, i.e., the curve has a double point at infinity. In the first case, we call the curve *real quadratic*, in the second case, *imaginary quadratic*. Here and in the sequel, we omit the case that the infinite place is inert, since in this case a constant field extension of $K(H)$ of degree 2 leads to a real quadratic curve.

As nicely described in [PR99] (see also [Ste97, Zuc98]), there exists a one-to-one correspondence between elements of the Jacobian variety and reduced ideals in the imaginary case. Thus, the result on Jacobian elements required in [Eng99] and [EG00] can as well be formulated in terms of reduced ideals. The smoothness result needed in [MST99] already concerns reduced ideals.

Thus, we treat in this paper the number of semireduced ideals of degree n all of whose prime factors have degree at most m. Such ideals are called *m-smooth*. Of special interest is the case $n = g$, corresponding to the biggest portion of the m-smooth reduced ideals.

3. Prime ideal densities

The question how many reduced ideals of degree n are m-smooth is basically combinatorial: Given a certain set of *components* (prime ideals) of size at most m, how many objects (ideals) of size n can be composed from them with respect to certain additional constraints (properties 1) to 3) of Section 2)? Of course, a crucial point is to determine the number of components of a given size, a problem we address in this section.

In our context, we are interested in the number of splitting or ramified prime ideals of given degree, which is intimately related to the number of points on the curve with coordinates in extension fields of $\mathbb{F}_q$.

Let $\pi_+(k)$, $\pi_0(k)$ and $\pi_-(k)$ denote the number of monic splitting, ramified and inert irreducible polynomials of degree k, respectively, $\pi(k) = \pi_+(k)+\pi_0(k)+\pi_-(k)$ and $\Pi_+(k) = \sum_{i=1}^{k} \pi_+(i)$. Each splitting or ramified prime ideal $\mathfrak{P} = (p, b - Y)$ of degree k gives rise to k points on the curve whose coordinates lie in $\mathbb{F}_{q^k}$, but in no subfield of $\mathbb{F}_{q^k}$. Namely, if $x_1, \ldots, x_k$ are the distinct roots of p in $\mathbb{F}_{q^k}$, then these points are given by $(x_1, b(x_1)), \ldots, (x_k, b(x_k))$. If $\mathfrak{P} = (p)$ is inert of degree k, then k is even and p of degree $k/2$. Let $x \in \mathbb{F}_{q^{k/2}}$ be a root of p. As p is inert, the equation $Y^2 + h(x)Y - f(x) = 0$ does not have a solution in $\mathbb{F}_{q^{k/2}}$, but two distinct solutions y, $\overline{y} \in \mathbb{F}_{q^k}$, and (x, y) and $(x, \overline{y})$ are two points on H. Thus, $\mathfrak{P}$ corresponds to k points on the curve which are defined over $\mathbb{F}_{q^k}$, but over no subfield. By convention, let $\pi_-(i) = 0$ for half integral, but not integral i. In addition to these finite points, we have to take into account η points on the smooth projective model resulting from the resolution of the singularity of H at infinity. We have $\eta = 1$ for imaginary and $\eta = 2$ for real curves, and these additional points are rational over $\mathbb{F}_q$. Thus, the total number of points on the smooth projective model of H with coordinates in $\mathbb{F}_{q^k}$ is given by

$$N_k = \sum_{i \mid k} \left(2i\pi_+(i) + i\pi_0(i) + i\pi_- \left(\frac{i}{2} \right) \right) + \eta. \tag{1}$$

We remark here that we can also derive this formula in the notation of [Sti93]. Namely, (1) corresponds to [Sti93, (2.23), p. 178], i.e., $N_k = \sum_{i=1}^{k} iB(k)$, where B_k denotes the number of prime divisors of degree k. Since there exists a one-to-one correspondence between finite prime divisors and prime ideals, we know that B_k is equal to the number of prime ideals of degree k if $k > 1$. The number of prime ideals of degree 1 is given by $B(1) - \eta$, where η is 1 or 2, respectively, depending on whether $K(H)$ is imaginary or real. By the above-mentioned results in [Art24] on how irreducible polynomials split in $K(H)$, we can proceed as in [SW99, p. 126] to obtain that

$$B(k) = 2\pi_+(i) + \pi_0(i) + \pi_-(i/2)$$

if $k > 1$, and $B(1) = 2\pi_+(1) + \pi_0(1) + \eta$.

On the other hand, Weil's theorem gives a good approximation of the number N_k.

Theorem 1 (Weil). *The number N_k lies in the interval*

$$\left[q^k - 2gq^{k/2} + 1, q^k + 2gq^{k/2} + 1 \right].$$

We obtain the following result:

Theorem 2. *The number of monic splitting irreducible polynomials of degree at most k is given by $\Pi_+(k)$ with*

$$\Pi_+(k) \geq \frac{1}{2k} \left(q^k - (2g+2)q^{k/2} - (2g+3) \right).$$

If $0 < \varepsilon \le \frac{1}{4}$ *and* $k \ge \frac{1}{\varepsilon}\log_q(2g+6+\sqrt{2})$, *then furthermore*

$$\frac{1}{2k}\left(q^k - q^{k(\frac{1}{2}+\varepsilon)}\right) \le \pi_+(k) \le \frac{1}{2k}\left(q^k + q^{k(\frac{1}{2}+\varepsilon)}\right).$$

Proof. Weil's Theorem and (1) imply

$$q^k - 2gq^{k/2} - \sum_{i=1}^{\infty} i\pi_0(i) - \sum_{i\,|\,k} i\pi_-\left(\frac{i}{2}\right) - 1 \le \sum_{i\,|\,k} 2i\pi_+(i) \le q^k + 2gq^{k/2}.$$

As $\sum_{i=1}^{\infty} i\pi_0(i)$ is the summed up degree of all ramified prime polynomials and a prime polynomial is ramified if and only if it divides the discriminant h^2+4f of H, which has degree at most $2(g+1)$, we have $\sum_{i=1}^{\infty} i\pi_0(i) \le 2(g+1)$. If k is odd, then $\sum_{i\,|\,k} i\pi_-\left(\frac{i}{2}\right)$ is zero; otherwise it is

$$\sum_{i\,|\,\frac{k}{2}} 2i\pi_-(i) \le 2\sum_{i\,|\,\frac{k}{2}} i\pi(i) = 2q^{k/2}.$$

This shows that

$$q^k - (2g+2)q^{k/2} - (2g+3) \le \sum_{i\,|\,k} 2i\pi_+(i) \le q^k + 2gq^{k/2}. \tag{2}$$

Taking into account that

$$\Pi_+(k) = \sum_{i=1}^{k} \pi_+(i) \ge \frac{1}{2k}\sum_{i\,|\,k} 2i\pi_+(i),$$

the first assertion is proved.

With $g(k) = \sum_{i\,|\,k} 2i\pi_+(i)$, Möbius inversion implies $2k\pi_+(k) = \sum_{i\,|\,k} \mu(k/i)g(i)$, where the Möbius function μ takes values in $\{0, \pm 1\}$ and $\mu(1) = 1$. Hence for $k \ge \frac{1}{\varepsilon}\log_q(2g+6+\sqrt{2})$ we have

$$\begin{aligned}
2k\pi_+(k) &\ge g(k) - \sum_{i=1}^{\lfloor k/2\rfloor} g(i) \\
&\ge q^k - (2g+2)q^{k/2} - (2g+3) - \sum_{i=1}^{\lfloor k/2\rfloor}(q^i + 2gq^{i/2}) \text{ by (2)} \\
&\ge q^k - (2g+2)q^{k/2} - \frac{q}{q-1}(q^{k/2}-1) - 2 \\
&\quad -2g\frac{\sqrt{q}}{\sqrt{q}-1}(q^{k/4}-1) - 2g - 1 \\
&\ge q^k - (2g+4)q^{k/2} - (2g+1)(2+\sqrt{2})q^{k/4} \text{ since } q \ge 2 \\
&\ge q^k - (2g+4)q^{k/2} - (2+\sqrt{2})q^{k/2} \\
&\quad \text{since } 2g+1 \le 2g+6+\sqrt{2} \le q^{k\varepsilon} \le q^{k/4} \\
&\ge q^k - q^{k(\frac{1}{2}+\varepsilon)}.
\end{aligned}$$

The upper bound for $\pi_+(k)$ is derived in a similar way. □

We remark that the above theorem can be derived from [ST99, Theorem 1.1] in a similar fashion. We only have to introduce a character $\chi(p)$ on the monic

irreducible polynomials as in [Art24] which is 1, 0, or -1, respectively, depending on whether p is splitting, ramified or inert. Then we may use the fact that

$$\sum_{\deg(p)=k} (\chi(p)+1) = 2\pi_+(k) - \pi(k) + \pi_0(k).$$

4. The proportion of smooth semireduced ideals

Our aim in this section is to derive asymptotic results on the number of smooth semireduced ideals in hyperelliptic function fields. Hereby, we restrict our attention to ideals with only splitting prime factors; as the number of ramified prime ideals is bounded above by $2g+2$, it is asymptotically negligible. Theorem 2 shows that the number of splitting prime ideals of degree k is in $\frac{1}{k}(q^k + O(q^{\alpha k}))$ with $\alpha < 1$. For situations without additional constraints, in which the components can be joined arbitrarily to form elements, Knopfmacher introduced the very general framework of *(additive) arithmetical semigroups* in ([Kno75]) and Manstavičius obtained smoothness results within this context in ([Man92b], [Man92a]). The special cases of univariate polynomials ([Car87], [AD93], [BP98], [PGF98], [Sou98]) and divisors in algebraic function fields ([Heß99], Chapter 4) have received considerable attention in the literature. In our case, an additional complication is introduced by the fact that the splitting prime ideals come in pairs and at most one of each ideal can be used to compose semireduced ideals (see condition 2) in Section 2). The distribution of such reduced objects has been investigated in [Sey87] in the context of imaginary quadratic number fields. To the best of our knowledge, the present paper is the first one to deal with reducedness in the function field case.

Let $N(n,m)$ be the number of m-smooth semireduced ideals of degree n in $K[H]$.

Using similar techniques we obtain the following analogue for hyperelliptic function fields of Theorem 2.2 in [BP98].

Theorem 3. *Let* $\max\left\{8\log_q\left(2g+6+\sqrt{2}\right), 2\log_q\left(\left(6+\frac{10}{3}\sqrt{2}\right)n\right)\right\}+2 \leq m$ *and* $u = \frac{n}{m}$. *Then*

$$N(n,m) \geq \frac{q^n}{2n^{\lceil u \rceil}}.$$

Proof. Assume first that $m \leq n$. Since Theorem 2 shows that the number of splitting prime ideals grows with their degree, we restrict ourselves to counting a set of special semireduced ideals all of whose prime factors have a rather large degree, hoping to cover the biggest part of all semireduced ideals. To ensure a large degree for all its prime factors, an ideal should have as few of them as possible, and for an m-smooth ideal of degree n this means $\lceil u \rceil$ prime factors. We distribute the degrees of these prime factors as evenly as possible. Thus, let $m_0 = \left\lfloor \frac{n}{\lceil u \rceil} \right\rfloor$, $m_1 = m_0 + 1$, $r_1 = n - \lceil u \rceil m_0$ and $r_0 = \lceil u \rceil - r_1$, and let $\tilde{N}(n,m)$ be the number of semireduced ideals with r_0 distinct splitting prime factors of degree m_0 and r_1 distinct splitting prime factors of degree m_1. As $m_0 r_0 + m_1 r_1 = n$, these ideals are of degree n, and as $m_0 \leq \frac{n}{\lceil u \rceil} \leq m$, they are m-smooth unless $m_0 = m$ and $m_1 = m+1$. In this case, however, $\lceil u \rceil$ divides n and $r_1 = 0$, so that they are m-smooth nevertheless. Thus, $N(n,m) \geq \tilde{N}(n,m)$. To estimate the latter number, notice that there are $\binom{\pi_+(m_i)}{r_i}$ possibilities for choosing r_i monic splitting irreducible polynomials of degree m_i and that each irreducible polynomial leaves the choice of

one out of two prime ideals. So the following relations hold:

$$\begin{aligned}
\tilde{N}(n,m) &= 2^{r_0}\binom{\pi_+(m_0)}{r_0}2^{r_1}\binom{\pi_+(m_1)}{r_1} \\
&\geq 2^{r_0+r_1}\frac{(\pi_+(m_0)-(r_0-1))^{r_0}}{r_0!}\frac{(\pi_+(m_1)-(r_1-1))^{r_1}}{r_1!} \\
&\geq \frac{\sqrt{2}^{r_0+r_1-2}}{r_0^{r_0}r_1^{r_1}}2^{r_0+r_1}\frac{\left(q^{m_0}-q^{\frac{3}{4}m_0}-2m_0(r_0-1)\right)^{r_0}}{(2m_0)^{r_0}} \\
&\quad \cdot\frac{\left(q^{m_1}-q^{\frac{3}{4}m_1}-2m_1(r_1-1)\right)^{r_1}}{(2m_1)^{r_1}} \\
&\quad \text{by } r!\leq\frac{r^r}{\sqrt{2}^{r-1}} \text{ for } r\geq 0 \text{ and by Theorem 2 with } \varepsilon=\frac{1}{4} \\
&\geq \frac{\sqrt{2}^{r_0+r_1-2}}{n^{\lceil u\rceil}}\left(q^{m_0}-q^{\frac{3}{4}m_0}-2n\right)^{r_0}\left(q^{m_1}-q^{\frac{3}{4}m_1}-2n\right)^{r_1}
\end{aligned}$$

Theorem 2 is applicable because $m_1 > m_0 > \frac{n}{\frac{n}{m}+1} - 1 \geq \frac{1}{2}m - 1$. Notice now that $m_0 \geq 4\log_q(2g+6+\sqrt{2}) \geq 4\log_q(8+\sqrt{2})$ implies $q^{\frac{1}{4}m_0} \geq 8+\sqrt{2}$ and $q^{\frac{3}{4}m_0} \leq \frac{q^{m_0}}{8+\sqrt{2}}$. Similarly, $q^{\frac{3}{4}m_1} \leq \frac{q^{m_1}}{8+\sqrt{2}}$. Furthermore, letting $c = 1 - \frac{1}{8+\sqrt{2}} - \frac{1}{\sqrt{2}}$, we deduce that $2n \leq cq^{m_0} \leq cq^{m_1}$ as soon as m satisfies the second lower bound. Hence,

$$\tilde{N}(n,m) \geq \frac{\sqrt{2}^{r_0+r_1}}{2n^{\lceil u\rceil}}\frac{q^{m_0r_0}}{\sqrt{2}^{r_0}}\frac{q^{m_1r_1}}{\sqrt{2}^{r_1}} = \frac{q^n}{2n^{\lceil u\rceil}}.$$

Finally, if $m > n$, then

$$N(n,m) = N(n,n) \geq \frac{q^n}{2n} = \frac{q^n}{2n^{\lceil u\rceil}}.$$

□

Theorem 3 is not yet sufficient to prove the subexponentiality result of Section 5. In fact, we need a bound for $N(n,m)$ of about $\frac{q^n}{u^u}$, so that we have to improve the bound of the theorem above by a factor of about m^u.

When m is of the order of $\log n$, the desired result can be derived easily from Theorem 3.

Corollary 4. *Suppose that, under the conditions of Theorem 3, we have furthermore $m \leq k\log n$ for some constant $k > 0$. Then*

$$N(n,m) \geq \frac{q^n}{u^{u\left(\left(1+\frac{1}{u}\right)\left(1+\frac{\log(k\log n)}{\log u}\right)+\frac{\log 2}{u\log u}\right)}} \in \frac{q^n}{u^{u(1+o(1))}} \text{ for } u\to\infty.$$

Proof. In this special case, the denominator of the formula in Theorem 3 satisfies

$$2n^{\lceil u\rceil} = 2m^{\lceil u\rceil}u^{\lceil u\rceil} \leq 2(k\log n)^{u+1}u^{u+1} = u^{u\left(\left(1+\frac{1}{u}\right)\left(1+\frac{\log(k\log n)}{\log u}\right)+\frac{\log 2}{u\log u}\right)}.$$

The asymptotic result follows from $n\to\infty$ as $u\to\infty$ and $\frac{\log\log n}{\log u} \leq \frac{\log\log n}{\log n-\log(k\log n)}$ $\to 0$ $(n\to\infty)$ □

For larger m, we need to follow a different approach, since n and u differ considerably. Still, we have to assume that m is not too large compared to n; precisely, we require $m \leq n^{1-\varepsilon}$ for some $\varepsilon \in (0;1)$. As hyperelliptic function fields are the

function field analogue of quadratic number fields, it can be expected that results and techniques concerning smooth ideals in quadratic number fields carry over to our problem. Indeed, this is the case. The following theorem and its proof are inspired by Theorem 5.2 in [Sey87]. We can use Theorem 3 above to simplify the proof.

Theorem 5. *If there is a constant $\varepsilon \in (0;1)$ such that m, n and $u = \frac{n}{m}$ satisfy*

$$\max\left\{16\log_q(2g+6+\sqrt{2})+4, 4\log_q\left(\left(6+\frac{10}{3}\sqrt{2}\right)n\right)+4, \log n\right\} \leq m \leq n^{1-\varepsilon},$$

$$n \geq 29 \text{ and } \frac{4}{\varepsilon}u\log u \geq 1,$$

then

$$N(n,m) \geq \frac{q^n}{u^{u\left(1+\frac{\log\log u+6+\log\frac{4}{\varepsilon}}{\log u}+\frac{3}{\varepsilon u}\right)}} \in \frac{q^n}{u^{u(1+o(1))}} \text{ for } u \to \infty.$$

Proof. For Theorem 3, we counted all ideals with $\lceil u \rceil$ prime factors all of which had the degrees m_0 or one more. To show a higher number of smooth ideals, we must allow more flexibility in the size of the components. Thus, we consider ideals with $\lfloor u \rfloor$ prime factors whose degrees vary within a certain factor of m. To reach the total degree n, we pad by prime ideals of smaller degree.

Specifically, let $m-1 \geq w := \left\lfloor\left(1-\frac{1}{\log n}\right)m\right\rfloor \geq \left(1-\frac{1}{\log n}-\frac{1}{m}\right)m \geq \frac{m}{2}$ for $m \geq 5$ and $n \geq 29$. Let $\mathcal{P}$ be a set of prime ideals containing exactly one ideal above each monic splitting irreducible polynomial p with $w+1 \leq \deg p \leq m$. We consider ideals of the form $\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2$, where $\mathfrak{A}_1$ has exactly $\lfloor u \rfloor$ (not necessarily distinct) prime factors from $\mathcal{P}$ and $\mathfrak{A}_2$ is semireduced and w-smooth of degree $n - \deg\mathfrak{A}_1$. From the construction of $\mathcal{P}$ it follows that $\mathfrak{A}_1$ is semireduced and m-smooth and that $\mathfrak{A}_1$ and $\mathfrak{A}_2$ have no common prime factors. Furthermore, $\deg\mathfrak{A} = n$, so that $N(n,m)$ is bounded below by the number of such ideals $\mathfrak{A}$. Let $\mathcal{I}$ be the set of possible ideals $\mathfrak{A}_1$. Then the above discussion implies

$$N(n,m) \geq \sum_{\mathfrak{A}_1 \in \mathcal{I}} N(n-\deg\mathfrak{A}_1, w).$$

From $w \geq \frac{m}{2}$ and the restrictions imposed on m we see that Theorem 3 applies to the situation, so that

$$N(n-\deg\mathfrak{A}_1, w) \geq \frac{q^{n-\deg\mathfrak{A}_1}}{2(n-\deg\mathfrak{A}_1)^{\left\lceil\frac{n-\deg\mathfrak{A}_1}{w}\right\rceil}}.$$

The logarithm of the denominator is bounded above by

$$\begin{aligned}
\left(\frac{n-\deg\mathfrak{A}_1}{w}+2\right)\log n &\leq \left(\frac{n}{w}-(u-1)+2\right)\log n \\
&\leq \left(\frac{1}{1-\frac{1}{\log n}-\frac{1}{m}}-1\right)u\log n + 3\log n \\
&\leq \frac{2\log n}{\log n - 2}u + 3\log n \text{ since } m \geq \log n \\
&\leq 6u + \frac{3}{\varepsilon}\log u \text{ since } \log n \geq 3 \text{ and } n^{\varepsilon} \leq u.
\end{aligned}$$

Hence,

$$N(n,m) \geq \frac{q^n}{u^{u\left(\frac{6}{\log u}+\frac{3}{\varepsilon u}\right)}} \sum_{\mathfrak{A}_1 \in \mathcal{I}} q^{-\deg \mathfrak{A}_1}.$$

The last sum can be computed using our results on the density of prime ideals of Section 3. Let $\mathcal{P} = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_l\}$.

$$\begin{aligned}
\sum_{\mathfrak{A}_1 \in \mathcal{I}} q^{-\deg \mathfrak{A}_1} &= \sum_{a_i \geq 0,\, a_1+\cdots+a_l=\lfloor u \rfloor} q^{-a_1 \deg \mathfrak{P}_1 - \cdots - a_l \deg \mathfrak{P}_l} \\
&\geq \frac{\left(\sum_{i=1}^{l} q^{-\deg \mathfrak{P}_i}\right)^{\lfloor u \rfloor}}{\lfloor u \rfloor!} \\
&\quad \text{since by multiplying out } \left(\sum_{i=1}^{l} q^{-\deg \mathfrak{P}_i}\right)^{\lfloor u \rfloor} \text{ each term of the} \\
&\quad \text{previous sum is obtained at most } \lfloor u \rfloor! \text{ times} \\
&\geq u^{-\lfloor u \rfloor} \left(\sum_{j=w+1}^{m} \pi_+(j) q^{-j}\right)^{\lfloor u \rfloor} \\
&\geq u^{-\lfloor u \rfloor} \left(\sum_{j=w+1}^{m} \frac{1}{2j}\left(1 - \frac{1}{q^{j\left(\frac{1}{2}-\frac{1}{8}\right)}}\right)\right)^{\lfloor u \rfloor} \\
&\quad \text{by Theorem 2 with } \varepsilon = \frac{1}{8} \\
&\geq u^{-\lfloor u \rfloor} \left(\frac{1}{4} \sum_{j=w+1}^{m} \frac{1}{j}\right)^{\lfloor u \rfloor} \quad \text{since } q^{\frac{3}{8}(w+1)} \geq 2^{\frac{3}{2}} > 2 \\
&\geq u^{-\lfloor u \rfloor} \left(\frac{m-w}{4m}\right)^{\lfloor u \rfloor} \\
&\geq (4u \log n)^{-\lfloor u \rfloor} \\
&\geq \left(\frac{4}{\varepsilon} u \log u\right)^{-\lfloor u \rfloor} \geq \left(u^{1+\frac{\log\log u + \log\frac{4}{\varepsilon}}{\log u}}\right)^{-u}.
\end{aligned}$$

This achieves the proof of the theorem. □

5. Subexponentiality

As mentioned in the introduction, results on smooth ideals are needed for estimating the running time of algorithms for computing discrete logarithms in hyperelliptic function fields as described in [MST99, Eng99, EG00]. To prove a subexponential running time of these algorithms, one has to show that one out of a subexponential number of reduced ideals factors completely over a factor base of subexponential size, which is composed of prime ideals whose degrees are bounded by some constant m. To make this statement more precise, let

$$L(\rho) = e^{\rho\sqrt{(g \log q)\log(g \log q)}}$$

denote the subexponential function with respect to the input size $g \log q$; notice that a hyperelliptic curve can be specified by $O(g \log q)$ bits by the polynomials h and f of degree $O(g)$ over $\mathbb{F}_q$. Being interested in reduced ideals, we have $n = g$, and since there are $O(q^m)$ prime ideals of degree at most m in the factor base, we let

$$m = \lceil \log_q L(\rho) \rceil = \left\lceil \rho \sqrt{\frac{g \log(g \log q)}{\log q}} \right\rceil$$

with a constant $\rho > 0$ depending on the application. (In fact, rounding up the value for m may make the factor base exponential. Conditions preventing this situation, which has no influence on the results of this section, are discussed in [Eng99].) Our aim is to use Corollary 4 and Theorem 5 to obtain asymptotic results for $g \to \infty$. Notice that either the conditions of the corollary or of the theorem are fulfilled for any $\varepsilon \in (0; \frac{1}{2})$ and g large enough. Since $u \to \infty$ as $g \to \infty$, we have

$$N(g, m) \geq \frac{q^g}{u^{u(1+\alpha(g))}}$$

with $\alpha(g) \to 0$ for $g \to \infty$. In our special situation,

$$u = \frac{g}{m} \leq \frac{1}{\rho} \sqrt{\frac{g \log q}{\log(g \log q)}} \leq \frac{1}{\rho} \sqrt{g \log q}$$

and hence

$$\log u \leq \frac{1}{2} \log(g \log q) - \log \rho,$$

and the logarithm of the denominator of $N(g, m)$ is given by

$$\begin{aligned} (1 + \alpha(g)) u \log u &\leq \frac{1}{2\rho}(1 + \alpha(g)) \left(1 - \frac{2 \log \rho}{\log(g \log q)}\right) \sqrt{(g \log q) \log(g \log q)} \\ &\in \left(\frac{1}{2\rho} + o(1)\right) \sqrt{(g \log q) \log(g \log q)}. \end{aligned}$$

This proves the following result:

Theorem 6. *Let $m = \lceil \log_q L(\rho) \rceil$ for a constant $\rho > 0$. Then there is a function $\beta(g)$ in $o(1)$ for $g \to \infty$ such that*

$$N(g, m) \geq L\left(-\frac{1}{2\rho} - \beta(g)\right) q^g.$$

Acknowledgments

We are indebted to the Centre for Applied Cryptographic Research at the University of Waterloo; we especially wish to thank Alfred Menezes and Scott Vanstone for their support. Most of this contribution is a result of a research visit of the first author's at the Centre for Applied Cryptographic Research. We also thank Bruce Richmond for fruitful discussions and for pointing out Knopfmacher's and related work to us.

References

[AD93] Leonard M. Adleman and Jonathan DeMarrais. A subexponential algorithm for discrete logarithms over all finite fields. *Mathematics of Computation*, 61(203):1–15, 1993. MR **94e:**11140

[ADH94] Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In [AH94], pages 28–40, 1994. MR **96b:**111078

[AH94] Leonard M. Adleman and Ming-Deh Huang, editors. *Algorithmic Number Theory*, volume 877 of *Lecture Notes in Computer Science*, Berlin, 1994. Springer-Verlag. MR **95j:**11119

[Art24] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Mathematische Zeitschrift*, 19:153–206, 1924.

[Bau98] Mark Bauer. A subexponential algorithm for solving the discrete logarithm problem in the Jacobian of high genus hyperelliptic curves over arbitrary finite fields. Preprint, 1998.

[BP98] Renet Lovorn Bender and Carl Pomerance. Rigorous discrete logarithm computations in finite fields via smooth polynomials. In [BT98], pages 221–232, 1998. MR **99c:**11156

[BT98] D. A. Buell and J. T. Teitelbaum, editors. *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin*, volume 7 of *Studies in Advanced Mathematics*. American Mathematical Society, 1998. MR **98g:**11001

[Buh98] J. P. Buhler, editor. *Algorithmic Number Theory — ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, Berlin, 1998. Springer-Verlag. MR **2000g:**11002

[Car87] Mireille Car. Théorèmes de densité dans $\mathbb{F}_q[x]$. *Acta Arithmetica*, 68:145–165, 1987. MR **88g:**11090

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–655, November 1976. MR **55:**10141

[EG00] Andreas Enge and Pierrick Gaudry. A general framework for subexponential discrete logarithm algorithms. Research Report LIX/RR/00/04, LIX, June 2000. Available at http://www.math.uni-augsburg.de/~enge/vorabdrucke/subexp.ps.gz.

[Eng99] Andreas Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. Combinatorics and Optimization Research Report CORR 99-04, University of Waterloo, February 1999. Available at http://-cacr.math.uwaterloo.ca/techreports/1999/corr99-04.ps; to appear in *Mathematics of Computation*.

[Heß99] Florian Heß. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*. PhD thesis, Technische Universität Berlin, 1999.

[Kno75] John Knopfmacher. *Abstract Analytic Number Theory*, volume 12 of *North-Holland Mathematical Library*. North-Holland Publishing Company, Amsterdam, 1975. MR **54:**7404

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathemathics of Computation*, 48:203–209, 1987. MR **88b:**94017

[Kob89] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989. MR **90k:**11165

[Man92a] E. Manstavičius. Remarks on the semigroup elements free of large prime factors. *Lithuanian Mathematical Journal*, 32(4):400–409, 1992. MR **94j:**11093

[Man92b] E. Manstavičius. Semigroup elements free of large prime factors. In [SM92], pages 135–153, 1992. MR **93m:**11091

[Mil86] V. Miller. Use of elliptic curves in cryptography. In *CRYPTO'85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1986. MR **88b:**68040

[MST99] V. Müller, A. Stein, and C. Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. *Mathematics of Computation*, 68(226):807–822, 1999. MR **99i:**11119

[PGF98] D. Panario, X. Gourdon, and P. Flajolet. An analytic approach to smooth polynomials over finite fields. In [Buh98], pages 226–236, 1998. MR **2001e:**11119

[PR99] S. Paulus and H.-G. Rück. Real and imaginary quadratic representations of hyperelliptic function fields. *Mathematics of Computation*, 68:1233–1241, 1999. MR **99i:**11107

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public–key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. MR **83m:**94003

[Sey87] M. Seysen. A probabilistic factorization algorithm with quadratic forms of negative discriminant. *Mathematics of Computation*, 48(178):757–780, 1987. MR **88d:**11129

[SM92] F. Schweiger and E. Manstavičius, editors. *New Trends in Probab. and Statist.*, 1992. MR **93g:**11005

[Sou98] K. Soundararajan. Smooth polynomials: Analogies and asymptotics. Preprint, July 1998.

[SSW96] R. Scheidler, A. Stein, and H. C. Williams. Key-exchange in real quadratic congruence function fields. *Designs, Codes and Cryptography*, 7:153–174, 1996. MR **97d:**94009

[ST99] A. Stein and E. Teske. Explicit bounds and heuristics on class numbers in hyperelliptic function fields. Technical Report CORR 99-26, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, 1999; Math. Comp., posted on October 4, 2001, PII S0025-5718(01)01385-0 (to appear in print).

[Ste97] A. Stein. Equivalences between elliptic curves and real quadratic congruence function fields. *Journal de Theorie des Nombres de Bordeaux*, 9:75–95, 1997. MR **98d:**11144

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer, Berlin, 1993. MR **94k:**14016

[SW99] A. Stein and H. C. Williams. Some methods for evaluating the regulator of a real quadratic function field. *Experimental Mathematics*, 8(2):119–133, 1999. MR **2000f:**11152

[Zuc98] R. Zuccherato. The equivalence between elliptic curve and quadratic function field discrete logarithms in characteristic 2. In *Algorithmic Number Theory Seminar ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 621–638. Springer, 1998. MR **2000j:**14043

Lehrstuhl für Diskrete Mathematik, Optimierung und Operations Research, Universität Augsburg, 86135 Augsburg, Germany

E-mail address: enge@math.uni-augsburg.de

University of Illinois at Urbana-Champaign, Department of Mathematics, 1409 West Green Street, Urbana, Illinois 61801

E-mail address: andreas@math.uiuc.edu