Доказательство основано на теореме Ф. Н. Сохацкого [4] о решении обобщённого уравнения общей ассоциативности для сильно зависимых операций.

Как следствие из предыдущей теоремы, получается следующее обобщение теоремы Глускина — Хоссу на случай сильно зависимых функций.

Теорема 4. Если сильно зависимая n-арная операция $[x_1, \ldots, x_n]$ на конечном множестве X удовлетворяет тожеству ассоциативности

$$[[x_1, \ldots, x_n], x_{n+1}, \ldots, x_{2n-1}] = [x_1, [x_2, \ldots, x_{n+1}], x_{n+2}, \ldots, x_{2n-1}],$$

то для некоторого моноида «$*$» на множестве X, автоморфизма θ моноида «$*$», такого, что $\theta^{n-1}(x) = a{*}x{*}a^{-1}$, $a \in X$ — обратимый элемент моноида «$*$», $\theta(a) = a$, справедливо тождество

$$[x_1, \ldots, x_n] = x_1 * \theta(x_2) * \theta^2(x_3) * \ldots * \theta^{n-2}(x_{n-1}) * a * x_n, \quad x_i \in X,\ i = 1, \ldots, n.$$

В заключение приведём обобщение обратной теоремы Глускина — Хоссу.

Теорема 5. Если для сильно зависимой n-арной операции $[x_1, \ldots, x_n]$ справедливо представление

$$[x_1, \ldots, x_n] = x_1 * \theta(x_2) * \theta^2(x_3) * \ldots * \theta^{n-2}(x_{n-1}) * a * x_n,$$

где «$*$» — моноид на множестве X; θ — автоморфизм моноида «$*$», такой, что $\theta^{n-1}(x) = a^{-1} * x * a$, $a \in X$ — обратимый элемент моноида «$*$», $\theta(a) = a$, то она является n-полугруппой.

ЛИТЕРАТУРА

1. *Гальмак А. М., Воробьев Г. Н.* О теореме Поста — Глускина — Хоссу // Проблемы физики, математики и техники. 2013. Вып. 1(14). С. 55–59.
2. *Малышев Ф. М.* О теореме Поста — Глускина — Хоссу для конечных квазигрупп и самоинвариантные семейства подстановок // Математический сборник. 2016. Т. 207. Вып. 2. С. 81–92.
3. *Малышев Ф. М.* Теорема Поста — Глускина — Хоссу для n-квазигрупп // Исследования по алгебре, теории чисел, функциональному анализу и смежным вопросам: межвуз. сб. науч. тр. Саратов: Изд-во Сарат. ун-та, 2016. Т. 8. С. 59–62.
4. *Сохацкий Ф. Н.* Обобщение двух теорем Белоусова для сильно зависимых функций k-значной логики // Исследования по теории бинарных и n-арных квазигрупп. Математические исследования. Кишинев: Штиинца, 1985. № 85. С. 105–115.

UDC 512.772.7 DOI 10.17223/2226308X/11/8

NFS FACTORIZATION: NEW HOPES

P. Kirchner

We describe new Number Field Sieve techniques. While *none* is proved (even under heuristics) to work for a concrete family of number fields, we hope such a family exist. If this is the case, we can factor a special integer n in time $L_n(1/3, (16/9)^{1/3})$, which doubles the length of n with respect to SNFS for the same time. This algorithm works by finding a strongly-ambiguous ideal in order to factor the relative discriminant of a prime degree Galois extension. In case this method can be adapted for factoring general numbers, it may reach a complexity $L_n(1/3, (32/9)^{1/3})$. A variant of the same

technique for computing number fields of constant degree d would allow multiplying by d the length of the discriminant at the same complexity. We emphasize that for these running times to hold, we need to build highly specific number fields, and there is no evidence it can be done. Finally, we give another technique for finding the maximum order of number fields, and may run as fast as $L_{|\Delta|}(1/3, (16/9)^{1/3})$. This method is likely to work, and can therefore find *some* square factors in some numbers.
Keywords: *integer factorization, number field sieve.*

1. Introduction

In 1993, the Number Field Sieve algorithm was invented [1] with a complexity of $L_n(1/3, (64/9)^{1/3})$ for factoring any n, and since then, it has been mostly unchallenged (though a variant is asymptotically faster [2]). A variant for *s*pecial numbers was also given, with a complexity of $L_n(1/3, (32/9)^{1/3})$.

We give a method for factoring very special n (so special that we do not know how to find them, or if they even exist) with a complexity of only $L_n(1/3, (16/9)^{1/3})$, ***if*** we can find a number field with the desired properties. This algorithm is in fact a generalization of the class group relations method [3, 4].

We also give a method for finding the maximal order of a number field, which may run just as fast, and needs no unknown construction. It *might* possibly be used for finding square factors in an integer.

We will use standard algorithms in number theory, such as the ones for computing the class group and units of a number field, without describing them. A complete description can be found in Cohen's book [5].

2. Background

We fix a Galois extension of number fields $[\mathbb{L} : \mathbb{K}] = p$, p is prime, and the Galois group is generated by σ. The goal is to factor the discriminant ideal $\Delta_{\mathbb{L}/\mathbb{K}}$, and we assume $\mathbb{L} = \mathbb{Q}[X]/f(X)$ with f of degree d, and the height (maximal absolute value of coefficients) of f being $\approx \mathcal{N}(\Delta_{\mathbb{L}/\mathbb{K}})^{1/2/(d-1)}$ where $\mathcal{N}()$ denotes the norm of the ideal (the discriminant is a homogeneous polynomial of degree $2d-2$ in the coefficients of f). We let $\mathcal{O}_{\mathbb{L}}$ be the ring of integers of $\mathbb{L}$.

The principle consists in finding a non-trivial ideal $\mathfrak{a}$ such that $\sigma(\mathfrak{a}) = \mathfrak{a}$. These ideals are called strongly ambiguous [6], and known to be exactly the divisors of a power of $\Delta_{\mathbb{L}/\mathbb{K}}$ up to an ideal of $\mathbb{K}$. Therefore, $\gcd(\Delta_{\mathbb{L}/\mathbb{K}}, \mathfrak{a})$ is non-trivial.

For example, $\mathbb{Q}[X]/(X^4+13X^3-43X^2-39X+9)$ is a degree two extension of $\mathbb{Q}[\sqrt{317}]$, and the norm of the relative discriminant is $4429 = 43 \cdot 103$.

While the technique works for all p, it is unlikely to be useful for any $p > 2$ since the relative discriminant is a $p-1$ power.

3. CM case

We assume here $\mathbb{L}$ is a (strict) CM-field and $\mathbb{K}$ is principal (a small $h(\mathbb{K})$ does not pose any problem). Then $\mathfrak{a}\sigma(\mathfrak{a}) = \mathfrak{a}^2$ is an ideal of $\mathbb{K}$ so that it is principal. The algorithm therefore computes the class group, and we can then hopefully enumerate all classes $[\mathfrak{a}]$ whose square is principal.

Therefore, we can find $\mathfrak{a}$ such that there exists v with $\sigma(v\mathfrak{a}) = v\mathfrak{a}$. Then $\dfrac{\mathfrak{a}}{\sigma(\mathfrak{a})} = \dfrac{\sigma(v)}{v}\mathcal{O}_{\mathbb{L}}$, and Gentry-Szydlo [7] recovers v, from which we deduce $v\mathfrak{a}$ (in fact, one can do the same if $\mathbb{L}$ has a tiny regulator (a "simplest field") by replacing Gentry-Szydlo with Schoof's algorithm [8]).

How to find a "random" ideal whose square is principal: generate relations as usual, and put them in a sparse integer matrix A. It has the property that for all column j, $\prod_i \mathfrak{p}_i^{A_{i,j}}$ is principal and known where $\mathfrak{p}_i$ are all prime ideals less than some bound. Then compute x such that $Ax = 0[2]$, and return the ideal corresponding to $(Ax)/2$, namely

$$\prod_i \mathfrak{p}_i^{(Ax/2)_i}.$$

The overall complexity is $L_{\mathcal{N}(\Delta_{\mathbb{L}/\mathbb{K}})}(1/3, (16/9)^{1/3})$ for a well-chosen d.

4. Non-CM

We assume here $\mathbb{L}$ is not a CM-field, so that each class of ideals is represented by a small integral ideal $\mathfrak{a}$ (this excludes the families of the rare "simplest fields", though). Therefore, we can find $\mathfrak{a}$ such that $\sigma(v\mathfrak{a}) = v\mathfrak{a}$. We first compute g a generator of $\dfrac{\mathfrak{a}}{\sigma(\mathfrak{a})} = \dfrac{\sigma(v)}{v}\mathcal{O}_{\mathbb{L}}$. Then, we compute the units of $\mathbb{L}$, and $\mathbb{K}$. From there, we can in polynomial time deduce $u \in \mathbb{L}$ a unit, such that $\mathbb{N}_{\mathbb{L}/\mathbb{K}}(gu) = 1$ ($\sigma(v)/v/g$ is such a unit). Then, we solve[1] $\sigma(w) = wgu$ ($w \neq 0$), an equation which is linear in w (there is a solution, because of Hilbert's Theorem 90). Finally, $\sigma(w\mathfrak{a}) = w\mathfrak{a}$.

The overall complexity is $L_{\mathcal{N}(\Delta_{\mathbb{L}/\mathbb{K}})}(1/3, (16/9)^{1/3})$ for a well-chosen d, if we can multiply matrices in time $n^{2+o(1)}$. The sparse linear algebra exponent is in fact a bit higher (2.38), so the complexity will also be a bit higher.

If we take the field $\mathbb{Q}[X]/(X^4 + 13X^3 - 43X^2 - 39X + 9)$, and the ideal $\mathcal{O}_{\mathbb{L}}$, units are generators, and generated by $u_0 = 5/3X^3 + 65/3X^2 - 200/3X - 77$, $u_1 = 121/3X^3 - - 320/3X^2 - 286/3X + 22$ and $u_2 = 2183/3X^3 + 26399/3X^2 - 117815/3X + 7238$. u_1 is of norm 1, which indicates the element $w_0 = 92X^2 + 1471X + 283$ with $w_0/\sigma(w_0) = u_1$, and is of norm 103×421^2, revealing the factor 103 of the discriminant. $u_0^{-1}u_1^1u_2^2$ is of norm 1, which indicates the corresponding element $w_1 = 557995X^2 + 9207617X + 7889384$, of norm 43×162092^2, revealing the other factor 43 of the discriminant.

Average-case factorization? It may seem that by relaxing the height of f to $\approx n^{1/d}$, we may hope to factor the integer n in time which is only $L_n(1/3, (32/9)^{1/3})$ for most n. Of course, we also need the density of such f with a suitable subfield to be not too tiny, and a fast way to generate such a f.

5. Computing constant degree fields

The best known heuristic algorithm which computes a field $\mathbb{K}$ of constant degree d runs in $L_{\Delta}(1/2, 1)$, and Δ is the discriminant (up to sign).

Now, we propose to instead find some extension $\mathbb{L}$ of $\mathbb{K}$ of degree $k = \omega(1)$ but sufficiently small. Then, we can hope that $\mathbb{L} = \mathbb{Q}[X]/f(X)$ with f a polynomial of height $\approx (\Delta^k\delta)^{1/(2dk-2)} = \Delta^{1/2d+o(1)}\delta^{(1+o(1))/2dk}$ where δ is the norm of the relative discriminant. Thus, the numbers which are to be smooth in the algorithm are of this size, instead of $\Delta^{1/2}$. We can then deduce some units of $\mathbb{K}$ as norms of the units of $\mathbb{L}$. The index is a power of k, so that the units can be recovered through a saturation method. Also, if $h(\mathbb{K})$ is coprime with k, then the norm of the class group of $\mathbb{L}$ is the class group of $\mathbb{K}$ (otherwise, we know that the p-Sylow differs only when p divides $\gcd(k, h(\mathbb{K}))$). Furthermore, in case the extension is abelian, class field theory describes the norm map.

[1]Since w may have huge coefficients, we solve the equation on the log-embedding, and convert back into a formal product.

In the case of δ small, we can therefore compute fields whose discriminants are d times the size of the previous algorithm.

We add that if a family of such extensions exists with $d \geqslant 3$, k prime and the extension is Galois, then either we can factor δ faster than the SNFS algorithm, or we can compute the base field in a faster way than the previous algorithm. Hence, the last possibility for this method to get only trivial results (if $\mathbb{L}$ exists), is that δ must be smooth. While this is the case when $\mathbb{L}$ has lots of subfields, this should not be the general case.

6. Finding the maximal order

We collect relations in $\mathbb{Z}[X]/f(X)$ as usual, and form a matrix $A_{i,j}$ such that $\prod_i \mathfrak{p}_i^{A_{i,j}}$ is generated by v_j. The initial order $\mathcal{O}$ is $\mathbb{Z}[X]/f(X)$, and we make it p-maximal for each prime number p in the factor base (see [5]).

Then, we choose some small prime p and we compute a random x such that $Ax = 0 \pmod p$. The final step is to extract a p-th root of $\prod_i v_i^{x_i}$ and look for non trivial denominators in the coordinate. We may ensure it is an element of $\mathcal{O}_\mathbb{L}$ using characters (as in [9])— or alternatively, hope that it is the case. Then, consider g a generator of $\prod_i \mathfrak{p}_i^{(Ax)_i/p}$. This ideal is "random" in $\mathrm{Cl}(\mathcal{O})/\mathrm{Cl}(\mathcal{O}_\mathbb{L})[p]$, and in case it is not trivial, we get a non trivial denominator. Consider now $g^{-p}\prod_i v_i^{x_i}$; this is a "random" (well-defined) element in $\mathcal{O}_\mathbb{L}^\times/\mathcal{O}^\times[p]$, and again if it is not trivial, we discover a non trivial denominator.

We have the exact sequence

$$1 \to \mathcal{O}_\mathbb{L}^\times/\mathcal{O}^\times \to (\mathcal{O}_\mathbb{L}/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_\mathbb{L}) \to 1$$

where the conductor $\mathfrak{f}$ is $\{x \in \mathbb{L}; x\mathcal{O}_\mathbb{L} \subset \mathcal{O}\}$. It implies that

$$|\mathrm{Cl}(\mathcal{O})/\mathrm{Cl}(\mathcal{O}_\mathbb{L})||\mathcal{O}_\mathbb{L}^\times/\mathcal{O}^\times| = |(\mathcal{O}_\mathbb{L}/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times|.$$

In particular, if $p\big||(\mathcal{O}_\mathbb{L}/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times|$, we should obtain quickly the corresponding factors. In our experiments, any large prime factor q of the index gave rise either to a factor of $q+1$ or $q-1$, so that $p=2$ seems enough. We may however find factors of the type $\dfrac{q^{d_0}-1}{q^{d_1}-1}$ with $d_1|d_0 \leqslant d$, which can be tackled with $p|d_0/d_1$.

Another technique is to compute $|\mathrm{Cl}(\mathcal{O})|$, and then use it to factor the discriminant. Indeed, we may hope to find large primes of $|(\mathcal{O}_\mathbb{L}/\mathfrak{f})^\times|$, and then use them in the $p-1$ [10], $p+1$ [11] method, or a generalization of them [12] (while we might have been forced with the $p-1$ method to factor the class number so that they do not find all factors of the conductor at the same time, this does not happen with Bach — Shallit's method). In the particular case of imaginary quadratic fields of large discriminant, $\mathfrak{f}$ is generated by an integer and we recover a product of $p + \left(\dfrac{\Delta}{p}\right)$, see [13]. However, experiments seem to indicate that for typical fields, large primes do not divide $|\mathrm{Cl}(\mathcal{O})/\mathrm{Cl}(\mathcal{O}_\mathbb{L})|$ [14]. Perhaps $|(\mathcal{O}_\mathbb{L}/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times|$ splits in the two components in a way similar to $\sqrt{|\Delta_\mathbb{L}|}$. This excludes fields where units are constrained, of course (such as CM-fields, simplest fields).

We can now take the inverse position of Buchmann — Lenstra [15]: since finding the maximal order of some number field may be easier than factoring, we should try reducing the factorization of a number with square factors to finding the maximal order of a number field which is easy to compute.

Our first example is $\mathbb{Z}[X]/(X^3 + 14748982211X^2 + 330465312475655912644X - 4541929250363265152095834584323)$. The index of the order is 31415926535897932429, the index of the unit group is 15707963267948966215 and the discriminant of the field is the prime number $-10312194704439519935458 07$. The maximal order is principal, the order has a class number of 2.

Our second example is $\mathbb{Z}[X]/(X^3 + 778669X^2 - 11461680097X + 400204890996)$. Computing its class group, we find $\mathbb{Z}/1468825548960\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$. Therefore, we compute $2^{4\cdot 1468825548960}-1$ modulo the discriminant of the order, 84855839117718748443550622974949, and searching its inverse leads to the factor 314161. The maximal order has a class group isomorphic to $\mathbb{Z}/9350812\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so that the index is 314160. $X - 14417$ and $X - 35$ are generating units of the maximal order. The discriminant of the field is the prime number 859759911423970846469.

Both polynomials were found by searching the roots of the discriminant of a polynomial modulo p^2. When one of them is small, it implies a small (or convenient) f such that $\mathbb{Z}[X]/f(X)$ has a discriminant divisible by p^2. In *all* cases found, it has a suborder of index divisible by p.

We give the following challenge:

$$\mathbb{Z}[X]/(X^5 + 349545300459049164 2X^4 + 180994857869926433565628676598524675713X^3 + \\ +4080542158246926001840448564437517681525979747052560162169X^2 + \\ +2999133115941859238422175138175774173646033689324599471184750910905856654541 1X - \\ -6152273627649125817906560750215727039516242802160147351967902776042470214158323837989680533780 87).$$

The discriminant of the polynomial has 1287 bits, the discriminant of the field is a prime number of 948 bits and the index is a prime number of 170 bits (51 digits). (In particular, it is faster to use ECM to factor the discriminant.)

7. Conclusion

We conclude that when number fields verify the given conditions, then either the norm of the relative discriminant is easily factored, either the unit group[2] and the class group are not both explicit. There are known examples of the first case (any cyclotomic field), and of the second case (respectively "simplest" fields and CM fields; and "generic" fields). It suggests that for these fields, this is essentially the best we can do, i.e. there are no explicit (efficient) formulas for the class group of most CM fields and "simplest" fields, and likewise no explicit formulas for the unit group of most "generic" fields.

The author thanks Thomas Espitau and Antoine Joux for interesting discussions on this subject.

REFERENCES

1. *Buhler J. P., Lenstra H. W., and Pomerance C.* Factoring integers with the number field sieve. The Development of the Number Field Sieve, Springer, 1993, pp. 50–94.
2. *Coppersmith D.* Modifications to the number field sieve. J. Cryptology, 1993, vol. 6, no. 3, pp. 169–180.
3. *Seysen M.* A probabilistic factorization algorithm with quadratic forms of negative discriminant. Mathematics of Computation, 1987, vol. 48, no. 178, pp. 757–780.
4. *Lenstra H. W. and Pomerance C.* A rigorous time bound for factoring integers. J. Amer. Math. Soc., 1992, vol. 5, no. 3, pp. 483–516.

[2]We swept in a footnote that we may also need to produce a generator of an ideal.

5. *Cohen H.* A Course in Computational Algebraic Number Theory. Springer Science & Business Media, 2013.
6. *Lemmermeyer F.* The Ambiguous Class Number Formula Revisited. arXiv preprint arXiv:1309.1071,2013.
7. *Kirchner P.* Algorithms on Ideal over Complex Multiplication Order. arXiv preprint arXiv:1602.09037, 2016.
8. *Schoof R.* Computing Arakelov class groups. arXiv preprint arXiv:0801.3835, 2008.
9. *Adleman L. M.* Factoring numbers using singular integers. Proc. 23th Ann. ACM Symp. Theory of Computing, ACM, 1991, pp. 64–71.
10. *Pollard J. M.* Theorems on factorization and primality testing. Math. Proc. of the Cambridge Philosophical Soc., Cambridge Univ. Press, 1974, vol. 76, no. 3, pp. 521–528.
11. *Williams H. C.* A $p + 1$ method of factoring. Math. Computation, 1982, vol. 39, no. 159, pp. 225–234.
12. *Bach E. and Shallit J.* Factoring with cyclotomic polynomials. Math. Computation, 1989, vol. 52, no. 185, pp. 201–219.
13. *Cox D. A.* Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. John Wiley & Sons, 2011, vol. 34.
14. *Klüners J. and Pauli S.* Computing residue class rings and Picard groups of orders. J. Algebra, 2005, vol. 292, no. 1, pp. 47–64.
15. *Buchmann J. A. and Lenstra H. W.* Approximating rings of integers in number fields. J. de théorie des nombres de Bordeaux, 1994, vol. 6, no. 2, pp. 221–260.

UDC 512.772.7 DOI 10.17223/2226308X/11/9

COUNTING POINTS ON HYPERELLIPTIC CURVES OF TYPE $y^2 = x^{2g+1} + ax^{g+1} + bx^1$

S. A. Novoselov

In this work, we investigate hyperelliptic curves of type $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ over the finite field $\mathbb{F}_q$, $q = p^n$, $p > 2$. For the case of $g = 3$ or 4, $p \nmid 4g$ and b is a $4g$-root, we provide efficient methods to compute the number of points in the Jacobian of the curve.

Keywords: *hyperelliptic curves, Cartier — Manin matrix, Legendre polynomials, point counting.*

Let $\mathbb{F}_q$ be a finite field, $q = p^n, p > 2$. Hyperelliptic curves with equation

$$C : y^2 = x^{2g+1} + ax^{g+1} + bx$$

were investigated in [1 – 3]. For genus 2 case it is known [4] that Jacobian of such curves splits into product of certain elliptic curves over some extension of the base field. There are explicit formulae [5] expressing number of points in the Jacobian of curve in terms of traces of Frobenius of elliptic curves.

In this work, we generalize this approach to genus $3, 4$ case combining it with computing Cartier — Manin matrices where it's possible. Using the method of Paulhus [6, 7] we can obtain decompositions of the Jacobian over the extensions of the ground field. The Cartier — Manin matrix of the curve allows us to find the number of points on the curve modulo p.

[1]The reported study was funded by RFBR according to the research project no. 18-31-00244.