MATHEMATICS OF COMPUTATION
Volume 81, Number 279, July 2012, Pages 1663–1668
S 0025-5718(2011)02567-6
Article electronically published on November 15, 2011

CONSTRUCTING IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

SAN LING, ENVER OZDEMIR, AND CHAOPING XING

Abstract. We describe a new method for constructing irreducible polynomials modulo a prime number p. The method mainly relies on Chebotarev's density theorem.

Introduction

Finite fields are the main tools in areas of research such as coding theory and cryptography. In order to do operations in an extension field of degree n over a given base field, one first needs to construct an irreducible polynomial of degree n over the base field. That task is not tedious for fields of small characteristic. In fact, for such fields, it is common to use the Conway polynomials which provide standard notation for extension fields. However, for finite fields with large characteristic, it is time consuming to find Conway polynomials even for small degrees [8]. Hence finding irreducible polynomials in finite fields with large characteristic is still an important task. There are some algorithms presented for this problem ([1], [11], [12]). For example, one of the efficient methods described in [12] constructs an irreducible polynomial through the factorization of some special polynomials over finite fields. However, the method that is mostly used in practice for fields of larger characteristic is the trial-and-error method. Since the density of irreducible polynomials of degree n modulo a prime number p is around $1/n$, the method is efficient especially for small degrees.

The method that we present here is also similar to the trial-and-error method. In our case, we first construct a certain polynomial, which is called the Hilbert class polynomial, of degree n and check if it is irreducible or not. The method is efficient since the probability that a Hilbert class polynomial of degree n is irreducible mod p is $\phi(n)/n$ when n is square-free, where ϕ is Euler's phi function. The probability is again $\phi(n)/n$ for more than 97% of the case when n is odd by Cohen and Lenstra's conjecture [4]. Another advantage of our method is that it might also provide a standardization for fields of larger characteristic as Conway polynomials do for small characteristics. Since some Hilbert class polynomials can be computed and stored in advance, the only task to find an irreducible polynomial of a certain degree is an irreducibility test which can be performed in a very efficient way for the Hilbert class polynomials.

Received by the editor March 5, 2011 and, in revised form, April 11, 2011.

2010 *Mathematics Subject Classification.* Primary 11Y99, 11T06, 11R11, 11Y11.

Key words and phrases. Finite fields, Hilbert class polynomials.

The research was partially supported by the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03 and the Singapore Ministry of Education under Research Grant T208B2206.

The paper is organized as follows. In Section 1, we introduce some preliminaries and basic results on Hilbert class polynomials. Our algorithm will be presented at the beginning of Section 2 and analyses on the probability of success and time complexity are discussed in Subsections 2.1 and 2.2, respectively.

1. Hilbert class polynomials

In this section we briefly introduce Hilbert class polynomials for imaginary quadratic orders. The main reference of this section is [5] and especially Section 5 of [5].

Let K be an imaginary quadratic number field and let $\mathcal{O}_D$ be an order in K with discriminant D. The ideal class group $C(\mathcal{O}_D)$ of $\mathcal{O}_D$ is isomorphic to the group $C(D)$ of the reduced binary quadratic forms of discriminant D. Hence any ideal class I of $C(\mathcal{O}_D)$ is represented by a triple $[A, B, C]$ such that $B^2 - 4AC = D$ and the number $\tau = \frac{-B+\sqrt{D}}{2A}$ is in the standard fundamental domain. The corresponding j value for the ideal I is $j\left(\frac{-B+\sqrt{D}}{2A}\right)$, where $j(\tau)$ is Klein's j-function, and each j value is the j-invariant of an elliptic curve over $\mathbb{C}$ with the endomorphism ring $\mathcal{O}_D$. This implies that there are $h(D)$ isomorphism classes of elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}_D$, where $h(D)$ is the class number of $C(D)$. The extension field L of K generated by these j values is called *the ring class field* for $\mathcal{O}_D$. The extension is finite and has degree $h(D)$. The common minimal polynomial $P_D(x)$ for the j values is called the Hilbert class polynomial for $\mathcal{O}_D$.

The discussion above shows that the Hilbert class polynomial $P_D(x)$ for a discriminant D is $\prod_{i=1}^{h}(x - j(I_i))$, where I_i is an ideal class in $C(\mathcal{O}_D)$ and $h = h(D)$. In the current state of the art, finding the Hilbert class polynomial is a necessary step for constructing elliptic curves over finite fields with a desired endomorphism ring. The classical method to find $P_D(x)$ for given D first searches all positive definite reduced forms $[A_i, B_i, C_i]$ in the group $C(D)$, then computes $j\left(\frac{-B_i+\sqrt{D}}{2A_i}\right)$ with sufficient precision. Since the polynomial $P_D(x)$ has integer coefficients, the result of $\prod_{i=1}^{h}\left(x - j\left(\frac{-B_i+\sqrt{D}}{2A_i}\right)\right)$ with high precision yields the exact value of $P_D(x)$ [13, Chapter 10]. The running time of this method approximately depends on the size of $|D|^{1/2}$ (see [6]). Therefore, the method is not efficient except for small sizes of D. Recent work on constructing Hilbert class polynomials and more details on this subject can be found in [6].

2. Constructing irreducible polynomials

We first present an algorithm for constructing irreducible polynomials modulo a prime number p, then describe the theory behind it. The symbol D represents a discriminant of an order in an imaginary quadratic field.

Algorithm. Input a prime number p and an integer n and output an irreducible polynomial of degree n mod p.

(1) Find a discriminant D such that $(\frac{D}{p}) = 1$, $h(D) = n$ and the class group $C(D)$ is cyclic.
(2) Compute the Hilbert class polynomial $P_D(x)$ for D.
(3) If $P_D(x)$ is irreducible mod p, return $P_D(x)$; else go to Step 1.

2.1. **Irreducibility of Hilbert class polynomials.** In this subsection, we explain why the polynomial $P_D(x)$ is often irreducible modulo a number p. We have the following result from Gauss's class number problem.

Theorem 2.1. *Let n be a positive integer. There exists a discriminant D such that $h(D) = n$.*

For $n \leq 100$, we know all D such that $h(D) = n$ by [15]. For all other n's we know that there exist finitely many D such that $h(D) = n$ [3, Chapter 5].

Lemma 2.2. *Let $D < 0$ be a discriminant and let p be a prime such that $(\frac{D}{p}) = 1$. Let $P_D(x)$ be the Hilbert class polynomial for the order $\mathcal{O}_D$. Then all the irreducible factors of $P_D(x) \bmod p$ have the same degree.*

Proof. Let $K = \mathbb{Q}(\sqrt{D})$ and let L be the ring class field for $\mathcal{O}_D$. The extension is abelian and the Hilbert class polynomial is $P_D(x)$. Since $(\frac{D}{p}) = 1$, the prime p splits completely in the ring of integers $\mathcal{O}_K$ of K, i.e., we have $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are conjugate prime ideals in the ring $\mathcal{O}_K$. As L is Galois over the field K, the inertial degrees of the primes above $\mathfrak{p}$ in the ring of integers $\mathcal{O}_L$ of L are all equal. This means that the degrees of the irreducible factors of $P_D(x) \bmod \mathfrak{p}$ in $\mathcal{O}_K$ are all the same. Since $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p] = 1$, the inertial degree is equal to the degree of the irreducible factors of $P_D(x) \bmod p$. □

Let K, $P_D(x)$, L, $\mathcal{O}_D$ be the same as above. Suppose that

$$[L : K] = n = \deg(P_D(x)).$$

Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the rings of integers of the fields K and L, respectively. The proposition below shows that by using Chebotarev's density theorem, it is possible to give the density of primes $\mathfrak{p}$ in $\mathcal{O}_K$ which are inert in $\mathcal{O}_L$.

Proposition 2.3. *Let G =Gal(L/K) be the Galois group of the field extension L/K. If the group G is cyclic, then the density of primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that $P_D(x)$ is irreducible mod $\mathfrak{p}$ is $\phi(n)/n$ where ϕ is Euler's phi function.*

Proof. Let $\sigma_\mathfrak{p}$ be the Artin symbol corresponding to the prime $\mathfrak{p}$. Then $\mathfrak{p}$ splits into $[G : \langle\sigma_\mathfrak{p}\rangle]$ primes in L (see [2, Proposition 2.3 on page 165]). Thus, if $\sigma_\mathfrak{p}$ is a generator of G, then $\mathfrak{p}$ is inert in L/K and hence the polynomial $P_D(x)$ is irreducible over the residue class field $O_K/\mathfrak{p}$. On the other hand, for a fixed generator σ of G, by Chebotarev's density theorem [10, Theorem 3.1], the density of primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that $\sigma_\mathfrak{p} = \sigma$ is $1/n$ since G is commutative and the conjugacy class of σ contains only one element. Therefore, the density of primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that $\sigma_\mathfrak{p}$ is a generator of the group G (or $P_D(x) \bmod \mathfrak{p}$ is irreducible) is $\phi(n)/n$ as there are $\phi(n)$ generators of G. □

Let p be a prime number such that D is a quadratic residue mod p. Suppose that $\mathfrak{p}$ in $\mathcal{O}_K$ divides $p\mathcal{O}_K$. Since $(D/p) = 1$, the prime p splits completely in $\mathcal{O}_K$ and we have $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p] = 1$. Hence, the factorization pattern of the polynomial $P_D(x) \bmod \mathfrak{p}$ is the same as the factorization pattern of it mod p. Therefore the probability that $P_D(x)$ is irreducible mod p is equal to the probability that $P_D(x)$ is irreducible mod $\mathfrak{p}$ where $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. For example, if the degree of $P_D(x) = n$ is prime and $(D/p) = 1$, then the probability that $P_D(x)$ is irreducible mod p is $(n-1)/n$; and if n is square-free, then the probability is $\phi(n)/n$ since G=Gal(L/K) is cyclic for both cases.

As for the other n, the probability depends on the structure of $\mathrm{Gal}(L/K)$ which is isomorphic to the class group $C(D)$ of discriminant D. For instance, if n is odd for a random D with $h(D) = n$, the group $C(D)$ has more than a 97% chance to be cyclic based on a conjecture (see [4] and [3, Conjecture 5.10.1]). As for even non-square-free n's, again we have more than a 97% chance that the odd part $C_0(D)$ of the class group $C(D)$ is cyclic by [4]. The subgroup $C_0(D)$ consists of elements in $C(D)$ of odd order. We should also note that in practice it is not hard to check whether the group $C(D)$ (or $\mathrm{Gal}(L/K)$) is cyclic for a random D by assuming $h(D)$ is not too large. This can be done efficiently by the method described in [7] or by any method described in Section 5.4 of [3]. For example, for $n = 128$, there are 10 discriminants D with $h(D) = n$ in the first 28 such discriminants such that $C(D)$(=$\mathrm{Gal}(L/K)$) is cyclic. The ratio is 10 to 39 for $n = 256$, 10 to 20 for $n = 144$, 10 to 42 for $n = 512$ and 10 to 15 for $n = 1024$. Therefore, in practice one can compute and store the first 10 discriminants D for each $n < 10000$ such that the class group $C(D)$ is cyclic.

2.2. **The running time.** For a given integer n, $|D|$ is approximately n^2 by [3] and if n is odd, then $|D|$ must be a prime number. The efficient methods described in [3, Section 5.4] and [7] for computing class numbers also give the structure of the class group while computing the class numbers. Note that the class group $C(D)$ is always cyclic when n is square-free and 97% of the time when n is odd [4]. Hence searching D can be performed efficiently. We should also note that one might need to work with extensions of degree at most 5000 (or maybe 10000) of fields of large (more than 5 digits) characteristic, since in practice computing in an extension field of degree more than 5000 is a time consuming task. Hence, we might assume that the degree n is at most around 10000. The time complexity of constructing $P_D(x)$ is $O(n^2)$ [6]. Therefore, in terms of time complexity, the dominating step is Step 3 for large primes. The following lemma suggests that Step 3 can also be performed efficiently by using a method similar to that in [9]. Then the running time of this step is $O(n^\beta \log p)$ with $\beta < 1.9$.

Lemma 2.4. *Let $P_D(x)$ be the Hilbert class polynomial with degree n for a discriminant D and let p be a prime number such that $(\frac{D}{p}) = 1$. If n is prime, then $P_D(x)$ is irreducible* mod$p$ *if and only if* $\gcd(x^p - x, P_D(x)) = 1$. *If n is composite such that $n = ab$ with $1 < a < n$, then $P_D(x)$ is irreducible* mod p *if and only if* $\gcd(x^{p^a} - x, P_D(x)) = 1$ *and* $\gcd(x^{p^b} - x, P_D(x)) = 1$.

Proof. See [3, Proposition 3.4.4] and Lemma 2.2. □

In the current state of the art, the method that is mostly being used in practice to find an irreducible polynomial over fields of large characteristic is the trial-and-error method. This method also works since the density of irreducible polynomials of degree n is around $1/n$ mod any prime p [12]. Although our algorithm also needs to check if a polynomial is irreducible or not, the probability of success in our case is $\phi(n)/n$ for most of the time. Although $O(n^\beta \log p)$ with $\beta < 1.9$ is efficient enough to determine an irreducible polynomial, one may reduce the running time by avoiding any polynomial arithmetic in Step 3. The following observation might lead one to achieve this.

Theorem 2.5. *Let $D < 0$ be a negative discriminant and let $P_D(x)$ be the corresponding Hilbert class polynomial. If $P_D(x)$ has a root in the field $\mathbb{F}_q$, then there* *exists an integer t such that $|t| < 2q$ and $(t+2q, t-2q)$ is either of the form (b^2, Dy^2) or $(2b^2, 2Dy^2)$ for some integers b and y, where $q = p^r$ and $(\frac{D}{p}) = 1$.*

Proof. That $P_D(x)$ has a root in $\mathbb{F}_q$ implies that $P_D(x)$ splits completely over $\mathbb{F}_q$. Each root gives the j-invariant of an elliptic curve with endomorphism ring $\mathcal{O}_D$. Let E be one of these elliptic curves over $\mathbb{F}_q$. The curve E is also defined over $\mathbb{F}_{q^2}$. Let $t = q^2 + 1 - \#E(\mathbb{F}_{q^2})$. The discriminant D_1 of the q^2th Frobenius morphism lies in $\mathcal{O}_D$ hence $D_1 = t^2 - 4q^2 = (t-2q)(t+2q) = v^2 D$ for some integer v. Since the curve E is not supersingular, $\gcd(t,p) = 1$. Therefore $(t-2q)$ is of the form y^2D or $2y^2D$ for some integer y. □

Corollary 2.6. *Let p and n be primes such that $n = h(D)$ for some discriminant $D < 0$. Let $P_D(x)$ be the Hilbert class polynomial for $\mathcal{O}_D$. Then $P_D(x)$ has a root* mod p *if and only if there exists an integer t such that $|t| \leq 2p$ and $(t+2p, t-2p)$ is either of the form (b^2, Dy^2) or $(2b^2, 2Dy^2)$ for some integer b and y.*

Acknowledgments

The authors are grateful to the anonymous referee for his/her invaluable comments and suggestions. Without these suggestions, the paper could not have appeared in the current form.

References

1. L. Adleman and H. Lenstra, Finding irreducible polynomials over finite fields, Proc. 18th Annual ACM Symp. on Theory of Computing, 350-355.
2. J. W. S. Casseles and A. Fröhlich, Algebraic Number Theory, Academic Press, London and New York, 1967. MR0215665 (35:6500)
3. H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, 2000. MR1228206 (94i:11105)
4. H. Cohen, H. W. Lenstra , Heuristics on class groups of number fields, Number Theory, Noordwijkerhout 1983, Lecture Notes in Math. 1068, Springer-Verlag, 1984, 33-62. MR756082 (85j:11144)
5. David A. Cox, Primes of the form $x^2 + ny^2$ - Fermat, class field theory, and complex multiplication, John Wiley & Sons, New York, 1989. MR1028322 (90m:11016)
6. Andreas Enge, The complexity of class polynomial computation via floating point approximations. Mathematics of Computation 78 (266), 2009, pp. 1089-1107. MR2476572 (2010h:11097)
7. J. Hafner and K. McCurley, A rigorous subexponential algorithm for computation of class groups, Journal of American Math. Soc. 2 (1989), 837-850. MR1002631 (91f:11090)
8. L. S. Heath, N. A. Comman, New algorithms for generating Conway polynomials over finite fields, SODA 99, Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms.
9. E. Kaltofen, V. Shoup, Subquadratic-time factoring of polynomials over finite fields. Math. Comput., 67(223):1179-1197, 1998. MR1459389 (99m:68097)
10. H. Lenstra, The Chebotarev Density Theorem, Algebra Lecture Notes: `http://websites.math.leidenuniv.nl/algebra/Lenstra-Chebotarev.pdf`
11. Rabin, M., Probabilistic algorithms in finite fields, SIAM Journal of Computing, vol. 9, no. 2, 273-280. MR568814 (81g:12002)
12. V. Shoup, New algorithms for finding irreducible polynomials over finite fields, Mathematics of Computation 54:435-447, 1990. MR993933 (90j:11135)
13. L. C. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd edition. Chapman & Hall/CRC 2008. MR2404461 (2009b:11101)

14. W. W. Waterhouse, Abelian varieties over finite fields, Ann. Scient. Ec. Norm. Sup., (4), 1969, 521-560. MR0265369 (42:279)
15. M. Watkins, Class numbers of imaginary quadratic fields, Mathematics of Computation, Volume 73, Number 246, 907-938. MR2031415 (2005a:11175)

Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore
E-mail address: lingsan@ntu.edu.sg

Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore
E-mail address: eozdemir@ntu.edu.sg

Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore
E-mail address: xingcp@ntu.edu.sg