Advances in Mathematics of Communications
Volume X, No. 0X, 200X, X–XX
Web site: http://www.aimSciences.org

SOME REMARKS ON THE CONSTRUCTION OF CLASS POLYNOMIALS

Elisavet Konstantinou

Department of Information and Communication Systems Engineering
University of the Aegean, 83200, Samos, Greece

Aristides Kontogeorgis

Department of Mathematics
University of Athens, Panepistimioupolis 15784, Athens, Greece

(Communicated by Aim Sciences)

Abstract. Class invariants are singular values of modular functions which generate the class fields of imaginary quadratic number fields. Their minimal polynomials, called class polynomials, are uniquely determined by a discriminant $-D < 0$ and are used in many applications, including the generation of elliptic curves. In all these applications, it is desirable that the size of the polynomials is as small as possible. Among all known class polynomials, Weber polynomials constructed with discriminants $-D \equiv 1 \pmod 8$ have the smallest height and require the least precision for their construction. In this paper, we will show that this fact does not necessarily lead to the most efficient computations, since the congruences modulo 8 of the discriminants affect the degrees of the polynomials.

1. Introduction

The most commonly used application of class polynomials is the generation of elliptic curves via the Complex Multiplication (CM) method [10]. In the original version of the method, a special polynomial called Hilbert class polynomial is constructed with input a fundamental discriminant $d < 0$. A discriminant $d < 0$ is fundamental if and only if d is free of any odd square prime factors and either $-d \equiv 3 \pmod 4$ or $-d/4 \equiv 1, 2, 5, 6 \pmod 8$. The disadvantage of Hilbert class polynomials is that their coefficients grow very large as the absolute value of the discriminant $D = |d|$ increases and thus their construction requires high precision arithmetic.

Let K be an imaginary quadratic field of discriminant d with ring of integers $\mathcal{O} = \mathbb{Z}[\theta]$. According to the first main theorem of complex multiplication, the modular function $j(\theta)$ generates the Hilbert class field over K. However, the Hilbert class field can also be generated by modular functions of higher level. If f is a modular function, we will call the value $f(\theta)$ a *class invariant* if $f(\theta)$ and $j(\theta)$ generate the same field over K. If $f(\theta)$ is a class invariant then its minimal polynomial over K is called *class polynomial*.

2000 *Mathematics Subject Classification:* Primary: 11R29; Secondary: 94A60,11T71.
Key words and phrases: Class Polynomials, Precision Estimates, Experimental Results, Generation of Elliptic Curves.

There are several known families of class polynomials having integer coefficients which are much smaller than the coefficients of their Hilbert counterparts. Therefore, they can substitute Hilbert class polynomials in the CM method and their use can considerably improve its efficiency. Some well known families of class polynomials are: Weber polynomials [15], $M_{D,l}(x)$ polynomials [11], Double eta (we will denote them by $M_{D,p_1,p_2}(x)$) polynomials [6] and Ramanujan polynomials [8]. The logarithmic height of the coefficients of all these polynomials is smaller by a constant factor than the corresponding logarithmic height of the Hilbert class polynomials and this is the reason for their much more efficient construction.

A crucial question is which polynomial leads to the most efficient construction. Possibly, one cannot give the correct answer without taking into consideration the algorithm to be used. There are three approaches to computing class polynomials; the complex analytic method [4], the p-adic method [3] and a method based on the Chinese remainder theorem [2, 7, 16]. We follow the first method which is the classical approach to computing class polynomials and is based on floating point approximations of their roots. Our results are also useful for the other two methods, but might not always be applicable *.

Thus, in our case, the answer to the above question can be derived by the precision requirements of the polynomials or (in other words) the logarithmic height of their coefficients. There are asymptotic bounds which estimate with remarkable accurancy the precision requirements for the construction of the polynomials. The polynomials with the smallest (known so far) asymptotic bound are Weber polynomials constructed with discriminants d satisfying the congruence $D = |d| \equiv 7 \pmod 8$. Naturally, this leads to the conclusion that these polynomials will require less precision for their construction than all other class polynomials constructed with values D' close enough to the values of D.

In this paper, we will show that this is not really true in practice. Clearly, the degrees of class polynomials vary as a function of D, but we will see that on average these degrees are affected by the congruence of D modulo 8. In particular, we establish with extensive experimental assessments that on average, class polynomials (with degree equal to their Hilbert counterparts) constructed with values $D \equiv 3 \pmod 8$ have three times smaller degree than polynomials constructed with comparable in size values of D that satisfy the congruence $D \equiv 7 \pmod 8$. Class polynomials with even discriminants (e.g. $D \equiv 0 \pmod 4$) have on average two times smaller degree than polynomials constructed with comparable in size values $D \equiv 7 \pmod 8$. This phenomenon is proved theoretically and we generalize it for congruences of D modulo larger numbers. This leads to the (surprising enough) result that there are families of polynomials which seem to have asymptotically larger precision requirements for their construction than Weber polynomials with $D \equiv 7 \pmod 8$, but they can be constructed more efficiently than them in practice (for comparable values of D).

*The cost of constructing a class polynomial is proportional to its precision requirements for the complex analytic method. However, we can not always assume that for the CRT method. See for example in [7, §5.2] how a polynomial with degree 149299 can be constructed faster than a polynomial with degree 16259.

2. Class Polynomials and Their Degrees

It is known that the class number of an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ of discriminant $-D < -4$ is given by the formula [14, p. 436]

$$h_D = \frac{\sqrt{D}}{2\pi} L(1,\chi) = \frac{\sqrt{D}}{2\pi} \prod_p \left(1 - \frac{\chi(p)}{p}\right)^{-1},$$

where χ is the quadratic character defined by $\chi(x) = \left(\frac{-D}{x}\right)$. Let us now consider the Euler factor

$$\left(1 - \frac{\chi(p)}{p}\right)^{-1} = \begin{cases} 1 & \text{if } p \mid D \\ \frac{p}{p-1} & \text{if } \left(\frac{-D}{p}\right) = 1 \\ \frac{p}{p+1} & \text{if } \left(\frac{-D}{p}\right) = -1. \end{cases} \tag{1}$$

Observe that smaller primes have a bigger influence on the value of h_D. For example if $p = 2$ then we compute

$$\left(1 - \frac{\chi(2)}{2}\right)^{-1} = \begin{cases} 1 & \text{if } 2 \mid D \\ 2 & \text{if } D \equiv 7 \pmod 8 \\ \frac{2}{3} & \text{if } D \equiv 3 \pmod 8. \end{cases}$$

This leads us to the conclusion that on average the degree of a class polynomial with $D \equiv 3 \pmod 8$ will have three times smaller degree than a polynomial constructed with a comparable value of $D \equiv 7 \pmod 8$. Similarly, the degree of a polynomial constructed with even values of $D \equiv 0 \pmod 4$ will have on average two times smaller degree than a polynomial with $D \equiv 7 \pmod 8$ [†].

In order to verify this argument in practice, we conducted some experiments with several values of D. In particular, we computed the degrees of all polynomials with $D \equiv 7 \pmod 8$ starting from the value $D = 3{,}928{,}167$ to the value $D = 327{,}680{,}103$ adding every time a step of 40960. This means that we computed the degrees of approximately $8,000$ class polynomials with $D \equiv 7 \pmod 8$. We repeated the same process for all congruences $D \equiv 3 \pmod 8$ and $D/4 \equiv 1, 2, 5, 6 \pmod 8$. Then, for every congruence, we calculated the mean value of every 100 values of degrees. The result of our experiments is summarized in Figure 2. We notice that indeed the degrees of the polynomials are affected by the congruences of D. The results for all even values of D are almost identical.

In order to see the relation between the class numbers for all congruences modulo 8 of the discriminants, we calculated the values $r(D) = h(P_{D \equiv 7 \pmod 8)})/h(P_{D' \not\equiv 7 \pmod 8)})$ where $h(P_D)$ is the degree of the class polynomial P_D constructed with discriminant $-D$ and $-D'$ is the closest discriminant to the value $-D$ (e.g. for $D = 32{,}871 \equiv 7 \pmod 8$ the closest discriminant $D' \equiv 3 \pmod 8$ is equal to 32,883). In Figure 2 we see the mean values of $r(D)$ for every 100 values of discriminants. As expected, the ratio $r(D)$ is very close to 2 for even discriminants and close to 3 for discriminants $D \equiv 3 \pmod 8$.

Going back to Eq. (1), we can see that for discriminants of the same congruence modulo 8, we can proceed to the next prime $p = 3$ and compute

$$\left(1 - \frac{\chi(3)}{3}\right)^{-1} = \begin{cases} 1 & \text{if } 3 \mid D \\ \frac{3}{2} & \text{if } \left(\frac{-D}{3}\right) = 1 \\ \frac{3}{4} & \text{if } \left(\frac{-D}{3}\right) = -1. \end{cases}$$

[†] We suppose that the degree of every class polynomial is equal to the degree of the corresponding Hilbert class polynomial.

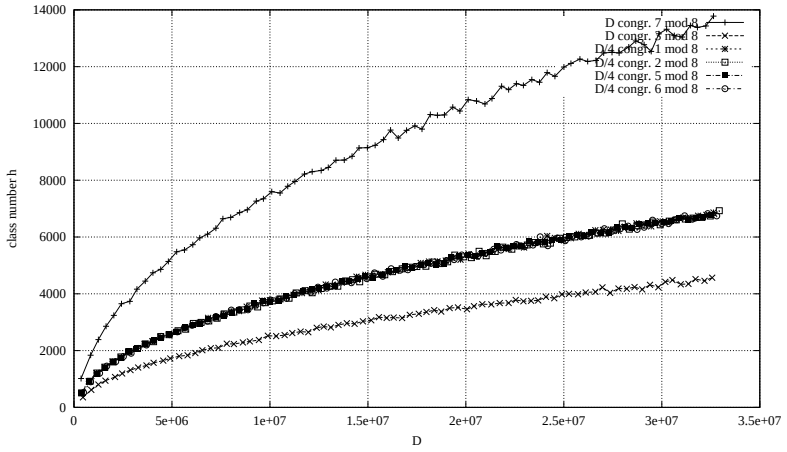

FIGURE 1. Degrees of polynomials for various D.

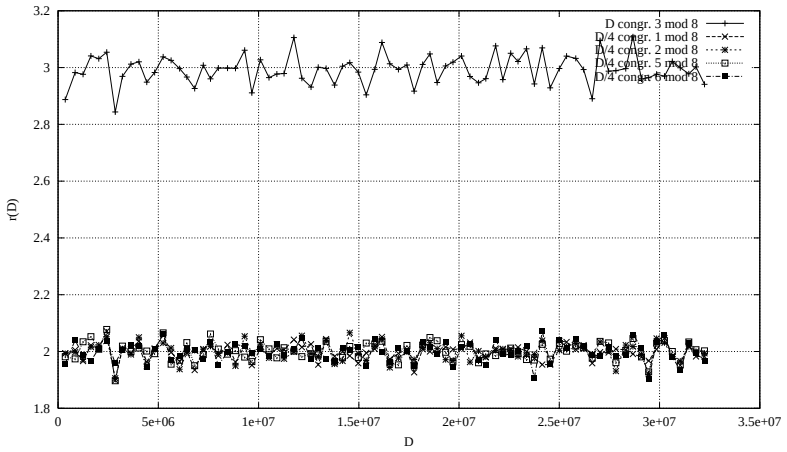

FIGURE 2. Values $r(D)$ for various D.

This means that for values of D such that $\left(\frac{-D}{3}\right) = -1$ the value of h_D is on average two times smaller than class numbers corresponding to values with $\left(\frac{-D}{3}\right) = 1$. Consider for example, the cases $D \equiv 3 \pmod 8$ and $D \equiv 7 \pmod 8$. If we now include in our analysis the prime $p = 3$, then we can distinguish 6 different subcases $D \equiv 3, 11, 19 \pmod{24}$ and $D \equiv 7, 15, 23 \pmod{24}$. Having in mind the values $\left(1 - \frac{\chi(2)}{2}\right)^{-1}$ and $\left(1 - \frac{\chi(3)}{3}\right)^{-1}$, we can easily see for example that the polynomials with $D \equiv 19 \pmod{24}$ will have on average 6 times smaller degrees than the polynomials with $D \equiv 23 \pmod{24}$. This is experimentally verified as it can be seen in Figure 2 where we have included the cases $D \equiv 7, 11, 19, 23 \pmod{24}$.

What happens if we continue selecting larger primes p? Eq. (1) implies that if we select a discriminant $-D$ such that for all primes $p < N$ we have $\left(\frac{-D}{p}\right) = -1$ then the class number corresponding to D has a ratio that differ from other discriminants

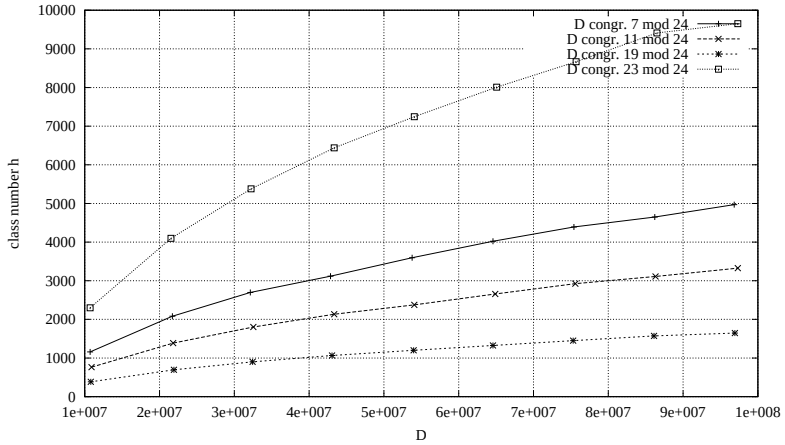

FIGURE 3. Degrees of polynomials for various D.

by a factor of at most

$$\prod_{p<N}\left(\frac{p-1}{p+1}\right)=\prod_{p<N}\left(1-\frac{2}{p+1}\right). \tag{2}$$

Since the series $\sum_p \frac{2}{p+1}$ diverges (p runs over the prime numbers), the product in Eq. (2) diverges as well [1, p.192 th. 5]. Therefore, the product in Eq. (2) can have arbitrarily high values for sufficiently large values of N.

Example: We observe first that the product in Eq. (2) converges very slowly. If we consider the primes which are smaller than 100, then we gain a factor of about 42. With the aid of magma [13] we consider all Euler factors for all primes $p < 100$. A discriminant that contributes to a small class number is then computed using Chinese remainder theorem (e.g. satisfying for all primes $p < 100$ the equation $\left(\frac{-D}{p}\right) = -1$) and equals to $D_{small} = 124314131120033571095603525318269576 3$ and we do the same for finding a discriminant $D_{big} = 17067248000875193685413241799269616 79$ which contributes to a big class number (e.g. satisfying for all primes $p < 100$ the equation $\left(\frac{-D}{p}\right) = 1$). Actually we have that $h(D_{small}) = 66948034227303296$ and $h(D_{big}) = 3093012003194938688$ while $h(D_{big})/h(D_{small}) \sim 46.2$. Clearly, these values of D are far beyond the range of any feasible computation but are interesting from an asymptotic perspective. In particular, the current record for the complex analytic method is $|D| \sim 10^{10}$ and for the CRT method is $|D| \sim 10^{15}$.

In the next section, we will see how the above results affect the precision requirements for the construction of class polynomials.

3. Precision Requirements for the Construction of the Polynomials

Let f be a modular function, such that $f(\tau)$ for some $\tau \in \mathbb{Q}(\sqrt{-D})$ generates the Hilbert class field of $\mathbb{Q}(\sqrt{-D})$. It was shown in [5] that the logarithmic height of class polynomials for different functions f is smaller by a *constant factor* than the corresponding logarithmic height of the Hilbert class polynomials. If j is the modular function used for the construction of Hilbert class polynomials, then this constant factor depends on the degrees of f and j of the modular polynomial which

D	prec. estimate
$D \equiv 7 \pmod 8$	$\frac{1}{72}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$D \equiv 3 \pmod 8$	$\frac{1}{24}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$D/4 \equiv 1,2,6 \pmod 8$	$\frac{1}{36}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$D/4 \equiv 5 \pmod 8$	$\frac{1}{18}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$

TABLE 1. Precision estimates for $D \not\equiv 0 \pmod 3$.

D	prec. estimate
$D \equiv 7 \pmod 8$	$\frac{1}{24}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$D \equiv 3 \pmod 8$	$\frac{1}{8}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$D/4 \equiv 1,2,6 \pmod 8$	$\frac{1}{12}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$D/4 \equiv 5 \pmod 8$	$\frac{1}{6}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$

TABLE 2. Precision estimates for $D \equiv 0 \pmod 3$.

connects these functions. A heuristic estimate of the logarithmic height of Hilbert class polynomials is given by [5]:

$$\text{H-Prec}(D) \approx \frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$$

with the sum running over the values A of all primitive reduced quadratic forms of $-D$. As it was indicated in [5], the above equation is a very accurate estimate of the precision requirements for the construction of a Hilbert class polynomial.

The class polynomials with the smallest (known so far) logarithmic height are Weber polynomials constructed by discriminants d with $D = |d| \equiv 7 \pmod 8 \not\equiv 0 \pmod 3$. Depending on the congruences of D, ten cases of Weber polynomials are defined. In particular, estimates of the precision requirements of all Weber polynomials are given in Tables 1 and 2. We would like to note that Weber polynomials constructed from values $D \equiv 3 \pmod 8$ have three times larger degree than their corresponding Hilbert class polynomials. However, this factor was considered in the computation of the precision estimate (see [9] for more details).

It was also concluded in [5] that the precision required for the construction of the $M_{D,l}(x)$ polynomials is approximately $\frac{1}{(l+1)}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$ and for $M_{D,p_1,p_2}(x)$ polynomials is approximately $\frac{(p_1-1)(p_2-1)}{12(p_1+1)(p_2+1)}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$. Finally, for the newly introduced Ramanujan polynomials $T_D(x)$ which are defined only for values $D \equiv 11 \pmod{24}$, their logarithmic height is approximately $\frac{1}{36}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$. The above precision estimates are summarized in Table 3 for some cases of l, p_1 and p_2.

Let $S(D) = \sum_{[A,B,C]}\frac{1}{A}$. We calculated all values $S(D)$ for the same discriminants we used in Figure 2 and 2 and then computed the mean values for every group of consecutive 100 discriminants. Our results are summarized in Figure 3. As it was expected, the values of $S(D)$ are bigger on average for discriminants $D \equiv 7 \pmod 8$ and smaller for $D \equiv 3 \pmod 8$. The values for $D \equiv 7 \pmod 8$ are approximately 1.8 times bigger than the corresponding values for even discriminants and 2.7 times bigger than discriminants $D \equiv 3 \pmod 8$. Notice that the values 1.8 and 2.7 are

class polynomial	precision estimate
$M_{D,3}(x)$	$\frac{1}{4}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$M_{D,5}(x)$	$\frac{1}{6}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$M_{D,7}(x)$	$\frac{1}{8}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$M_{D,13}(x)$	$\frac{1}{14}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$M_{D,5,7}(x)$	$\frac{1}{24}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$M_{D,3,13}(x)$	$\frac{1}{28}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$
$T_D(x)$	$\frac{1}{36}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$

TABLE 3. Precision estimates for $M_{D,l}(x)$, $M_{D,p_1,p_2}(x)$ and $T_D(x)$ polynomials.

quite close to the values $r(D)$ in Figure 2. Clearly, this difference in the values of $S(D)$ affects also the precision requirements for the construction of the polynomials.

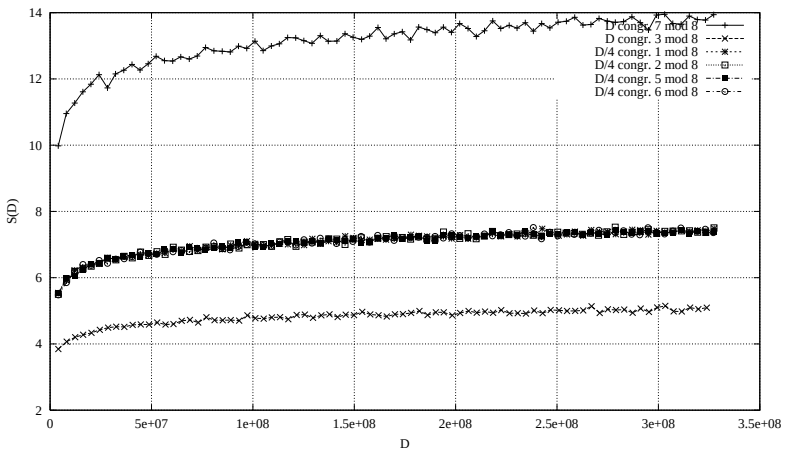

FIGURE 4. Values of $S(D)$ for various D.

In order to compare the precision requirements for the construction of different class polynomials for similar values of D, we discarded the value $\frac{\pi\sqrt{D}}{\ln 2}$ from the logarithmic height and multiply every value $S(D)$ with 72 (since $\frac{1}{72}\frac{\pi\sqrt{D}}{\ln 2}S(D)$ is the smallest logarithmic height known so far for all class polynomials). We used for our comparison the precision requirements for Weber polynomials with $D \equiv 7 \pmod 8$, $D \equiv 3 \pmod 8$ and $D/4 \equiv 1, 2, 5, 6 \pmod 8$ (see Table 1) and for Ramanujan polynomials with $D \equiv 11 \pmod{24}$. We computed all values $P(D) = 72 \cdot S(D)$ for the same discriminants we used in all previous figures. Our results are summarized in Figure 3.

We notice that Weber polynomials with $D/4 \equiv 5 \pmod 8$ have the largest precision requirements and this is also obvious from Table 1. Weber polynomials with $D \equiv 3 \pmod 8$, $D/4 \equiv 1, 2, 6 \pmod 8$ and $D \equiv 7 \pmod 8$ have quite similar precision requirements. Taking a careful look in Table 1 we will see that the theoretical estimates are equal to $\frac{1}{24}\frac{\pi\sqrt{D}}{\ln 2}S(D)$, $\frac{1}{36}\frac{\pi\sqrt{D}}{\ln 2}S(D)$ and $\frac{1}{72}\frac{\pi\sqrt{D}}{\ln 2}S(D)$ respectively.

However, the precision requirements are so close in practice for similar values of D because of the difference on the mean values of the degrees of polynomials for different congruences of the discriminants [‡]. This actually led to the surprising result that Ramanujan polynomials which are constructed with $D \equiv 11 \pmod{24} \equiv 3 \pmod 8$ require much smaller precision for their construction than the (theoretically best) Weber polynomials with $D \equiv 7 \pmod 8$.

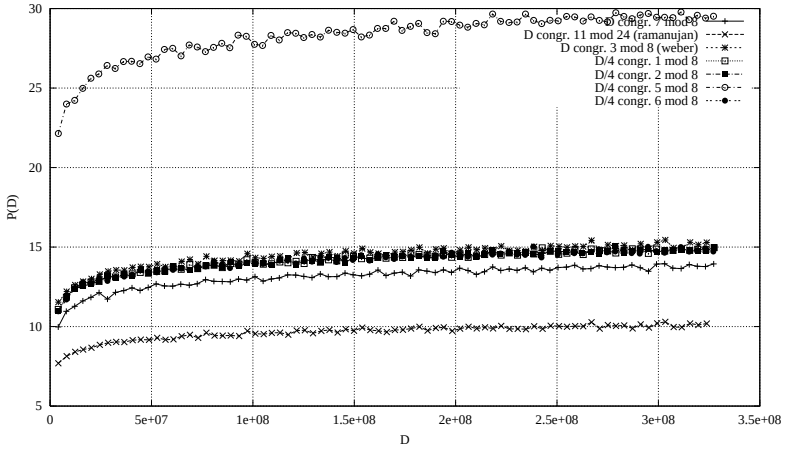

FIGURE 5. Relative precision requirements of all polynomials for various D.

Following our experimental results, we can give the next conjecture:

Conjecture 1. *Suppose that the precision requirements for the construction of a class polynomial are equal to* $\frac{1}{x}\frac{\pi\sqrt{D}}{\ln 2}S(D)$. *Then, if the discriminant* D *is even and* x *is larger than 40, the class polynomial is constructed more efficiently (on average) than the corresponding Weber polynomials with similar in size values of* $D \equiv 7 \pmod 8 \not\equiv 0 \pmod 3$. *The same argument is true also in the case that the discriminant satisfies the congruence* $D \equiv 3 \pmod 8$ *and* x *is larger than 26.*

For example, the double eta polynomials $M_{D',3,13}(x)$ are constructed on average more efficiently than Weber polynomials with $D \equiv 7 \pmod 8$ for comparable values of $D' \equiv 3 \pmod 8$ even though their theoretical precision requirements are equal to $\frac{1}{28}\frac{\pi\sqrt{D}}{\ln 2}S(D)$ and thus much smaller than $\frac{1}{72}\frac{\pi\sqrt{D}}{\ln 2}S(D)$ (which is the theoretical estimate for Weber polynomials).

Class polynomials can also be constructed with the use of Atkin functions A_N [7, 12]. The function A_{71} leads to the most efficient constructions among the Atkin functions and the corresponding polynomials $A_{71,D}(x)$ require $\frac{1}{36}\frac{\pi\sqrt{D}}{\ln 2}\sum_{[A,B,C]}\frac{1}{A}$ bit precision for their computation. Polynomials $A_{71,D}(x)$ can be constructed from every value D such that $\left(\frac{-D}{71}\right) \neq 1$ and this gives an additional flexibility compared to Ramanujan polynomials which have the same precision requirements but require that $D \equiv 11 \pmod{24}$. Finally, another advantage of Atkin functions is that if D is divisible by N then one may use the square root of its class polynomial. Thus, if one

[‡]Notice that the ratio $r(D)$ computed in Section 2 is close to 3 for discriminants with $D \equiv 3 \pmod 8$ and close to 2 for even discriminants.

picks $D \equiv 0 \pmod{71}$ and the Atkin function A_{71}, the corresponding polynomials would yield better results than all the other alternatives.

4. Conclusions

We have presented extensive experimental results regarding the degrees of several class polynomials and their precision requirements. We have shown that the congruence modulo 8 of the discriminant is crucial for the size of the polynomials and this affects the efficiency of the construction of the polynomials. The theoretical estimates of the logarithmic height of the polynomials (and thus of the precision requirements for their construction) give us a ranking of the polynomials but this is not enough in practice. We have seen that there are polynomials which have asymptotically larger precision requirements in theory, but they are constructed more efficiently in practice. We believe that our results are very useful for everyone who wishes to construct class polynomials and needs to make his/her computations as efficient as possible.

Acknowledgements

We would like to thank the referees very much for their valuable comments and suggestions.

`<ekonstantinou@aegean.gr; kontogar@math.uoa.gr>`

References

[1] L. V. Ahlfors, *Complex analysis. An introduction to the theory of analytic functions of one complex variable*, 3rd edition, International Series in Pure and Applied Mathematics, McGraw-Hill Book Co., New York, 1978.

[2] J. Belding, R. Bröker, A. Enge, and K. Lauter, Computing Hilbert class polynomials, in *Algorithmic Number Theory Symposium* - ANTS 2008, Lecture Notes in Computer Science Vol. 5011, Springer-Verlag (2008), 282–295.

[3] R. Bröker, A p-adic algorithm to compute the Hilbert class polynomial, *Mathematics of Computation*, **77** (2008), 2417–2435.

[4] A. Enge, The complexity of class polynomial computation via floating point approximations, *Mathematics of Computation*, **78** (2009), 1089–1107.

[5] A. Enge and F. Morain, Comparing invariants for class fields of imaginary quadratic fields, in *Algorithmic Number Theory Symposium* – ANTS 2002, Lecture Notes in Computer Science Vol. 2369, Springer-Verlag (2002), 252–266.

[6] A. Enge and R. Schertz, Constructing elliptic curves over finite fields using double eta-quotients, *J. Théor. Nombres Bordeaux*, **16** (2004), 555–568.

[7] A. Enge and A. V. Sutherland, Class invariants for the CRT method, in *Algorithmic Number Theory Symposium* - ANTS 2010, Lecture Notes in Computer Science Vol. 6197, Springer-Verlag (2010), 142–156.

[8] E. Konstantinou and A. Kontogeorgis, Computing Polynomials of the Ramanujan t_n Class Invariants, in *Canadian Mathematical Bulletin*, **52** (2009), 583–597.

[9] E. Konstantinou and A. Kontogeorgis, Ramanujan's Class Invariants and Their Use in Elliptic Curve Cryptography, in *Computers and Mathematics with Applications*, **59** (2010), Elsevier, 2901–2917.

[10] G.J. Lay and H. Zimmer, Constructing Elliptic Curves with Given Group Order over Large Finite Fields, in *Algorithmic Number Theory* – ANTS-I, Lecture Notes in Computer Science Vol. 877, Springer-Verlag (1994), 250–263.

[11] F. Morain, Modular curves and class invariants, *Preprint,* June 2000.

[12] F. Morain, Advances in the CM method for elliptic curves, *Slides of Fields Cryptography Retrospective Meeting*, May 11-15, 2009, `http://www.lix.polytechnique.fr/ morain/Exposes/fields09.pdf`.

[13] W. Bosma, J. Cannon, and C. Playoust, The Magma Algebra System I: The User Language, *J. Symbolic Comput.*, **24** (1997), 235–265.
[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd edition, Springer-Verlag, 1990.
[15] R. Schertz, Weber's class invariants revisited, *Journal de Théorie des Nombres de Bordeaux*, **4** (2002), 325–343.
[16] A. V. Sutherland, Computing Hilbert class polynomials with the Chinese Remainder Theorem, *Mathematics of Computation* (2009), to appear, `http://arxiv.org/abs/0903.2785`.

Received September 2004; revised February 2005.