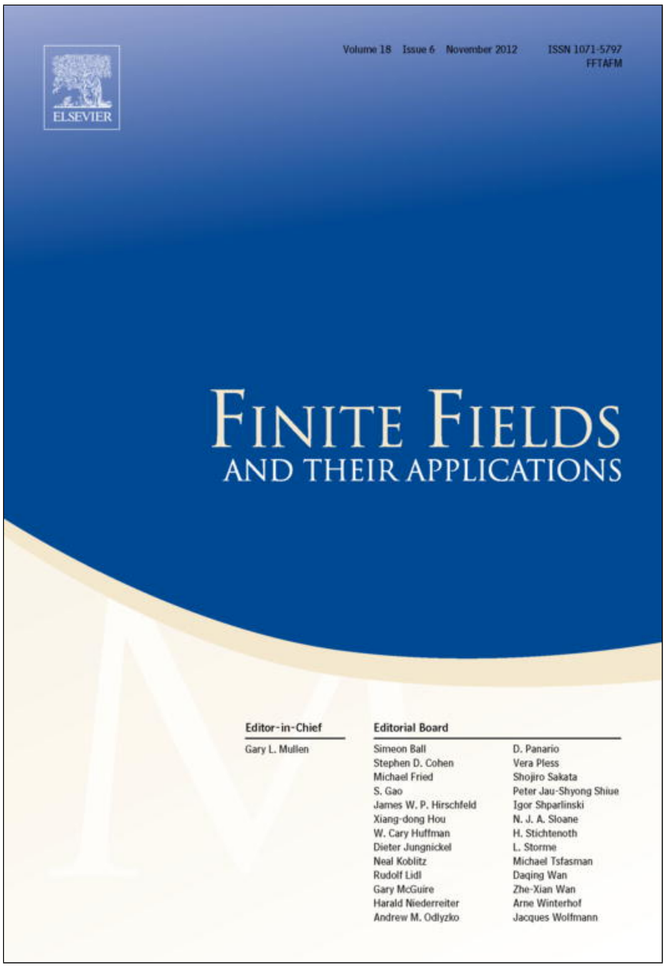
ELSEVIER
Volume 18 Issue 6 November 2012 ISSN 1071-5797
FFTAFM
FINITE FIELDS
AND THEIR APPLICATIONS
Editor-in-Chief
Gary L. Mullen
Editorial Board
Simeon Ball
Stephen D. Cohen
Michael Fried
S. Gao
James W. P. Hirschfeld
Xiang-dong Hou
W. Cary Huffman
Dieter Jungnickel
Neal Koblitz
Rudolf Lidl
Gary McGuire
Harald Niederreiter
Andrew M. Odlyzko
D. Panario
Vera Pless
Shojiro Sakata
Peter Jau-Shyong Shiue
Igor Shparlinski
N. J. A. Sloane
H. Stichtenoth
L. Storme
Michael Tsfasman
Daqing Wan
Zhe-Xian Wan
Arne Winterhof
Jacques Wolfmann

Finite Fields and Their Applications 18 (2012) 1232–1241

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

What is your “birthday elliptic curve”?

Heng Huat Chan[a,*], Elisavet Konstantinou[b], Aristides Kontogeorgis[c], Chik How Tan[d]

[a] *Department of Mathematics, National University of Singapore, 2 Science Drive 2, 117543, Singapore*
[b] *Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Karlovassi, Samos, Greece*
[c] *Department of Mathematics, University of Athens, Panepistimioupolis, Athens 15784, Greece*
[d] *Temasek Laboratories, National University of Singapore, 5A Engineering Drive 1, 117411, Singapore*

ARTICLE INFO

Article history:
Received 7 May 2012
Revised 14 September 2012
Accepted 16 September 2012
Available online 29 September 2012
Communicated by Neal Koblitz

Dedicated to all those who can have their birthday curves generated without the use of Hilbert class polynomials

MSC:
11G15
11Y40
11R37
11G20

Keywords:
Class invariants
Elliptic curves

ABSTRACT

In this article, Ramanujan–Weber class invariants and its analogue are used to derive *birthday elliptic curves*.

1. Introduction

In 2009 at *Max Planck Institut für Mathematik* (*Bonn*), P. Stevenhagen asked the following question:

“Given any N, can one find a variety and a prime p such that the number of points over the finite field $\mathbf{F}_p$ is N?”

* Corresponding author.
E-mail addresses: matchh@nus.edu.sg (H.H. Chan), ekonstantinou@aegean.gr (E. Konstantinou), kontogar@math.uoa.gr (A. Kontogeorgis), tsltch@nus.edu.sg (C.H. Tan).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2012.09.005

In the case when the variety is of genus 1, we are looking for elliptic curves and a prime number p for which the number of points on the elliptic curves over the finite field $\mathbf{F}_p$ is N. Stevenhagen highlighted a method which allowed him to produce an elliptic curve rapidly if N (more than 60 digits) is given. For more details, see his work with R. Bröker [4].

As an "application" of this work, Stevenhagen mentioned that when N is a birthdate, written as an eight-digit number in the form DDMMYYYY, one can construct an elliptic curve and a prime p such that the number of points of the curve over $\mathbf{F}_p$ is exactly N. For example, S. Ramanujan's birthdate is 22 December 1887 and the curve

$$y^2 = x^3 + 5\,887\,973x + 11\,302\,155$$

has exactly 22 121 887 solutions over $\mathbf{F}_{22\,130\,519}$. We shall call an elliptic curve attached to a birthdate a "*birthday elliptic curve*".

Stevenhagen's constructions of such curves require the computations of Hilbert polynomials satisfied by certain special values of the j-invariant. In this article, we illustrate how "birthday elliptic curves" can be constructed with the aid of computer algebra and the Ramanujan–Weber class invariants and their analogues. We *emphasize* here that our method is unlikely to be as powerful as that of Bröker and Stevenhagen. However, the main purpose of this article is to connect Ramanujan's work to the constructions of "birthday elliptic curves" by computing the values of the j-invariant (instead of its minimal polynomials) explicitly using various class invariants.

2. Class invariants

Suppose $n > 4$ is a squarefree integer. Let K_n be the imaginary quadratic field $\mathbf{Q}(\sqrt{-n})$ and C_n be the corresponding ideal class group. It is known, via class field theory, that there exists a maximal unramified abelian extension of K_n, say H_n, such that the Galois group $\mathrm{Gal}(H_n|K_n)$ is isomorphic to C_n. The field H_n is called the *Hilbert class field* of K_n.

Let

$$j(\tau) = 1728\frac{g_2^3(\tau)}{\Delta(\tau)}, \qquad \operatorname{Im}\tau > 0,$$

where

$$g_2(\tau) = 1 + 240\sum_{k=1}^{\infty}\frac{k^3 e^{2\pi i\tau k}}{1 - e^{2\pi i\tau k}}$$

and

$$\Delta = e^{2\pi i\tau}\prod_{k=1}^{\infty}\left(1 - e^{2\pi i\tau k}\right)^{24}.$$

It is known that the Hilbert class field H_n of K_n can be generated by special values of the j-invariant over K_n [7, Theorem 11.1].

The use of special values of the j-invariant to generate H_n is far from satisfactory as their absolute values are often very large. Computing the minimal polynomials satisfied by these values also involved large integers. As such, other class invariants are more desirable. For more details about the disadvantage of using j-invariants, see the paper by Gee and Stevenhagen [8] and the references there.

We collect here a list of class invariants g_n, G_n, t_n and λ_n used to replace j-invariants as functions that generate the Hilbert class fields.

(a) Let $n \equiv 2 \pmod 4$ and

$$g_n = 2^{-1/4} e^{\pi\sqrt{n}/24} \prod_{k=1}^{\infty} \left(1 - e^{-\pi\sqrt{n}(2k-1)}\right).$$

Then

$$H_n = \begin{cases} K_n(g_n^{12}) & \text{if } 3|n, \\ K_n(g_n^4) & \text{if } 3 \nmid n. \end{cases}$$

(b) Let $n \equiv 1 \pmod 4$ and

$$G_n = 2^{-1/4} e^{\pi\sqrt{n}/24} \prod_{k=1}^{\infty} \left(1 + e^{-\pi\sqrt{n}(2k-1)}\right).$$

Then

$$H_n = \begin{cases} K_n(G_n^{12}) & \text{if } 3|n, \\ K_n(G_n^4) & \text{if } 3 \nmid n. \end{cases}$$

(c) Let $n \equiv 7 \pmod 8$. Then

$$H_n = \begin{cases} K_n(2^{-3} G_n^{12}) & \text{if } 3|n, \\ K_n(2^{-1} G_n^4) & \text{if } 3 \nmid n. \end{cases}$$

(d) Let $n \equiv 3 \pmod{24}$ and

$$\lambda_n = \frac{e^{\pi\sqrt{n/3}/2}}{3\sqrt{3}} \prod_{k=1}^{\infty} \left(\frac{1 - (-1)^k e^{-\pi\sqrt{n/3}k}}{1 - (-1)^k e^{-\pi\sqrt{3n}k}} \right)^6.$$

Then

$$H_n = K_n\left(\lambda_{n/3}^2\right).$$

(e) Let $n \equiv 11 \pmod{24}$ and

$$t_n = \sqrt{3} e^{-\pi\sqrt{n}/18} \prod_{k=1}^{\infty} \frac{(1 - (-1)^k e^{-\pi\sqrt{n}k/3})(1 - (-1)^k e^{-3\pi\sqrt{n}k})}{(1 - (-1)^k e^{-\pi\sqrt{n}k})^2}.$$

Then

$$H_n = K_n(t_n).$$

(f) Let $n \equiv 19 \pmod{24}$. In this case, we compute $\sqrt{27}/t_n^{12}$ and derive H_n as

$$H_n = K_n\left(t_n^6 - 6 - \frac{27}{t_n^6}\right).$$

For more details about G_n, λ_n and t_n, we refer the readers to [5,6,1,9].

Readers might wonder why we write $H_n = K_n(2^{-1}G_n^4)$ instead of $H_n = K_n(G_n)$ when $n \equiv 7 \pmod{24}$ and $3 \nmid n$ even though both fields are the same. The reason being that $2^{-1}G_n^4$ is a unit in this case while G_n is not. Evaluating units is easier than evaluating algebraic integers. We use extensively the fact that if $\sigma \in \mathrm{Gal}(H_n|K_n)$ then $\sigma(u)$ is a unit if and only if u is a unit. For more details of such computations, see [5].

The use of units such as $2^{-1}G_n^4$ (when $n \equiv 7 \pmod 8$ and $3 \nmid n$) and t_n (when $n \equiv 11 \pmod{24}$) allow us to compute explicitly the values of these class invariants when C_n is of the form

$$C_n \cong (\mathbf{Z}/2\mathbf{Z})^r \oplus \mathbf{Z}/s\mathbf{Z}, \tag{2.1}$$

where $s = 3, 4, 8$. The restriction on the values of s is due to the fact that we can solve polynomial equation with degree of the polynomial less than 5.

With the explicit values of the various class invariants, we could evaluate special values of j-invariants that generate H_n (see [7, p. 264], [6,1]). We have

$$j(\sqrt{-n}) = \left(\frac{2^4}{g_n^{16}} + 2^2 g_n^8\right)^3,$$

$$j\left(\frac{1+\sqrt{-n}}{2}\right) = \left(\frac{2^4}{G_n^{16}} - 2^2 G_n^8\right)^3,$$

$$j(\sqrt{-n/3}) = -27\frac{(\lambda_{n/3}^2 - 1)(9\lambda_{n/3}^2 - 1)^3}{\lambda_{n/3}^2}$$

and

$$j\left(\frac{1+\sqrt{-n}}{2}\right) = \left(t_n^6 - 6 - \frac{27}{t_n^6}\right)^3.$$

These relations are derived from the facts that g_n^{12} and G_n^{12} are special values of a modular function of level 2, λ_n^{12} is a special value of a modular function of level 3 and t_n^{12} is a modular function of level 9.

We next show that the number of integers satisfying (2.1) is finite. We need the following theorem:

Theorem 2.1. *Let $h(d)$ denote the class number of the imaginary quadratic field with discriminant d and let $g(d)$ denote the order of the group of genera. Then*

$$\lim_{d \to -\infty} \frac{g(d)}{h(d)} = 0.$$

For a proof of Theorem 2.1, see [10, p. 458, Proposition 8.8].

Corollary 2.2. *The class group cannot be isomorphic to $\mathbf{Z}/2\mathbf{Z}^r \times H$, where H is a fixed finite group, for infinitely many discriminants.*

Proof. Indeed in this case $g(d)/h(d)$ is constant and cannot tend to zero. □

We have done an extensive computer search using magma [3] for discriminants of value $\leqslant 7 \times 10^5$ and we list them in Tables 1, 2 and 3 for $s = 3, 4$ and 8 respectively.

Table 1
Discriminants of the form (2.1) with $s = 3$.

26	29	38	53	61	87	106	109	110	118	129	157	170
174	182	186	201	202	214	222	231	237	246	247	249	255
262	277	286	298	309	318	339	358	366	370	393	397	411
417	430	451	453	473	493	515	517	533	537	546	565	597
606	610	618	665	669	670	682	685	705	707	714	730	741
753	762	771	813	814	817	826	835	843	861	885	913	930
942	949	966	969	970	973	993	1030	1038	1059	1090	1099	1147
1162	1173	1177	1203	1218	1219	1222	1230	1235	1254	1258	1267	1281
1285	1309	1315	1330	1347	1363	1419	1482	1491	1515	1518	1533	1545
1547	1554	1558	1563	1603	1722	1729	1830	1833	1843	1905	1915	1955
1963	1978	2037	2065	2091	2185	2190	2193	2227	2235	2262	2283	2346
2355	2370	2373	2387	2418	2443	2485	2515	2530	2553	2555	2562	2563
2590	2595	2613	2622	2635	2685	2697	2787	2795	2805	2905	2923	2937
2955	2982	3094	3102	3115	3157	3190	3235	3270	3417	3427	3445	3451
3523	3553	3565	3619	3633	3723	3738	3745	3763	3835	3885	3910	3913
3955	3990	4035	4147	4155	4218	4290	4389	4485	4510	4522	4585	4587
4755	4785	4795	4947	5035	5278	5307	5313	5395	5523	5565	5595	5610
5763	5797	5811	5835	6045	6090	6097	6105	6235	6510	6555	6603	6630
6643	6699	6715	6765	6955	6963	6987	7107	7161	7293	7410	7590	7665
7683	7905	8155	8211	8265	8323	8395	8745	8778	8787	8827	9030	9139
9177	9282	9570	9843	9870	9933	10 353	10 465	10 707	10 795	10 857	10 915	11 155
11 235	11 305	11 685	11 803	12 243	12 597	13 035	13 090	13 395	14 235	14 443	14 595	14 835
15 283	15 555	15 873	16 107	17 043	18 795	18 915	19 803	20 355	20 955	20 995	21 945	23 115
24 115	24 123	24 915	24 955	25 347	25 707	25 755	25 795	26 187	26 565	27 115	27 435	34 827
36 465	37 555	42 315	42 427	47 355	51 051	64 155	70 035	86 955	94 395			

Table 2
Discriminants of the form (2.1) with $s = 4$.

14	17	34	39	46	55	65	66	69	73	77	82	97
114	138	141	142	145	154	155	193	203	205	213	217	219
238	258	259	265	282	285	291	301	310	322	323	355	390
418	429	438	442	445	465	498	505	510	553	561	570	598
609	645	651	658	667	690	697	723	742	763	777	793	798
805	858	870	897	910	915	955	957	987	1003	1005	1027	1045
1065	1105	1110	1113	1122	1131	1185	1227	1243	1290	1302	1353	1387
1411	1443	1507	1555	1605	1635	1645	1653	1659	1677	1705	1771	1785
1870	1885	1947	2002	2013	2035	2067	2139	2145	2163	2170	2233	2310
2451	2667	2715	2730	2737	2755	3045	3243	3355	3507	3570	3705	3795
4123	4305	4323	4515	4830	4845	5005	5083	5115	5187	5467	6195	6307
7035	7315	7395	7755	7995	8547	8715	8835	9867	11 067	11 715	13 195	14 763
16 555	19 635	31 395	33 915	40 755								

Table 3
Discriminants of the form (2.1) with $s = 8$.

41	62	94	95	111	113	137	158	161	178	183
185	221	226	295	299	305	313	337	354	371	377
382	395	399	402	406	410	457	466	469	478	481
501	518	562	573	574	577	579	582	583	589	642
646	663	717	721	745	770	785	786	790	834	862
865	889	903	933	938	939	946	979	994	995	1002
1015	1023	1043	1054	1057	1081	1085	1149	1178	1195	1221
1245	1246	1299	1339	1345	1357	1393	1410	1417	1430	1462
1465	1474	1477	1498	1510	1513	1537	1578	1582	1590	1595
1610	1633	1651	1698	1717	1731	1738	1794	1795	1803	1842
1897	1918	1938	1939	1945	1957	1974	2010	2046	2059	2077
2085	2130	2211	2242	2265	2289	2307	2323	2337	2353	2365
2379	2395	2397	2410	2419	2442	2445	2465	2470	2478	2490
2533	2542	2587	2605	2611	2665	2706	2717	2739	2773	2821
2827	2829	2865	2893	2947	2958	2985	2995	3010	3021	3145
3165	3171	3193	3198	3201	3210	3237	3298	3318	3322	3333
3363	3390	3403	3435	3477	3502	3531	3595	3597	3787	3819
3883	3939	3963	4002	4053	4110	4137	4173	4179	4195	4251
4267	4270	4278	4387	4422	4470	4602	4641	4669	4683	4690
4747	4810	4818	4843	4867	4890	4899	4902	4930	4953	5037
5185	5217	5434	5457	5478	5538	5587	5590	5593	5605	5658
5685	5698	5707	5757	5785	5817	5845	5865	5883	5907	5910
5947	5973	5995	6006	6042	6099	6118	6123	6270	6315	6355
6402	6405	6490	6545	6622	6693	6745	6747	6771	6853	6923
7030	7077	7210	7345	7347	7378	7473	7491	7579	7585	7638
7645	7707	7770	7843	7917	7923	8043	8283	8385	8398	8418
8437	8515	8635	8643	8710	8845	9165	9219	9345	9373	9430
9435	9483	9595	9690	9835	9955	9982	10 005	10 203	10 227	10 374
10 387	10 545	10 563	10 605	10 635	10 803	11 005	11 130	11 193	11 445	11 505
11 523	11 571	11 635	11 713	11 739	11 985	12 027	12 090	12 259	12 369	12 390
12 558	12 595	12 747	12 765	12 835	12 859	13 110	13 363	13 398	13 515	13 585
13 629	13 755	13 795	13 827	14 155	14 190	14 245	14 385	14 430	14 547	14 637
14 707	15 067	15 387	15 477	15 645	15 715	15 810	15 990	16 027	16 185	16 195
16 269	16 779	16 835	16 995	17 017	17 115	17 227	17 290	17 347	17 355	17 385
17 427	17 490	17 515	17 985	18 285	18 291	18 330	18 403	18 445	18 705	18 715
18 753	18 907	19 195	19 227	19 285	19 947	19 987	19 995	20 155	20 163	20 202
20 235	20 553	20 757	20 805	21 147	21 385	21 505	21 715	21 835	22 155	22 243
22 515	22 737	22 971	23 142	23 205	23 485	23 835	23 970	24 035	24 882	26 013
27 307	28 083	28 203	29 667	30 030	31 515	32 235	32 395	32 890	34 755	35 763
35 805	36 363	36 915	37 515	37 587	37 947	38 595	39 235	39 270	39 435	40 227
40 443	40 467	40 803	43 435	43 890	44 115	45 843	45 885	46 410	47 523	47 595
49 665	50 955	51 870	52 003	53 130	53 515	54 723	55 315	57 057	57 387	57 715
60 027	63 427	64 515	65 395	66 045	73 315	74 347	74 613	74 635	76 245	76 323
76 755	82 555	84 315	89 355	89 947	92 235	96 915	100 947	102 795	105 315	111 435
112 035	113 883	119 595	123 123	126 555	130 515	140 595	143 115	155 155	198 835	199 563
212 667	323 323	435 435								

3. Finding birthday elliptic curves

It is known that [2, Chapter 8] if

$$4p = x^2 + ny^2,$$

then the number of solutions N_p of $\mathcal{E}_n$ over $\mathbf{F}_p$ is given by

$$p + 1 + \delta$$

where $\delta = \pm x$. In order to construct a birthday curve for a given birthdate b, we set $N_p = b$. Suppose that

$$b = p + 1 - x$$

with $4p = x^2 + ny^2$. Then we must have

$$-ny^2 = (p-1)^2 + b^2 - 2(p+1)b. \tag{3.1}$$

We search for primes $p \in (b + 1 - 2\sqrt{b}, b + 1 + 2\sqrt{b})$ such that the expression

$$(p-1)^2 + b^2 - 2(p+1)b$$

factors into $-ny^2$ with y as large as possible so that we have an integer n such that the class group associated with K_n is as in (2.1). The key point here is that the suitable values of n are somehow rare but we have many choices of pairs (p, n) that solve (3.1).

We then compute a special value of j-invariant, say j_n,[1] that generates H_n and construct the elliptic curve $\mathcal{E}_n$ be

$$y^2 = x^3 - 3c_n x - 2c_n$$

where

$$c_n = \frac{j_n}{j_n - 1728}.$$

The curve $\mathcal{E}_n$ may or may not have $N_p = b$. When $N_p \neq b$, we search for an ℓ such that

$$\left(\frac{\ell}{p}\right) \neq 1$$

and replace $\mathcal{E}_n$ by the "*twist*" of $\mathcal{E}_n$, say $\mathcal{E}_{\ell,n}$ given by

$$y^2 = x^3 - 3\ell^2 c_n x - 2\ell^3 c_n.$$

[1] There are $h(n)$ such values where $h(n) = |C_n|$ but we only need one such value. We obtain this value from Section 2.

4. Examples

We first discuss Ramanujan's birthday curve mentioned in Section 1. In this case, we find that

$$(p-1)^2+b^2-2(p+1)b=-163\cdot 293^2,$$

where $p=22\,130\,519$ and $b=22\,121\,887$. The corresponding field is K_{163}, which has class number 1. The j_n that we used is then the well-known value

$$j\left(\frac{1+\sqrt{-163}}{2}\right)=-640\,320^3$$

and this value is all we need to construct Ramanujan's birthday elliptic curve.

We now discuss a more "complicated" birthday curve. We shall use the birthdate of Tom Osler, a mathematician at Rowan University. The birthdate is 26 April 1940. It turns out that with $b=26\,041\,940$ and $p=26\,031\,737$

$$(p-1)^2+b^2-2(p+1)b=-2^6\cdot 7\cdot 103.$$

The class number of K_{721} is 16 and

$$C_{721}\simeq \mathbf{Z}/2\mathbf{Z}\oplus \mathbf{Z}/8\mathbf{Z}.$$

If we were to use the Hilbert class polynomial, then we would need to construct a polynomial of degree 16. Instead of deriving the Hilbert class polynomial, we compute G_{721} since $721\equiv 1 \pmod 4$. This is obtained by computing the following identities (see [5] for examples of such computations):

$$\left(\frac{G_{721}}{G_{103/7}}\right)^2+\left(\frac{G_{103/7}}{G_{721}}\right)^2=104+39\sqrt{7}+2\sqrt{5336+2018\sqrt{7}} \tag{4.1}$$

and

$$(G_{721}G_{103/7})^2+\left(\frac{1}{G_{103/7}G_{721}}\right)^2=384+146\sqrt{7}+\sqrt{297\,731+112\,532\sqrt{7}}. \tag{4.2}$$

We can compute (4.1) and (4.2) because we know that the values on the left hand sides are algebraic integers in a degree 4 extension over $\mathbf{Q}$ (see [5] for more details).

From (4.1) and (4.2), it is clear that we can determine G_{721}^4. We then determine G_{721}^4 modulo p by solving the congruence

$$x^2\equiv 7 \pmod p$$

and using this to derive values of radicals such as $\sqrt{297\,731+112\,532\sqrt{7}}$ in $\mathbf{F}_p$. This will allow us to determine a value of G_{721}^4 modulo p.

Using the relation between j_{721} and G_{721}, we conclude that over $\mathbf{F}_p$, one of the two curves

$$y^2=x^3+25\,598\,199x+17\,065\,466$$

and

$$y^2 = x^3 + 15\,193\,287x + 24\,612\,553$$

has exactly 26 041 940 solutions. It turns out that the latter yields the correct number of solutions.

Acknowledgments

The first author is funded by NUS Academic Research Grant R-146-000-103-112. The second and third authors supported by the Project "*Thalis, Algebraic modelling of topological and computational structures*". "THALIS" is implemented under the Operational Project "Education and Life Long Learning" and is co-funded by the European Union (European Social Fund) and National Resources (ESPA). We also thank Prof. J. Antoniadis for pointing us to Theorem 2.1. We are also grateful to the anonymous referees for their helpful suggestions.

References

[1] B.C. Berndt, H.H. Chan, Ramanujan and the modular j-invariant, Canad. Math. Bull. 42 (4) (1999) 427–440.
[2] I.F. Blake, G. Seroussi, N.P. Smart, Elliptic Curves in Cryptography, London Math. Soc. Lecture Note Ser., vol. 265, Cambridge University Press, Cambridge, 2000.
[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system, I. The user language, J. Symbolic Comput. 24 (1997) 235–265.
[4] R. Bröker, P. Stevenhagen, Constructing elliptic curves of prime order, Contemp. Math. 463 (2008) 17–28.
[5] H.H. Chan, Ramanujan's class invariants and Watson's empirical process, J. Lond. Math. Soc. (2) 57 (1998) 545–561.
[6] H.H. Chan, A. Gee, V. Tan, Cubic singular moduli, Ramanujan's class invariant λ_n and the explicit Shimura reciprocity law, Pacific J. Math. 208 (1) (2003) 23–37.
[7] D.A. Cox, Primes of the Form $x^2 + ny^2$, John Wiley & Sons, 1989.
[8] A. Gee, P. Stevenhagen, Generating class fields using Shimura reciprocity, in: Algorithmic Number Theory, Portland, OR, 1998, in: Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 441–453.
[9] E. Konstantinou, Aristides Kontogeorgis, Computing polynomials of the Ramanujan t_n class invariants, Canad. Math. Bull. 52 (2009) 583–597.
[10] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, second edition, Springer Monogr. Math., Springer, Berlin, 1990.