Integer Sequences, Discriminants and the Dedekind Eta Function

In this chapter I discuss the interesting connection of numbers like the plastic number ψ, complex elliptic functions, elliptic curves and imaginary quadratic numbers. I will explore in more detail the connection of numbers such as ψ known as algebraic integers as solutions to irreducible polynomials. I will concentrate on cubic polynomials.

The Dedekind eta function is a function defined on the upper imaginary plane of complex numbers. For any complex number τ with Im(τ)>0 the eta function is defined by;

$$n(\tau) = e^{\pi i\tau/12}\prod_{n=1}^{\infty}(1 - e^{-2n\pi i\tau})$$

It was known in the 19th century that an algebraic integer can be expressed by the ratio of eta functions known as Weber's functions [see Weber,1908 Cox, 2013]. In the literature $n(\tau)$ is expressed by the 24th power as:

$$\Psi^{24} = -\left|n(\tau)/(n(2\tau)\sqrt{2})\right|^{24}$$

where $\tau = \frac{1+\sqrt{-23}}{2}$ is an extension of the quadratic number field Q($\sqrt{-23}$).

The number or order of the quadratic field (Z($\sqrt{-23}$)) can be viewed as the discriminant of a quadratic equation with solutions of the quadratic form $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ where b^2-4ac = -23 for certain combinations of [a,b,c]. If $|b| \leq a \leq c$ and $|b| > 0$ then the quadratic form is said to be reduced. For this discriminant there are only 3 reduced forms possible [1,1,6], [2,1,3] and [2,-1,3].

The definition of the class number of a quadratic field is defined as the number h(d) of an order of the quadratic field with d<0 equal to the number of the reduced binary quadratic forms of d. In our example h(-23) = 3.

Since d can be any negative integer (more precisely any square-free integer) it seems there could be a large or even an infinite number of class numbers equal to three. As it turns out, surprisingly there are only 16 such numbers! The class number h(d) is a measure of the failure of unique factorization in the ring of integers τ. Unique factorization is possible for only 9 discriminants: -1,-2,-3,-7,-11,-19,-43,-67,and -163.

In this chapter I will show that knowledge of the reduced quadradic forms for the 16 members of class number 3 generate two eta functions n(τ1) and n(τ2). The modulus* of the ratio of these two eta functions (eta quotient) can be used to find the solutions to the cubic irreducible polynomials of all 16 discriminants.

Motivation of this study came from the observation that the Weber functions, although useful in calculating the j-invariant of an elliptic function did not provide in many cases a solution to the corresponding irreducible polynomial. This is observed in the third discriminant of the group d=-59. Although the j- invariant was accurately calculated from the three Weber functions (f(τ), f1(τ) and f2(τ)) [see Cox, 2013], none of these functions provided a solution to the irreducible polynomial of cubic root discriminant (-59). Although the Weber functions are eta quotients of one variable (τ), they can only provide a solution under the conditions that either $\tau = \tau1 = \tau2/2$, $\tau = 2*\tau1 = \tau2$, or $\tau = \tau1+1 = \tau2$. Unfortunately, for most discriminants in class number 3, these conditions do not hold true.

For all calculations, I use Mathematica 10 (Wolfram Research) where n(τ) = DedekindEta[τ]. Only the quadratic forms with b>0 are used the calculate the modulus. Let these forms be [a1,b1,c1] and [a2,b2,c2] then the modulus of the eta quotient is | DedekindEta[τ2]/DedekindEta[τ1]|. In the remainder of the chapter the function f3(-d), see below, is used to find the solutions of the irreducible cubic polynomials.

$$f3(-d) = |\,\mathrm{DedekindEta}[\tau2]/\mathrm{DedekindEta}[\tau1]| * \frac{\sqrt{2a1}}{\sqrt{2a2}}$$

with $\tau1 = \frac{b1+\sqrt{b1^2-4a1c1}}{2a1}$ and $\tau2 = \frac{b2+\sqrt{b2^2-4a2c2}}{2a2}$

The minimal polynomials for all class number 3 discriminants can be found in [Berwick, 1927]. These polynomials are used to test the value of the algebraic integer solution x= γ(-d) found from f3(-d).

In [Cox, 2013] primes of the form x^2+ny^2 are discussed. I show that for n = |-d| where -d is a class number 3 discriminant the following theorem is true:

Theorem 0.5[Cox] – Let n = 1,2 mod 4 be a square free integer. There is an irreducible polynomial $f_n(x)$ such that a prime p = x^2+ny^2 implies that (-n/p) = 1 and $f_n(x)$=0 mod p has integer solutions.

In this theorem **(-n/p)** is the Legendre or Jacobi symbol +/- 1. The theorem shows that the irreducible polynomial is split by p into integers x1, x2, x3 such that $f_n(x)$ = (x-x1)(x-x2)(x-x3) = 0 mod p. Elements of this theorem were observed in Chapter 3 where primes of the form p = x^2+23y^2 split the irreducible polynomial x^3-x-1 mod p into three integer solutions. The remarkable consequences of Theorem 0.5 extend to all class number 3 polynomials. The theorem actually extends for all n provided an irreducible polynomial $f_n(x)$ can be found. In many cases the degree of the polynomial can be quite large.

In Table II – Table IV I show the functionality of the solution x=γ(-d) to f3(-d) for all 16 discriminants -d. The corresponding irreducible polynomial with cubic root discriminant -d is shown. Table I shows a total of 10 different functions of the solution x to the minimal polynomial that are equal to f3(-d). Several other irreducible polynomials (non-minimal) are derived from the solution x and f3(-d)[Table III – Table IV).

- For a complex number z= (z1+z2*i) the modulus |z| is a real number where |z|= $z1^2+z2^2$ = zz* =(z1+z2*i)* (z1-z2*i) where z* is the complex conjugate of z.

TABLE I- Function of solutions x of the minimal polynomial to the modulus of the eta quotient f3(-d)

Discriminants d (negated)	f3(-d) = f(x, x^2,x^3,x^4,x^5)	Number of irreducible polynomials found from x and f3(-d) (1)
23, 31, 59, 83	f3(-d) = x	1
107, 139	f3(-d) = x + 1	1
283, 331, 643	f3(-d) = x^2	1
211	f3(-d) = x^2 + 1	1
307	f3(-d) = (x^2 + ½)/3	2
379	f3(-d) = (x^2 + x)/2	2
499	f3(-d) = (x^2 +x + ½)/2	2
547	f3(-d) = f (x^2, x^3)	4
883	f3(-d) = f (x, x^3, x^4)	4
907	f3(-d) = f (x^3, x^4, x^5)	4

(1) See tables II to IV for details of these polynomials

Table II- Discriminants with F3(-d) = f(x)

Discriminant d (negated)	Quadratic forms [a,b,c]	f(X)	Minimal polynomial	Irreducible polynomials with solution as function of x and f3(-d)
23	[1,1,6] [2,1,3]	X	X^3 - X - 1	none
31	[1,1,8] [2,1,4]	X	X^3 - X^2 - 1	none
59	[1,1,15] [3,1,5]	X	X^3 – $2X^2$ - 1	none
83	[1,1,21] [3,1,7]	X	X^3 – $2X^2$ – 2X - 1	none
107	[1,1,27] [3,1,9]	X + 1	X^3 - X^2 – 3X - 2	none
139	[1,1,35] [5,1,7]	X + 1	X^3 –3 X^2 – 5X - 2	none

Table III- Discriminants with F3(-d) = f(x , x^2)

Discriminant d (negated)	Quadratic forms [a,b,c]	f(X)	Minimal polynomial	Irreducible polynomials with solution as function of x and f3(-d)
283	[1,1,71] [7,5,11]	X^2	$X^3 – 4X^2 - 1$	none
331	[1,1,83] [5,3,17]	X^2	$X^3 – 4X^2 -2X - 1$	none
643	[1,1,161] [7,1,23]	X^2	$X^3 – 10X^2 -6X - 1$	none
211	[1,1,53] [5,3,11]	$X^2 + 1$	$X^3 – 3X^2 + X - 2$	none
307	[1,1,77] [7,1,11]	$(2X^2 + 1)/3$	$X^3 - 5X^2 – 1X - 4$	$27A^3-63A^2+57A-16$ X^2= 3A*f3(-307)
379	[1,1,95] [5,1,19]	$(X^2 + X)/2$	$X^3 – 6X^2 – 5X - 2$	$4A^3-2A^2+A-2$ X^2= 2A*f3(-379)
499	[1,1,125] [5,1,25]	$X(X+1)^2/4$	$X^3 – 4X^2 – 5X - 4$	$4A^3-22A^2+35A-8$ X^2= 2A*f3(-499)

Table IV- Discriminants with F3(-d) = f(x, x^2,x^3,x^4,x^5)

Discriminant d (negated)	Quadratic forms [a,b,c]	f(X)	Minimal polynomial	Irreducible polynomials with solution as function of x and f3(-d)
547	[1,1,137] [11,5,13]	$\frac{X(2+X+2X^2)}{X^2-12}$	$X^3 - 4X^2 + 2X - 3$	$A^3 + 14A^2+50A-9$ X^2= A*f3(-547) $B^3 + 13B^2+101B-90$ X^3+X^2= B*f3(-547) $C^3 - C^2+43C-27$ X^3= C*f3(-547) X=A + (2/ f3(-547)) + (12+B)(A/C)
883	[1,1,221] [13,1,17]	$\frac{(X^4+X^3)}{X-2}$	$X^3 – 5X^2 – 5X - 2$	$A^3 - 13A^2+43A-4$ X^2= A*f3(-883) $B^3 - 8B^2+23B-12$ X^3+X^2= B*f3(-883) $C^3 +5C^2+11C-8$ X^3= C*f3(-883) X=(B*C/A) – 2
907	[1,1,227] [13,9,19]	$\frac{X^3(X^2+X-1)}{8}$	$X^3 – 5X^2 + X - 2$	$A^3 + 9A^2+67A-4$ X^2= A*f3(-907) $B^3 + 18B^2+97B-36$ X^3+X^2= B*f3(-907) $C^3 + 9 C^2+25C-8$ X^3= C*f3(-907) $X=\frac{A+\sqrt{A^2+32B}}{2B}$

Looking at the results of these Tables, the algebraic integer solution of the minimal polynomial is easily obtained from f3(-d), either directly or by a square root, in 11 of the 16 discriminants. In two discriminants (379 and 499) a quadratic equation in x^2 and x is solved. Only for the last three largest discriminants is the functionality in x of a higher degree than the minimal polynomial. In [Weber,1908] only the first 2 discriminants (23,31) can be solved using Weber functions. None of the other Class number 3 discriminants are directly solved using f(τ),f1(τ) or f2(τ). [See the Appendix *Tabelle VI* of Weber,1908].

Irreducible polynomials with cubic root discriminants divisible by d are found in six cases, 307,379,499,547,883 and 907. Some of these polynomials are not monic (leading coefficient is unity). All these polynomials, including the minimal polynomial, satisfy Theorem 0.5.

For example: n=907 and p= 18^2+907*1^2 = 1231, the polynomials for X, A, B, and C in Table IV split as:

E1. (X-161) *(X-1087) *(X-1219) = X^3-5X^2+X -2= 0 mod 1231

E2. (A-23) *(A-394) *(A-805) = A^3+9A^2+67A -4= 0 mod 1231

E3. (B-404) *(B-993) *(B-1047) = B^3+18B^2+97B -36= 0 mod 1231

E4. (C-188) *(C-381) *(C-653) = C^3+9C^2+25C -8= 0 mod 1231

For n = 499 the non-monic polynomial in variable A and p=8^2+499*1^2= 563 the polynomial splits as:

E5. (A-185) *(A-186) *(A-479) = 4A^3-22A^2+35A = A^3+276A^2+431A-2 = 0 mod 563

Note that the split polynomial can be written as a monic polynomial mod p since the ring of integers mod p is closed to multiplication. In the above example -22 = 4*276 mod 563 and 35=4*431 mod 563. If n=p then Theorem 0.5 is also true:

For n=p= 307 the polynomial in A splits as:

E6. (A-45) *(A-45) *(A-117) = 27A^3-63A^2+57A = A^3+100A^2+275A+79 = 0 mod 307

where 45 is a double root. Note that under mod p, the above non-monic polynomials derived in class number 3 discriminants can be written as monic polynomials! This property provides a method of deriving integer sequences mod p.

Since the first three numbers that generate the sequence can be obtained from powers of the three cubic roots of the polynomial the next term and all subsequent numbers in the sequence can be calculated mod p. Using the examples above the following sequences a(0), a(1),a(2)……a(n) are derived:

E1a. 3, 5, 23, ……(5*a(n-1) - (n-2) + 2*(n-3)) mod 1231

E2a. 3, -9, -53, ……(-9*a(n-1) – 67*(n-2) + 4*(n-3)) mod 1231

E3a. 3, -18, 130, ……(-18*a(n-1) – 97*(n-2) + 36*(n-3)) mod 1231

E4a. 3, -9, 31, ……(-9*a(n-1) – 25*(n-2) + 8*(n-3)) mod 1231

E5a. 3, 541, 435, ……(-276*a(n-1) – 431*(n-2) + 2*(n-3)) mod 563

E6a. 3, 207, 240, ……(-100*a(n-1) – 275*(n-2) - 79*(n-3)) mod 307

In Chapter 3 I discuss the properties of type 3 primes of discriminant = -23. The period length of the sequence mod p where p = x^2+23y^2 was shown to be p-1. Now using Theorem 0.5 we can show that this is true for any prime discriminant in class number 3! As in the cases of type 1 and type 2 primes in Chapter 3, for some sequences of type 3 mod p, the period can be (p-1)/2 or divisible by any integer (not proven!).

For the above examples the periods are E1a/1230, E2a/1230, E3a/615, E4a/1230, E5a/562, E6a/306, respectively.

The application of the above method for finding the real root of cubic polynomials using the eta quotients can also be reversed to find the eta quotient knowing the real roots of an irreducible polynomial of degree 3. It is mentioned in [Chapman and Hart,2006] that a method developed in 1949 by Chowla and Selberg could be applied for evaluating eta functions of reduced forms from the discriminant of binary quadratics. For discriminants of class number 3 and various discriminants divisible by primes of class number 1 (Chapman and Hart show example of D=-44 which is a product of the class 1 discriminant d=-11) the modulus of the individual eta functions can be determined.

The Chowla-Selberg formula involves the product of the modulus of the eta function for each reduced form of -D. The left had side of this formula is the product of $|n(\tau 1)| * |n(\tau 2)| * |n(\tau 3)|$ = $|n(\tau 1)| * |n(\tau 2)|^2$,(since $|n(\tau 2)| = |n(\tau 3)|$) with τ derived from the 3 forms [a1,b1,c1], [a2,b2,c2], [a3,b3,c3]. The eta quotient f3(-d) multiplied by $\sqrt{a2}/\sqrt{a1}$ is the eta quotient $|n(\tau 2)/n(\tau 1)|$. A knowledge of f3(-d) calculated from the root of the minimal polynomial and the a1 and a2 coefficients of the reduced forms provides a rearrangement of the LHS of the Chowla Selberg formula to $|n(\tau 2)|^3$.

The value of $|n(\tau 2)|$ then is obtained from the cube root of the RHS of the Chowla Selberg formula and $|n(\tau 1)|$ is easily obtained from $|n(\tau 2| * f3(-d) * \sqrt{a2}/\sqrt{a1}$.

The RHS of the Chowla Selberg formula is a product of the gamma functions for each value of m/|d|, in the ring of integers mod |-d|, with each value put in the numerator or denominator depending on the sign of the Legendre symbol (d/m) = +1 or -1.

The formula I derive for d= -23 and d=-59 is,

[CS-1a,1b]

$$n(\tau 1) * n(t2)^2 = a2 * (\prod_{m=1}^{\mathrm{d}-1} \Gamma\left(\frac{m}{|d|}\right)^{\left(\frac{d}{m}\right)})^{\frac{1}{2}} * \left(\frac{1}{2\pi|d|}\right)^{\frac{3}{2}}$$

with $n(\tau 1) = n(\tau 2) * f3(-d) * \sqrt{a2}/\sqrt{a1}$

Solving for n (τ2)

[CS-2]

$$n(\tau 2) = \left(\frac{a2 * (\prod_{m=1}^{\mathrm{d}-1} \Gamma\left(\frac{m}{|d|}\right)^{\left(\frac{d}{m}\right)})^{\frac{1}{2}} * \left(\frac{1}{2\pi|d|}\right)^{\frac{3}{2}}}{f3(-d) * \sqrt{a2}/\sqrt{a1}^{\;2}}\right)^{1/3}$$

Using the values for d=-59, Gamma values Gamma[m,d] and Legendre symbols JacobiSymbol[-d,m] are calculated using Mathematica, I get,

$$X = f3(-59) = 2.20556943040059$$

$$f3(-59) * \sqrt{6}/\sqrt{2} = 3.82015831307457$$

Product of all Gamma functions = 6937.320525834101705

RHS of equation [CS-1a] = $3 * 6937.320525834101705^{1/2} * (1/(2*\pi*59))^{3/2}$

$= 3*0.011669387469399969483$

From [CS-2]: $n(\tau 2) = ((3*0.011669387469399969483)/ 3.82015831307457^{2})^{1/3}$

$n(\tau 2) = 0.13386556159532384741$

From [CS-1b]: $n(\tau 1) = n(\tau 2) * 3.82015831307457$

$= 0.511387637962772$

Checking the results:

$X = |n(\tau 2)|/|n(\tau 1)| * \sqrt{2}/\sqrt{6} = (0.511387637962772/0.13386556159532384741)/\sqrt{3}$

$X = 2.20556943040059$

In support of this paper [Enge and Schertz,2004] in their introduction state that the commonly used Weber functions cannot be used for discriminants congruent to 5 modulo 8. Of the 16 discriminants tested in this paper all but two (-23, -31) are congruent 5 modulo 8.

Richard Turk **February 7, 2017**

References

David A. Cox, **Primes of the form x^2+ny^2**, John Wiley and Sons, Hoboken, New Jersey, 2013.

W.E.H. Berwick, *Modular Invariants Expressible in Terms of Quadratic and Cubic Irrationalities*, Proc. Lon. Math. Soc. **28** (1927), pp.53-69.

Heinrich Weber, **Elliptische Funktionen**, Friedrich Vieweg & Sohn, Braunschwig, Germany, 1908.

R. Chapman and W.B. Hart, *Evaluation of the Dedekind Eta Function*, Canad. Math. Bulletin, March 2006.

A. Enge, and R. Schertz, *Constructing elliptic curves over finite fields using double eta-quotients*, Journal de Theorie des Nombres de Bordeaux, **16**, 2004.