Notes on the period polynomial for the cubic Gaussian periods

Peter Bala, Nov 2021

A cubic field K is called a cyclic cubic field if it contains all three roots of its generating polynomial $f(x)$. The Galois group of K over $\mathbb{Q}$ is cyclic of order 3. Shanks [4] studied a 1-parameter family of cyclic cubic fields K_a, defined as the splitting field of the polynomial $x^3 - ax^2 - (a+3)x - 1$, $a \in \mathbb{Z}$. Shank's cubic has polynomial discriminant $\left(a^2+3a+9\right)^2$. In the case when $p = a^2 + 3a + 9$ is prime (so necessarily $p \equiv 1(3)$) Shank's cubic is easily seen to be an integer translation of the period polynomial of the classical cubic Gaussian periods of modulus p (see, for example, [3]). The purpose of this note is to extend this result to all primes $p \equiv 1(3)$ by suitably generalising Shanks' cubic.

- -

Let $p \equiv 1(3)$ be prime. A result of Gauss says that there are integers L and M, unique up to sign, such that $4p = L^2 + 27M^2$ [1, Prop. 8.3.2]. We fix the values of L and M by choosing the positive value of M and requiring $L \equiv 1(3)$. Clearly, L and M have the same parity. Hence $L - 3M$ is even. We set $L = 2a + 3M$. It follows from our choice of L that the integer $a \equiv 2(3)$. The prime p is given in terms of a and M by

$$p = a^2 + 3aM + 9M^2.$$

For primes of this type see A005471 ($M = 1$), A227622 ($M = 2$) and A349461 ($M = 3$).

Table: Values of L, M and a for $7 \le p \le 103$

Prime $p \equiv 1(3)$	L	M	a	Prime $p \equiv 1(3)$	L	M	a
7	1	1	-1	61	1	3	-4
13	-5	1	-4	67	-5	3	-7
19	7	1	2	73	7	3	-1
31	4	2	-1	79	-17	1	-10
37	-11	1	-7	97	19	1	8
43	-8	2	-7	103	13	3	2

We define the **generalised Shanks cubic polynomial** for the prime $p = a^2 + 3aM + 9M^2$ to be the polynomial

$$S(x) \equiv S(a, M, x) = x^3 - ax^2 - M(a + 3M)x - M^3 \tag{1}$$

with discriminant $\mathrm{Disc}(S(x)) = p^2M^2$. When $M = 1$, the prime p has the form $p = a^2 + 3a + 9$ and the polynomial $S(a, 1, x) = x^3 - ax^2 - (a+3)x - 1$ is

Shanks' cubic. The polynomial $S(a,M,x)$ may be reducible over $\mathbb{Q}$; for example, when $M=6a$ we find $S(a,6a,x)=(x+2a)(x+9a)(x-12a)$. However, in all cases of interest to us, the polynomial $S(a,M,x)$ will be irreducible over $\mathbb{Q}$.

We shall show that the generalised Shanks' cubic $S(a,M,x)$ is the translation by an integer of the period polynomial of the three cubic Gaussian periods of modulus p. We give some relations between the cubic Gaussian periods.

Cubic Gaussian periods and the period polynomial

Let ζ_p denote a primitive pth root of unity. Let $\mathbb{Z}_p$ denote the finite field with p elements. The group of units $\mathbb{Z}_p^*$, which we identify with the numbers $\{1,2,...,p-1\}$, has a subgroup C of index 3 consisting of the nonzero cubic residues modulo p. The **principal cubic Gaussian period** for the modulus p is defined as the sum

$$\eta_0=\sum_{i\in C}\zeta_p^i.$$

The other two **cubic Gaussian periods** are

$$\eta_1=\sum_{i\in C_1}\zeta_p^i \quad \text{and} \quad \eta_2=\sum_{i\in C_2}\zeta_p^i,$$

where C_1 and C_2 denote the cosets of C in the group $\mathbb{Z}_p^*$. Clearly,

$$\eta_0+\eta_1+\eta_2=-1.$$

The three Gaussian periods η_i are the roots of the **period polynomial**

$$P(x)=(x-\eta_0)(x-\eta_1)(x-\eta_2).$$

The period polynomial $P(x)$ has integer coefficients and is given by [3, equation 3.1]

$$P(x)=x^3+x^2-\frac{(p-1)}{3}x-\left(\frac{(L+3)p-1}{27}\right). \tag{2}$$

The discriminant of the period polynomial $\mathrm{Disc}(P_3(x))=p^2M^2$. Since the polynomials $P(x)$ and $S(x)$ have the same discriminant we might suspect that they are related by a linear transformation: indeed one easily checks that

$$S(x)=P\left(x-\frac{a+1}{3}\right)=P\left(x-\frac{L+2-3M}{6}\right). \tag{3}$$

Since $a\equiv 2(3)$ we see that $(a+1)/3$ is an integer. Since the cubic period polynomial is irreducible it follows that the generalised Shanks' cubic $S(x)$ associated with the prime $p=a^2+3aM+9M^2$ is also irreducible.

The roots of S(x)

From (3), the three roots of the generalised Shanks' cubic $S(x)$ are

$$\eta_i + \frac{a+1}{3}, \quad i = 0, 1, 2. \tag{4}$$

We define the root s_0 of $S(x)$ by

$$s_0 = \eta_0 + \frac{a+1}{3}.$$

This unambiguously defines the root s_0 in terms of the principal cubic Gaussian period η_0. Next we find a linear fractional transformation that cyclically permutes the roots of the cubic $S(x)$. One easily verifies that

$$S\left(-\frac{M^2}{x+M}\right) = -\frac{M^3}{(x+M)^3} S(x). \tag{5}$$

Substituting $x = s_0$ into (5), we see that $s_1 := -M^2/(s_0 + M)$ is a second (distinct) root of the irreducible cubic $S(x)$ and $s_2 := -M^2/(s_1 + M)$ is the remaining root of $S(x)$. This determines the roots of $S(x)$ without ambiguity. Thus the roots s_i of the cubic $S(x)$ are cyclically permuted by the linear fractional transformation $x \to -M^2/(x + M)$ of order 3:

$$s_1 = -\frac{M^2}{s_0 + M}, \quad s_2 = -\frac{M^2}{s_1 + M}, \quad s_0 = -\frac{M^2}{s_2 + M}, \tag{6}$$

or equivalently

$$s_i s_{i+1} = -M s_{i+1} - M^2, \quad i \in \{0, 1, 2\} \text{ viewed as } \mathbb{Z}/3\mathbb{Z}. \tag{7}$$

We can now determine the periods η_1 and η_2 unambiguously by setting

$$\eta_1 = s_1 - \frac{a+1}{3}, \quad \eta_2 = s_2 - \frac{a+1}{3}.$$

There is also a quadratic mapping that cyclically permutes the roots of the generalised Shanks' cubic $S(x)$. One easily checks that

$$\frac{S(x)}{M(x+M)} = \left(\frac{x^2}{M} - (a+M)\frac{x}{M} - 2M\right) - \left(\frac{-M^2}{x+M}\right). \tag{8}$$

By succesively setting $x = s_0$, $x = s_1$ and $x = s_2$ in this identity and using (6), we arrive at the relations

$$s_1 = \frac{s_0^2}{M} - (a+M)\frac{s_0}{M} - 2M, \quad s_2 = \frac{s_1^2}{M} - (a+M)\frac{s_1}{M} - 2M, \quad s_0 = \frac{s_2^2}{M} - (a+M)\frac{s_2}{M} - 2M. \tag{9}$$

Thus the mapping $x \to \dfrac{x^2}{M} - (a+M)\dfrac{x}{M} - 2M$ also cyclically permutes the roots s_i of the polynomial $S(x)$.

Period relations Substituting $s_i = \eta_i + \frac{a+1}{3}$ in (6) we find that the Gaussian cubic periods are related by the linear fractional transformation

$$\eta_{i+1} = \frac{-\frac{(L-3M+2)}{6}\eta_i - \frac{(L+p+1)}{9}}{\eta_i + \frac{(L+3M+2)}{6}}, \quad i \in \{0,1,2\} \tag{10}$$

of determinant -1 and order 3.

Therefore we have the relations for the cubic Gaussian periods

$$\eta_i\eta_{i+1} = -\left(\frac{L-3M+2}{6}\right)\eta_i - \left(\frac{L+3M+2}{6}\right)\eta_{i+1} - \frac{(L+p+1)}{9}, \quad i \in \{0,1,2\}. \tag{11}$$

The period relations corresponding to (9) are

$$\eta_i^2 = M\eta_{i+1} + \frac{(a+3M-2)}{3}\eta_i + \frac{(2p-1+a+6M)}{9}. \tag{12}$$

Delta cyclotomy

Let

$$\delta_0 = \eta_0 - \eta_1, \quad \delta_1 = \eta_1 - \eta_2, \quad \delta_2 = \eta_2 - \eta_0$$

denote the differences of the cubic Gaussian periods. In the particular case $M = 1$, Lehmer and Lehmer [2] show that the differences δ_i are the roots of the cubic $x^3 - px + p$, a simpler polynomial than the period polynomial (2). In the case of general M, it is straightforward to evaluate the elementary symmetric function in the δ_i using the above relations for the cubic periods to show that the differences δ_i are the roots of the polynomial

$$(x - \delta_0)(x - \delta_1)(x - \delta_2) = x^3 - px + Mp$$

with discriminant $p^2\left(4p - 27M^2\right) = p^2L^2$. The polynomial $x^3 - px + Mp$ generates a cyclic cubic field since it is irreducible by Eisenstein's criteria and has square discriminant.

Exercise 1. Show that Shanks' generalised cubic $S(a, M, x)$ factors as

$$S(a, M, x) = \left(x - M\frac{\delta_0}{\delta_1}\right)\left(x - M\frac{\delta_1}{\delta_2}\right)\left(x - M\frac{\delta_2}{\delta_0}\right).$$

Exercise 2. Show that the irreducible cubic $x^3 + \frac{p}{M}(x+M)^2$ with discriminant equal to p^2L^2 has roots $\delta_i + \frac{\delta_i^2 - p}{M}$, $0 \leq i \leq 2$. (The polynomial $x^3 + p(x+1)^2$ has been considered by Uchida [5] in connection with a theorem about the class numbers of cyclic cubic fields.)

Exercise 3. Let

$$\varrho_0 = \frac{s_0}{s_1}, \quad \varrho_1 = \frac{s_1}{s_2}, \quad \varrho_2 = \frac{s_2}{s_0}$$

denote the quotients of the roots s_i of Shank's generalised cubic $S(a, M, x) = x^3 - ax^2 - M(a+3M)x - M^3$. Show that the quotients ϱ_0, ϱ_1 and ϱ_2 are the roots of the cubic equation

$$x^3 + \left(\frac{p - 3M^2}{M^2}\right)x^2 + 3x - 1 = 0$$

with discriminant p^2L^2/M^6.

Exercise 4. Show that the differences of the quotients $\varrho_0 - \varrho_1$, $\varrho_1 - \varrho_2$ and $\varrho_2 - \varrho_0$ are the roots of the irreducible cubic

$$x^3 - \frac{p\left(p - 6M^2\right)}{M^4}x + \frac{Lp}{M^3}$$

with discriminant $p^2\left(2p^2 - 18M^2p + 27M^4\right)^2/M^{12}$.

References

[1] K. Ireland and M.Rosen, A Classical Inroduction to Modern Number Theory, Graduate texts in mathematics; 84, Springer Verlag.

[2] D. H. Lehmer and Emma Lehmer, The Lehmer Project , Math. of Comp., Vol. 61, No. 203, (1993): 313-317.

[3] E. Lehmer, Connection between Gaussian periods and cyclic units, Math. Comp. Vol. 50, No. 182, (1988): 535-541.

[4] D. Shanks, The simplest cubic fields, Math. Comp., Vol. 28, No. 128, (1974): 1137-1152.

[5] K. Uchida, Class numbers of cubic cyclic fields, J. Math. Soc. Japan, Vol. 26, No. 3, (1974): 447-453.