Mersenne primes and class field theory

Jansen, B.J.H.

Chapter 2

The Lucas-Lehmer-test

In this chapter we discuss the Lucas-Lehmer-test, which is a primality test for integers of the form $M_q = 2^q - 1$, where $q \in \mathbb{Z}_{>1}$. To apply the test one calculates a sequence of elements in $\mathbb{Z}/(2^q-1)\mathbb{Z}$ by iterating the map $x \mapsto x^2 - 2$ on a suitable *starting value* $s \in \mathbb{Z}/(2^q-1)\mathbb{Z}$. The integer $2^q - 1$ is prime if after $q-2$ iterations we get 0. Starting values will be obtained from a certain field K of algebraic numbers. This field has the property that any given element can be interpreted in $\mathbb{Z}/(2^q-1)\mathbb{Z}$ for all $q \in \mathbb{Z}_{>1}$ relatively prime to some integer. Certain well-chosen elements in K can be used as starting values for each M_q with q relatively prime to some fixed integer. These well-chosen starting values will in Definition 2.5 be called *universal starting values*. The classical examples of universal starting values are $4, 10 \in \mathbb{Z}$. We will construct infinitely many additional universal starting values in K.

Many starting values

Denote the Jacobi symbol by $\left(\frac{\cdot}{\cdot}\right)$ (see [1, §1, page 16]).

Theorem 2.1. *Let $q \in \mathbb{Z}_{>1}$ and $M_q = 2^q - 1$. Let $s \in \mathbb{Z}/M_q\mathbb{Z}$. Define $s_i \in \mathbb{Z}/M_q\mathbb{Z}$ for $i \in \{1, 2, \ldots, q-1\}$ by $s_1 = s$ and $s_{i+1} = s_i^2 - 2$. Then we have*

$$s_{q-1} = 0 \iff M_q \text{ is prime and } \left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1.$$

The Lucas-Lehmer-test (Theorem 2.1) will be proved in the next section. To illustrate this theorem we give the example $q = 7$ and $s = (4 \bmod 127)$. We calculate

$$\begin{aligned} s_1 &= 4, \\ s_2 &= 4^2 - 2 = 14, \\ s_3 &= 14^2 - 2 = 194 = 67, \\ s_4 &= 67^2 - 2 = 4487 = 42, \end{aligned}$$

$$s_5 = 42^2 - 2 = 1762 = -16,$$
$$s_6 = (-16)^2 - 2 = 254 = 0$$

in the ring $\mathbb{Z}/127\mathbb{Z}$. Hence using the theorem we conclude that 127 is prime and that $\left(\frac{2}{127}\right) = \left(\frac{-6}{127}\right) = 1$.

To apply Theorem 2.1 as a prime test one uses an element $s \in \mathbb{Z}/M_q\mathbb{Z}$ such that $\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$. Such an element is called a *starting value for* q. With the quadratic reciprocity laws (see [2, Introduction]) one calculates that for the numbers $s = (4 \bmod M_q)$ and $s = (10 \bmod M_q)$ we have $\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$ for all odd integers $q \in \mathbb{Z}_{>1}$. It follows that the numbers $s = (4 \bmod M_q)$ and $s = (10 \bmod M_q)$ are starting values for all odd integers $q \in \mathbb{Z}_{>1}$. In the same way one can show that number $s = (2 \bmod M_q)(3 \bmod M_q)^{-1}$ found by S.Y. Gebre-Egziabher is a starting value for all odd integers $q \in \mathbb{Z}_{>0}$ (see [3]). We prefer to denote $(2 \bmod M_q)(3 \bmod M_q)^{-1}$ by $(\frac{2}{3} \bmod M_q)$. In this case q is assumed to be odd to make sure that division by $(3 \bmod M_q)$ is possible. Below we will express the properties of 4, 10, and 2/3 just described, by saying that these numbers are universal starting values. Later we show that the number $s = (\frac{238}{507} + \frac{160}{169} \cdot 2^{(q+1)/2} \bmod M_q)$ is also a starting value for all odd $q \in \mathbb{Z}_{>1}$. Since $(2^{(q+1)/2} \bmod M_q)$ is a square root of $(2 \bmod M_q)$, we will denote s by $(\frac{238}{507} + \frac{160}{169} \cdot \sqrt{2} \bmod M_q)$. Hence we have the following example.

Example 2.2. *The number* $s = \frac{238}{507} + \frac{160}{169} \cdot \sqrt{2}$ *is a universal starting value.*

To make all this precise, we define K to be the subfield of the field $\mathbb{R}$ of real numbers obtained by adjoining all positive real roots of 2 to $\mathbb{Q}$, so $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ with $\sqrt[n]{2} \in \mathbb{R}$ the positive zero of the polynomial $x^n - 2$. We write $\sqrt{2}$ for $\sqrt[2]{2}$. We proceed to show that for every $s \in K$ there exists a positive integer k_s such that $s \bmod M_q$ has a natural meaning whenever q is relatively prime to k_s.

We fix $q \in \mathbb{Z}_{>1}$ and construct a large subring of K that maps to $\mathbb{Z}/(2^q - 1)\mathbb{Z}$. Define the ring R_q by

$$R_q = \bigcup_{\gcd(n,q)=1} \mathbb{Z}[\sqrt[n]{2}],$$

where n runs over all positive integers relatively prime to q. There is a unique ring homomorphism φ_q from R_q to $\mathbb{Z}/M_q\mathbb{Z}$ that sends $\sqrt[n]{2}$ to 2^a, where $a \in \mathbb{Z}_{>0}$ is such that $an \equiv 1 \bmod q$. Note that $2^a \bmod M_q$ is an n-th root of $2 \bmod M_q$, since $(2^a)^n = (2^q)^{(an-1)/q} \cdot 2 \equiv 2 \bmod M_q$. Let $(\mathbb{Z}/M_q\mathbb{Z})^*$ be the group of units of $\mathbb{Z}/M_q\mathbb{Z}$ and denote the multiplicatively closed subset $\varphi_q^{-1}((\mathbb{Z}/M_q\mathbb{Z})^*)$ of R_q by S_q. Clearly we can extend φ_q uniquely to a ring homomorphism from the ring $S_q^{-1}R_q = \{\frac{v}{w} \in K : v \in R_q \text{ and } w \in S_q\}$ to $\mathbb{Z}/M_q\mathbb{Z}$, which we again denote by φ_q.

The following theorem, which will be proved in the next section, leads directly to our definition of $s \bmod M_q$.

Theorem 2.3. *For every* $s \in K$ *there exists a non-zero integer* k_s *such that for all* $q \in \mathbb{Z}_{>1}$ *with* $\gcd(q, k_s) = 1$ *we have* $s \in S_q^{-1}R_q$.

We motivate Theorem 2.3 with the universal starting value s of Example 2.2. So let s be as in Example 2.2. We can choose $k_s = 2$. To illustrate this we show that $s \in S_q^{-1}R_q$ for $q \in \mathbb{Z}_{>1}$ odd. The integer k_s is relatively prime to q. Therefore $\sqrt{2}$ is an element of R_q. The map $\varphi_q : R_q \to \mathbb{Z}/(2^q-1)\mathbb{Z}$ sends $\sqrt{2}$ to $(2^{(q+1)/2} \bmod 2^q - 1)$. The only prime divisors of 169 and 507 are 3 and 13. The multiplicative orders of (2 mod 3) and (2 mod 13) are 2 and 12 respectively. Since both orders are divisible by k_s, it follows that neither 3 nor 13 divides $2^q - 1$ for q relatively prime to k_s. This implies that both $(3 \bmod 2^q - 1)$ and $(13 \bmod 2^q - 1)$ are elements of $(\mathbb{Z}/(2^q-1)\mathbb{Z})^*$. Therefore the multiplicative set S_q contains the elements 3 and 13. Hence $s \in S_q^{-1}R_q$. In particular one can calculate that $\varphi_5(s)$ equals

$$(21 \bmod 31)(11 \bmod 31)^{-1} + (5 \bmod 31)(14 \bmod 31)^{-1}(2^3 \bmod 31)$$

which is (10 mod 31).

Definition 2.4. *Let $q \in \mathbb{Z}_{>1}$ be an integer and let $s \in S_q^{-1}R_q$. We define $(s \bmod M_q) \in \mathbb{Z}/M_q\mathbb{Z}$ and $\left(\frac{s}{M_q}\right)$ by*

$$(s \bmod M_q) = \varphi_q(s) \text{ and } \left(\tfrac{s}{M_q}\right) = \left(\tfrac{\varphi_q(s)}{M_q}\right).$$

By the phrase "for almost all" we mean that a finite number of exceptions are allowed. For the next definition it is useful to note that if $s \in K$ then for almost all prime numbers p we have $s \in S_p^{-1}R_p$ (see Theorem 2.3).

Definition 2.5. *Let $q \in \mathbb{Z}_{>1}$. A starting value for q is an element $s \in S_q^{-1}R_q$ with the property $\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$. We call s a universal starting value if s is a starting value for almost all prime numbers.*

To prove Example 2.2 one verifies the equalities

$$s - 2 = \frac{(24 - 10\sqrt{2})^2}{-3 \cdot 13^2},$$

$$-s - 2 = \frac{(10 + 24\sqrt{2})^2}{-3 \cdot 13^2},$$

and $\left(\frac{-3}{M_q}\right) = 1$ for $q \in \mathbb{Z}_{>1}$ odd, and then one applies the multiplicative property of the Legendre symbol to conclude that

$$\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1.$$

Hence the value of s in Example 2.2 is a universal starting value.

For a universal starting value s we call a prime number p *bad* if s is not a starting value for p. For the universal starting value of Example 2.2 only 2 is a bad prime. From Theorem 2.1 and the fact that M_q is prime only if q is prime, one easily derives the following theorem, which justifies the term 'universal starting value' in Definition 2.5.

Theorem 2.6. *Let $s \in K$ be a universal starting value, let $k_s \in \mathbb{Z}_{>0}$ be as in Theorem 2.3, let $q \in \mathbb{Z}_{>1}$ be an integer relatively prime to k_s and q not a bad prime, and let $M_q = 2^q - 1$. Define $s_i \in \mathbb{Z}/M_q\mathbb{Z}$ for $i \in \{1, 2, \ldots, q-1\}$ by $s_1 = (s \bmod M_q)$ and $s_{i+1} = s_i^2 - 2$. Then we have*

$$s_{q-1} = 0 \Leftrightarrow M_q \text{ is prime.}$$

In the next section we prove Theorem 2.6. The proof shows that the theorem is also valid with the condition $\gcd(k_s, q) = 1$ replaced by the weaker condition $s \in S_q^{-1}R_q$.

We illustrate Theorem 2.6 with the universal starting value s of Example 2.2 and $q = 5$. We already showed that $s_1 = (10 \bmod 31)$. The next values in the sequence are $s_2 = s_1^2 - 2 = (5 \bmod 31)$, $s_3 = s_2^2 - 2 = (23 \bmod 31)$ and $s_4 = s_3^2 - 2 = (0 \bmod 31)$. Theorem 2.6 implies that M_5 is prime.

In the last section of the present chapter we describe a method to construct families of universal starting values. The following example is made with this method.

Example 2.7. *For every $t \in K$ the element*

$$4 \cdot \frac{t^4 + \sqrt{2}t^3 + 3t^2 - \sqrt{2}t + 1}{(t^2 - \sqrt{2}t - 1)^2}$$

is a universal starting value.

In the next section we prove Example 2.7 using the two equalities

$$4 \cdot \frac{t^4 + \sqrt{2}t^3 + 3t^2 - \sqrt{2}t + 1}{(t^2 - \sqrt{2}t - 1)^2} - 2 = \frac{(\sqrt{2}(t^2 + 2\sqrt{2}t - 1))^2}{(t^2 - \sqrt{2}t - 1)^2},$$

$$-4 \cdot \frac{t^4 + \sqrt{2}t^3 + 3t^2 - \sqrt{2}t + 1}{(t^2 - \sqrt{2}t - 1)^2} - 2 = \frac{-3(\sqrt{2}(t^2 + 1))^2}{(t^2 - \sqrt{2}t - 1)^2}$$

and $\left(\frac{-3}{M_q}\right) = 1$ for $q \in \mathbb{Z}_{>0}$ odd. Taking $t = 0$ and $t = 1$ in Example 2.7 we obtain the two well-known universal starting values 4 and 10 respectively.

Correctness of the Lucas-Lehmer-test

In this section we prove Theorem 2.1, Theorem 2.3, Theorem 2.6, and Example 2.7. We start with a lemma that will be applied in the proof of Theorem 2.1.

Lemma 2.8. *Let $R \neq 0$ be a finite commutative ring. Suppose that for all ideals $\mathfrak{a} \neq R$ of R we have $\#\mathfrak{a} < \sqrt{\#R}$. Then R is a field.*

Proof. Take $x \in R$. Define $\mathfrak{a} = \{r \in R : rx = 0\}$. Then we have $\#Rx = [R : \mathfrak{a}]$, so $\#Rx \cdot \#\mathfrak{a} = \#R$. Since Rx and $\mathfrak{a}$ are both ideals, it follows by our assumption that either $Rx = R$ or $\mathfrak{a} = R$. Hence either $x \in R^*$ or $x = 0$. Since R is also commutative, we conclude that R is a field. □

Proof of Theorem 2.1. Let $M = M_q$. Define the ring R by

$$R = (\mathbb{Z}/M\mathbb{Z})[x]/(x^2 - sx + 1).$$

The equality $x^2 - sx + 1 = 0$ in R implies $x \in R^*$ and $s = x + x^{-1}$. Hence from $s_1 = s = x + x^{-1}$ and $s_{i+1} = s_i^2 - 2$ we get $s_i = x^{2^{i-1}} + x^{-2^{i-1}}$ for all $i \geq 1$, and in particular

$$s_{q-1} = x^{2^{q-2}} + x^{-2^{q-2}}. \tag{2.1}$$

The straightforward calculation $(x-1)^2 = x^2 - 2x + 1 = sx - 2x = (s-2)x$ shows that

$$(x-1)^2 = (s-2)x. \tag{2.2}$$

Assume that R is a field. Then M is prime, $x^2 - sx + 1$ is irreducible in $\mathbb{Z}[x]$ and R over $\mathbb{Z}/M\mathbb{Z}$ is a Galois extension of degree two. The Frobenius map $R \to R$ defined by $\mathrm{Frob} : a \mapsto a^M$ is the non-trivial element of this group (see [6, Chapter 5, §5]). On the other hand one knows that Frob maps one zero of the polynomial $x^2 - sx + 1$ to the other zero of this polynomial, therefore

$$\mathrm{Frob}(x) = x^{-1}. \tag{2.3}$$

The element x is not in the prime field of R, so $x-1$ is nonzero in the field R and therefore a unit. Raising both sides of (2.2) to the power $\frac{M-1}{2}$ yields $\frac{(x-1)^M}{x-1} = \left(\frac{s-2}{M}\right)x^{(M-1)/2}$. The numerator $(x-1)^M$ equals $\mathrm{Frob}(x-1)$ by definition of the Frobenius map, so via (2.3) we see that $\frac{(x-1)^M}{x-1} = \frac{x^{-1}-1}{x-1} = -x^{-1}$. Therefore $-x^{-1} = \left(\frac{s-2}{M}\right)x^{(M-1)/2}$, hence

$$x^{(M+1)/2} = -\left(\frac{s-2}{M}\right). \tag{2.4}$$

Now we drop the assumption R is a field.

"$\Leftarrow$": Suppose that M is prime and $\left(\frac{s-2}{M}\right) = \left(\frac{-s-2}{M}\right) = 1$. The discriminant of $x^2 - sx + 1$ is $s^2 - 4$. From $\left(\frac{-1}{M}\right) = -1$ it follows that $\left(\frac{s^2-4}{M}\right) = \left(\frac{s+2}{M}\right) = -1$. Hence the ring R is a field. From (2.4) it follows that $x^{(M+1)/2} = -1$. Hence by (2.1) we have $s_{q-1} = x^{(M+1)/4} + x^{-(M+1)/4} = (x^{(M+1)/2} + 1)x^{-(M+1)/4} = 0$.

"$\Rightarrow$": Suppose $s_{q-1} = 0$. Recall that $x \in R^*$. Then we have $s_{q-1} = x^{(M+1)/4} + x^{-(M+1)/4} = (x^{(M+1)/2} + 1)x^{-(M+1)/4} = 0$. Therefore $x^{(M+1)/2}$ equals -1. Let $\mathfrak{a} \neq R$ be an ideal of R. We have the natural ring homomorphism $R \to R/\mathfrak{a}$. The integers 2 and M are relatively prime. So $1 \neq 0$ and $M = 0$ in $R/\mathfrak{a}$ imply $2 \neq 0$ in $R/\mathfrak{a}$. Hence $1 \neq -1$ in $R/\mathfrak{a}$. Note that $(M+1)/2$ is a power of 2. Therefore the identity $x^{(M+1)/2} = -1$ in $R/\mathfrak{a}$ implies that the order of x in $(R/\mathfrak{a})^*$ is $M+1$. This yields $\#(R/\mathfrak{a}) > M = \sqrt{\#R}$, which implies $\#\mathfrak{a} < \sqrt{\#R}$. By Lemma 2.8 it follows that R is a field. Hence M is prime and $x^2 - sx + 1$ is irreducible in $(\mathbb{Z}/M\mathbb{Z})[x]$. The discriminant of the irreducible polynomial $x^2 - sx + 1$ is $s^2 - 4$, therefore $\left(\frac{s^2-4}{M}\right) = -1$. From $x^{(M+1)/2} = -1$ and (2.4) it follows that $\left(\frac{s-2}{M}\right) = 1$. Since $\left(\frac{s^2-4}{M}\right) = \left(\frac{s-2}{M}\right)\left(\frac{s+2}{M}\right) = -1$ and $\left(\frac{-1}{M}\right) = -1$, we conclude that $\left(\frac{-s-2}{M}\right) = 1$. □

Proof of Theorem 2.3. Let $n \in \mathbb{Z}_{>0}$ be such that $s \in \mathbb{Q}(\sqrt[n]{2})$. Write s as

$$\frac{1}{2^e c} \cdot \sum_{i=0}^{n-1} a_i \sqrt[n]{2}^i,$$

where $a_i \in \mathbb{Z}$, $c, e \in \mathbb{Z}_{\geq 0}$ and c odd. Take $k_s \in \mathbb{Z}_{>0}$ divisible by n and by order$(2 \bmod p)$ for all prime divisors p of c, where order$(2 \bmod p)$ denotes the order of $(2 \bmod p)$ in the group $(\mathbb{Z}/p\mathbb{Z})^*$. Let $q \in \mathbb{Z}_{>0}$ be such that $\gcd(q, k_s) = 1$. We prove that $s \in S_q^{-1} R_q$. From the definition of R_q it follows that $\sqrt[n]{2} \in R_q$. The inverse of $(2 \bmod 2^q - 1)$ is $(2^{q-1} \bmod 2^q - 1)$, so $2 \in S_q$. In order to prove that $s \in S_q^{-1} R_q$, it suffices to show that for all prime divisors p of c we have $p \in S_q$. Let p be any prime divisor of c. By our assumption on k_s we have $\gcd(q, \text{order}(2 \bmod p)) = 1$. Since order$(2 \bmod p) > 1$, this implies $2^q - 1 \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Therefore $\gcd(2^q - 1, p) = 1$, and so $p \in (\mathbb{Z}/(2^q - 1)\mathbb{Z})^*$. Hence we can conclude that $p \in S_q$. □

Proof of Theorem 2.6. Since $\gcd(q, k_s) = 1$, we have $s \in S_q^{-1} R_q$, hence $s \bmod M_q$ is well defined. Suppose that $s_{q-1} = 0$. Then from Theorem 2.1 it follows that M_q is prime.

Suppose M_q is prime. Then q is prime. Since s is a universal starting value, q is prime and $q \notin B_s$, we conclude that s is a starting value for q. Applying Theorem 2.1 yields $s_{q-1} = 0$. □

Proof of Example 2.7. The discriminant of $t^2 - \sqrt{2}t - 1$ is 6. Now we apply Theorem 3.4 (the proof of Theorem 3.4 does not use Example 2.7) to conclude that $t^2 - \sqrt{2}t - 1$ has no zeros in K. By Theorem 2.3 there exists an integer $k \in \mathbb{Z}_{>0}$ such that t, $t^2 - \sqrt{2}t - 1$, $t^2 + 2\sqrt{2}t - 1$, $t^2 + 1$ and $\sqrt{2}$ are elements of $S_q^{-1} R_q$ if $\gcd(k, q) = 1$. Hence

$$s = 4 \cdot \frac{t^4 + \sqrt{2}t^3 + 3t^2 - \sqrt{2}t + 1}{(t^2 - \sqrt{2}t - 1)^2} \in S_q^{-1} R_q$$

and the two equalities below Example 2.7 can be interpreted in $S_q^{-1} R_q$ if k and q are relatively prime. Let p be an odd prime number not dividing k. Then we have $s \in S_p^{-1} R_p$. From the two equalities below Example 2.7, the identity $\left(\frac{-3}{M_p}\right) = 1$ and the fact that φ_p is a ring homomorphism it follows that s is a starting value for p. Hence s is a universal starting value. □

Constructing universal starting values

In this section we give a method to produce theorems similar to Example 2.7. In particular we show how one can find identities just like the one following Example 2.7.

In this section we call an element $a \in K$ a *pseudo-square* if $\left(\frac{a}{M_p}\right) = 1$ for almost all prime numbers p. Anarghya Vardhana found the following 9 multiplicatively independent pseudo-squares (see [17]):

$$\begin{aligned} 2, \\ -3 &= -1 \cdot 3, \\ -91 &= -1 \cdot 7 \cdot 13, \\ -6355 &= -1 \cdot 5 \cdot 31 \cdot 41, \\ -76627 &= -1 \cdot 19 \cdot 37 \cdot 109, \\ -8435 &= -1 \cdot 5 \cdot 7 \cdot 241, \\ 790097 &= 7 \cdot 11 \cdot 31 \cdot 331, \\ 133845041 &= 11 \cdot 61 \cdot 151 \cdot 1321, \\ -33678726917899 &= -1 \cdot 7 \cdot 43 \cdot 1429 \cdot 5419 \cdot 14449. \end{aligned}$$

Theorem 2.9. *Let $a, b \in K$ be pseudo-squares, let $x, y \in K$ be such that $-4 = ax^2 + by^2$. Then $\frac{ax^2 - by^2}{2}$ is a universal starting value. Moreover if we write*

$$\begin{aligned} c_0 &= a^3x^2 - a^2by^2, \\ c_1 &= 8a^2bxy, \\ c_2 &= -6a^2bx^2 + 6ab^2y^2, \\ c_3 &= -8ab^2xy, \\ c_4 &= ab^2x^2 - b^3y^2. \end{aligned}$$

then for each $t \in K$ the element $(c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/(2(bt^2 + a)^2)$ is a universal starting value.

Proof. Define s by $2s = ax^2 - by^2$. We will prove that s is a universal starting value. From the identity $2s = ax^2 - by^2$ and the identity $-4 = ax^2 + by^2$ it follows that $s - 2 = ax^2$ and $-s - 2 = by^2$. Theorem 2.3 and the fact that both a and b are pseudo-squares imply that $\left(\frac{s-2}{M_p}\right) = \left(\frac{-s-2}{M_p}\right) = 1$ for almost all prime numbers p. Hence $s = (ax^2 - by^2)/2$ is a universal starting value.

Next we show that $bt^2 + a \neq 0$. Suppose for a contradiction that there exists $t \in K$ such that $bt^2 + a = 0$. This yields $bt^2 = -a$, but then both a and $-a$ are pseudo-squares. This is a contradiction since $\left(\frac{-1}{M_p}\right) = -1$ for all integers $p > 1$. Hence $bt^2 + a \neq 0$.

Via the identity $-4 = ax^2 + by^2$ we can parametrize all $v, w \in K$ such that $-4 = av^2 + bw^2$ (see [15, Chapter 1, §1]). The parametrization $w(t) = t \cdot (v(t) - x) + y$ and some calculations (as described in [15, Chapter 1, §1]) yield $v(t) = \frac{-bxt^2 + 2byt + ax}{bt^2 + a}$ and $w(t) = \frac{-byt^2 - 2axt + ay}{bt^2 + a}$. Now the definition of c_0, c_1, c_2, c_3 and c_4 are such that $(c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/2(bt^2 + a)^2 = (a \cdot v(t)^2 - b \cdot w(t)^2)/2$ holds. Hence the first part of Theorem 2.9 implies that $(c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/2(bt^2 + a)^2$ is a universal starting value. □

Example 2.10. Take $a = b = -3$ as pseudo-squares. Take $x = \frac{2}{3}$ and $y = \frac{2}{3}\sqrt{2}$. Then

$$
\begin{aligned}
c_0 &= 12,\\
c_1 &= -96\sqrt{2},\\
c_2 &= -72,\\
c_3 &= 96\sqrt{2},\\
c_4 &= 12
\end{aligned}
$$

and for every $t \in K$ the value $f(t) = (c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/(2(a + bt^2)^2)$ is a universal starting value. For example

$$
\begin{aligned}
&f(0) = \tfrac{2}{3},\\
&f(2) = -\tfrac{14}{75} + \tfrac{32}{25}\sqrt{2} \text{ and}\\
&f(-\tfrac{1}{2}\sqrt[4]{2}) = \tfrac{118}{49} - \tfrac{800}{147}\sqrt[4]{2} - \tfrac{96}{49}\sqrt[4]{2}^2 + \tfrac{704}{147}\sqrt[4]{2}^3
\end{aligned}
$$

are all three examples of universal starting values.

Example 2.11. Take $a = b = -3 \cdot 5 \cdot 13 \cdot 241$ as pseudo-squares. Take $x = -121 + 32\sqrt{2}$ and $y = 32 + 121\sqrt{2}$. Then

$$
\begin{aligned}
c_0 &= 54468 - 61952\sqrt{2},\\
c_1 &= 123904 - 435744\sqrt{2},\\
c_2 &= 326808 + 371712\sqrt{2},\\
c_3 &= -123904 + 435744\sqrt{2},\\
c_4 &= -54468 - 61952\sqrt{2}.
\end{aligned}
$$

and for every $t \in K$ the value $(c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/(2(a + bt^2)^2)$ is a universal starting value.

Remark. Searching for $x, y \in K$ such that $-4 = ax^2 + by^2$ can be done using Hasse-Minkowski theorem as described in the introduction of [16, § Introduction, page 2], or in the case that $a = b \in \mathbb{Z}$ by solving the equation $-4a = (x + \mathrm{i}y)(x - \mathrm{i}y)$ in the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers.