International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452
Maths 2020; 5(5): 41-47

www.mathsjournal.com
Received: 23-06-2020
Accepted: 26-07-2020

Simon Davis
Research Foundation of Southern California, Villa La, Jolla Drive, La Jolla, California

Corresponding Author:
Simon Davis
Research Foundation of Southern California, Villa La, Jolla Drive, La Jolla, California

Approximate Roots to a Thue equation

Simon Davis

Abstract
The roots of a Thue equation are investigated. A new form of the sixth-order equation is derived. The irreducibility of certain classes of polynomials of degree six over ℤ[x] is established. Conditions for factorizability by linear and quadratic factors are given.

Keywords: Approximate Roots, investigated, equation

1. Introduction
The Thue equation is an equation in two variables with integer coefficients which is homogeneous except for a constant term. When one of the variables is set equal to a fixed value, it becomes analgebraic equation in one variable that has a maximum number of roots equal to the degree. Similarly, the number of solutions to the Thue equation is finite [1]. It has been proven that the maximum number is five for binary cubic forms with integral coefficients [2] and a negative determinant and it equals seven for this class of forms with sufficiently large positive determinants [3]. An algorithm for deriving the bounds on magnitudes of the two variables in a solution to the equation also can be given [4].

The Thue equation for a relation of nth degree, which can be factorized into product of quadratic and degree n-2 polynomials, is analyzed. The coefficient of the linear term is known to be a solution to an equation of degree n-3 for odd n and n-4 for even n. Given the form of the auxiliary equation, statistical methods can be used to deduce the approximate location of the roots in the complex plane. From the mean and the variance, the range of the solutions may be determined with a probability of 99%. These estimates compare favourably with the bounds found from a basis reduction algorithm [2]. This analysis is extended to general sixth order equations. The condition of real integer roots restricts an arbitrary sixth-order equation to a special form. The factorization of these polynomials with is investigated methodically beginning with the partitions of the maximal degree. The factorizations with linear terms may be checked through congruences. Since the degree is 6, the products of quadratic and degree 4 polynomials together with the factorizations into two cubics will yield conditions on the coefficients which can be solved. It is found that the polynomial x^6-Bx-1
is irreducible over ℤ[x] for B not equal to zero. Furthermore, the solutions to the conditions
for the product of two cubics generates two different representations of x^6-1. Such representations may determine for other degrees and factorizations. The irreducibility of more general polynomials of degree 6 is considered by deriving congruence conditions for linear and quadratic factors.

2. The Location of the Roots of the Thue Equation
Upon consideration of the factorization of X^n-BX-A,

$$X^n-BX-A=(X^2-bX-a)(X^{n-2}+c_{n-3}X^{n-3}+...+c_0) \quad (2.1)$$

Where

$$A=ac_0$$
$$B=ac_1+bc_0 \quad (2.2)$$
$$0 = -ac_2-bc_1+c_0:$$
$$0 = -b+c_{n-3}.$$

Consider the functions $F_0(X)=1$, $F_1(X)=1$, $F_i(X)=F_{i-1}(X)+XF_{i-2}(X)$
and
$f_i(X,Y)=Y^j Fi\,(X/Y)$ where $j=[i/2]$ [5]. If n is even,

$$F_{n-2}(1/Y^2)=1/Y^{n-2}+\binom{n/2}{n/2-2}1/Y^{n-4}+\dots+\binom{n-3}{1}1/Y^2+1. \qquad (2.3)$$

If n is odd,

$$F_{n-2}(1/Y^2)=(n-1)/2\;1/Y^{n-3}+\binom{(n+1)/2}{(n-5)/2}1/Y^{n-5}+\dots+\binom{n-3}{1}1/Y^2+1. \qquad (2.4)$$

Suppose that A=1 and a=1. Then, it can be shown that the integer b belongs to the set of solutions to

$$F_{n-2}(1/Y^2) = 1/Y^{n-2} \text{ n even} \qquad (2.5)$$

and

$$F_{n-2}(1/Y^2)=1/Y^{n-3} \text{ n odd.} \qquad (2.6)$$

For n odd,

$$(n-1)/2\;1/Y^{n-3}+\binom{(n+1)/2}{(n-5)/2}1/Y^{n-5}+\dots+\binom{n-3}{1}1/Y^2+1=1/Y^{n-3} \qquad (2.7)$$

and multiplying by Y^{n-3},

$$Y^{n-3}+(n-3)Y^{n-5}+\dots+(n+1)(n-1)(n-3)/48\,Y^2+(n-3)/2=0. \qquad (2.8)$$

Let $W=Y^2$. Then, Eq. (2.8) is

$$W^{(n-3)/2}+(n-3)\,W^{(n-5)/2}+\dots+(n+1)(n-1)(n-3)/48\,W+(n-3)/2=0. \qquad (2.9)$$

If $\lambda_1,\dots,\lambda_{(n-3)/2}$ are the roots of this equation,

$$\lambda_i < 0 \text{ for all } i$$
$$\sum_{i=1}^{n-3/2}\lambda_i = 3-n$$
$$\sum_{i<j}\lambda_i\lambda_j=(n-3)(n-4)/2 \qquad (2.10)$$
$$\sum_{i<j<k}\lambda_i\lambda_j\lambda_k = -(n-5)(n-6)(n-7)/3!\,.$$

Then the distribution of roots will have the average

$$\bar{\lambda}=(3-n)/((n-3)/2)=-2 \qquad (2.11)$$

and variance

$$\bar{\sigma}^2=1/((n-3)/2)\sum_{i=1}^{(n-3)/2}\lambda_i^2-\lambda^2$$

$$=2/(n-3)\left[\left(\sum_{i=1}^{n-3}\lambda_i\right)^2-2\sum_{i<j}\lambda_i\lambda_j\right]-4 \qquad (2.12)$$

$$=2/(n-3)\left[(3-n)^2-2\cdot(n-4)(n-5)/2\right]-4$$

$$=2/(n-3)(3n-11)-4=(2n-10)/(n-3).$$

Since the standard deviation equals

$$\sigma=\sqrt{(2n-10)/(n-3)}, \qquad (2.13)$$

99% of the roots in a normal distribution would be located within the circle $|\lambda+2|\le$

$3\sqrt{(2n-10)/(n-3)}$.

In the determination of the a factorization of the n^{th}-order polynomial, the coefficient b in the quadratic factor X^2-bx-a can be restricted approximately to the interval

$[-2-3\sqrt{(2n-10)/(n-3)},\ 2+3\sqrt{(2n-10)/(n-3)}]$.

For lower values of the odd degree, exceptional values might occur. For example, when n=5, there are only six known monic polynomials X^5-X-A equal to a product of irreducible quadratic and cubic polynomials in Z[X], and if A=1, the only known factorization is
$X^5+X-1=(X^2-X+1)(X^3+X^2-1)$, for which b=1 and a=-1 [5].

For n even,

$$1/Y^{n-2}+\binom{n/2}{n/2-2}\binom{n/2}{1}1/Y^{n-4}+\ldots+\left(n-3\right)1/Y^{2}+1=1/Y^{n-2}. \quad (2.14)$$

and

$$Y^{n-4}+(n-3)Y^{n-6}+\ldots+1/2\ n/2\ (n/2-1)=0. \quad (2.15)$$

Since each of the coefficients is positive for $n\geq 6$, there are no real solutions for b. It follows that are no integer solutions for a factorization of the form $X^n-BX-1=(X^2-bX-1)(X^{n-2}+c_{n-3}X^{n-3}+\ldots+1)$ for even n
larger than 4. This is consistent with Thue's theorem on the set of integer solutions to the to
g(x,y)=m for a homogeneous polynomial g(X,Y), where $G(X/Y)=1/Y^{\deg g}\, g(x,y)$ has three distinct roots [1]

3. The Distribution of Coefficients of the Linear Term when A≠1 and a≠1

Since the Thue equation is $f_{n-2}(a,Y^2)=A/a$,

$$aY^{n-2}F_{n-2}(a/Y^2) = A \text{ if n is even}$$
$$(3.1)$$
$$aY^{n-3}F_{n-2}(a/Y^2) = A \text{ if n is odd}$$

The equations and the means and variances distributions of the roots may be found generally.
When n is even,

$$F_{n-2}(a/Y^2) = a^{n-2/2}\binom{}{n/2-2}/Y^{n-2}+\binom{n/2}{1}a^{n-2/2}/Y^{n-4}+\ldots+\left(n-3\right)a/Y^{2}+1=1/Y^2. \quad (3.2)$$

and

$$aY^{n-2}F_{n-2}(a/Y^2) = a^{n/2}+a^{n/2-1}\binom{n/2}{n/2-2}Y^{2}+\ldots+a^{2}(n-3)Y^{n-4}+aY^{n-2}=A \quad (3.3)$$

Then

$$Y^{n-2}+a(n-3)Y^{n-4}+\ldots+a^{n/2-2}\binom{n/2}{n/2-2}Y^{2}+a^{n/2-1}-A/a=0 \quad (3.4)$$

and, if $W=Y^2$,

$$W^{n-2/2}+a(n-3)W^{n-4/2}+\ldots+a^{n/2-2}\left(n/2\right)W\,a^{n/2-1}-A/a=0 \quad (3.5)$$

n/2-2

Again, there are no real solutions for b if a> $A^{2/n}$ and a>0.

The roots would satisfy

$$\sum_{i=1}^{n-2/2} \lambda_i = a(3-n)$$

$$\sum_{i<j} \lambda_i \lambda_j = a^2 (n-4)(n-5)/ 2 \qquad (3.6)$$

and

$$\bar{\lambda}=-2a(n-3)/(n-2) \qquad (3.7)$$

While

$$\sigma^2=1/ ((n-2)/2) \sum_{i=1}^{(n-2)/2} \lambda_i^2 - \bar{\lambda}^2$$

$$=2/(n-2) \ [((n-2)/2)^2 \bar{\lambda}^2 -2 \sum_{i<j} \lambda_i \lambda_j] - \bar{\lambda}^2$$

$$= 2/(n-2) \ \{a^2(n-3)^2-a^2(n-4)(n-5)\}- \bar{\lambda}^2$$

$$=(2a^2)/(n-2)\{[(n^2-6n+9)-(n^2-9n+20)]-4a^2(n-3)^2\}/(n-2)^2$$

$$=2a^2 (n-1)(n-4)/(n-2)^2 \qquad (3.8)$$

The range containing 99% of the roots in a normal distribution

$[-2a(n-2)/(n-3)-3\sqrt{2}a \sqrt{(n-1)(n-4)/ n-2}, -2a(n-2)/(n-3)+3\sqrt{2}a \sqrt{(n-1)(n-4)/ n-2}]$

As $n\to\infty$, $\sigma\to$ 2a2 and this range tends to $[(-2-3\sqrt{2})a, (-2+3\sqrt{2})a]$.

4. An Alternative Form of the Sixth-Order Equation

When n=6, the factorization would have the form

$$X^6-BX-A=(X^2-bX-a)(X^4+c_3X^3+c_2X^2+c_1X+c_0) \qquad (4.1)$$

Where the quadratic and quartic polynomials are irreducible, From the results of the previous section, there is no such equality with A=1, a=1 integer and B, b, c_0, c_1, c_2, $c_3 \in \mathbb{Z}$.

Suppose that three quadratic factors are multiplied.

$$(x^2-b_1x-1)(x^2-b_2x-1)(x^2-b_3x-1)=x^6-(b_1+b_2+b_3)x^5 +(b_1b_2+b_1b_3+b_2b_3-3)x^4 \qquad (4.2)$$

$$+(2(b_1+b_2b_3)-b_1b_2b_3)x^3-(b_1b_2+b_1b_3+b_2b_3-3)x^2$$

$$- (b_1+b_2+b_3)x-1$$

The sixth-order polynomial has integer coefficients if

$$b_1+b_2+b_3 \in \mathbb{Z}$$

$$b_1b_2+b_1b_3+b_2b_3 \in \mathbb{Z} \qquad (4.3)$$

$$b_1b_2b_3 \in \mathbb{Z}$$

Let $\arg(b_3)=-1/2 \arg(b_1+b_2)$ and $| b_1+b_2 |=m/ |b_3|^2$.

$$(b_1+b_2)= | b_1+b_2 | (\cos \theta_{12}+i \sin \theta_{12})$$

$$b_3= | b_3 | (\cos \theta_3+i \sin \theta_3) \qquad (4.4)$$

Then

$| b_1+b_2 | \sin \theta_{12} + | b_3 | \sin \theta_3 = m/| b_3 |^2 \sin \theta_{12} + | b_3| \sin \theta_3$

$= m/ | b_3|^2 \sin \theta_{12} - | b_3 | \sin (\theta_{12}/2) = 0$ (4.5)

and

$| b_1+b_2 | \cos \theta_{12} + | b_3 | \cos \theta_3 = m/| b_3|^2 \cos \theta_{12} + |b_3| \cos (\theta_{12}/2) \in \mathbb{Z}$ (4.6)

Eq.(4.5) implies that

$| b_3 |^3 = 2m \cos (\theta_{12}/2)$ (4.7)

and Eq.(4.6) gives

$m/(2^{2/3} m^{2/3}) (\cos \theta_{12})/\cos (\theta_{12} /2)^{2/3} + |b_3| \cos (\theta_{12}/2) \in \mathbb{Z}$ (4.8)

Since $\cos \theta_{12} = 2 \cos 2(\theta_{12}/ 2)-1$, it follows that

$2^{4/3} \cos^{4/3}(\theta_{12}/2) -1/2^{2/3} 1/\cos^{2/3}(\theta_{12}/2) = m'/m^{1/3}$ (4.9)

Let $x=2^{1/3} \cos^{1/3} (\theta_{12}/2)$. Then

$x^4-1/x^2=m'/m^{1/3}$ (4.10)

and

$x^6- m'/m^{1/3} x^2-1=0.$ (4.11)

This special form has been derived entirely from the conditions on the coefficients.

5. Congruence Conditions for Factorization

Consider the polynomial x^6 -Bx-1. If x+1 is a factor, (-1)^6-B(-1)-1-B=0. Again, B must be zero. If B≠0, it has not linear factors over $\mathbb{Z}[x]$. Consider the partitions of 6:
51 411 3111 21111 111111
42 321 222 2211
33

The factorizations corresponding to the partitions 42 and 222 may be eliminated. Suppose, for example,

$x^6-Bx-1=(x^2-bx+1)(x^4+c_3x^3+c_2x^2+c_1x-1)$

Then

$c_3-b=0 \quad c_3=b$

$c_2-bc_3+1=0 \quad c_2=b^2-1$

$c_1-bc_2+c_3=0 \quad c_1-b^3+2b=0$ (5.1)

$-1-bc_1+c_2=0 \quad b^4-3b^2+2=(b^2-2)(b^2-1)=0$

$b+c_1=-B.$

The only integer solutions for b are ±1. If b=1, c_1=-1 and B=0. When b=-1, c_1=1 and, again, B=0. Therefore, there is factorization into a product of polynomials of degree 4 and 2 with integer coefficients. Since the product of two monic quadratic polynomials is a monic quartic polynomials, there does not exist a factorization into the product of three quadratic polynomials over ℤ[x].

The factorization corresponding to 33 is

$(x^3+b_2x^2+b_1x+1)(x^3+c_2x^2+c_1x-1)$

$=x^6+(b_2+c_2)x^5+(b_2c_2+b_1+c_1)x^4+(b_1c_2+b_2c_1)x^3+(-b_2+c_2+b_1c_1)x^2+(-b_1+c_1)x-1$

$b_2+c_2=0 \quad c_2=-b_2$

$b_2c_2+b_1+c_1=0 \quad b_2^2 - (b_1+c_1)=0$ (5.2)

$b_1c_2+b_2c_1=0 \quad -b_2b_1+b_2(b_2^2-b_1)=b_2^3-2b_1b_2=0$

$-b_2+c_2+b_1c_1=0 \quad -2b_2+b_1(b_2^2-b_1)=b_1b_2^2-b_1^2-2b_2=0$

$-b_1+c_1=-B.$

One solution to $b_1b_2^2-b_1^2-2b_2=0$ is $b_1=b_2=-1$ and $c_2=1$ and $c_1=2$. However, the equation $b_2^3-2b_1b_2=0$ is not satisfied. Now consider the general formula $b_1=k\,b_2^2$. Then $kb_2^4-k^2b_2^4-2b_2=0$, which requires $(k-k^2)b_2^3=2$ with the integer solution k=2 and $b_2=-1$. It would follow that $b_1=-2$, $c_2=1$ and $c_1=3$, which is not a solution to $b_2^3-2b_1b_2=0$. If k=1/2 and $b_2=2$ and $b_1=2$. Then $b_2^3-2b_1b_2$ would equal zero and $c_1=2$. Consequently, there are two factorizations with integer coefficients when B=0:
$x^6-1=(x^3+1)(x^3-1)=(x^3+2x^2+2x+1)(x^3-2x^2+2x-1)$. The polynomial x^6-Bx-1 is irreducible over ℤ[x] for B≠0.

When A is prime, any linear factor of x^6-Bx-A must be x-A, x+A, x-1 or x+1 If x=1, A=1-B, and $x^6-Bx-A=x^6-Bx+B-1$. Consider the factorization of the sixth-order polynomial

$$x^6-BX+B-1=(x^5+x^4+x^3+x^2+x-(B-1))(x-1). \quad (5.3)$$

Like the cyclotomic polynomials, Eisenstein's criterion cann be used immediately for the remaining factor $x^5+x^4+x^3+x^2+x-(B-1)$. However, the shift $x \rightarrow x+1$ yields the polynomial $x^5+\binom{6}{1}x^4+\dots+\binom{6}{4}x+(5-(B-1))$.

The primes 2 and 3 do not divide $\binom{6}{k}$ for all k, $1 \leq k \leq 4$. Then $2 \mid (5-(B-1))$ if B is even, and $3 \mid (5-(B-1))$ if B=3k, k∈ ℤ.
Since Eisenstein's criterion cannot be used,
$x^5+6x^4+\dots+\binom{6}{4}x+(5-(B-1))$ might be reducible over ℤ [X] when B is even and
$4 \nmid (5-(B-1))$ or B=3k and $9 \nmid (5-(B-1))$.
Suppose $4 \nmid (5-(B-1))$. Then $4 \nmid (B-6)$ and $B \nmid 4k+2$, k ∈ℤ. It follows that B=4k, k ∈ ℤ. Let
$9 \nmid (5-(B-1))$.
Then $9 \nmid (B-6)$ and $B \neq 9k+6$ for k ∈ ℤ.
Similarly, $x^5+x^4+x^3+x^2+x-(B-1)$ could be reducible over ℤ[x] when $B \equiv 0 \pmod 4$ and $B \equiv 0 \pmod 3$, $B \not\equiv 6 \pmod 9$. For example, $x^5+x^4+x^3+x^2+x+1=(x^4+x^2+1)(x+1)=(x^3+1)(x^2+x+1)$. Suppose that the powers of a variable t are found modulo the linear monomial t+a.
Then,

$$t \equiv -a t^2 \equiv a^2 \quad (5.4)$$
$$t^3 \equiv -a^3:$$
$$t^n \equiv (-1)^n a^n.$$

The factorization of t^n+t+b by t^2-t+a over follows from the congruences

$t^2 \equiv t-a \quad (\text{mod } t^2-t+a)$

$t^3 \equiv (1-a)t-a \quad (\text{mod } t^2-t+a)$ (5.5)

$t^k \equiv f_k(a)t-a f_{k-1}(a) \quad (\text{mod } t^2-t+a)$

$f_{k+1}(a)=f_k(a)-af_{k-1}(a), \quad k\geq 2.$

The polynomial t^n+t+b is divisible by t^2-t+a if and only if $f_n(a)+1=0$ and $b=af_{n-1}(a)$.
An example is $f_n(2)=-1$ for n=3, 5, 13.

$t^3+t+2=(t^2-t+2)(t+1)$

$t^5+t-6=(t^2-t+2)(t^3+t^2+t-3)$
(5.6)

$t^{13}+t+90=(t^2-t+2)(t^{11}+t^{10}-t^9-3y^8-t^7+5t^6+7t^5-3t^4-17t^3-11t^2+23t+45)$

There exists only a finite number of solutions to $f_n(a)=-1$ for each value of n.
Similarly, t^k-Bt-A is divisible by t^2-t+a if $f_k(a)=B$ and $af_{k-1}(a)=-A$.
Iteration of the congruence $t^k\equiv f_k(a)t-af_{k-1}(a)$ (mod t^2+bt+a) yields

$t^{k+1} \equiv f_k(a)t^2-a f_{k-1}(a)t$
$\equiv f_k(a)(-bt-a)-af_{k-1}(a)t$ (5.7)
$\equiv (-bf_k(a)-a f_{k-1}(a))t-af_k(a)$
$=f_{k+1}(a)t-af_k(a)$

Setting $f_1(a)=1$ and $f_2(a)=-b$,
$f_3(a)=b^2-a$
$f_4(a)=-b^3+2ab$ (5.8)
$f_5(a)=b^4-3ab^2+a2$
$f_6(a)=-b^5+4ab^3-3a^2b$

It follows that
$t^3 \equiv (b^2-a)t+ab$
$t^4 \equiv (-b^3+2ab)t-a(b^2-a)$ (5.9)

$t^5 \equiv (b^4-3ab^2+a^2)t+a(b^3-2ab)$
$t^6 \equiv (-b^5+4ab^3-3a^2b)t+a(b^4-3ab^2+a^2)$ and the polynomials t^n-Bt-A divisible by t^2+bt+a can be deduced from this list of congruences. The factorization can be used to determine irreducibility criteria for polynomials of degree less than or equal to six.

6. Conclusion

The factorization of the polynomial X^n-Bx-A yields a Thue equation for the linear coefficient in any quadratic factor over $\mathbb{Z}[x]$. The auxiliary equations for n odd and n even have degrees n-3 and n-4 respectively. The average value of the roots and the variance may be determined by the expressions for the symmetric polynomials in terms of the coefficients. Given a random Gaussian distribution, the region including the roots with a probability of 99% may be defined.
These estimates reduce the time necessary to search for the location of the roots and refine the procedure for determining their values through previous bounds.
It may be concluded from the Thue equation that there exists no factorization of X^n-BX-1 with a quadratic factor over $\mathbb{Z}[x]$ if $n\geq 6$ is even.
Therefore, any partitions of the degree n representing the products of factors with integer coefficients would not include 2. Therefore, this result improves the efficiency of the search for the factorization of this polynomial for even n. An example is given by n=6, where a linear factor is excluded by congruence conditions.
There remains the product of two cubics which is found to be valid only for B=0. The two factorizations of x^6-1 are $(x^3+1)(x^3-1)$ and $(x^3+2x^2+2x+1)(x^3-2x^2+2x-1)$. The polynomial X^6-BX-1 is irreducible over $\mathbb{Z}[x]$ when $B\neq 0$.
The polynomials x^n-1 have unique factorizations with integer coefficients for $n\leq 7$ and $n\neq 6$.
For each fachtorization, there will be a set of n-1 nonlinear conditions for n-2 undetermined coefficients which will not have integer solutions generally. This result raises the problem of establishing the existence of all polynomials with integer coefficients with a minimum of two representations for some set of degrees of the factors.

7. References

1. Thue A. Űber Annäherungswerte algebraischer Zahlen, J. Reine Angew. Math. 1909; 135:284-305.
2. Tzanakis N, de Weger BMM. On the Practical Solution of the Thue Equation, J. Number Theory. 1989; 31:99-132.
3. Delaunay B. Űber die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante, Math. Zeit. 1930; 31:1-26.
4. Nagell T. Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante, Math. Zeit. 1928; 28:10-29.
5. Ribenboim P. On the Factorization of Xn-BX-A, L'Enseignement Mathèmatique. 1991; 37:191-200.