

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 37 (1991)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ON THE FACTORIZATION OF $X^n - BX - A$
Autor: Ribenboim, P.
DOI: <https://doi.org/10.5169/seals-58737>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 01.04.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

ON THE FACTORIZATION OF $X^n - BX - A$

by P. RIBENBOIM

1. Rabinowitz [Ra] proved that the only integers A , for which $X^5 - X - A$ is a product of an irreducible quadratic and an irreducible cubic polynomial with coefficients in \mathbf{Z} , are $A = \pm 15$, ± 22440 , and ± 2759640 . The factorizations are

$$X^5 - X \pm 15 = (X^2 \pm X + 3) (X^3 \mp X^2 - 2X \pm 5) ,$$

$$X^5 - X \pm 22440 = (X^2 \mp 12X + 55) (X^3 \pm 12X^2 + 89X \pm 408) ,$$

$$X^5 - X \pm 2759640 = (X^2 \pm 12X + 377) (X^3 \mp 12X^2 - 233X \pm 7320) .$$

Similarly

$$X^5 + X \pm 1 = (X^2 \pm X + 1) (X^3 \mp X^2 \pm 1) ,$$

$$X^5 + X \pm 6 = (X^2 \pm X + 2) (X^3 \mp X^2 - X \pm 3)$$

are the only similar decompositions for polynomials $X^5 + X - A$.

This rather interesting result requires, in last analysis, the fact that 1, 144 are the only non-zero Fibonacci numbers which are squares.

We shall extend this result for the polynomials $X^n - BX - A$, where A is a given non-zero integer and $n \geq 5$, and also for the polynomials of the same type, where B is a given non-zero integer, and $n > 5$.

The proof is elementary, except in one of the cases, where Thue's theorem (see [Th]) is required. Due to Baker's work (see [Sh-Ti], page 99), an explicit bound for the solutions of Thue's equation is now known, making our result also effective.

I am grateful to J. Top for discussions about this paper.

The proof is elementary, except for the use of Thue's theorem and a theorem of Pethö, Shorey & Stewart concerning the squares in recurring sequences.

2. For the convenience of the reader, we recall all needed facts.

Thue's theorem [Th] states:

Let $G \in \mathbf{Z}[X]$ be a polynomial with at least three distinct roots, let $g(X, Y)$ be the associated homogeneous polynomial.

For every integer m , there exist at most finitely many pairs of integers (x, y) such that $g(x, y) = m$. Due to the work of Baker (see [Sh-Ti], page 99), an explicit bound for the solutions x, y of Thue's equation is now known.

We shall encounter also the diophantine equation $X^2 - 5Y^4 = 4B$. This will lead to the study of $X^2 - 5Y^2 = 4B$ and to the determination of its solutions (x, y) such that y is a square.

The equation $X^2 - 5Y^2 = 4B$ has been studied by Stolt [St] and we gather here the results to be needed.

Let $S = \left\{ \alpha = \frac{a + b\sqrt{5}}{2} \mid a, b \in \mathbf{Z}, a^2 - 5b^2 = 4B \right\}$. If $S \neq \emptyset$ then $B \neq 0$,

and if $\frac{a + b\sqrt{5}}{2} \in S$ then $a \equiv b \pmod{2}$. Also $b = 0$ exactly when B is a

square, and if $\frac{a + b\sqrt{5}}{2}, \frac{a' + b'\sqrt{5}}{2} \in S$, then $a = \pm a'$.

We recall that the units of the number field $\mathbf{Q}(\sqrt{5})$ are $\pm \omega^n$ (for $n \in \mathbf{Z}$), where $\omega = \frac{1 + \sqrt{5}}{2}$; since ω has norm equal to -1 , then the units of norm 1

are $\pm \zeta^n$ (for $n \in \mathbf{Z}$) where $\zeta = \omega^2 = \frac{3 + \sqrt{5}}{2}$.

We say that $\alpha, \alpha' \in S$ are equivalent when $\frac{\alpha}{\alpha'} = \pm \zeta^n$ (where $n \in \mathbf{Z}$). We

say that $\alpha = \frac{a + b\sqrt{5}}{2} \in S$ is fundamental when $0 \leq b$ and if $\alpha \sim \alpha'$

$= \frac{a' + b'\sqrt{5}}{2}$ then $b \leq |b'|$. Thus each equivalence class contains one, and

at most four fundamental elements.

Now we show that there are only finitely many equivalence classes in S ; more explicitly, the number of equivalence classes is at most equal to $\sqrt{|B|}$.

It suffices to show that if $\alpha = \frac{a + b\sqrt{5}}{2}$ is a fundamental element, then

$b \leq \sqrt{|B|}$. Indeed $\frac{a + b\sqrt{5}}{2} + \frac{3 + \sqrt{5}}{2} = \frac{1}{2} \left(\frac{3a + 5b}{2} + \frac{3b + a}{2} \sqrt{5} \right)$ and

$\frac{a + b\sqrt{5}}{2} + \frac{3 - \sqrt{5}}{2} = \frac{1}{2} \left(\frac{3a - 5b}{2} + \frac{3b - a}{2} \sqrt{5} \right)$. Since $\frac{a + b\sqrt{5}}{2}$ is funda-

mental, then $b \leq \left| \frac{3b + a}{2} \right|$, $b \leq \left| \frac{3b - a}{2} \right|$.

If $0 \leq \frac{3b+a}{2}$ then $-a \leq b$ hence $5b^2 + 4B = a^2 \leq b^2$ so $b^2 \leq -B = |B|$ hence $b \leq \sqrt{|B|}$. If $\frac{3b+a}{2} \leq 0$ then $5b \leq -a$ and $25b^2 \leq a^2 = 5b^2 + 4B$ so $b \leq \sqrt{\frac{B}{5}} \leq \sqrt{|B|}$. The other cases give the same bound for b .

Now, we consider the equivalence class of the fundamental element $\frac{a+b\sqrt{5}}{2}$. Define the integers x_n, y_n (for every $n \in \mathbf{Z}$) by the relation

$$\frac{a+b\sqrt{5}}{2} \left(\frac{3+\sqrt{5}}{2}\right)^n = \frac{x_n+y_n\sqrt{5}}{2}.$$

Since $\frac{a-b\sqrt{5}}{2} \left(\frac{3-\sqrt{5}}{2}\right)^n = \frac{x_n-y_n\sqrt{5}}{2}$ then $\frac{a^2-5b^2}{4} = \frac{x_n^2-5y_n^2}{4} = B$.

And from what precedes, if $x^2 - 5y^2 = 4B$ there exists a fundamental element $\frac{a+b\sqrt{5}}{2}$ and $n \in \mathbf{Z}$ such that $x = \pm x_n, y = \pm y_n$.

We may describe the sequences $(x_n)_{n \in \mathbf{Z}}$ and $(y_n)_{n \in \mathbf{Z}}$ by linear recurrences of order 2.

Let $U_0(3, 1) = 0, U_1(3, 1) = 1$ and for $n \geq 2, U_n(3, 1) = 3U_{n-1}(3, 1) - U_{n-2}(3, 1)$, while for $n < 0, U_n(3, 1) = -U_{-n}(3, 1)$.

Similarly, let $V_0(3, 1) = 2, V_1(3, 1) = 3$, for $n \geq 2, V_n(3, 1) = 3V_{n-1}(3, 1) - V_{n-2}(3, 1)$, while for $n < 0, V_n(3, 1) = V_{-n}(3, 1)$.

With this notation, we verify by a simple induction, that

$$\begin{cases} 2x_n = V_n(3, 1)a + 5U_n(3, 1)b, \\ 2y_n = U_n(3, 1)a + V_n(3, 1)b. \end{cases}$$

We are interested in finding an effective bound for $n \geq 1$ such that y_n is a square.

But $U_n(3, 1) = \frac{\zeta^n - \zeta^{-n}}{\sqrt{5}}, V_n(3, 1) = \zeta^n + \zeta^{-n}$

hence
$$2y_n = \frac{a}{\sqrt{5}} (\zeta^n - \zeta^{-n}) + b(\zeta^n + \zeta^{-n})$$

$$= \left(\frac{a}{\sqrt{5}} + b\right) \zeta^n - \left(\frac{a}{\sqrt{5}} - b\right) \zeta^{-n}.$$

By the theorem of Pethö [Pe] and Shorey & Stewart [Sh-St] (see also [Sh-Ti], theorem 9.6) there exists an effective constant $C(a, b) > 0$ such that if $\left(\frac{a}{\sqrt{5}} + b\right) \zeta^n - \left(\frac{a}{\sqrt{5}} - b\right) \zeta^{-n} = 2\Box$ (twice a square), then $n < C(a, b)$.

Letting $C = \max\{C(a, b) \mid \frac{a + b\sqrt{5}}{2} \text{ is a fundamental element of } S\}$, then if $x^2 - 5y^4 = 4B$ it follows that $|y|$ is effectively bounded, since $y = y_n = 2\Box$ (for some fundamental element $\frac{a + b\sqrt{5}}{2} \in S$).

3. Here is our proposition:

PROPOSITION. *Let $n \geq 5$.*

1) *For every non-zero integer A , there exists an effectively determined integer $\beta > 0$, such that if $X^n - BX - A \in \mathbf{Z}[X]$ has a quadratic factor in $\mathbf{Z}[X]$ which is monic, then $|B| < \beta$.*

2) *For every non-zero integer B , there exists an effectively determined integer $\alpha > 0$, such that if $X^n - BX - A \in \mathbf{Z}[X]$ has a quadratic factor in $\mathbf{Z}[X]$ which is monic, then $|A| < \alpha$.*

Proof. Write

$$X^n - BX - A = (X^2 - bX - a)(X^{n-2} + c_{n-3}X^{n-3} + \cdots + c_1X + c_0),$$

where $a, b, c_i \in \mathbf{Z}$.

Then

$$A = ac_0$$

$$B = ac_1 + bc_0$$

$$0 = -ac_2 - bc_1 + c_0$$

$$0 = -ac_3 - bc_2 + c_1$$

.....

$$0 = -ac_{n-3} - bc_{n-4} + c_{n-5}$$

$$0 = -a - bc_{n-3} + c_{n-4}$$

$$0 = -b + c_{n-3}.$$

From these relations, we obtain successively

$$c_{n-3} = b$$

$$c_{n-4} = a + bc_{n-3} = a + b^2$$

$$c_{n-5} = ac_{n-3} + bc_{n-4} = 2ab + b^3 .$$

$$c_{n-6} = ac_{n-4} + bc_{n-5} = a^2 + 3ab^2 + b^4$$

.....

$$c_1 = ac_3 + bc_2,$$

$$c_0 = ac_2 + bc_1,$$

$$B = ac_1 + bc_0,$$

$$A = ac_0.$$

In order to determine explicitly c_i in terms of a, b , consider the following linear recurring sequence of polynomials:

$$F_0(X) = 1, F_1(X) = 1, \text{ and for every } i \geq 2, F_i(X) = F_{i-1}(X) + XF_{i-2}(X).$$

By induction, it may be seen that $F_i(X)$ has degree $j = \left\lfloor \frac{i}{2} \right\rfloor$. Moreover, if i is even then

$$F_i(X) = X^j + \binom{j+1}{j-1} X^{j-1} + \binom{j+2}{j-2} X^{j-2} + \dots + \binom{j+k}{j-k} X^{j-k}$$

$$+ \dots + \binom{2j-1}{1} X + 1$$

and if i is odd then

$$F_i(X) = \binom{j+1}{j} X^j + \binom{j+2}{j-1} X^{j-1} + \dots + \binom{j+k}{j-k+1} X^{j-k+1}$$

$$+ \dots + \binom{2j}{1} X + 1 .$$

Note that $F_i(0) = 1, F_i(1) > 0$ for every $i \geq 0$. Also, if $r \in \mathbf{Z}$ and $F_i(r) = 0$ then $r = -1$.

Let $f_i(X, Y) = Y^j F_i\left(\frac{X}{Y}\right)$ so $f_i(X, Y)$ is a homogeneous polynomial of degree j . As easily seen,

$$f_i(X, Y) = \begin{cases} f_{i-1}(X, Y) + Xf_{i-2}(X, Y) & \text{when } i \text{ is odd} \\ Yf_{i-1}(X, Y) + Xf_{i-2}(X, Y) & \text{when } i \text{ is even} . \end{cases}$$

Hence

$$c_{n-3} = b = bf_1(a, b^2)$$

$$c_{n-4} = a + b^2 = f_2(a, b^2)$$

$$c_{n-5} = b(2a + b^2) = bf_3(a, b^2)$$

$$c_{n-6} = a^2 + 3ab^2 + b^4 = f_4(a, b^2)$$

.....

$$c_1 = ac_3 + bc_2 = \begin{cases} f_{n-3}(a, b^2) & \text{when } n \text{ is odd} \\ bf_{n-3}(a, b^2) & \text{when } n \text{ is even,} \end{cases}$$

$$c_0 = ac_2 + bc_1 = \begin{cases} bf_{n-2}(a, b^2) & \text{when } n \text{ is odd} \\ f_{n-2}(a, b^2) & \text{when } n \text{ is even,} \end{cases}$$

$$B = ac_1 + bc_0 = \begin{cases} af_{n-3}(a, b^2) + b^2f_{n-2}(a, b^2) = f_{n-1}(a, b^2) & \text{when } n \text{ is odd} \\ abf_{n-3}(a, b^2) + bf_{n-2}(a, b^2) = bf_{n-1}(a, b^2) & \text{when } n \text{ is even,} \end{cases}$$

$$A = ac_0 = \begin{cases} abf_{n-2}(a, b^2) & \text{when } n \text{ is odd} \\ af_{n-2}(a, b^2) & \text{when } n \text{ is even.} \end{cases}$$

First let n be even. Given A , a belongs to the finite set of integers dividing A ; thus b belongs to the finite set of integers which are solutions of any one of the equations $af_{n-2}(a, Y^2) = A$. Therefore B , which is expressed in terms of a, b , belongs to a finite set.

Given B , b belongs to the finite set of integers dividing B ; thus a belongs to the finite set of integers which are solutions of any one of the equations $bf_{n-1}(X, b^2) = B$. Therefore A , which is expressed in terms of a, b , belongs to a finite set.

Now, let n be odd. Given A , both a and b belong to the finite set of divisors of A . Therefore B , which is expressible in terms of a, b , belongs to a finite set too.

Finally, we treat the more interesting case, where n is odd, $n \geq 5$ and B is given. First let $n \geq 7$. Now $F_{n-1}(X)$, has degree $M = \frac{n-1}{2} \geq 3$.

We consider the following cases.

- 1) $F_{n-1}(X)$ has an irreducible factor in $\mathbf{Z}[X]$, of degree at least 3.
- 2) $F_{n-1}(X)$ has at least two distinct irreducible factors in $\mathbf{Z}[X]$, each of degree 2.
- 3) $F_{n-1}(X)$ has an irreducible factor of degree 2 and a linear factor in $\mathbf{Z}[X]$.

- 4) $F_{n-1}(X)$ has at least three distinct linear factors in $\mathbf{Z}[X]$.
- 5) $F_{n-1}(X)$ is a power of an irreducible polynomial of degree 2 in $\mathbf{Z}[X]$.
- 6) $F_{n-1}(X)$ has exactly two distinct linear factors in $\mathbf{Z}[X]$.
- 7) $F_{n-1}(X)$ is a power of a linear factor in $\mathbf{Z}[X]$.

In cases (1), (2), (3), (4), $F_{n-1}(X)$ has a factor $G(X) \in \mathbf{Z}[X]$ with at least three distinct roots. Let $g(X, Y)$ be the homogeneous polynomial associated to $G(X)$.

Then a, b belong to the set I of integers such that $g(a, b^2)$ is a divisor of B . By Thue's theorem (in its effective version), there is an effective bound for the possible integers a, b , thus a, b belong to a finite set, and therefore A belongs to finite set too.

In case (5), $F_{n-1}(X) = (X^2 + rX + s)^k$. Comparing degrees, $\frac{n-1}{2} = m = 2k$ and comparing the constant terms, $1 = s^k$, hence $s = \pm 1$. Comparing the coefficients of X^{n-1} , we have: $\binom{m+1}{m-1} = kr$, hence $\frac{(m+1)m}{2} = \frac{mr}{2}$, so $r = m + 1$.

Comparing the coefficients of X^{m-2} , we have: $\binom{m+2}{m-2} = ks + \binom{k}{2} r^2$, hence

$$\frac{(m+2)(m+1)m(m-1)}{24} = \pm \frac{m}{2} + \frac{m(m-2)(m+1)^2}{8}$$

and this gives

$$m^3 - m^2 - 4m + 4 = 0,$$

respectively

$$m^3 - m^2 - 4m - 8 = 0.$$

The first equation has only solutions $m = 1, m = 2$ in positive integers — but this has been excluded.

The second equation has no solution in positive integers. Therefore, the case (5) cannot happen.

In case (6), $F_{n-1}(X) = (X + r)^k(X + s)^h$ with $r, s \in \mathbf{Z}, r \neq s$. Then $m = k + h$. Comparing the constant term, we have $1 = r^k s^h$, so $r, s = \pm 1$, and therefore say, $r = 1, s = -1$.

Comparing the coefficients of X^{m-1} , $\binom{m+1}{m-1} = kr + hs$, hence $\frac{m(m+1)}{2} = k - h$. But $k - h < k + h = m < \frac{(m+1)m}{2}$, so this case is impossible.

Finally, in case (7), $F_{n-1}(X) = (X+r)^k$, with $r \in \mathbf{Z}$. Comparing degrees, constant terms and coefficients of X^{m-1} , we have $m = k$, $1 = r^k$, so $r = \pm 1$, and $\binom{m+1}{m-1} = kr$, so $\frac{(m+1)m}{2} = \pm m$; this gives $m = 1$, which is excluded.

It remains to treat the case $n = 5$. Then $F_4(X) = X^2 + 3X + 1$, so $f_4(X, Y) = X^2 + 3XY + Y^2$. Given B , we consider the set E of all pairs of integers (a, b) such that $f_4(a, b^2) = B$, that is $a^2 + 3ab^2 + b^4 = B$; this may be rewritten as $\left(a + \frac{3}{2}b\right)^2 - \frac{5}{4}b^2 = B$, hence $x^2 - 5y^2 = 4B$, where, $x = 2a + 3b$, $y = b^2$.

As it was indicated in §2, there is an explicitly computable constant $C > 0$, such that if (x, y) satisfies the above relations, then $y < C$, this yields explicit bounds for b , x and therefore also for a .

This concludes the proof.

Remarks.

1) An effective bound for the size of solutions of Thue's equation is indicated, for example, in [Sh-Ti], page 99. It is far too large for any practical purpose. It should however be noted that what is required is to determine the solutions in integers x, y of the equations $g(X, Y) = m$ (for every divisor m of B), such that y is a square.

If $n = 5$ and $B = \pm 1$, the calculations lead to $\pm 1 = B = b^4 + 3ab^2 + a^2$ and $A = ab(2a + b^2)$, hence

$$\left(a + \frac{3}{2}b^2\right)^2 - \frac{5b^4}{4} = \pm 1,$$

so

$$(2a + 3b^2)^2 - 5b^4 = \pm 4.$$

The solutions of $X^2 - 5Y^2 = \pm 4$ are known to be $x = L_{2n}$, $y = F_{2n}$ (for the + sign), $x = L_{2n+1}$, $y = F_{2n+1}$ (for the - sign), for every $n \geq 0$; here

$F_k, L_k (k \geq 0)$ are respectively the Fibonacci and the Lucas numbers. So b^2 is a Fibonacci number. As it is well known, $b^2 = 1 = F_1 = F_2$ or $b^2 = 144 = F_{12}$, and this leads eventually to the decompositions indicated by Rabinowitz.

2) Let $n \geq 5$ and $E = \{(A, B) \in \mathbf{Z} \times \mathbf{Z} \mid X^n - BX - A \text{ has a factor of degree 2 in } \mathbf{Z}[X]\}$; for each $A, B \in \mathbf{Z}$, let $E'_A = \{B \in \mathbf{Z} \mid (A, B) \in E\}$, $E''_B = \{A \in \mathbf{Z} \mid (A, B) \in E\}$.

It is easy to see that E is an infinite set. Indeed, if $a, b \in \mathbf{Z}$, let

$$X^n = q(X^2 - bX - a) + BX + A, \quad \text{where}$$

$q \in \mathbf{Z}[X]$, then $X^2 + bX + a$ divides $X^n - BX - A$. Since each polynomial $X^n - BX - A$ has at most finitely many factors of second degree, then the set E is infinite.

The propositions proved in the paper state that each set E'_A, E''_B (for $n \geq 5$) is finite, and also its members may be found effectively. However it is not ruled out that E'_A or E''_B be empty for values of A or B .

It is feasible to determine congruence conditions on A , resp. B which must be satisfied if $E'_A \neq \emptyset$, respectively $E''_B \neq \emptyset$.

Calculations made at my request by Y. Gérard, indicated that if $n = 5$ and $E''_B \neq \emptyset$ then $B \equiv 0, \pm 1 \pmod{5}$. Gérard has also noted that if $B \equiv \pm 1 \pmod{5}$ and there exists a prime p dividing B and $p \equiv \pm 2 \pmod{5}$ then $E''_B = \emptyset$.

For $B = -11, -19, -29, -31$, the following factorizations hold

$$X^5 + 11X + 12 = (X + 1)(X^2 + 2X + 3)(X^2 - 3X + 4)$$

$$X^5 + 19X + 60 = (X^2 + 2X + 5)(X^3 - 2X^2 - X + 12)$$

$$X^5 + 29X + 15 = (X^2 + 3X + 5)(X^3 - 3X^2 + 4X + 3)$$

$$X^5 + 31X + 56 = (X^2 - 4X + 7)(X^3 + 4X^2 + 9X + 8).$$

BIBLIOGRAPHY

- [Pe] PETHÖ, A. Perfect powers in second order linear recurrences. *J. Number Th.* 15 (1982), 5-13.
- [Ra] RABINOWITZ, S. The factorizations of $x^5 \pm x + n$. *Math. Mag.* 61 (1968), 191-193.
- [Sh-St] SHOREY, T.N. and C.L. STEWART. On the diophantine equation $ax^{2t} + bx^t y + cx^2 = d$ and pure powers in recurrence sequences. *Math. Scand.* 52 (1983), 24-36.
- [Sh-Ti] SHOREY, T.N. and R. TIJDEMAN. *Exponential Diophantine Equations*. Cambridge University Press, Cambridge, 1986.
- [St] STOLT, B. On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, I, II, III. *Ark. Mat.* 2 (1952), 1-23, 251-268 and *Ark. Mat.* 3 (1953), 117-132.
- [Th] THUE, A. Über Annäherungswerte algebraischer Zahlen. *J. reine u. angew. Math.* 135 (1909), 284-305. Reprinted in *Selected Mathematical Papers*, Universitetsforlaget, Oslo, 1982.

(Reçu le 7 avril 1990)

Paulo Ribenboim

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
Canada K7L 3N6