

# $p$ -Adically Resolving Trinomials

Robert Dougherty-Bliss, Natalya Ter-Saakov,  
Mits Kobayashi and Eugene Zima

**Abstract.** We study when resultants of trinomials of the form  $x^n - x^k + 1$  for fixed  $n$  are powers of a prime. The case  $p = 2$  has implications for modular computations with the Chinese Remainder Theorem.

## Introduction

In the context of accelerating modular arithmetic computations with the Chinese Remainder Theorem [2], the family of “trinomial moduli”

$$2^n - 2^k + 1 \quad (0 < k < n) \tag{1}$$

were recently introduced [1]. For computational reasons, it was necessary to find sets of trinomial moduli with the same bitlength  $n$  that were pairwise relatively prime and had easy-to-compute modular inverses. By easy-to-compute, we mean that there exists a polynomial  $f(x)$  with dyadic coefficients such that

$$(2^{cn} - 2^{ck} + 1)^{-1} \bmod (2^{cn} - 2^{cj} + 1) = f(2^c) \tag{2}$$

for all sufficiently large  $c$ .

This problem can be rephrased in terms of the trinomials

$$x^n - x^k + 1 \quad (0 < k < n). \tag{3}$$

Condition (2) is equivalent to stating that the resultant of two trinomials is a signed power of 2. We propose to study such pairs of polynomials, and give them the following name.

**Definition 1.** Let  $p$  be a prime. Two monic polynomials  $f(x)$  and  $g(x)$  in  $\mathbb{Z}[x]$   *$p$ -adically resolve* if their resultant is  $\pm p^k$  for some integer  $k$ . When  $p = 2$ , we will also say that the polynomials *dyadically resolve*.

size	exponents
1	{1}
2	{1, 2}
3	{2, 3, 4}
4	{12, 15, 16, 18}
5	{720, 760, 765, 768, 780}
6	{48372480, 48434496, 48435465, 48435712, 48436128, 48439664}

TABLE 1. Exponents constructed in the proof of Theorem 1. For each size, the given set consists of  $k$  such that the polynomials  $x^n - x^k + 1$  have resultant  $\pm 1$ , so they  $p$ -adically resolve for any  $p$ . The degree  $n$  is any fixed integer larger than the largest element of the set.

### 1. Properties of $p$ -adically resolving pairs

We do not know of any simple, widely applicable condition that implies  $p$ -adic resolvability. The following matrix shows the resultant of all pairs of trinomials of degree 10. Observe that powers of primes appear sporadically.

$$\begin{pmatrix} 0 & 1 & 3 & 1 & 3 & 31 & 9 & 8 & 3 \\ 1 & 0 & 1 & 1 & 4 & 1 & 31 & 16 & 8 \\ 3 & 1 & 0 & 1 & 3 & 1 & 3 & 31 & 9 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 31 \\ 3 & 4 & 3 & 1 & 0 & 1 & 3 & 4 & 3 \\ 31 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 9 & 31 & 3 & 1 & 3 & 1 & 0 & 1 & 3 \\ 8 & 16 & 31 & 1 & 4 & 1 & 1 & 0 & 1 \\ 3 & 8 & 9 & 31 & 3 & 1 & 3 & 1 & 0 \end{pmatrix}$$

FIGURE 1.  $\text{res}(x^{10} - x^i + 1, x^{10} - x^j + 1)$  for  $1 \leq i, j \leq 9$ .

Inspired by applications with the Chinese Remainder Theorem, our main interest is to find sets of pairwise  $p$ -adically resolving trinomials.

**Definition 2.** A set of trinomials of degree  $n$  which pairwise dyadically resolve is called a  $p$ -adic clique of degree  $n$ .

As a first step to understanding trinomials and their resultants, we report the following results.

**Theorem 1.** Let  $\omega_p(n)$  be the size of the smallest  $p$ -adic clique of degree  $n$ . Then  $\omega_p(n) \rightarrow \infty$  as  $n \rightarrow \infty$ .

Theorem 1 implies that every possible size will appear as a clique for large enough degrees. (Our proof is constructive; see Table 1.) When a clique of a given

$p$ -adically resolving trinomials

set size $k$	smallest $n$
2	3
3	5
4	5
5	10
6	11
7	22
8	41
9	82
10	1668
11	???

TABLE 2. Smallest  $n$  such that there exists a 2-adic clique of size  $k$ .

size will first appear is a mystery. Table 2 shows the smallest degree  $n$  such that there is a 2-adic clique of degree  $n$  of a given size  $k$  up to  $k = 10$ . We do not know the smallest degree with a 2-adic clique of size 11.

**Theorem 2.** *Let  $k, j < n$  be positive integers.*

1. *The resultant of  $x^n - x^k + 1$  and  $x^n - x^j + 1$  is  $\pm 1$  if  $k - j$  divides  $k$ .*
2.  *$x^n - x^k + 1$  and  $x^n - x^j + 1$   $p$ -adically resolve if and only if  $x^n - x^{n-k} + 1$  and  $x^n - x^{n-j} + 1$   $p$ -adically resolve.*

We mention that  $p$ -adically resolving is a much stronger condition than relative primality. Empirically, very few pairs of trinomials  $p$ -adically resolve, while almost all pairs are relatively prime. The following theorem gives very strict conditions under which two trinomials can share a common factor over the rationals.

**Theorem 3.** *If  $g(x) = \gcd(x^n - x^k + 1, x^n - x^j + 1)$  is not constant, then:*

1.  *$n$  is even;*
2.  *$k - j$  is divisible by 6; and*
3.  *$g(x)$  is a product of cyclotomic polynomials whose orders are multiples of 6.*

## 2. Roots of trinomials

As a final curiosity, the roots of trinomials  $x^n - x^k + 1$  are related to the roots of  $x^n + 1$  in a way that we do not understand. For a picture worth a thousand words, see Figure 2.

**Theorem 4.** *Let  $n$  and  $k$  be positive integers with  $k < n$ . If  $z^n + 1 = 0$ , then there exist constants  $r_n$  and  $R_n$  such that*

$$\{w : |\arg w - \arg z| < \pi/n, \quad r_n < |w| < R_n\}$$

*contains exactly one root of  $x^n - x^k + 1$ . The constants  $r_n < 1$  and  $R_n > 1$  can be chosen so that  $r_n \rightarrow 1$  and  $R_n \rightarrow 1$  as  $n \rightarrow \infty$ .*

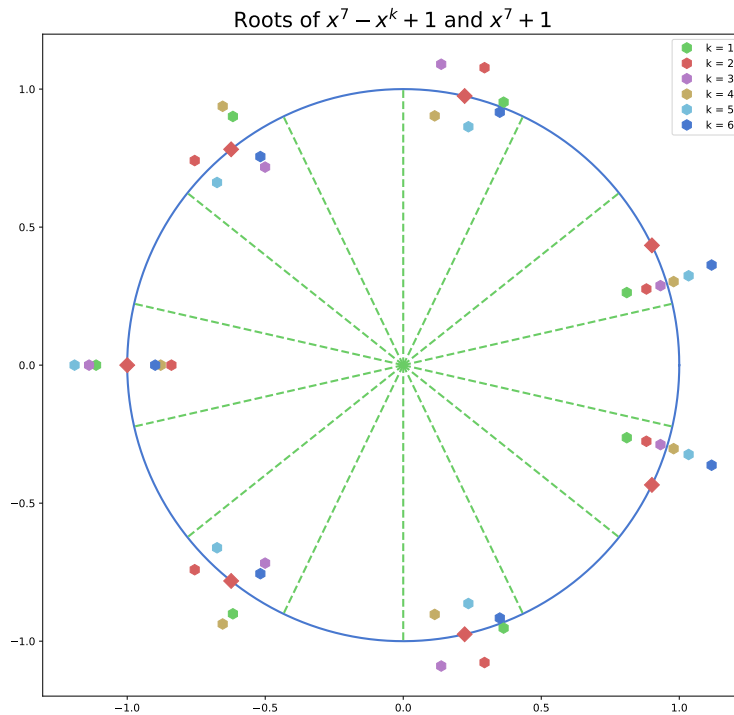


FIGURE 2. Roots of  $x^7 + 1$  (red diamonds) and  $x^7 - x^k + 1$  (colored hexagons) for  $k = 1, 2, \dots, 6$ .

The more puzzling behavior is that, for fixed  $k$ , the roots of  $x^n - x^k + 1$  seem to *orbit around* the roots of  $x^n + 1$  as they traverse the unit circle. It appears that the roots of  $x^n - x^k + 1$  make  $k + 1$  orbits as the unit circle is traversed. We are currently unable to explain this.

## References

- [1] Benjamin Chen, Yu Li, and Eugene Zima. “On a Two-Layer Modular Arithmetic”. In: *ACM Commun. Comput. Algebra* 57.3 (Dec. 2023), pp. 133–136.
- [2] Donald E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley Professional, 2014.

Robert Dougherty-Bliss  
 Department of Mathematics  
 Dartmouth College  
 Hanover, United States  
 e-mail: [rdbliss@dartmouth.edu](mailto:rdbliss@dartmouth.edu)

$p$ -adically resolving trinomials

Natalya Ter-Saakov  
Department of Mathematics  
Rutgers University  
New Brunswick, United States  
e-mail: [nt399@rutgers.edu](mailto:nt399@rutgers.edu)

Mits Kobayashi  
Department of Mathematics  
Dartmouth College  
Hanover, United States  
e-mail: [Mits.Kobayashi@dartmouth.edu](mailto:Mits.Kobayashi@dartmouth.edu)

Eugene Zima  
Department of Physics and Computer Science  
Wilfrid Laurier University  
Waterloo, Canada  
e-mail: [ezima@wlu.ca](mailto:ezima@wlu.ca)