On Cauchy–Mirimanoff and related polynomials

Paul M. Nanninga

May 2013

A thesis submitted for the degree of Doctor of Philosophy of The Australian National University
Dedication

For Helen, Nick, Lilly and Meg
Declaration

The work in this thesis is my own except where otherwise stated.

Paul M. Nanninga
Acknowledgements

My thanks are extended to Prof. Murray Batchelor and Prof. Markus Hegland who provided essential support and advice during this study. Helpful comments were also made by Dr Keith Matthews and Dr John Campbell.
Abstract

The focus of this thesis is to investigate the Cauchy–Mirimanoff polynomials $E_n$ and their close relatives $R_n$, $S_n$ and $T_n$, with an emphasis on irreducibility. The Cauchy–Mirimanoff polynomials were first identified and studied by Cauchy and Liouville in 1839 in relation to Fermat’s Last Theorem, but it was Mirimanoff in 1903 who first proposed their irreducibility over $\mathbb{Q}$ for $n$ a prime number. None of the standard irreducibility criteria apply directly, for example Helou showed $E_n$ is always reducible modulo any prime for all odd $n \geq 9$. Computing irreducibility is problematic as the largest coefficients grow rapidly with $n$. The difficulty of the problem is apparent since it remains unresolved after more than 100 years. Helou, Filaseta and Beukers in 1997, Tzermias in 2007 and 2012, Irick in 2010 and Lynch in 2012 have progressed the area using a range of methods, but this thesis describes an alternative original method and it is used to generalize some of the earlier results. In essence the method uses proven properties of the polynomials to reveal an inconsistency in the $2$–adic or $3$–adic valuation of their coefficients, depending on the polynomial under consideration.

After proving several properties of the polynomials the new method is used here to prove that $R_m$, $S_m$, $T_m$ are irreducible over $\mathbb{Q}$ for odd $m \geq 3$, and $E_n$, $R_n$, $S_n$ are irreducible over $\mathbb{Q}$, for $n = 2^q m$, $q = 1, 2, 3, 4, 5$, and $m \geq 1$ odd. And using the same approach it is proved that $E_{3^q m}$ is irreducible over $\mathbb{Q}$ for $q = 1, 2, 3, 4$ and for any odd $m \geq 1$, not divisible by 3. It is likely the results could be extended to higher values of $q$. It is proved that for most odd $n$, assuming $E_n$ is reducible over $\mathbb{Q}$, $E_n$ is proportional to the product of two primitive irreducible polynomials over $\mathbb{Z}$, both of which share all 6 of the automorphisms of $E_n$.

Mirimanoff’s conjecture is also investigated. Tzermias has shown $E_p$ is irre-
ducible for every prime $p$ less than 1,000, and by considering a decomposed form of $E_p$ this result is extended here to all primes less than 10,000. Several new irreducibility criteria and theorems relating to the number and size of factors over $\mathbb{Q}$ are proved including some based on the approach of Schönemann which are shown to be effective.

A good approximation to all the roots of $E_n$ (for odd and even $n$) is proved. For $n$ a prime this is used to prove an upper bound on the number of factors of $E_n$ over $\mathbb{Q}$. Using the estimate it is shown that for large $n$ the roots take the form of simple linear fractional functions of the $n$’th roots of unity.

The Newton polygon of $E_n$ is studied for composite $n$. Using this it is shown that if $p$ is any prime divisor of $n$, then $E_n$ is always reducible over the field of $p$–adics $\mathbb{Q}_p$. Irreducible factors in $\mathbb{Q}_p[x]$ of $E_n$, $R_n$, $S_n$, $T_n$, are identified for $n = Kp^r$, where $p$ is any prime, with $1 \leq K \leq p - 1$ and $r \geq 1$. A complete factoring of $E_n$ into irreducibles in $\mathbb{Q}_p[x]$ is given for $n = 2p^r$. Similar results are proved for $R_n$, $S_n$ and $T_n$.

The thesis concludes with some possible future directions.
## Contents

Dedication i  
Declaration iii  
Acknowledgements v  
Abstract vii  

1 Introduction 1  
1.1 Background ................................................. 1  
1.2 Principal results ........................................... 2  

2 Cauchy–Mirimanoff and related polynomials 9  
2.1 Introduction ................................................. 9  
2.2 The polynomials $E_n$, $R_n$, $S_n$ and $T_n$ ................. 10  
2.3 Irreducibility of $E_n$, $R_n$, $S_n$ and $T_n$ in $\mathbb{Q}[x]$ 17  

3 Irreducibility of Cauchy–Mirimanoff polynomials $E_{6k+3}$ 25  
3.1 Introduction ............................................... 25  
3.2 Further properties of $E_n$ for odd $n$ .......................... 26  
3.3 Irreducibility of $E_n$ in $\mathbb{Q}[x]$ for $n = 6k + 3$ ............... 33  

4 On Mirimanoff’s conjecture 39  
4.1 Introduction ............................................... 39  
4.2 Irreducibility of $C_p$ for prime $p \geq 5$ ......................... 41  
4.3 Irreducibility of $D_p$ for prime $p \geq 5$ ......................... 45
4.4 Factors of $D_p$ in $\mathbb{Q}[t]$ ................................. 47
4.5 Schönenmann’s approach applied to $D_p$ .......................... 53

5 Locating the roots of $E_n$, $R_n$, $S_n$ and $T_n$ ............................ 59
  5.1 Introduction ............................................................ 59
  5.2 Location of the roots of $E_n$ for odd $n$ ............................. 60
  5.3 Location of the roots of $E_n$ for even $n$ ............................ 65
  5.4 Location of the roots of $R_n$, $S_n$ and $T_n$ ........................ 73

6 Factors of $E_n$, $R_n$, $S_n$ and $T_n$ in $\mathbb{Q}_p[x]$, for composite $n$ .............................. 77
  6.1 Introduction ............................................................ 77
  6.2 Factors of $E_n$ in $\mathbb{Q}_p[x]$ for composite $n$ .................... 78
  6.3 Factors of $R_n$, $S_n$ and $T_n$ in $\mathbb{Q}_p[x]$ for composite $n$ ................ 88

Future directions .......................................................... 91

Appendix A Explicit coefficients for Cauchy–Mirimanoff and related polynomials .......................... 95
  A.1 Coefficients of $E_n$ .................................................. 95
  A.2 Coefficients of $R_n$ .................................................. 98
  A.3 Coefficients of $S_n$ .................................................. 98
  A.4 Coefficients of $T_n$ .................................................. 98

Appendix B Irreducibility of $D_p$ in $\mathbb{Q}[t]$ for all primes $11 \leq p < 10,000$ .......................... 101