Cyclotomic properties of the Rudin-Shapiro polynomials

By *John Brillhart*, *J. S. Lomont*, and *Patrick Morton* at Tucson

1. Introduction

The Rudin-Shapiro polynomials $P_n(x)$, $Q_n(x)$ (which have degree 2^n-1) are defined recursively by the formulas

$$P_{n+1}(x)=P_n(x)+x^{2^n}Q_n(x) \tag{1.1}$$

$$Q_{n+1}(x)=P_n(x)-x^{2^n}Q_n(x), \qquad n\geqq 0, \tag{1.2}$$

where $P_0(x)=Q_0(x)=1$.

Alternatively, as will be shown in Corollary 2. 3, they can also be defined recursively and independently by the formulas

$$P_{n+2}(x)=(1-x^{2^{n+1}})P_{n+1}(x)+2x^{2^{n+1}}P_n(x), \qquad n\geqq 0,$$

$$Q_{n+2}(x)=(1-x^{2^{n+1}})Q_{n+1}(x)+2x^{2^n}Q_n(x), \qquad n\geqq 0,$$

where $P_0(x)=Q_0(x)=1$ and $P_1(x)=1+x$, $Q_1(x)=1-x$.

The present algebraic investigation arose from the observation that the values of $P_n(\omega_r)$, $n\geqq 1$, ω_r an r-th root of unity, $r\leqq 6$, satisfy a constant coefficient, 3-term linear recurrence relation with rational integral coefficients. The principal result of this paper is that for $r\geqq 2$, $\{P_n(\omega_r)\}$ satisfies a constant coefficient, 3-term linear relation (whose central coefficient need not be a rational integer). It will also be shown that if the central coefficient is not a rational integer, then the $P_n(\omega_r)$ nonetheless still satisfy a recurrence relation with integral coefficients, but with more than three terms.

The secondary purpose of this paper is to investigate the nature of the central coefficient (which is a cyclotomic integer) through the use of the Galois group of the cyclotomic field generated by the root of unity at which $P_n(x)$ is evaluated. Sufficient conditions for the central coefficient to be a rational integer are derived. Also, a table of values of the central coefficient is given in Section 7.

A number of formulas derived in [2] and [3] are used in the present paper, and are listed in the appendix for ease of reference.