Comments for the Selecta of A. Schinzel

Let $a$ and $b$ be coprime integers with $|a| > |b| > 0$ and let $n$ be a positive integer. A prime $p$ is said to be a primitive divisor of $a^n - b^n$ if $p$ divides $a^n - b^n$ but does not divide $a^m - b^m$ for any positive integer $m$ which is smaller than $n$. The study of primitive divisors had its origins in the work of Bang [1], Zsigmondy [24] and Birkhoff and Vandiver [3] from 1886, 1892 and 1904 respectively. It follows from their analysis that the primitive divisors of $a^n - b^n$ are the prime factors of the $n$-th cyclotomic polynomial evaluated at $a$ and $b$, $\Phi_n(a, b)$, with at most one exception. The exception, if it exists, is a prime factor of $n$. Gauss [7], Aurifeuille and Le Lasseur [11] and Dirichlet [6] gave factorizations of $\Phi_n(x, 1)$ over a suitable quadratic number field. Aurifeuille and Le Lasseur [11] deduced from it explicit non-trivial factorizations of the number $\Phi_n(x, y)$ for certain integers $n$, $x$ and $y$. Factorizations of the type they considered are now known as Aurifeuillian factorizations. In a paper written during a stay at Trinity College in Cambridge in 1962, Schinzel [14] gave some new Aurifeuillian factorizations. In addition, he used Aurifeuillian factorizations to give conditions under which $a^n - b^n$ has at least two primitive divisors. Stevenhagen [21] and Brent [4] have shown how to efficiently compute the factorizations given by Schinzel [14]. In [8], Granville and Pleasants show that Schinzel determined all possible such Aurifeuillian factorizations.

One may extend the notion of a primitive divisor to sequences of Lucas numbers and sequences of Lehmer numbers. In 1913 Carmichael [5] proved that if $u_n$ is the $n$-th term, for $n > 12$, of a Lucas sequence whose associated characteristic polynomial has real roots and coprime coefficients then $u_n$ possesses a primitive divisor. Rotkiewicz [13], in 1962, generalized Schinzel’s argument [14] to give conditions under which $u_n$ has at least two primitive divisors.

In 1930 Lehmer [10] introduced sequences which are more general than Lucas sequences but retain their striking divisibility properties and these sequences are now referred to as Lehmer sequences. Twenty-five years later Ward [23] established the analogue of Carmichael’s result for Lehmer sequences. In a sequence of three papers [16], [17] and [18] Schinzel used the Aurifeuillian factorizations from [14] to establish conditions under which Lucas or Lehmer numbers have at least $k$ primitive prime factors with $k$ equal to 2, 3, 4, 6 or 8.

Let $A$ and $B$ be non-zero integers in an algebraic number field $K$ and let $n$ be a positive integer. A prime ideal of the ring of algebraic integers of $K$ is said to be a primitive divisor of $A^n - B^n$ if it divides the ideal generated by $A^n - B^n$ but does not divide the ideal generated by $A^m - B^m$ for any positive
integer $m$ with $m < n$. In [19] Schinzel proves that if $A$ and $B$ are non-zero coprime algebraic integers whose quotient is not a root of unity then $A^n - B^n$ has a primitive divisor provided that $n$ exceeds $N(d)$, a number which is effectively computable in terms of $d$ where $d$ is the degree of $A/B$ over $\mathbb{Q}$. In 1968 Postnikova and Schinzel [12] proved a weaker version of this result where $N(d)$ was replaced by $N(A,B)$, a number which is effectively computable in terms of $A$ and $B$. The case $d = 2$ is of considerable interest since it gives information on non-degenerate Lucas and Lehmer sequences whose associated characteristic polynomial has coprime coefficients. In particular, if $u_n$ is the $n$-th term of such a sequence and $n$ exceeds $N(2)$ then $u_n$ has a primitive divisor. Schinzel [15] had earlier established that $u_n$ has a primitive divisor if $n$ exceeds a number which is effectively computable in terms of the coefficients of the associated characteristic polynomial of the sequence. Stewart [22] proved that one may take $N(d) = \max\{2(2^d - 1), e^{452}d^{67}\}$ and that there are only finitely many such Lehmer sequences whose $n$-th term, $n > 6$, $n \neq 8$, 10 or 12, does not possess a primitive divisor; for Lucas sequences the appropriate requirement is $n > 4$, $n \neq 6$. Further these sequences may be determined by solving certain Thue equations. Bilu, Hanrot and Voutier [2] used a theorem of Laurent, Mignotte and Nesterenko [9] concerning lower bounds for linear forms in the logarithms of two algebraic numbers, as elaborated by Mignotte [2], to help explicitly determine all such exceptional Lucas and Lehmer sequences. In particular, they proved that if $n$ exceeds 30 and $u_n$ is a Lucas or Lehmer number, from a sequence as above, then $u_n$ has a primitive prime factor.

Let $A$, $B$ and $d$ be as above and let $k$ be a positive integer, $\zeta_k$ be a primitive $k$-th root of unity and $K$ be an algebraic number field containing $A$, $B$ and $\zeta_k$. In [20] Schinzel proves that for each positive real number $\varepsilon$ there exists a positive number $c$ which depends on $d$ and $\varepsilon$ such that if $n$ exceed $c(1 + \log k)^{1+\varepsilon}$ then there is a prime ideal of the ring of algebraic integers of $K$ that divides $A^n - \zeta_k B^n$ but does not divide $A^m - \zeta_k^j B^m$ for $m < n$ and any integer $j$. The case when $k = 1$ is the main result of [19].

References


C.L. Stewart

Department of Pure Mathematics
University of Waterloo