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, ζ_k be a primitive k-th root of unity and K be an algebraic number field containing A, B and ζ_k. In [20] Schinzel proves that for each positive real number ε there exists a positive number c which depends on d and ε 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

[1] A.S. Bang, Taltheoretiske Undersøgelser, *Tidsskrift for Mat.* **4** (1886), 70–80, 130–137.

[2] Y. Bilu, G. Hanrot and P.M. Voutier, with an appendix by M. Mignotte, Existence of primitive divisors of Lucas and Lehmer numbers, *J. reine angew. Math.* **539** (2001), 75–122.

[3] G.D. Birkhoff and H.S. Vandiver, On the integral divisors of $a^n - b^n$, *Ann. of Math.* **5** (1904), 173–180.

[4] R.P. Brent, On computing factors of cyclotomic polynomials, *Math. Comp.* **61** (1993), 131–149.

[5] R.D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913), 30–70.

[6] P.G. Lejeune Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed., Friedr. Vieweg & Sohn, Braunschweig, 1894.

[7] C.F. Gauss, *Disquisitiones Arithmeticae*, G. Fleischer, Leipzig, 1801.

[8] A. Granville and P. Pleasants, Aurifeuillian factorization, *Math. Comp.* **75** (2005), 497–508.

[9] M. Laurent, M. Mignotte and Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Theory* **55** (1995), 285–321.

[10] D.H. Lehmer, An extended theory of Lucas functions, *Ann. of Math.* **31** (1930), 419–448.

[11] E. Lucas, Théorèmes d'arithmétique, *Atti. R. Acad. Sc. Torino* **13** (1877–78), 271–284.

[12] L.P. Postnikova and A. Schinzel, Primitive divisors of the expression $a^n - b^n$ in algebraic number fields, *Mat. Sbornik* **75** (1968), 171–177.

[13] A. Rotkiewicz, On Lucas numbers with two intrinsic divisors, *Bull. Acad. Polon. Sci. Sér. Math. Astr. Phys.* **10** (1962), 229–232.

[14] A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Camb. Phil. Soc.* **58** (1962), 555–562.

[15] A. Schinzel, The intrinsic divisors of Lehmer numbers in the case of negative discriminant, *Ark. Mat.* **4** (1962), 413–416.

[16] A. Schinzel, On primitive prime factors of Lehmer numbers I, *Acta Arith.* **8** (1963), 213–223.

[17] A. Schinzel, On primitive prime factors of Lehmer numbers II, *Acta Arith.* **8** (1963), 251–257.

[18] A. Schinzel, On primitive prime factors of Lehmer numbers III, *Acta Arith.* **15** (1968), 49–69.

[19] A. Schinzel, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields, *J. reine angew. Math.* **268/269** (1974), 27–33.

[20] A. Schinzel, An extension of the theorem on primitive divisors in algebraic number fields, *Math. Comp.* **61** (1993), 441–444.

[21] P. Stevenhagen, On Aurifeuillian factorizations, *Indag. Math.* **49** (1987), 451–468.

[22] C.L. Stewart, Primitive divisors of Lucas and Lehmer numbers, in *Transcendence Theory: Advances and Applications*, A. Baker and D.W. Masser (eds.), Academic Press (1977), 79–92.

[23] M. Ward, The intrinsic divisors of Lehmer numbers, *Ann. of Math.* **62** (1955), 230–236.

[24] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892), 265–284.

C.L. Stewart
Department of Pure Mathematics
University of Waterloo