Commentary on H: Divisibility and congruences

by H. W. Lenstra jr.

The eleven papers in Section H are naturally divided in two categories: four papers in elementary number theory, and seven papers on local-global results concerning exponential equations.

The four papers **H1**, **H3**, **H6**, **H8** in the first category show Schinzel's resourcefulness in elementary arithmetic. Problem **P217**, formulated in **H1**, has been studied by E. Burkacka and J. Piekarczyk in their master dissertations at the University of Warsaw; see *Colloq. Math.* 10 (1963), 365. The joint paper **H6** with G. Baron, which has a combinatorial flavour, has applications in ring theory. An algebraic proof of the main result of this paper was obtained by M. Van Den Bergh and M. Van Gastel [5]. Especially noteworthy is the joint paper **H8** with J. Wójcik, which was suggested by work in group theory. The theme of the paper is reminiscent of the local-global results discussed below, but the tools used are quite different and more elementary. A negative answer to the question posed at the end of the paper was given by J. Wójcik [7].

The seven papers **H2**, **H4**, **H5**, **H7**, **H9**, **H10**, **H11** in the second category address fundamental issues related to exponential diophantine equations, the emphasis being on local-global results such as the following Theorem 2 from **H4**: *if H is a finitely generated subgroup of the multiplicative group of an algebraic number field K, and a non-zero element $b \in K$ has the property that for almost all primes $\mathfrak{p}$ of K the element $b \bmod \mathfrak{p}$ belongs to $H \bmod \mathfrak{p}$, then b belongs to H.* The result admits numerous variations and applications, and Schinzel investigated many of them. His work helped inspire a development in which the role of the multiplicative group is played by general algebraic groups. A good discussion and a substantial bibliography can be found in a paper by E. Kowalski [1].

The technique used by Schinzel in most papers in the second category, consists of combining density theorems from algebraic number theory with information on Galois groups of field extensions obtained by adjoining radicals. Several of Schinzel's auxiliary results on such Galois groups are new. The most notable one (**H5**, Theorem 2) asserts the following. *Let K be a field, n a positive integer not divisible by the characteristic of K, and w the number of nth roots of unity in K. Then, for $a \in K$, the Galois group of $X^n - a$ over K is abelian if and only if there exists $b \in K$ with $a^w = b^n$.* This basic result has been finding its way into the field-theoretic literature as *Schinzel's theorem*. It is important in the context of Stark's conjectures (J. Tate, [4]; see Chapitre IV, Exercice 1.4).

One also encounters Schinzel's theorem when one attempts to describe, for any field K with algebraic closure $\bar{K}$, the Galois group of the "maximal radical extension" of K, which one obtains by adjoining all $\alpha \in \bar{K}$ for which there exists an integer n not divisible by the characteristic of K with $\alpha^n \in K$.

P. Stevenhagen ([3], cf. [6]) gave a proof of Schinzel's theorem that is so elegant that it deserves to be included here. We may assume $a \neq 0$. Denote by L the splitting field of $X^n - a$ over K, and generally by ζ_m a primitive mth root of unity. First suppose $a^w = b^n$ with $b \in K$. Then L is contained in the composite of the Kummer extension $K(b^{1/w})$ and the cyclotomic extension $K(\zeta_{wn})$ of K. Both of these extensions are abelian, and therefore so is L. For the converse, suppose L has an abelian Galois group G. We fix an nth root α of a in L. For each $\sigma \in G$, one has $\sigma(\alpha)/\alpha = \zeta_\sigma \in \langle \zeta_n \rangle$, and $\sigma(\zeta_n) = \zeta_n^{c(\sigma)}$ with $c(\sigma) \in \mathbb{Z}$. For any $\sigma, \tau \in G$ one has $\tau(\alpha^{c(\sigma)})/\alpha^{c(\sigma)} = \zeta_\tau^{c(\sigma)} = \sigma(\tau(\alpha)/\alpha) = \tau\sigma(\alpha)/\sigma(\alpha)$; hence $\alpha^{c(\sigma)}/\sigma(\alpha)$ is fixed by all τ so belongs to K, and taking the nth power one sees that $a^{c(\sigma)-1} \in K^{*n}$. Thus, if v denotes the gcd of n and all numbers $c(\sigma) - 1$ (for $\sigma \in G$), then one has $a^v \in K^{*n}$. To finish the proof it suffices to show $v = w$. A divisor d of n divides v if and only if d divides all numbers $c(\sigma) - 1$, if and only if all elements $\sigma(\zeta_d)/\zeta_d = \zeta_d^{c(\sigma)-1}$ are 1, if and only if $\zeta_d \in K$, and if and only if d divides w. Therefore we have $v = w$, as required.

The Corollary to Theorem 5 in **H5** has the condition $a \neq d^3 + 3d$. Schinzel himself proved that this condition can be omitted [2].

References

[1] E. Kowalski, *Some local-global applications of Kummer theory*. Manuscripta Math. 111 (2003), 105–139.

[2] A. Schinzel, *On the congruence* $u_n \equiv c \pmod{\mathfrak{p}}$, *where* u_n *is a recurring sequence of the second order*. Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) 30 (2003), 147–165.

[3] P. Stevenhagen, *Ray class groups and governing fields*. Thesis, Universiteit van Amsterdam, 1989.

[4] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s* $= 0$. Progr. Math. 47, Birkhäuser, Boston 1984.

[5] M. Van Den Bergh, M. Van Gastel, *On the structure of non-commutative regular local rings of dimension two*. Comm. Algebra 30 (2002), 4575–4588.

[6] J. Wójcik, *Criterion for a field to be abelian*. Colloq. Math. 68 (1995), 187–191.

[7] —, *On a problem in algebraic number theory*. Math. Proc. Cambridge Philos. Soc. 119 (1996), 191–200.