Let $p \equiv 1 \pmod{4}$ be a prime and $m$ an integer such that $p$ does not divide $m$. The basic problem of quartic residues is to characterize those primes $p$ for which $m$ is a quartic residue modulo $p$. A very celebrated result in this direction being the result of Gauss that 2 is a quartic residue modulo $p$ if and only if $p = x^2 + 64y^2$ for some integers $x$ and $y$. The author solves the problem for general $m$ by giving a similar result, but with $p$ being represented by one from a set of binary quadratic forms. Let $d > 1$ be a squarefree integer and $\epsilon_d$ be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$. Suppose that $p \equiv 1 \pmod{4}$ is a prime such that $(d/p) = 1$ (the Legendre symbol). Many mathematicians tried to characterize primes of this form such that $\epsilon_d$ is a quadratic residue modulo $p$. For example, A. Aigner and H. Reichardt [J. Reine Angew. Math. 184, 158–160 (1942; Zbl 0027.01102)], and independently P. Barrucand and H. Cohn [J. Reine Angew. Math. 238, 67–70 (1969; Zbl 0207.36202)] proved that $\epsilon_2 = 1 + \sqrt{2}$ is a quadratic residue of a prime $p \equiv 1 \pmod{8}$ iff $p = x^2 + 32y^2$. The author establishes a much more general result of this form and likewise he characterizes when $\epsilon_d$ is a quartic residue modulo $p$.

On p. 418 of his book “Reciprocity laws: From Euler to Eisenstein” (2000; Zbl 0949.11002), F. Lemmermeyer proposed the problem of determining $\epsilon_d^{(p+1)/4}$ modulo $p$ in terms of binary quadratic forms. The author solves this problem. For integers $a$ and $b$ the Lucas sequence $\{u_n(a,b)\}$ is defined as follows: $u_0(a,b) = 0, \ u_1(a,b) = 1$ and, for $n \geq 1, \ u_{n+1}(a,b) = bu_n(a,b) - au_{n-1}(b)$. Let $P_n = u_n(-1,2)$ be the Pell sequence. In 1974 Emma Lehmer [J. Reine Angew. Math. 268/269, 294–301 (1974; Zbl 0289.12007)] showed that $p$ divides the $(p-1)/4$th terms of the Pell sequence iff $p = x^2 + 32y^2$ for some integers $x$ and $y$. The author characterizes the primes $p$ dividing the $(p - (1/p))/4$th term of the Lucas sequence $u_n(a,b)$ in terms of representability by binary quadratic forms. This generalizes Lehmer’s result and several similar results.

The results of the author concerning the above problems generalize a large body of hitherto isolated results, but are unfortunately too complicated to be stated in this review. The proofs are quite computational and only involve a modest amount of conceptual machinery.

Pieter Moree (Bonn)

Keywords: quartic residue; quartic Jacobi symbol; binary quadratic form

Classification:
* 11A15 Power residues, etc.
* 11E25 Sums of squares, etc
* 11B39 Special numbers, etc.