Notes on the Diophantine equation $y^2 - k = x^3$

By Ove Hemer

The purpose of this article is to give some corrections and additions to my dissertation "On the Diophantine equation $y^2 - k = x^3$ " (Uppsala 1952). In the following I denote that paper by H and refer to the bibliography given there as e.g. (H, [4]). In fact I have succeeded in solving all the equations with $0 < k \le 100$.

The problem of solving an equation $y^2 - k = x^3$ is equivalent to solving a finite number of equations (a, b, c, d) = 1, where (a, b, c, d) is a binary cubic form. To be short I name this form soluble and (u, v) a solution of the form, if there is any integer solution (u, v) of (a, b, c, d) = 1. In the first part of H it is shown how to determine those equations and further their solubility is discussed. A soluble form may be written

(1)
$$F(u, v) = u^3 + p u^2 v + q u v^2 + r v^3 = (1, p, q, r)$$

and corresponds to a cubic ring $R(\theta)$, where

(2)
$$F(\theta, -1) = \theta^3 - p \theta^2 + q \theta - r = 0.$$

If k>0, the form F(u,v) has always a negative discriminant. Then every integer solution of (1) corresponds to a unit of the type

$$\varepsilon^n = u + v \theta$$

and vice versa, where ε is the fundamental unit of the ring $R(\theta)$. Hence the decisive question is to determine all such units (3).

If $0 < \varepsilon < 1$, the case n < 0 can easily be examined by H, Lemma 7, p. 25. This lemma was inserted a short time before the printing and hence it is not applied all through. Further, for want of space, the proof was too short. Hence I repeat the lemma here with a detailed proof:

Lemma 7. A soluble irreducible form can always by a unimodular substitution be written F(u, v) = (1, p, q, r), where $p \le 1$ and r > 0. Suppose D(F) < 0 and $0 < \varepsilon < 1$, where ε is the fundamental unit in the corresponding cubic ring. Then, if v_1 and v_2 are positive integers and if $D\left(1, p, q, r - \frac{1}{v_1^3}\right)$ and $D\left(1, p, q, r + \frac{1}{v_2^3}\right)$