Computation of the Solution of $x^3 + Dy^3 = 1$

By H. C. Williams and R. Holte

Abstract. A computer technique for finding integer solutions of
$x^3 + Dy^3 = 1$

is described, and a table of all integer solutions of this equation for all positive $D < 50000$ is presented. Some theoretic results which describe certain values of $D$ for which the equation has no nontrivial solution are also given.

1. Introduction. Let $D$ be an integer which is not a perfect cube; let $K = \mathbb{Q}(\sqrt[3]{D})$, the field formed by adjoining $\sqrt[3]{D}$ to the rationals $\mathbb{Q}$; and let $\epsilon > 1$ be the fundamental unit of $K$. By a nontrivial solution of

\[ x^3 + Dy^3 = 1, \]

we mean a pair of integers $(e, f)$ such that $e$ and $f$ satisfy (1) and $ef \neq 0$. We say that (1) is solved when we have either found all its nontrivial solutions or we have shown that no nontrivial solutions of (1) exist. If (1) has a nontrivial solution, we say that $D$ is admissible; otherwise, we say that $D$ is inadmissible.

It has long been known that the solution of (1) can be obtained from the following theorem.

Theorem (Deleone-Nagell [6], [7]). The equation (1) has at most one nontrivial solution. If $(e, f)$ is such a solution, then $e + f\sqrt[3]{D}$ is either $e$ or $e^2$, the latter case occurring only for $D = 19, 20, 28$.

By using this theorem, Williams and Zarnke [9] determined all nontrivial solutions of (1) for all $D$ such that $1 < D < 15000$. The difficulty in using this theorem to solve (1) lies in the fact that the calculation of $\epsilon$ is frequently very difficult and time consuming. The best algorithm for computing $\epsilon$, which is currently available, still seems to be that of Voronoi (see, for example, [4] and [2]); however, this algorithm is both intricate and lengthy. For example, when $D = 34607$, the number of iterations required to find $\epsilon$ is 66931 and $\epsilon > 10^{32873}$.

There appear to be relatively few values of $D$ which are admissible and, when a value of $D$ is admissible, the corresponding $\epsilon$ is usually quite small. Consequently, the best strategy for solving (1) would seem to consist of finding simpler techniques than the calculation of $\epsilon$ for determining when $D$ is inadmissible. The purpose of this paper is to develop some of these techniques. We also present an extended version of the table in [9] for all $D < 50000$. Finally, some theorems are given which can be used for showing that certain values of $D$ are inadmissible.

Received September 16, 1976.


Copyright © 1977, American Mathematical Society

778
2. Some Criteria for Determining When D is Inadmissible. Since \( x^3 + Dxy^3 = x^3 + d_1d_2^3y^3 \), we need only consider those values of \( D \) which have no perfect cube divisor; hence, we assume that \( D = cd^2 \), where \( c, d \) are square-free integers. We also let \( D = 3^iAB \), where \( 0 \leq i \leq 2 \), every prime divisor of \( A \) is congruent to \(-1\) modulo 3, and every prime divisor of \( B \) is congruent to \(+1\) modulo 3. Cohn [3] has shown that, if \( D \neq 2, 9, 17, 20 \), then \( D \) is inadmissible whenever \( B = 1 \). In what follows we will assume that \( D \neq 2, 9, 17, 20 \). The following simple result is also frequently useful.

**Theorem.** If \( D \equiv \pm 4, \pm 3 \pmod{9} \) and \( B > 1 \), then \( D \) is inadmissible if no factor \((\neq 1)\) of \( B \) is of the form \( 1 + 9t \).

**Proof.** Suppose \( D \) is admissible and suppose \((e, f)\) is the nontrivial solution of (1). Since \( e^3 + Df^3 = 1 \) and \( e^3 \equiv 0, 1, -1, f^3 \equiv 0, 1, -1 \pmod{9} \), we must have \( 3 \mid f \). Since \( e^2 + e + 1 \equiv 0 \pmod{9} \) and \((A, e^2 + e + 1) = 1 \), we get \( e \equiv 1 \pmod{9} \),

\[
e^2 + e + 1 = 3B'^2g^3,
\]

where \( B' > 1 \) and \( B' \mid B \). It follows that \( B' \equiv 1 \pmod{9} \).

Let \( \rho \) be a primitive cube root of unity; let \( Q(\rho) \) be the field formed by adjoining \( \rho \) to the rationals; let \( Q[\rho] \) be the ring of integers in \( Q(\rho) \); and let \( Z \) be the set of rational integers. Put \( \lambda = 1 - \rho \) and, if \( p \equiv 1 \pmod{3} \) is any rational prime, define

\[
\pi_p = a + b\rho, \quad \pi_p = a + b\rho^2, \quad \text{where } a \equiv -1 \pmod{3}, 3 \mid b, \text{ and } p = N(\pi_p) = N(\pi_p) = a^2 - ab + b^2.
\]

If \( P = p_1p_2 \cdots p_j \), where \( p_i \equiv 1 \pmod{3} \) is prime for \( i = 1, 2, \ldots, j \), we define \( \Gamma(P) = \{ \gamma \mid \gamma = \pi_1\pi_2\pi_3 \cdots \pi_m \} \) where \( \pi_i = \pi_{p_i} \) or \( \pi_{p_i}^* \); and if \( p_k = p_h \), then \( \pi_k = \pi_h \). Thus, if there are \( l \) distinct prime factors of \( P \), we have \( 2^l \) elements in \( \Gamma(P) \).

With these conventions we can now give the following four theorems.

**Theorem 1.** Let \( D = AB \not\equiv \pm 1 \pmod{9} \). If \( D \) is admissible, there must be a unitary* factor \( B_2 \) of \( B \) such that \( B_2 > 1 \) and either

\[
(2) \quad \rho^2\gamma r^3 + B_1Ar^3 = \lambda
\]

or

\[
(3) \quad \gamma r^3 + 3p^2\lambda B_1Ar^3 = 1 \quad (B_2 \equiv 1 \pmod{9})
\]

must have a solution where \( \tau \in Q[\rho], r \in Z, B_1 = B/B_2, \) and \( \gamma \in \Gamma(B_2) \).

**Theorem 2.** Let \( D = AB \equiv \pm 1 \pmod{9} \). If \( D \) is admissible, there must be a unitary factor \( B_2 \) of \( B \) such that \( B_2 > 1 \) and either

\[
(4) \quad \rho\gamma r^3 + B_1Ar^3 = \lambda
\]

or

\[
(5) \quad \gamma r^3 + 3p^2\lambda B_1Ar^3 = 1 \quad (B_2 \equiv 1 \pmod{9})
\]

must have a solution, where \( \tau \in Q[\rho], r \in Z, B_1 = B/B_2, \) and \( \gamma \in \Gamma(B_2) \).

**Theorem 3.** Let \( D = 3AB \), if \( D \) is admissible, there must be a unitary factor \( B_2 \) of \( B \) such that \( B_2 > 1 \) and

*We say that \( m \) is a unitary factor of \( n \) if \( (m, m/n) = 1 \).
must have a solution, where \( \tau \in \mathbb{Q}[\rho], r \in \mathbb{Z}, B_1 = B/B_2, \) and \( \gamma \in \Gamma(B_2). \)

**Theorem 4.** Let \( D = 9AB. \) If \( D \) is admissible, there must be a unitary factor \( B_2 \) of \( B \) such that \( B_2 > 1, B_2 \not\equiv 4 \pmod{9} \), and

\[
(7) \quad \rho \gamma^3 + \rho^2 \lambda AB_1 t^3 = 1 \quad (B_2 \equiv 7 \pmod{9}),
\]

\[
(8) \quad \rho^2 \gamma^3 + \rho^2 \lambda AB_1 t^3 = 1 \quad (B_2 \equiv 1 \pmod{9})
\]

or

\[
(9) \quad \gamma^3 + \rho^2 \lambda AB_1 t^3 = 1 \quad (B_2 \equiv 1 \pmod{9}),
\]

must have a solution, where \( \tau \in \mathbb{Q}[\rho], r \in \mathbb{Z}, B_1 = B/B_2, \) and \( \gamma \in \Gamma(B_2). \)

Since the proofs of these four theorems are similar, we will prove Theorem 1 only.

**Proof of Theorem 1.** Suppose \( D \) is admissible and that \( (e, f) \) is the nontrivial solution of (1). We divide the proof into two cases.

**Case 1.** \( 3 \nmid f. \) Since \( D \not\equiv \pm 1 \pmod{9} \) and \( 3 \nmid f, \) we must have \( e \equiv -1 \pmod{3} \) and

\[
e - 1 = B_1 A r^3, \quad e^2 + e + 1 = B_2 r^3,
\]

where \( r, t \in \mathbb{Z}, B_1 B_2 = B, (B_1, B_2) = 1. \) Since \( D \not\equiv 17, 20, \) we have \( B_2 > 1 \) (Ljunggren [5]).

In \( \mathbb{Q}(\rho), \)

\[
(e - \rho)(e - \rho^2) = B_2 r^3;
\]

and it follows that \( e - \rho = \beta r^3, \) where \( \beta = \rho^\gamma \) for some \( \gamma \in \Gamma(B_2) \) and \( \tau \in \mathbb{Q}[\rho]. \)

Since \( e \equiv -1, \gamma \equiv \pm 1, \) and \( \tau^3 \equiv \pm 1 \pmod{3}, \) we must have \( j = 2. \) Since

\[
e = B_1 A r^3 + 1 \quad \text{and} \quad e = \rho^2 \gamma t^3 + \rho,
\]

we get (2).

**Case 2.** \( 3 \mid f. \) In this case we have \( e \equiv 1 \pmod{9} \) and

\[
e - 1 = 9B_1 A r^3, \quad e^2 + e + 1 = 3B_2 r^3.
\]

It follows that \( e - \rho = \rho^\lambda \gamma^3, \) where \( \tau \in \mathbb{Q}[\rho]. \) Since \( e \equiv 1 \pmod{9} \) and \( \gamma^3 \equiv \pm 1 \pmod{3}, \) we find that \( j = 0. \) It is now easy to deduce (3).

Let \( \pi \) be any prime of \( \mathbb{Q}[\rho]; \) and define the cubic character of \( \nu \in \mathbb{Q}[\rho] \) by

\[
[v|\pi] = 1, \rho \text{ or } \rho^2
\]

when

\[
j^{N(\pi)-1}/3 \equiv 1, \rho \text{ or } \rho^2 \pmod{\pi},
\]

respectively. Suppose, for example, that \( D = AB \not\equiv \pm 1 \pmod{9}. \) If \( D \) is admissible, we must have some unitary factor \( B_2 \) of \( B \) such that \( B_2 > 1; \) and we must also have some \( \gamma \in \Gamma(B_2) \) such that either (2) or (3) is solvable. If (2) is solvable,

\[
(10) \quad \left[ \frac{\lambda^2 \rho \gamma}{q} \right] = 1 \quad \text{for each prime } q \text{ which divides } A,
\]
COMPUTATION OF THE SOLUTION OF $x^3 + Dy^3 = 1$

(11) $\left[\frac{\lambda^2 \rho \gamma}{\pi_p}\right] = \left[\frac{\lambda^2 \rho \gamma}{\pi_p}\right] = 1$ for each rational prime $p$ which divides $B_1$.

(12) $\left[\frac{\lambda^2 B_1 A}{\pi_i}\right] = 1$ for $i = 1, 2, 3, \ldots, m$, where $\gamma = \pi_1 \pi_2 \cdots \pi_m$.

If (3) is solvable,

(13) $B_2 \equiv 1 \pmod{9}$,

(14) $\left[\frac{\gamma}{q}\right] = 1$ for each prime $q$ which divides $A$,

(15) $\left[\frac{\gamma}{\pi_p}\right] = \left[\frac{\gamma}{\pi_p}\right] = 1$ for each rational prime $p$ which divides $B_1$,

(16) $\left[\frac{3\rho^2 \lambda B_1 A}{\pi_i}\right] = 1$ for $i = 1, 2, 3, \ldots, m$, where $\gamma = \pi_1 \pi_2 \cdots \pi_m$.

If, for every possible unitary divisor $B_2 > 1$ of $B$ there does not exist a value for $\gamma$ such that either (10)--(12) or (13)--(16) are all true, then neither (2) nor (3) has a solution; thus, $D$ is inadmissible.

Similar results can also be obtained from Theorems 2, 3 and 4.

3. **Computer Algorithms.** In order to make use of the results described above, we must have a method for evaluating $[\nu/\pi]$. To do this we use an algorithm analogous to that of Jacobi for evaluating the Legendre Symbol. To evaluate $[(A + B\rho)(C + D\rho)]$, where $A, B, C, D \in \mathbb{Z}$ and $3 \nmid C, 3 \mid D$, we first find $E + F\rho$, where $E = A - xC + yD$, $F = B - yC -xD + yD$,

<table>
<thead>
<tr>
<th>Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D$</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>19</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td>26</td>
</tr>
<tr>
<td>28</td>
</tr>
<tr>
<td>37</td>
</tr>
<tr>
<td>43</td>
</tr>
<tr>
<td>63</td>
</tr>
<tr>
<td>65</td>
</tr>
<tr>
<td>91</td>
</tr>
<tr>
<td>124</td>
</tr>
<tr>
<td>126</td>
</tr>
<tr>
<td>182</td>
</tr>
<tr>
<td>215</td>
</tr>
<tr>
<td>217</td>
</tr>
<tr>
<td>254</td>
</tr>
<tr>
<td>342</td>
</tr>
<tr>
<td>344</td>
</tr>
</tbody>
</table>
Table 1 (Continued)

<table>
<thead>
<tr>
<th>D</th>
<th>e</th>
<th>f</th>
<th>D</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>2196</td>
<td>13</td>
<td>-1</td>
<td>17145</td>
<td>361</td>
<td>-14</td>
</tr>
<tr>
<td>2198</td>
<td>-13</td>
<td>1</td>
<td>17575</td>
<td>26</td>
<td>-1</td>
</tr>
<tr>
<td>2743</td>
<td>14</td>
<td>-1</td>
<td>17577</td>
<td>-26</td>
<td>1</td>
</tr>
<tr>
<td>2745</td>
<td>-14</td>
<td>1</td>
<td>18745</td>
<td>1036</td>
<td>-39</td>
</tr>
<tr>
<td>3155</td>
<td>-44</td>
<td>3</td>
<td>18963</td>
<td>-80</td>
<td>3</td>
</tr>
<tr>
<td>3374</td>
<td>15</td>
<td>-1</td>
<td>19441</td>
<td>-242</td>
<td>9</td>
</tr>
<tr>
<td>3376</td>
<td>-15</td>
<td>1</td>
<td>19682</td>
<td>27</td>
<td>-1</td>
</tr>
<tr>
<td>3605</td>
<td>46</td>
<td>-3</td>
<td>19684</td>
<td>-27</td>
<td>1</td>
</tr>
<tr>
<td>3724</td>
<td>-31</td>
<td>2</td>
<td>19927</td>
<td>244</td>
<td>-9</td>
</tr>
<tr>
<td>3907</td>
<td>-63</td>
<td>4</td>
<td>20421</td>
<td>82</td>
<td>-3</td>
</tr>
<tr>
<td>4095</td>
<td>16</td>
<td>-1</td>
<td>20797</td>
<td>-55</td>
<td>2</td>
</tr>
<tr>
<td>4097</td>
<td>-16</td>
<td>1</td>
<td>21951</td>
<td>28</td>
<td>-1</td>
</tr>
<tr>
<td>4291</td>
<td>65</td>
<td>-4</td>
<td>21953</td>
<td>-28</td>
<td>1</td>
</tr>
<tr>
<td>4492</td>
<td>33</td>
<td>-2</td>
<td>23149</td>
<td>57</td>
<td>-2</td>
</tr>
<tr>
<td>4912</td>
<td>17</td>
<td>-1</td>
<td>24388</td>
<td>29</td>
<td>-1</td>
</tr>
<tr>
<td>4914</td>
<td>-17</td>
<td>1</td>
<td>24390</td>
<td>-29</td>
<td>1</td>
</tr>
<tr>
<td>5080</td>
<td>361</td>
<td>-21</td>
<td>26110</td>
<td>-89</td>
<td>3</td>
</tr>
<tr>
<td>5514</td>
<td>-53</td>
<td>3</td>
<td>26999</td>
<td>30</td>
<td>-1</td>
</tr>
<tr>
<td>5831</td>
<td>18</td>
<td>-1</td>
<td>27001</td>
<td>-30</td>
<td>1</td>
</tr>
<tr>
<td>5833</td>
<td>-18</td>
<td>1</td>
<td>27910</td>
<td>91</td>
<td>-3</td>
</tr>
<tr>
<td>6162</td>
<td>55</td>
<td>-3</td>
<td>29790</td>
<td>31</td>
<td>-1</td>
</tr>
<tr>
<td>6858</td>
<td>19</td>
<td>-1</td>
<td>29792</td>
<td>-31</td>
<td>1</td>
</tr>
<tr>
<td>6860</td>
<td>-19</td>
<td>1</td>
<td>31256</td>
<td>-63</td>
<td>2</td>
</tr>
<tr>
<td>7415</td>
<td>-39</td>
<td>2</td>
<td>32006</td>
<td>-127</td>
<td>4</td>
</tr>
<tr>
<td>7999</td>
<td>20</td>
<td>-1</td>
<td>32042</td>
<td>667</td>
<td>-21</td>
</tr>
<tr>
<td>8001</td>
<td>-20</td>
<td>1</td>
<td>32767</td>
<td>32</td>
<td>-1</td>
</tr>
<tr>
<td>8615</td>
<td>41</td>
<td>-2</td>
<td>32769</td>
<td>-32</td>
<td>1</td>
</tr>
<tr>
<td>8827</td>
<td>-62</td>
<td>3</td>
<td>33542</td>
<td>129</td>
<td>-4</td>
</tr>
<tr>
<td>9260</td>
<td>21</td>
<td>-1</td>
<td>34328</td>
<td>65</td>
<td>-2</td>
</tr>
<tr>
<td>9262</td>
<td>-21</td>
<td>1</td>
<td>34859</td>
<td>-98</td>
<td>3</td>
</tr>
<tr>
<td>9709</td>
<td>64</td>
<td>-3</td>
<td>35936</td>
<td>33</td>
<td>-1</td>
</tr>
<tr>
<td>10647</td>
<td>22</td>
<td>-1</td>
<td>35938</td>
<td>-33</td>
<td>1</td>
</tr>
<tr>
<td>10649</td>
<td>-22</td>
<td>1</td>
<td>37037</td>
<td>100</td>
<td>-3</td>
</tr>
<tr>
<td>12166</td>
<td>23</td>
<td>-1</td>
<td>39303</td>
<td>34</td>
<td>-1</td>
</tr>
<tr>
<td>12168</td>
<td>-23</td>
<td>1</td>
<td>39305</td>
<td>-34</td>
<td>1</td>
</tr>
<tr>
<td>12978</td>
<td>-47</td>
<td>2</td>
<td>42874</td>
<td>35</td>
<td>-1</td>
</tr>
<tr>
<td>13256</td>
<td>-71</td>
<td>3</td>
<td>42876</td>
<td>-35</td>
<td>1</td>
</tr>
<tr>
<td>13538</td>
<td>-143</td>
<td>6</td>
<td>44739</td>
<td>-71</td>
<td>2</td>
</tr>
<tr>
<td>13823</td>
<td>24</td>
<td>-1</td>
<td>45372</td>
<td>-107</td>
<td>3</td>
</tr>
<tr>
<td>13825</td>
<td>-24</td>
<td>1</td>
<td>46011</td>
<td>-215</td>
<td>6</td>
</tr>
<tr>
<td>14114</td>
<td>145</td>
<td>-6</td>
<td>46655</td>
<td>36</td>
<td>-1</td>
</tr>
<tr>
<td>14408</td>
<td>73</td>
<td>-3</td>
<td>46657</td>
<td>-36</td>
<td>1</td>
</tr>
<tr>
<td>14706</td>
<td>49</td>
<td>-2</td>
<td>47307</td>
<td>217</td>
<td>-6</td>
</tr>
<tr>
<td>15253</td>
<td>-124</td>
<td>5</td>
<td>47964</td>
<td>109</td>
<td>-3</td>
</tr>
<tr>
<td>15624</td>
<td>25</td>
<td>-1</td>
<td>48627</td>
<td>73</td>
<td>-2</td>
</tr>
<tr>
<td>15626</td>
<td>-25</td>
<td>1</td>
<td>48949</td>
<td>4097</td>
<td>-112</td>
</tr>
<tr>
<td>16003</td>
<td>126</td>
<td>-5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ x = Ne \left( \frac{AC + BD - AD}{C^2 - CD + D^2} \right), \quad y = Ne \left( \frac{BC - AD}{C^2 - CD + D^2} \right), \]

and, by \( Ne(\alpha) \) (\( \alpha \) real), we denote the nearest rational integer to \( \alpha \).

If \( E \equiv -F \) (mod 3), divide \( E + F\rho \) by \( 1 - \rho \) \( m \) times until

\[ \frac{E + F\rho}{(1 - \rho)^m} = \bar{E} + \bar{F}\rho, \]
where \( E \neq -F \pmod{3} \). This can be easily done by using the result that, if \( E = -F + 3Q \), then \((E + Fp)/(1 - \rho) = 2Q - F + Q\rho\).

If \( 3 \mid F \), put \( n = 0, G = E, H = F \);
if \( 3 \mid E \), put \( n = 1, G = F - E, H = -E \); and
if \( 3 \nmid E, F \), put \( n = 2, G = -F, H = E - F \).

We have
\[
\begin{bmatrix} A + Bp \\ C + Dp \end{bmatrix} = \rho^{(2m+n)(c^2-1)/3-nC/3\cdot D/3} \begin{bmatrix} C + Dp \\ G + Hp \end{bmatrix}.
\]

We now apply the algorithm again to \([(C + Dp)(G + Hp)]\). Since \( N(G + Hp) < N(C + Dp) \), we can repeat this process until we ultimately get a symbol of the form \([\pm 1](A + Bp) = 1\). The accumulated power of \( \rho \) will give us the value of \([(A + Bp)(C + Dp)]\). By using well-known results concerning the symbol \([\nu|\pi]\) (see, for example, Bachmann \([1]\)), it is a simple matter to verify that if \( C + Dp \) is a prime in \( \mathbb{Q}(\rho) \), then this algorithm gives the cubic character of \( A + Bp \) modulo \( C + Dp \).

A computer program was written, which used the results of Section 2 in conjunction with the above algorithm, in order to solve (1). For any given value of \( D = cd^2 \), the program first attempted to prove that \( D \) is inadmissible; if this failed, the program used the algorithm of Voronoi to determine the fundamental unit
\[
e = (u + v\sqrt{D} + w\sqrt{D^2})/t \quad (u, v, w, t \in \mathbb{Z})
\]
of \( K \), where \( u, v, w, t \) were calculated modulo a large prime \( R \) (see \([9]\)). If either \( v \) or \( w \) were zero modulo \( R \), the program recalculated \( u, v, w, t \) exactly. If, at this stage, the solution of either \( x^3 + cd^2y^3 = 1 \) or \( x^3 + c^2dy^3 = 1 \) was discovered, the computer printed the solution and the appropriate \( D \) value.

This program was run on all values of \( D \) of the form \( cd^2 \), where \( c, d \) are square-free, \( c > d \), and \( 15000 < D < 50000 \). Over 89% of the \( D \) values considered are inadmissible by the criteria of Section 2 only. In Table 1 above we present all the non-trivial solutions of (1) for every \( D \) such that \( 1 \leq D \leq 50000 \).

4. Some Theoretical Results. When \( B \) is a single prime or the square of a prime, we can obtain some results concerning the inadmissibility of \( D \) which are similar to results of Sylvester and Selmer (see Selmer \([8, \text{Chapter 9}]\)) concerning \( x^3 + y^3 = Dz^3 \). In what follows we denote by \( p \) a rational prime of the form \( 3r + 1 \) and we denote by \((n|p)_3 \quad (n \in \mathbb{Z})\), the least positive residue of \( n^{(p-1)/3} \pmod{p} \). Note that \((n|p)_3 = 1\) if and only if \([n|\pi] = 1\), where \( \pi = \pi_p \) or \( \pi_p \).

**Theorem 5.** If \( D = p^\kappa A \quad (k = 1 \text{ or } 2), D \neq \pm 1 \pmod{9} \), then \( D \) is inadmissible if either
\[
(q | p)_3 \neq 1 \quad \text{for some prime divisor } q \text{ of } A
\]
or
\[
p \neq 1 \pmod{9} \quad \text{and} \quad (3 | p)_3 = 1.
\]

**Theorem 6.** If \( D = p^\kappa A \quad (k = 1 \text{ or } 2), D \equiv \pm 1 \pmod{9} \), then \( D \) is admissible if either
Theorem 7. If $D = 3p^\kappa A$ ($\kappa = 1$ or 2), then $D$ is inadmissible if either

$$p \not\equiv 1 \pmod{9};$$

or

$$p \equiv 1 \pmod{9}, \ (3 \mid p)^3 \neq 1;$$

or

$$p \equiv 1 \pmod{9}, \ (3 \mid p)^3 = 1 \text{ and } (q \mid p)^3 \neq 1$$

for some prime $q \mid A$.

Theorem 8. If $D = 9p^\kappa A$ ($\kappa = 1$ or 2), then $D$ is inadmissible if

$$p^\kappa \equiv 4 \pmod{9};$$

or

$$p^\kappa \equiv 7 \pmod{9}, \ A \equiv \pm 4 \pmod{9}, \ (3 \mid p)^3 \neq 1;$$

or

$$p^\kappa \equiv 7 \pmod{9}, \ A \not\equiv \pm 4 \pmod{9}, \ (3q \mid p)^3 \neq 1$$

for some prime of $q \mid A$, where $j = -(q + 1)(4A^2 - 1)/9 \pmod{3}$.

Since the proofs of these theorems are similar, we give here the proof of Theorem 6 only.

**Proof of Theorem 6.** From Theorem 2 we see that if (1) has a nontrivial solution, we must have either

(a) $[\lambda^2 A \mid \pi] = 1$ and $[\rho^2 \lambda^2 \pi^\kappa \mid q] = 1$ for each prime $q \mid A$ or $p \equiv 1 \pmod{9}$ and

(b) $[3\rho^2 \lambda A \mid \pi] = 1$ and $[\pi \mid q] = 1$ for each prime $q \mid A$, where $\pi = \pi_p$ or $\pi_{\bar{p}}$.

If (a) is true, we see that

$$[\rho \lambda^2 \pi^\kappa \mid q] = [\rho^2 \pi^\kappa \mid q] = 1;$$

consequently,

$$[\rho \pi^\kappa \mid q] = \rho^\kappa(q^2 - 1)/3$$

for each prime $q \mid A$, and it follows that $[A \mid \pi] = \rho^\kappa(A^2 - 1)/3$. Since $p^\kappa A \equiv \pm 1 \pmod{9}$, we have $(A^2 - 1)/3 = \kappa(p - 1)/3 \pmod{3}$ and $[A \mid \pi] = \rho^\kappa(p - 1)/3$. From the fact that $[\lambda^2 A \mid \pi] = 1$, we get $[3 \mid \pi] = \rho^{(p - 1)/3}$; hence $[3q \mid \pi] = \rho^\kappa(q + 1)/3 + (p - 1)/3$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
COMPUTATION OF THE SOLUTION OF $x^3 + Dy^3 = 1$

If $p \not\equiv 1 \pmod{9}$, then $D$ is inadmissible if $(3 \mid p)_3 = 1$ or if $(3 \mid q \mid p)_3 \neq 1$ for some prime $q \mid A$ when $j \equiv -\kappa(p - 1)(q + 1)/9 \pmod{3}$.

If $(\beta)$ is true, we must have $(p \mid q)_3 = 1$ for each prime $q \mid A$. Thus, if $p \equiv 1 \pmod{9}$, $(3 \mid p)_3 \neq 1$ and $(p \mid q)_3 \neq 1$ for some prime $q \mid A$, then neither $(\alpha)$ nor $(\beta)$ is true.

With these results it is frequently possible to determine the inadmissibility of a value of $D$ of the form $3^l p^a A$ by using a table of indices only. For example, if $D = 95545 = 5 \cdot 97 \cdot 197$, we have $p = 97$ and $p \not\equiv 1 \pmod{9}$. Also $(3 \mid p)_3 \neq 1$, $e = 0$, and $(197 \mid 97)_3 \neq 1$; hence, 95545 is inadmissible.

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada