MATHEMATICS OF COMPUTATION, VOLUME 31, NUMBER 139
JULY 1977, PAGES 778–785

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 $D \leqslant 50000$ 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 $K = Q(\sqrt[3]{D})$, the field formed by adjoining $\sqrt[3]{D}$ to the rationals Q; and let ϵ (> 1) be the fundamental unit of K. By a nontrivial solution of

$$x^3 + Dy^3 = 1, \tag{1}$$

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 (DELONE-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* ϵ *or* ϵ^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 $1 < D \leqslant 15000$. The difficulty in using this theorem to solve (1) lies in the fact that the calculation of ϵ is frequently very difficult and time consuming. The best algorithm for computing ϵ, 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 ϵ 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 ϵ is usually quite small. Consequently, the best strategy for solving (1) would seem to consist of finding simpler techniques than the calculation of ϵ 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 $D \leqslant 50000$. Finally, some theorems are given which can be used for showing that certain values of D are inadmissible.

Received September 16, 1976.
AMS (MOS) subject classifications (1970). Primary 10B10, 10–04.

2. **Some Criteria for Determining When D is Inadmissible.** Since $x^3 + d_1 d_2^3 y^3 = x^3 + d_1(d_2 y)^3$, 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 $D = 3^\iota AB$, where $0 \leqslant \iota \leqslant 2$, 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 $e^2 + e + 1 \not\equiv 0 \pmod 9$ and $(A, e^2 + e + 1) = 1$, we get $e \equiv 1 \pmod 9$,

$$e^2 + e + 1 = 3B'g^3,$$

where $B' > 1$ and $B' \mid B$. It follows that $B' \equiv 1 \pmod 9$.

Let ρ be a primitive cube root of unity; let $Q(\rho)$ be the field formed by adjoining ρ 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 $\pi_p = a + b\rho$, $\bar{\pi}_p = a + b\rho^2$, where $a \equiv -1 \pmod 3$, $3 \mid b$, and $p = N(\pi_p) = N(\bar{\pi}_p) = a^2 - ab + b^2$. If $P = p_1 p_2 \cdots p_j$, 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 $\bar{\pi}_{p_i}$; 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*

$$\rho^2 \gamma \tau^3 + B_1 A r^3 = \lambda \tag{2}$$

or

$$\gamma \tau^3 + 3\rho^2 \lambda B_1 A r^3 = 1 \qquad (B_2 \equiv 1 \pmod 9) \tag{3}$$

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*

$$\rho \gamma \tau^3 + B_1 A r^3 = \lambda \tag{4}$$

or

$$\gamma \tau^3 + 3\rho^2 \lambda B_1 A r^3 = 1 \qquad (B_2 \equiv 1 \pmod 9) \tag{5}$$

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 $(m, m/n) = 1$.

(6) $$\gamma\tau^3 + 9\lambda\rho^2 B_1 A r^3 = 1$$

must have a solution, where $\tau \in Q[\rho]$, $r \in Z$, $B_1 = B/B_2$, *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) $$\rho\gamma\tau^3 + \rho^2\lambda A B_1 r^3 = 1 \qquad (B_2 \equiv 7 \pmod 9),$$

(8) $$\rho^2\gamma\tau^3 + \rho^2\lambda A B_1 r^3 = 1 \qquad (B_2 \equiv 1 \pmod 9))$$

or

(9) $$\gamma\tau^3 + \rho^2\lambda A B_1 r^3 = 1 \qquad (B_2 \equiv 1 \pmod 9)),$$

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

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

$$e - 1 = B_1 A r^3, \qquad e^2 + e + 1 = B_2 t^3,$$

where $r, t \in Z$, $B_1 B_2 = B$, $(B_1, B_2) = 1$. Since $D \neq 17, 20$, we have $B_2 > 1$ (Ljunggren [5]).

In $Q(\rho)$,

$$(e - \rho)(e - \rho^2) = B_2 t^3;$$

and it follows that $e - \rho = \beta\tau^3$, where $\beta = \rho^j\gamma$ for some $\gamma \in \Gamma(B_2)$ and $\tau \in Q[\rho]$. Since $e \equiv -1$, $\gamma \equiv \pm 1$, and $\tau^3 \equiv \pm 1 \pmod 3$, we must have $j = 2$. Since

$$e = B_1 A r^3 + 1 \quad \text{and} \quad e = \rho^2\gamma\tau^3 + \rho,$$

we get (2).

Case 2. $3 \mid f$. In this case we have $e \equiv 1 \pmod 9$ and

$$e - 1 = 9B_1 A r^3, \qquad e^2 + e + 1 = 3B_2 t^3.$$

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

Let π be any prime of $Q[\rho]$; and define the cubic character of $\nu \in Q[\rho]$ by

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

when

$$\nu^{(N(\pi)-1)/3} \equiv 1, \rho \text{ or } \rho^2 \pmod \pi,$$

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) $$\left[\frac{\lambda^2\rho\gamma}{q}\right] = 1 \quad \text{for each prime } q \text{ which divides } A,$$

(11) $\left[\frac{\lambda^2\rho\gamma}{\pi_p}\right] = \left[\frac{\lambda^2\rho\gamma}{\bar{\pi}_p}\right] = 1$ 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) $\left[\frac{\gamma}{\pi_p}\right] = \left[\frac{\gamma}{\bar{\pi}_p}\right] = 1$ 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 γ 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 $A, B, C, D \in Z$ and $3 \nmid C$, $3 \mid D$, we first find $E + F\rho$, where $E = A - xC + yD$, $F = B - yC - xD + yD$,

TABLE 1

D	e	f	D	e	f
2	-1	1	422	-15	2
7	2	-1	511	8	-1
9	-2	1	513	-8	1
17	18	-7	614	17	-2
19	-8	3	635	361	-42
20	-19	7	651	-26	3
26	3	-1	728	9	-1
28	-3	1	730	-9	1
37	10	-3	813	28	-3
43	-7	2	999	10	-1
63	4	-1	1001	-10	1
65	-4	1	1330	11	-1
91	9	-2	1332	-11	1
124	5	-1	1521	-23	2
126	-5	1	1588	-35	3
182	-17	3	1657	-71	6
215	6	-1	1727	12	-1
217	-6	1	1729	-12	1
254	19	-3	1801	73	-6
342	7	-1	1876	37	-3
344	-7	1	1953	25	-2

TABLE 1 (*Continued*)

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

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

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

If $E \equiv -F \pmod 3$, divide $E + F\rho$ by $1 - \rho$ m times until

$$\frac{E + F\rho}{(1 - \rho)^m} = \bar{E} + \bar{F}\rho,$$

where $\bar{E} \not\equiv -\bar{F}$ (mod 3). This can be easily done by using the result that, if $E = -F + 3Q$, then $(E + F\rho)/(1 - \rho) = 2Q - F + Q\rho$.

If $3 \mid \bar{F}$, put $n = 0$, $G = \bar{E}$, $H = \bar{F}$;

if $3 \mid \bar{E}$, put $n = 1$, $G = \bar{F} - \bar{E}$, $H = -\bar{E}$; and

if $3 \nmid \bar{E}\bar{F}$, put $n = 2$, $G = -\bar{F}$, $H = \bar{E} - \bar{F}$.

We have

$$\left[\frac{A + B\rho}{C + D\rho}\right] = \rho^{(2m+n)(C^2-1)/3-nCD/3}\left[\frac{C + D\rho}{G + H\rho}\right].$$

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

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

$$\epsilon = (u + v\sqrt[3]{D} + w\sqrt[3]{D^2})/t \qquad (u, v, w, t \in Z)$$

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 squarefree, $c > d$, 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 nontrivial solutions of (1) for every D such that $1 \leqslant D \leqslant 50000$.

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, Chapter 9]) concerning $x^3 + y^3 = Dz^3$. In what follows we denote by p a rational prime of the form $3t + 1$ and we denote by $(n \mid p)_3$ $(n \in Z)$, the least positive residue of $n^{(p-1)/3}$ (mod p). Note that $(n \mid p)_3 = 1$ if and only if $[n|\pi] = 1$, where $\pi = \pi_p$ or $\bar{\pi}_p$.

THEOREM 5. *If* $D = p^\kappa A$ ($\kappa = 1$ *or* 2), $D \not\equiv \pm 1$ (mod 9), *then D is inadmissible if either*

$$(q \mid p)_3 \not\equiv 1 \quad \textit{for some prime divisor } q \textit{ of } A$$

or

$$p \not\equiv 1 \pmod 9 \quad \textit{and} \quad (3 \mid p)_3 = 1.$$

THEOREM 6. *If* $D = p^\kappa A$ ($\kappa = 1$ *or* 2), $D \equiv \pm 1$ (mod 9), *then D is admissible if either*

$$p \not\equiv 1 \pmod 9, \quad (3 \mid p)_3 = 1;$$

or

$$p \not\equiv 1 \pmod 9, \quad (3 \mid p)_3 \neq 1, \quad (3^j q \mid p)_3 \neq 1$$

for some prime divisor q of A, where $j \equiv -\kappa(p-1)(q+1)/9 \pmod 3$; or

$$p \equiv 1 \pmod 9, \quad (3 \mid p)_3 \neq 1, \quad (q \mid p)_3 \neq 1$$

for some prime $q \mid A$.

THEOREM 7. *If $D = 3p^\kappa A$ ($\kappa = 1$ or 2), then D is inadmissible if either*

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

or

$$p \equiv 1 \pmod 9, \quad (3 \mid p)_3 \neq 1;$$

or

$$p \equiv 1 \pmod 9, \quad (3 \mid p)_3 = 1 \quad \text{and} \quad (q \mid p)_3 \neq 1$$

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

$$p^\kappa \equiv 7 \pmod 9, \quad A \equiv \pm 4 \pmod 9, \quad (3 \mid p)_3 \neq 1;$$

or

$$p^\kappa \equiv 7 \pmod 9, \quad A \not\equiv \pm 4 \pmod 9, \quad (3^j q \mid p)_3 \neq 1$$

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

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

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

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

If (α) is true, we see that

$$\left[\frac{\rho\lambda^2\pi^\kappa}{q}\right] = \left[\frac{\rho^2\pi^\kappa}{q}\right] = 1;$$

consequently,

$$\left[\frac{q}{\pi}\right] = \rho^{\kappa(q^2-1)/3}$$

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

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

If (β) 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 (α) nor (β) is true.

With these results it is frequently possible to determine the inadmissibility of a value of D of the form $3^\iota p^\kappa A$ 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 $(3 \mid p)_3 \neq 1$, $\epsilon = 0$, and $(197 \mid 97)_3 \neq 1$; hence, 95545 is inadmissible.

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

1. P. BACHMANN, *Die Lehre von der Kreisteilung*, 2nd ed., Teubner, Leipzig, 1921.

2. B. D. BEACH, H. C. WILLIAMS & C. R. ZARNKE, "Some computer results on units in quadratic and cubic fields," *Proc. Twenty-Fifth Summer Meeting of Canad. Math. Congress*, Lakehead Univ., Thunder Bay, Ontario, 1971, pp. 609–648. MR **49** #2656.

3. J. H. E. COHN, "The Diophantine equation $x^3 = dy^3 + 1$," *J. London Math. Soc.*, v. 42, 1967, pp. 750–752. MR **36** #106.

4. B. N. DELONE & D. K. FADDEEV, "The theory of irrationalities of the third degree," *Transl. Math. Monographs*, vol. 10, Amer. Math. Soc., Providence, R.I., 1964. MR **28** #3955.

5. W. LJUNGGREN, "Einige Bemerkungen über die Darstellung ganzer Zahlen durch binären Kubischen Formen mit positiver Diskriminante," *Acta Math.*, v. 75, 1943, pp. 1–21.

6. T. NAGELL, "Solution complète de quelques équations cubiques à deux indéterminees," *J. Math. Pures Appl.*, (9), v. 4, 1925, pp. 209–270.

7. T. NAGELL, "Einige Gleichungen der Form $ay^2 + by + c = dx^3$," *Skr. Norske Vid.-Akad. Oslo*, 1930, No. 7.

8. E. S. SELMER, "The Diophantine equation $ax^3 + by^3 + cz^3 = 0$," *Acta Math.*, v. 85, 1951, pp. 203–362. MR **13**, 13.

9. H. C. WILLIAMS & C. R. ZARNKE, "Computation of the solutions of the Diophantine equation $x^3 + dy^3 = 1$," *Proc. Manitoba Conf. on Numerical Mathematics*, Univ. Manitoba, Winnipeg, Canada, 1971, pp. 671–676. MR **48** #10956.