# ON THE EQUATION $a^x - b^y = 1$.*

By J. W. S. CASSELS.

**1.** The solution of the title equation in integers $x$, $y$ for given integers $a > 1, b > 1$ has been dicussed by W. J. LeVeque [2]. The second paragraph of this note shows that $y$ is odd if $x > 1$, and that any prime divisor of $y$ which is less than $x$ divides $a$, and *vice versa.* The third paragraph proves simply a stronger form of LeVeque's theorem, that there is at most one solution, which can be specified completely. The third paragraph uses the results of the second only to secure a slight refinement of the enunciation.

It is conjectured that there are only a finite number of nontrivial solutions $a, b, x, y$ of the equation.

**2.** We first have the trivial

THEOREM I. $(x, y) = 1$.

*Proof.* Suppose that $x = px_1$, $y = py_1$ for $p > 1$. Then $a_1{}^p - b_1{}^p = 1$ with $a_1 = a^{x_1}$, $b_1 = b^{y_1}$; which is clearly impossible.

THEOREM II. *If* $x > 1$, *then* $2 \nmid y$.

*Proof.* Otherwise, by the preceding argument we should have a solution $a, b, x, y$ of $a^x - b^2 = 1$ with odd prime $x$. But then $1 + ib = \epsilon(p + iq)^x$, $p^2 + q^2 = a$ for some unit $\epsilon$ and by replacing $p + iq$ by $\eta(p + iq)$ with a suitable unit $\eta$ we may suppose that $\epsilon = 1$. Equating coefficients we now have

$$1 = p(p^{x-1} - \tfrac{1}{2}x(x-1)p^{x-3}q^2 + \cdots \pm xq^{x-1}),$$

and so $p = \pm 1$. By considering conguences modulo $x$ we have p $= 1$, and so

$$(1) \qquad (x-1)/2 - (x-1)(x-2)(x-3)q^2/4! + \cdots \pm q^{x-1} = 0.$$

Since $2 \mid (1 \pm i)^x$ we have $|q| > 1$. Let $r$ be a prime divisor of $q$. We shall show that all the terms on the left of (1) except the first are

* Received September 8, 1952.

divisible by a higher power of $r$ than that dividing $(x-1)/2$; which contradicts (1). It is enough to show that for $k \geqq 2$ the fraction

$$2(x-2)\cdots(x-2k+1)q^{2k-3}/(2k)!$$
$$=(x-2)\cdots(x-2k+1)/(2k-2)!\cdot q^{2k-3}/k(2k-1)$$

does not have $r$ in its denominator when reduced. The first factor is an integer. For $k \geqq 4$ we have $r^{2k-3} \mid q^{2k-3}$, but $r^{2k-3} \geqq 2^{2k-3} > k(2k-1)$, so then the statement is certainly true. For $k=2,3$ we have $r \mid q^{2k-3}$, but $r^2 \nmid k(2k-1)$ since $k(2k-1)=6, 15$ respectively is squarefree, and again the statement is true. Hence the assumption that $a^x - b^2 = 1$ is soluble leads to a contradiction.

We require two trivial lemmas.

LEMMA 1. *Let $p$ be an odd prime and $c > 1$ an integer. Then $f = (c^p - 1)/(c-1)$ is prime to $p$ or divisible by $p$ but not by $p^2$ according as $c \not\equiv 1\ (p)$ or $c \equiv 1\ (p)$. The number $f, f/p$ respectively is odd, greater than 1 and prime to $c-1$.*

*Further, $g = (c^p+1)/(c+1)$ is prime to $p$ or divisible by $p$ but not by $p^2$ according as $c \not\equiv -1\ (p)$ or $c \equiv -1\ (p)$. The number $g, g/p$ respectively is odd and prime to $c+1$; it is greater than 1 except when*

$$c = 2, \qquad p = 3. \tag{2}$$

*Proof.* If $q$ is a prime divisor of $c-1$, then $f = 1 + c + \cdots c^{p-1} \equiv p\ (q)$ and so $q \mid f$ implies $q = p$. If $c = 1 + rp$, then

$$f \equiv 1 + (1+rp) + (1+2rp) + \cdots + (1+(p-1)\,rp) \equiv p\,(p^2)$$

and so the greatest common divisor of $c-1$, $f$ is 1 or $p$. In particular $f$ is odd if $c$ is odd. If $c$ is even, then $f \equiv 1/1\ (2)$ is again odd. Finally, it is obvious that $f > p$.

As before, the greatest common divisor of $g$ and $c+1$ is 1 or $p$, and $g$ is odd. Also

$$\frac{g}{p} = \frac{c^p+1}{p(c+1)} \geqq \frac{2^p+1}{p.3} \geqq \frac{2^3+1}{3.3} = 1,$$

with equality in both places only if $c=2$, $p=3$.

LEMMA 2. *Let $c > 1$. If $c$ is even, then $c+1$, $c-1$ are coprime. If $c$ is odd, then one of $c+1$, $c-1$ say $c \pm 1$, is not divisible by 4; and then $\frac{1}{2}(c \pm 1)$ is prime to $c \mp 1$.*

*Proof.* Clear

We can now prove

THEOREM III. (i) *If $p$ is prime and $p \mid x$, $p \nmid b$, then $p > y$.*

(ii) *If $p$ is prime and $p \mid y$, $p \nmid a$, then $p > x$.*

*Proof.* We first prove (i) and put $x = px_1$. By Lemmas 1, 2 the numbers $(a^x - 1)/(a^{x_1} - 1)$ and $a^{x_1} - 1$ are coprime, and so $a^{x_1} - 1 = c^y$ for some $c \mid b$. Hence $b^y = (c^y + 1)^p - 1$ and so $b > c^p$, i.e. $b \geqq c^p + 1$. Then

$$(c^p + 1)^y \leqq b^y = (c^y + 1)^p - 1 < (c^y + 1)^p,$$

and so $p > y$ ([1] Theorem 19).

For (ii) we first note that $p > 2$ by Theorem II. Put $y = py_1$ and so, as before, $b^{y_1} + 1 = d^x > 1$ for some $d \mid a$. Hence $a^x = (d^x - 1)^p + 1$ and so $a \leqq d^p - 1$. Thus

$$(d^p - 1)^x \geqq a^y = (d^x - 1)^p + 1 > (d^x - 1)^p,$$

and so $p > x$.

We call a solution nontrivial if $x > 1$, $y > 1$ and deduce

COROLLARY 1. *For a non-trivial solution it is impossible that*

$$(x, b) = (y, a) = 1.$$

For a later purpose we require

COROLLARY 2. *There are no nontrivial solutions of $2^x - b^y = 1$.*

*Proof.* If $y > 1$, $b > 1$ then $x > 1$ and so $y$ is odd by Theorem II. Hence each prime factor of $y$ is greater than $x$ and in particular $b^y > 2^y > 2^x$, a contradiction.

**3.** The following theorem enables all solutions of the title equation to be found for given $a, b$.

THEOREM IV. *Let*

$$a^x - b^y = 1, \tag{3}$$

*where $x, y, a > 1$, $b > 1$ are positive integers and the equation is not*

$$3^2 - 2^3 = 1. \tag{4}$$

*Suppose that $\xi, \eta$ are the least positive solutions of*

$$a^{\xi} \equiv 1 \ (B), \qquad b^{\eta} \equiv -1 \ (A),$$

*where $A, B$ are the products of the odd primes dividing $a, b$ respectively.*

*Then $x = \xi$, $y = \eta$; except that $x = 2$, $y = 1$ may occur if $\xi = \eta = 1$ and $a + 1$ is a power of 2.*

*Proof.* We first prove $y = \eta$. Clearly $\eta \mid y$. Suppose $y/\eta$ is even. Then $b^y \equiv (-1)^{y/\eta} \equiv 1 \not\equiv -1 \ (A)$ unless $A = 1$, i.e. unless $a$ is a power of 2. But then $a^x = b^y + 1 \equiv 2 \ (4)$ and so $a^x = 2$, $b = 1$; which is excluded. Hence $y/\eta$ is odd. Suppose that $y/\eta$ is divisible by an odd prime $p$, say $y = py_1, \eta \mid y_1$. Then by the second part of Lemma 1 there is an odd prime $q$ dividing $(b^y + 1)/(b^{y_1} + 1)$ (and so $a$) but not dividing $b^{y_1} + 1$; except in the case (2) which corresponds to (4). Hence $b^{y_1} + 1 \not\equiv 0 \ (q)$ and a fortiori $b^{y_1} \not\equiv -1 \ (A)$. The contradiction proves $y = \eta$.

We now prove the statements about $x$. Clearly $\xi \mid x$. The proof that $x/\xi$ is a power of 2 runs exactly as before using now the first part of Lemma 1. If $2\xi \mid x$, say $x = 2x_1$, $\xi \mid x_1$, then a similar argument using Lemma 2 leads to an absurdity unless $a^{x_1} + 1$ contains no odd prime factors, i.e. $a^{x_1} + 1 = 2^m$ for some $m > 0$. If now $x_1 \neq \xi$, then $2 \mid x_1$ and so $2^m = a^{x_1} + 1 \equiv 2 \ (4)$ i.e. $m = a = 1$, which is excluded.

Hence $x = \xi$ or $x = 2\xi$, the latter only if

$$a^{\xi} + 1 = 2^m. \tag{5}$$

But (5) implies $\xi = 1$ by Theorem III, Corollary 2. Now $a + 1 = 2^m$, $a^2 - 1 = b^y$ and hence $a - 1 = 2c^y$ for some odd $c$, where $y \mid (m + 1)$. Finally, $2 = 2^m - 2c^y$ and hence $1 = 2^{m-1} - c^y$. By Theorem III, Corollary 2 this implies $c = 1$ or $y = \eta = 1$. The case $c = 1$ gives $a = 3$ and so the exception (4) of the theorem; and the case $y = \eta = 1$ gives the exception at the end of the enunciation.

TRINITY COLLEGE, CAMBRIDGE, ENGLAND.

---

## REFERENCES.

[1] G. H. Hardy, J. E. Littlewood and G. Polya, *Inequalities*, Cambridge, 1934.

[2] W. J. LeVeque, "On the equation $a^x - b^y = 1$," *American Journal of Mathematics*, vol. 74 (1952), pp. 325-331.